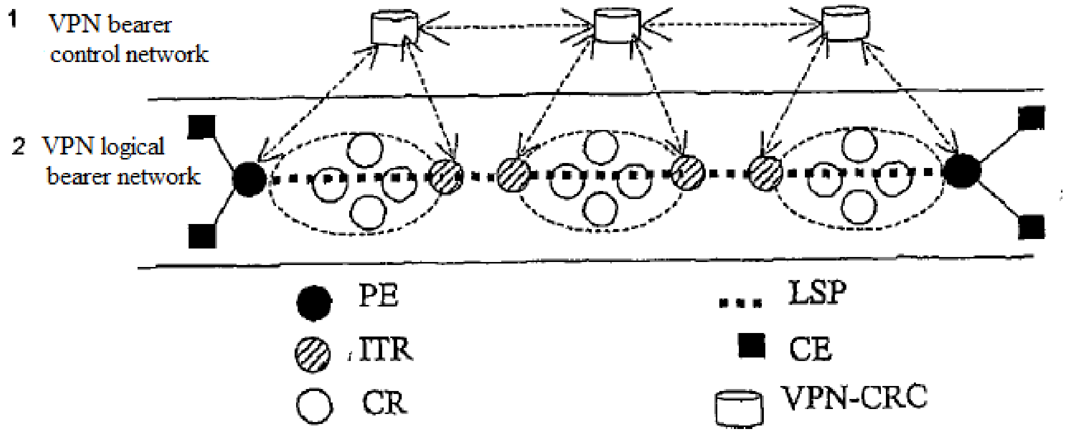
Abstract

The present invention relates to an implementation scheme of quality of service in a virtual private network, and discloses a system and a method for ensuring quality of service in a network based virtual private network, so that there is a practical solution to a QoS problem of an MPLS VPN. The system for ensuring quality of service in a network based virtual private network includes: a logical bearer network, which is formed by connecting label switch paths configured with reserved bandwidth to various routers over a basic IP network by using a multi-protocol label switch technique, and is dedicated to transmitting a service with a quality of service requirement; and a bearer control network, which is used to maintain the logical bearer network, and route the service. The present invention also provides a method for ensuring quality of service in a virtual private network.

Drawing of the Abstract



1 VPN BEARER CONTROL NETWORK

2 VPN LOGICAL BEARER NETWORK

Claims

1. A system for ensuring quality of service in a virtual private network, comprising:

a logical bearer network, which is formed by connecting label switch paths configured with reserved bandwidth to various routers over a basic IP network by using a multi-protocol label switch technique, and is dedicated to transmitting a service with a quality of service requirement; and

a bearer control network, which is used to maintain the logical bearer network, allocate a route to the service, mark a priority of the service in a quality of service field of a route label corresponding to a multi-protocol label switch data packet encapsulated from the service data stream, and route the service to an opposite end via the logical bearer network in accordance with the allocated route.

2. The system for ensuring quality of service in a virtual private network according to claim 1, wherein the bearer control network comprises centralized resource controllers for managing network resources in the logical bearer network, maintaining network topology of the logical bearer network, performing resource calculation and traffic route selection, sending traffic route indications to the routers, allocating resources and performing access control in the logical bearer network, and maintaining membership information and connectivity information for each virtual private network to implement automatic discovery and unilateral configuration of the membership.

3. The system for ensuring quality of service in a virtual private network according to claim 2, wherein one centralized resource controller is deployed in each domain of the logical bearer network; the centralized resource controllers are connected with each other, to exchange topology and resource information of the logical bearer network and routing information of the virtual private network.

4. The system for ensuring quality of service in a virtual private network according to claim 1, wherein the logical bearer network and the bearer control network distribute routes for the virtual private network, maintain membership for the virtual private network, and maintain connectivity between sites in the virtual private network in an out-of-band mode.

5. The system for ensuring quality of service in a virtual private network according to claim 2, wherein the routers comprise: provider edge routers, intermediate transfer routers, and core routers, wherein

the provider edge routers are used to identify the virtual private network with a quality of service requirement, encapsulate, by using a label stack indicated by the centralized resource controller, a service with a quality of service requirement entering from the virtual private network, set quality of service fields of all labels in the label stack in accordance with a priority of the service, and transmit encapsulated service data packets via the logical bearer network;

the intermediate transfer routers are used to implement static or dynamic configuration of label switch paths, differentiated-service-mode multi-protocol label switch, and stream processing by type of service; and

the core routers are used to implement differentiated-service-mode multi-protocol label switch and stream processing by type of service.

6. The system for ensuring quality of service in a virtual private network according to claim 2, wherein the centralized resource controller comprises an interface management module, a protocol processing module, a membership maintenance module, a topology and resource management module, a route management module, and an automatic signaling discovery module, wherein

the interface management module is used to implement and manage a communication interface between the virtual private network and an external device;

the protocol processing module is used to process protocols for communication between the centralized resource controller and various external devices, and forward communication data to the membership maintenance module, the topology and resource management module, the route management module, and the automatic signaling discovery module in accordance with requirements of the protocols; the protocol processing module receives/sends the communication data via the interface management module;

the membership maintenance module is used to maintain the membership information of the virtual private network and connectivity information between sites of the virtual private network;

the topology and resource management module is used to manage a topological relation and resources of the logical bearer network;

the route management module is used to manage a routing relation of the virtual private network; and

the automatic signaling discovery module is used to discover changes automatically, and notify the membership maintenance module and the topology and resource management module to correct the corresponding information.

7. A method for ensuring quality of service in a virtual private network, comprising the steps of:

A. in a basic IP network, constructing a logical bearer network, which is dedicated to transmitting a service with a quality of service requirement, by configuring label switch paths with reserved bandwidth by using a multi-protocol label switch technique;

B. deploying a centralized resource controller to centrally manage resources of the logical bearer network; and

C. if the service with a quality of service requirement is to be transmitted, marking a priority of the service in a quality of service field of a routing label corresponding to a multi-protocol label switch data packet encapsulated from the service data stream, and routing the service to an opposite end via the logical bearer network in accordance with a route allocated by the centralized resource controller.

8. The method for ensuring quality of service in a virtual private network according to claim 7, further comprising the following step between step B and step C: the centralized resource controller calculating and issuing access paths between sites to routers of the virtual private network, so that the routers can store the route allocated by the centralized resource controller.

9. The method for ensuring quality of service in a virtual private network according to claim 7, wherein the route is a serial label switch path determined by a label stack.

10. The method for ensuring quality of service in a virtual private network according to claim 7, wherein in the step C, the quality of service fields of all labels in the service route label stack are set as a same value.

11. The method for ensuring quality of service in a virtual private network according to claim 7, further comprising the step of: adjusting topology and resources of the logic bearer network dynamically by using a multi-protocol label switch traffic engineering technique.

12. The method for ensuring quality of service in a virtual private network according to claim 7, wherein in the step C, the priority of the service is determined by a type of the service.

13. The method for ensuring quality of service in a virtual private network according to claim 7, further comprising the steps of:

determining whether both service receiving and sending sites have a quality of service requirement; if yes, transmitting the service by using resources in the logical bearer network; and otherwise, transmitting the service by using other resources in the basic IP network.

14. The method for ensuring quality of service in a virtual private network according to claim 13, before the step of determining whether both service receiving and sending sites have a quality of service requirement, further comprising the following sub-step:

comparing route targets of the receiving and sending sites, and determining whether the connectivity between the receiving and sending sites is a general connectivity; if yes, proceeding to the next step; and otherwise, terminating the process.

15. The method for ensuring quality of service in a virtual private network

according to claim 13, wherein the step of determining whether both service receiving and sending sites have a quality of service requirement is performed in the following way: determining whether the connectivity between the receiving and sending sites is a connectivity with a quality of service requirement by comparing the route targets of the receiving and sending sites; if yes, determining that the service receiving and sending sites both have a quality of service requirement; and otherwise, determining that the service receiving and sending sites have no quality of service requirement.

16. The method for ensuring quality of service in a virtual private network according to claim 7, wherein the route allocated by the centralized resource controller to each pair of sites with a quality of service requirement is unique.

Specification

SYSTEM FOR ENSURING QUALITY OF SERVICE IN VIRTUAL PRIVATE NETWORK AND METHOD THEREOF

Field of the Invention

The present invention relates to a quality of service (QoS) implementing solution in a virtual private network, and in particular, to a QoS implementing solution in a virtual private network using multi-protocol label switch.

Background of the Invention

Virtual Private Networking (abbreviated as "VPN") refers to establishing a private network in a public network, so that data is transmitted via a secure "encrypted channel" in the public network. Branches of an enterprise can transfer information to each other once they access the Internet locally via leased local private data lines; in addition, the enterprise can also enable its users to dial up to the Internet and then access the Intranet by means of Internet dial-up access devices. The VPN has advantages of a reduced cost, remote access support, high expansibility, easy management and overall control, etc.

Multi-protocol Label Switch (abbreviated as "MPLS") is a standard protocol of Internet Engineering Task Force (abbreviated as "IETF"), evolved from CISCO's Tag Switching. MPLS is a label-based Internet Protocol (abbreviated as "IP") routing method and belongs to a Layer-3 switching technique. It introduced a label-based mechanism to separate routing from forwarding; that is, the route of a packet in the network is determined by the label, and data transmission is accomplished via a Label Switch Path (abbreviated as "LSP"). MPLS converts Layer-3 packet switching in an IP network into Layer-2 packet switching. The label includes a 3-bit EXP field to implement QoS.

FIG. 1 shows the structure of an MPLS network. The MPLS network 101 includes Label Switch Routers (abbreviated as "LSR") 104 in the core part and Label Edge Routers (abbreviated as "LER") 103 in the edge part. Wherein, the LERs 103 are designed to analyze IP packet headers, execute a Layer-3 network function, determine a corresponding transmission class and a Label Switch Path (abbreviated as "LSP"), and the LERs 103 are connected with external networks 102 and receive external packed switched data packets (IP packets) 105 from the external networks 102; the LSRs 104 are designed to establish LSPs, execute a label switching mechanism and ensure Quality of Service (QoS), and forward packed data packets (IP packets) 106 within the MPLS network 101; each LSR 104 includes a control unit and a switching unit, is located in the network, and is connected with the LERs 103 and other LSRs 104.

The label switching work flow of the MPLS is as follows: initially, a routing table and a label mapping table are created in an LSR through a Label Distribution Protocol (abbreviated as "LDP") and conventional routing protocols, e.g., an Open Shortest Path First (abbreviated as OSPF) protocol, etc.; during network operation, first, the LER at the ingress of the MPLS core network receives IP packets from an external network, accomplishes a Layer-3 network function, adds a label to the IP packet to form a packed data packet; next, the packed data packet is transmitted via an LSP. In this case, the LSR does not perform Layer-3 processing for the packed data packet but only forwards the packed data packet in accordance with the label via the switching unit, so that the packed data packet finally arrives at an LER at the opposite end (i.e., egress) of the network; finally, the LER at the egress of the MPLS network removes the label from the packed data packet to generate an IP packet, and proceeds to forward the IP packet according to a corresponding protocol of the external network.

Since the MPLS technique isolates the label distribution mechanism from the data stream, it can be implemented without depending on specific data link layer protocols, and thereby can support diverse physical layer and data link layer techniques. At present, MPLS-based services have been implemented in Frame Relay ("FR"), Asynchronous Transfer Mode ("ATM"), and Point-to-Point Protocol ("PPP") links, as well as a local area network (LAN) that employs an 802.3 protocol of the Institute of Electrical and Electronics Engineers ("IEEE"). Employing an MPLS network for IP service forwarding can simplify the route forwarding procedures between layers, speed up MPLS switching, and improve network efficiency while meeting the requirements for transmission of services of different grades; therefore, the MPLS incorporates a high speed and a flow control capability of a switch, and also achieves flexible functionality and a QoS assurance mechanism of a router.

The MPLS has been widely used in implementation of VPNs. A VPN implemented on the basis of MPLS is referred to as an MPLS VPN. MPLS VPNs can be classified into L3 (Layer 3, i.e., network layer) VPN, L2 (Layer 2, i.e., data link layer) VPN, and L1 (Layer 1, i.e., physical layer) VPN, depending on subscriber information that is used for forwarding by network equipment. Presently, in the standard organization of INTERNET ENGINEERING TASK FORCE (abbreviated as "IETF"), there are an L3 VPN workgroup and an L2 VPN workgroup, which study MPLS L3 VPN and MPLS L2 VPN, respectively. Typical examples of the MPLS L3 VPN include a Border Gateway Protocol (abbreviated as "BGP")/MPLS VPN based on RFC 2547bis and an IP VPN based on a Virtual Router (abbreviated as "VR"). Typical examples of the MPLS L2 VPNs include MARTINI, KOMPELLA, and implementing solutions of various Virtual Private LAN Segments (abbreviated as "VPLS"). Furthermore, SG13/Q11 of the International Telecommunication Union Telecommunication Standardization Sector (abbreviated as "ITU-T") made a lot of investigations on the L1 VPN, and presently, there are draft proposals such as Y.11vpnarch and Y.11vpnsdr, etc. Their reference models are similar in structure and VPN QoS processing, i.e., they either take no consideration of VPN QoS or utilize DiffServ (differentiated service mode) capability of the network itself; therefore, the above solutions cannot solve the QoS problem of the VPN due to the same reason. In this respect, they can be concluded as the same technique.

Hereinafter the prior arts are described with RFC 2547bis as an example of this kind of techniques. Since they have the same reference model structures as the L2

VPN and L3 VPN of the ITU-T and IETF, they face the same challenge regarding QoS processing.

The MPLS L3 VPN model defined in RFC 2547bis is as shown in FIG. 2. The model includes three components: Custom Edge Routers (abbreviated as "CEs"), Provider Edge Routers (abbreviated as "PEs"), and routers (P).

As a component of the customer premise network, a CE device has an interface, usually a router, directly connected to an operator's network. The CE cannot "sense" existence of a VPN and does not need to maintain the entire routing information of the VPN.

A PE router is an edge router of the operator. It is an edge device of the operator's network (also referred to as a backbone network), and is directly connected to CEs of subscribers. In an MPLS network, all processing work on the VPN is accomplished in the PE router.

As a backbone router in the operator's network, the router (P) is not connected directly with CEs. The router (P) shall have basic MPLS signaling capability and forwarding capability.

CEs and PEs are classified mainly in accordance with administrative domains of the operator and the subscribers; CEs and PEs form a boundary between the administrative domains.

CEs exchange routing information with PEs through an Exterior Border Gateway Protocol (abbreviated as "EBGP") or an Interior Gateway Protocol (abbreviated as "IGP") or via static routes. It is unnecessary for CEs to support MPLS or sense the routes across the entire VPN; the routes across the entire VPN are contracted out to the operator for implementation. PE devices of the operator exchange routing information across the entire VPN through a Multi-protocol Internal Border Gateway Protocol (abbreviated as "MP-IBGP").

Hereinafter, related attributes of the MPLS L3 VPN specified in the RFC 2547bis standard are described:

VRF:

A VPN includes multiple sites. In a PE, each site corresponds to a VPN Routing/Forwarding (abbreviated as "VRF") instance which mainly includes: an IP routing table, a label forwarding table, a cluster of interfaces that use the label forwarding table, and management information (including a route distinguisher, a route filtering policy, and a member interface list, etc.).

(The reason for modification is as follows: it is described above that a subscriber site is a component of the VPN, such a description may result in an unclear expression, and thus should be deleted.) A site may belong to multiple VPNs at the same time. In the implementation, each site is at least associated with one separate VRF. Actually, the VRF(s) at a site in the VPN combines/combine the VPN membership and routing rules of the site. Message forwarding information is stored in the IP routing table and the label forwarding table in each VRF. The system maintains a set of independent routing table and label forwarding table for each VRF, so as to prevent data leakage from the VPN and prevent external data from entering into the VPN.

VPN-IPv4 address family:

VPN routes are distributed among PEs by using a BGP, and a new address family: VPN-IPv4 address family, is used.

A VPN-IPv4 address includes 12 bytes; the first 8 bytes refer to a Route Distinguisher (abbreviated as "RD"), the rest 4 bytes refer to an IPv4 address. A PE identifies routing information from different VPNs by using an RD. The operator can allocate RDs independently, but has to take an ID of a dedicated Autonomous System (abbreviated as "AS") of the RDs as a part of the RDs to ensure global uniqueness of each RD. A VPN-IPv4 address with RD=0 is synonymous to a globally unique IPv4 address. As such, even if there is repetition in the 4-byte IPv4 address portion included in the VPN-IPv4 addresses, the VPN-IPv4 addresses are still globally unique.

The routes received by the PE from the CE are IPv4 routes, which shall be imported into the VRF routing table, and in this case, an RD needs to be attached. In common practice, the same RD is set for all routes from the same subscriber site.

Route Target attribute:

A Route Target attribute identifies a collection of sites where a route can be used, i.e., sites where the route can be received, in other words, sites from which routes can be received by the PE router. All PEs connected with the sites indicated in the Route Target will receive routes with such an attribute. After receiving a route with such an attribute, the PE router adds the route into the corresponding routing table.

There are two collections of Route Target attributes in the PE router: one collection is used to be attached to routes received from a certain site, and is referred to as Export Route Targets; the other collection is used to decide which routes can be imported into the routing table of the site, and is referred to as Import Route Targets.

Through matching the Route Target attribute carried with the routes, the VPN membership can be obtained. The Route Target attribute matching operation can be used to filter the routing information received by the PE router.

VPN message forwarding process:

In the RFC 2547bis standard, VPN message forwarding employs two layers of labels. The first layer (outer layer) label is exchanged in the backbone network, and represents an LSP from a PE to an opposite PE. With the label, a VPN message can reach the opposite PE along the LSP. When the message is transmitted from the opposite PE to a CE, the second layer (inner layer) label is used. The inner layer label indicates a destination site of the message, or more specifically, a destination CE. In this way, in accordance with the inner layer label, an interface for message forwarding can be found. In special cases, if two sites belonging to the same VPN are connected to the same PE, there is no problem about how to reach the opposite PE, and what is to be solved is how to reach the opposite CE.

Distribute VPN routing information by using the BGP:

In the RFC 2547bis standard, CEs and PEs transmit routing information to each other by using the IGP or EBGP; PEs obtain the routing table of the VPN, and store it in a separate VRF. General IP connectivity between PEs is ensured by using the IGP, VPN composition information and routing are transmitted by using the IBGP, and respective VRFs are updated accordingly. The routing tables in CEs are then updated through route switching between PEs and CEs directly connected thereto, and thereby the route switching between the CEs is accomplished.

BGP communication is carried out on two layers: inside the autonomous systems (IBGP) and between the autonomous systems (EBGP). PE-PE sessions are IBGP sessions; while PE-CE sessions are EBGP sessions.

The transmission of VPN composition information and routing between PEs in the BGP is accomplished through a Multiprotocol extensions BGP ("MBGP"). Details of the MBGP are described in IETF RFC 2283 "Multiprotocol Extensions for BGP-4". The MBGP is downward compatible, i.e., it supports both the conventional IPv4 address family and other address families (e.g., VPN-IPv4 address family). With the route target carried in the MBGP, the routes of a specific VPN can be known by only other members of the VPN, communication between BGP/MPLS VPN members becomes possible.

In data transmission via a VPN, a subscriber often designates the QoS, for example, a priority of data to be transmitted. The higher the priority of the data to be transmitted is, the sooner the VPN will transmit the data on the premise of ensured transmission reliability. In practical applications, there is no matured MPLS VPN QoS solution at present. As a result, requirements of subscribers cannot be met.

The main reason for the above situation is: different NBVPNs accessed by the same group of PEs share resources with each other by multiplexing outer layer labels in the MPLS label stack. Theoretically, though the resources of outer layer tunnels can be ensured by providing DiffServ-aware (performing forwarding in different priorities by using an IP differentiated services code point (DSCP) field) or with similar solutions. In these reference models, none of the devices in each VPN knows resource conditions in the backbone network; moreover, there is a resource competition between several VPNs at each node. Therefore, it is a difficult task to ensure resources for each VPN. Such a sharing and competition mechanism brings more complexity to QoS assurance for VPNs.

The Provider Provisioned Virtual Private Networks (abbreviated as "PPVPN") workgroup designated by IETF is divided into two workgroups after the Vienna Seminar held in July, 2003: L2 VPN and L3 VPN workgroups. In their latest charters, no QoS solution was included. In the current VPN reference models, the QoS problem still exists. In IETF's "draft-martini-12circuit-trans-mpls-10.txt" and "draft-martini-12circuit-encap-mpls-04.txt" (both are the foundation of L2 VPN), the representation for the QoS problem was "QoS related issues are not discussed in this draft". In "draft-ietf-l3vpn-rfc2547bis-01.txt" (it is the foundation of BGP/MPLS VPN), the representation for the VPN QoS problem was simply mentioned: "existing L3 QoS capabilities can be applied to labeled packets through the use of the 'experimental' bits in the shim header". However, the problem is that the L3 QoS itself is also a complex problem to be solved. Therefore, the QoS problem in L2 VPN/L3 VPN is left unsolved.

On the ITU-T SG13 Seminar held in July, 2003, the proposal for investigation of generalized VPN (GVPN) "Y.nbvpn-decomp" was approved as the initial documentation for function decomposition of generalized Network Based Virtual Private Network (abbreviated as "NBVPN") as well as the foundation for classification of building blocks of Generalized Virtual Private Network (abbreviated as "GVPN"). In "Y.nbvpn-decomp", some functional entities were classified, aiming to simplify VPN problems, so as to define the techniques and mechanisms required by network operators to provide expected VPN networks. However, the reference model provided in "Y.nbvpn-decomp" and corresponding QoS problems are identical to the VPN reference model and QoS problems put forth by IETF. Therefore, the QoS problems have not been solved satisfactorily. As a result, the entire VPN model is not generalized enough to meet the requirements of operators who expect to provide QoS assured VPN services. Furthermore, though VPN subscribers are permitted to access the VPN, it is uninsured that they can obtain required resources as in Asynchronous Transfer Mode (abbreviated as "ATM")/Frame Relay (abbreviated as "FR")/Digital Data Network (abbreviated as "DDN") networks.

Summary of the Invention

Therefore, a main objective of the present invention is to provide a system for ensuring quality of service in a virtual private network and a method thereof, so as to provide a practical solution to MPLS VPN QoS problems.

In order to achieve the above objective, the present invention provides a system for ensuring quality of service in a network based virtual private network, including:

a logical bearer network, which is formed by connecting label switch paths configured with reserved bandwidth to various routers over a basic nIP network by using a multi-protocol label switch technique, and is dedicated to transmitting a service with a quality of service requirement; and

a bearer control network, which is used to maintain the logical bearer network, and route the service.

Wherein, the bearer control network includes centralized resource controllers for managing network resources in the logical bearer network, maintaining network topology of the logical bearer network, performing resource calculation and route selection, sending route indications to the routers, allocating resources and performing access control in the logical bearer network, and maintaining membership information and connectivity information for each virtual private network to implement automatic discovery and unilateral configuration of the membership.

One centralized resource controller is deployed in each domain of the logical bearer network; the centralized resource controllers are connected with each other, to exchange topology and resource information of the logical bearer network and routing information of the virtual private network.

The logical bearer network and the bearer control network distribute routes for the virtual private network, maintain membership for the virtual private network, and maintain connectivity between sites in the virtual private network in an out-of-band mode.

The routers include: provider edge routers, intermediate transfer routers, and core routers.

The provider edge routers are used to identify a virtual private network with a quality of service requirement, encapsulate, by using a label stack indicated by the centralized resource controller, a service with a quality of service requirement entering from the virtual private network, set quality of service fields of all labels in the label stack in accordance with a priority of the service, and transmit encapsulated service data packets via the logical bearer network.

The intermediate transfer routers are used to implement functions of static or dynamic configuration of label switch paths, differentiated-service-mode multi-protocol label switch, and stream processing by type of service.

The core routers are used to implement functions of differentiated-service-mode multi-protocol label switch and stream processing by type of service.

The centralized resource controller includes an interface management module, a protocol processing module, a membership maintenance module, a topology and resource management module, a route management module, and an automatic signaling discovery module.

The interface management module is used to implement and manage an interface for communication with an external device.

The protocol processing module is used to process protocols for communication between the centralized resource controller and various external devices, and forward communication data to the membership maintenance module, the topology and resource management module, the route management module, and the automatic signaling discovery module in accordance with requirements of the protocols; the protocol processing module receives/sends the communication data via the interface management module.

The membership maintenance module is used to maintain the membership information of the virtual private network and connectivity information between sites of the virtual private network.

The topology and resource management module is used to manage a topological relation and resources of the logical bearer network.

The route management module is used to manage a routing relation of the virtual private network.

The automatic signaling discovery module is used to discover changes automatically, and notify the membership maintenance module and the topology and resource management module to correct the corresponding information.

The present invention further provides a method for ensuring quality of service in a network based virtual private network, including the steps of:

A. in a basic IP network, constructing a logical bearer network, which is dedicated to transmitting a service with a quality of service requirement, by configuring label switch paths with reserved bandwidth by using a multi-protocol label switch technique;

B. deploying a centralized resource controller to centrally manage resources of the logical bearer network; and

C. if the service with a quality of service requirement is to be transmitted, marking a priority of the service in a quality of service field of a routing label corresponding to a multi-protocol label switch data packet encapsulated from the service data stream, and routing the service via the logical bearer network in accordance with a route allocated by the centralized resource controller.

Wherein, one centralized resource controller is deployed in each domain of the logical bearer network.

The route can be a serial label switch path determined by a label stack.

In the step C, quality of service fields of all labels in the service route label stack are set as a same value.

The method further includes the step of:

adjusting topology and resources of the logic bearer network dynamically by using a multi-protocol label switch traffic engineering technique.

In the step C, the priority of the service is determined by a type of the service.

When the virtual private network includes sites with a quality of service requirement and sites without a quality of service requirement, the method further includes the step of:

determining whether both service receiving and sending sites have a quality of service requirement; if yes, transmitting the service by using resources in the logical bearer network; and otherwise, transmitting the service by using other resources in the basic IP network.

The determining whether both service receiving and sending sites have a quality of service requirement includes the steps of:

E1. comparing route targets of the receiving and sending sites, and determining whether the connectivity between the receiving and sending sites is a general connectivity; if yes, proceeding to step E2; and

E2. determining whether the connectivity between the receiving and sending sites is a connectivity with a quality of service requirement by comparing the route targets of the receiving and sending sites; if yes, determining that the service between the receiving and sending sites has a quality of service requirement; and otherwise, determining that the service between the receiving and sending sites has no quality of service requirement.

The route allocated by the centralized resource controller to each pair of sites with a quality of service requirement is unique.

In comparison, it can be seen that the difference between the technical solution of the present invention and the prior art lies in: by pre-configuring partial resources dedicatedly to a QoS-VPN (referred to as VPN-LBN) in the basic IP network by using an MPLS technique and adding centralized resource controllers in the conventional VPN reference model to maintain the network topology and resources of the VPN-LBN as well as membership information and connectivity information of each QoS-VPN, admission control and route calculation are implemented in accordance with the resource condition of the logical bearer network, and it is ensured that all accessed services can obtain expected QoS.

The difference in the technical solution brings obvious advantageous effects, i.e., it solves the QoS problem in the MPLS VPN, and drives operators to provide QoS-assured VPNs; it overcomes the challenges in complexity, planning-ability, manageability and operability of operation of large-scale VPNs and cross-domain operation of VPNs; it unifies the QoS solutions for MPLS L3/L2/L1 VPNs.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of an MPLS network structure;

FIG. 2 shows an MPLS L3 VPN model defined in RFC 2547bis;

FIG. 3A is a flow chart of a method for ensuring quality of service in a virtual private network according to the present invention;

FIG. 3B is a flow chart of a method for implementing QoS-VPN according to an embodiment of the present invention;

FIG. 4 shows a reference model of a QoS-VPN architecture according to an embodiment of the present invention;

FIG. 5 shows an MPLS-based VPN-LBN according to an embodiment of the present invention; and

FIG. 6 is a schematic diagram of an internal structure of VPN-CRC and external connectivity thereof according to an embodiment of the present invention.

Detailed Description of the Embodiments

In order to make the objectives, technical solutions, and advantages of the present invention much clearer, hereinafter the present invention is described in further detail with reference to the accompanying drawings.

FIG. 3A is a flow chart of a method for ensuring quality of service in a virtual private network according to the present invention. The method includes the following steps of: first, in a basic IP network, constructing a logical bearer network, which is dedicated to transmitting a service with a quality of service requirement, by configuring label switch paths with reserved bandwidth by using a multi-protocol label switch technique (step S10); then, deploying a centralized resource controller for managing resources of the logical bearer network centrally (step S20); finally, when the service with a quality of service requirement is to be transmitted, marking a priority of the service in a quality of service field of a routing label stack corresponding to a multi-protocol label switch data packet encapsulated from the service data stream, and routing the service to an opposite end via the logical bearer network in accordance with a route allocated by the centralized resource controller (step S30).

According to the present invention, through pre-configuring partial resources dedicatedly to a QoS-VPN in the basic IP network by using an MPLS technique, and then configuring centralized resource controllers to maintain the network topology and resources of the VPN-LBN, as well as various membership information and connectivity information, so that expected QoS can be ensured for all accessed services.

The detailed implementation procedures of the method are described now with reference to an embodiment.

FIG. 3B shows a flow chart of implementing the above method. In step 100, capacity planning is carried out: services with a QoS requirement in the Network Based Virtual Private Network (abbreviated as "NBVPN") are classified into a special service type, which is referred to as QoS-VPN service in the present invention, and this kind of NBVPN is referred to as QoS-VPN. A network operator shall be capable of identifying such services when accessing the same; the most straightforward method (of course, not limited to this method) is to enable PEs at sites in the QoS-VPN to identify interfaces or sub-interfaces connected to the sites and deem all incoming services from these interfaces or sub-interfaces are QoS-VPN services. The network operator shall make planning for the capacity for QoS-VPN services, including topology, route, and bandwidth, etc., in accordance with the current and anticipated QoS-VPN services.

Next, in step 110, the VPN-Logical Bearer Network (abbreviated as "LBN") is configured. In accordance with the result of the capacity planning, an LBN is pre-configured dedicatedly for the QoS-VPN in the basic IP network by using an MPLS technique; for QoS-VPN traffic streams, the routing, resource allocation, admission control, and label forwarding are processed only in the VPN-LBN; VPN traffic streams without a QoS requirement are routed and forwarded in accordance with the existing VPN mechanism in partial resources that are not pre-configured in the basic network.

Next, in step 120, VPN-Centralized Resource Controllers (abbreviated as "CRC") are provided. A VPN-CRC is deployed in each domain of the VPN-LBN and is usually separated from data plane equipment in the VPN. The VPN-CRC is responsible for resource calculation, access control, resource allocation, and routing between sites of the VPN, distributing MPLS label stacks that represent the routes to ingress PEs, maintaining membership information and connectivity information for each QoS-VPN, and processing necessary signaling. The reason for deploying a CRC in each domain is: if only one global CRC is deployed, information to be coordinated will be too huge in a large-scale network. Domains are logical areas divided by the operator, for example, a domain may cover a province or city. The domain size can be determined by the actual processing capacity of the CRC.

In the foregoing embodiment, the topology and bandwidth of the QoS-VPN are allocated statically. In another preferred embodiment of the present invention, the topology and bandwidth of the VPN-LBN are adjusted dynamically by using an MPLS Traffic Engineering (abbreviated as "TE") technique, so as to implement LSP protection or a capacity change.

Next, in step 130, the VPN-CRC calculates and distributes access paths between sites. Since information of all available resources in the VPN-LBN and membership and connectivity information of the QoS-VPN are logged in the VPN-CRC, the VPN-CRC can calculate the access path for each pair of sites with a QoS requirement and distribute the route to the PEs, and the PEs can take actions accordingly. In this way, the route between each pair of sites with a QoS requirement is uniquely determined.

Next, in step 140, the service priority is marked, and the service is transmitted via the VPN-LBN. In each QoS-VPN, though the routes of all services between two sites are exactly the same, the traffic streams can still be classified into different types, such as voice, video, and data services. The service types can be identified at the ingress PE and marked with different priorities; when the ingress PE performs MPLS encapsulation for the data streams with different priorities, it maps the priorities to the EXP field in all labels in the label stack, which represents routing information and is distributed from the VPN-CRC to the ingress PE (since a pop operation is carried out for all labels in the label stack when the labels are forwarded along these routes, the priority information of traffic streams can be kept, provided that the EXP field in all labels are identical). In this way, after the VPN-CRC determines the route and bandwidth for services between two sites, different levels of services can be forwarded in an MPLS-DiffServ mode (differentiated service mode), so as to meet the requirements for time delay, jitter/packet loss, etc., and ensure VPN QoS.

It should be noted that a hybrid QoS-VPN can be divided into two parts: one part includes sites with a QoS requirement, and the above mechanism can be applied to this part; the other part includes sites without a QoS requirement, and follows the existing VPN mechanism. That is, when a service is received, it is required to determine whether both the service receiving and sending sites have a QoS requirement; if yes, the service can be transmitted by using resources in the logical bearer network; and otherwise, the service can be transmitted by using other resources in the basic IP network. In addition, before the determination of whether both the service receiving and sending sites have a QoS requirement, the method includes the sub-steps of: comparing route targets of the receiving and sending sites, determining whether the connectivity between the receiving and sending sites is a general connectivity; if yes, proceeding to the subsequent step; and otherwise, terminating the process.

Wherein, the step of determining whether both the service receiving and sending sites have a QoS requirement is performed in the following way: determining whether the connectivity between the receiving and sending sites is a connectivity with a quality of service requirement by comparing the route targets of the receiving and sending sites; if yes, determining that the service receiving and sending sites both have a quality of service requirement; and otherwise, determining that the service receiving and sending sites have no quality of service requirement.

Hereinafter the overall framework of the QoS-VPN is described with reference to FIG. 4.

In a preferred embodiment of the present invention, the QoS-VPN framework includes two layers: a logical bearer network (also referred to as "logical bearer layer") and a bearer control network (also referred to as "bearer control layer"). The logical bearer layer is formed by connecting PEs to CRs and ITRs via LSPs which are pre-configured with reserved bandwidth in accordance with the pre-defined capacity planning by using an MPLS technique.

The bearer control network includes several VPN-CRCs, and a VPN-CRC (excluding VPN-CRC backups) is deployed in each domain. The VPN-CRC manages the network resources (including bandwidth, processors, buffer zones) of the VPN-LBN, maintains network topology of the VPN-LBN, performs resource calculation and routing, sends route indications to PEs, allocates resources in the VPN-LBN, performs access control, and maintains a membership information table, a connectivity information table, and relevant signaling for each QoS-VPN, to implement automatic discovery and unilateral configuration of the membership.

Hereinafter the division method of the VPN-LBN is described.

In order to ensure reliable transmission in the QoS-VPN network, it is necessary to separate QoS-VPN services from Best effort services (including VPN services without a QoS requirement and general Internet services) in resource allocation and routing aspects. The resources of the QoS-VPN are allocated in the pre-configured VPN-LBN, and explicit routes are chosen by using the VPN-CRC; while the Best effort VPN services are still routed and forwarded in line with the conventional VPN mechanism in the remaining unallocated network resources.

As shown in FIG. 5, the VPN-LBN includes PEs, ITRs, CRs, and LSPs that connect these routers. The LSPs can be configured statically or, configured dynamically in accordance with the capacity planning and flow measurement data.

In order to implement LSP protection or capacity change, MPLS TE techniques, such as Fast Reroute (abbreviated as "FRR"), can be used to dynamically adjust LSP bandwidth and maintain VPN-LBN topology.

When a service request from a local site to a remote site in the QoS-VPN is transmitted via a PE to the VPN-CRC, the QoS requirement determined in accordance with a Service Level Agreement (abbreviated as "SLA") between subscribers and the operator is also transmitted to the VPN-CRC along with the service request. The VPN-CRC determines whether to admit the access (if necessary, participation of other VPN-CRCs in the VPN bearer control network is required) according to the network resource status. If the access is admitted, the VPN-CRC will calculate routes that can meet the QoS requirement and send routing information to the ingress PE, the routing information representing a set of serial LSPs from an ingress PE to an egress PE. The ingress PE logs the routing information, the corresponding QoS-VPN (by a VPN-ID), and local and remote sites (by site IDs); all services belonging to the QoS-VPN and from the local site to the remote site will be forwarded along the route, unless the ingress PE receives other route indications.

The ingress PE identifies the QoS-VPN from related information such as interface or sub-interface. When a QoS-VPN traffic stream enters into the network, the ingress PE obtains stream description information (which usually includes a source address, a source port, a destination address, a destination port, and a protocol type), then encapsulates the packet/frame with the label stack indicated by the VPN-CRC, sets different EXP bytes for all labels in the label stack for different data types (voice/video/data), and imports the data packet/frame into the VPN-LBN. When the data stream is transmitted via ITRs along the route, the DiffServ-aware MPLS technique is followed.

Hereinafter the most important device VPN-CRC in the solution of the present invention is described in detail.

The VPN bearer control network includes VPN-CRCs in the domains and is the control plane and management plane of the VPN bearer layer. In a preferred embodiment of the present invention, the VPN-CRC shall have the following functions: calculation of resources in the domain, routing, admission control, inter-domain resource request, maintenance of network topology, maintenance of membership information, maintenance and automatic discovery of connectivity information, unilateral configuration signaling, and so on. Furthermore, the VPN-CRC may support policy management, SLA management, LSP flow measurement, and interfacing to an Authentication, Authorization, and Accounting Server (abbreviated as "AAA Server").

The internal structure and external connectivity of the VPN-CRC are as shown in FIG. 6. The VPN-CRC 10 mainly includes the following modules:

An interface management module 111 is used to implement and manage interfaces that conduct communication with external equipment, for example, communication with an upstream VPN-CRC 20, a downstream VPN-CRC 30, an ITR 40, and an ER 50. The protocols used in the communication will be described hereinafter.

A system function module 112 is used to provide an underlying platform for normal operation of the entire VPN-CRC 10. In a preferred embodiment of the present invention, the system function module 112 is an operating system in the VPN-CRC 10.

A protocol processing module 113 is used to process protocols for communication between the VPN-CRC 10 and various external equipment, and forward communication data to a membership maintenance module 114, a topology and resource management module 115, a route management module 116, and an automatic signaling discovery module 117 as required by the protocol. The protocol processing module 113 sends/receives the communication data via the interface management module 111.

The membership maintenance module 114 is used to maintain a membership information table and a connectivity information table. The membership information table contains information of site members of the same QoS-VPN. The membership information table is a list of site IDs in the same QoS-VPN, and is indexed by a VPN-ID. The connectivity information table contains connectivity between members of the same QoS-VPN, i.e., which sites can be accessed by a specific site. The can be obtained from the membership information table and Route Targets of each site; if an export Route Target of a site is identical to an Import Route Target of another site in the same QoS-VPN, it means that there is connectivity between the two sites. The VPN-CRC 10 will refer to the connectivity information table when performing admission control. Through accessing the connectivity information table, full-mesh, Hub-Spoke, or any other topological relationship can be established among sites of the QoS-VPN.

The topology and resource management module 115 is used to manage a topological relation and resources of the VPN-LBN. The topological relation refers to the connectivity among nodes in the VPN-LBN; the resources mainly refer to the bandwidth reserved for the connectivity. The recording and maintenance of topology and resources in the VPN-LBN are independent of the basic network, and initial resource data in the VPN-LBN needs to be configured manually in accordance with the capacity planning result.

The route management module 116 is used to manage routing relations of all the QoS-VPNs in a unified way.

The automatic signaling discovery module 117 is used to discover changes automatically. The automatic discovery means that the connectivity information is provided by external equipment (e.g., PE) automatically instead of being configured in the VPN-CRC 10 manually. If information obtained by the automatic signaling discovery module 117 includes a change in the membership or LBN topology, the automatic signaling discovery module 117 will notify the membership maintenance module 114 or the topology and resource management module 115 to perform a modification accordingly.

In order to maintain and transmit the connectivity information of the QoS-VPN, the VPN-CRC has to maintain connectivity between QoS-VPN members, i.e., topology of QoS-VPN sites. This can be implemented (but not limited to) by logging two site lists of each QoS-VPN: one is a list of sites allowing sending; the other is a list of sites allowing receiving. In order to support automatic discovery of changes in the QoS-VPN membership and the connectivity information, whenever a site is added to or deleted from the QoS-VPN, a relevant update message shall be transmitted between the PE and the VPN-CRC, and the related VPN-CRC shall update the membership information table and the connectivity information table. With such a mechanism, unilateral configuration can be implemented, i.e., whenever a site is added to or deleted from the QoS-VPN or the connectivity between sites changes, what has to do is to configure the PE for the site added or deleted or for the site where the connectivity has changed. The configuration will trigger an update message, which will be transmitted automatically through relevant VPN-CRCs and PEs; the VPN-CRCs receiving the update message will update the corresponding QoS-VPN membership information table and connectivity information table.

When sites are added to the QoS-VPN, service requests (containing a VPN-ID, a local site ID, a remote site ID, and a QoS requirement) will be transmitted to the VPN-CRC of the current domain. The VPN-CRC will calculate resources (if necessary, participation of relevant VPN-CRCs is required) for the newly added sites to access other sites. If the addition of the sites is permitted, the VPN-CRC will calculate routes for the new sites to access other sites, and indicate the routes to relevant PEs. The PEs will update their QoS-routing information tables. When remote PEs sense addition of these sites, the remote PEs will trigger their own local sites to access service requests of the new sites, and the VPN bearer control network will perform the same processing. Finally, all sites will obtain inter-access routing information.

When sites are deleted, the VPN-CRC will update the relevant membership information table and connectivity information table, release and delete resources related with the deleted sites, and notify relevant PEs to delete relevant entries from the QoS routing information tables; when remote PEs sense deletion of the sites, the remote PEs will trigger their own local sites to delete resources involved in access to the deleted sites.

A topology and resource table 118 is used to store a topological relation and resources of the VPN-LBN.

A routing table 119 is used to store routes of the QoS-VPN (substantively, a collection of accessible destination addresses of the sites). The collection of the destination addresses includes several address prefixes or addresses.

When the VPN-CRC receives a service request (containing a VPN-ID, a local site ID, a remote site ID, and a QoS requirement) from the ingress PE of the local domain or a resource request from another VPN-CRC, the VPN-CRC will perform resource calculation, routing, and admission control (if necessary, the VPN-CRC further transmits the resource request to the downstream VPN-CRC). If the resource calculation result of a certain VPN-CRC involved is "reject", the VPN-CRC has to transmit the response to upstream VPN-CRCs, till the response reaches the ingress PE. Otherwise, it is necessary to transmit the routing information determined by the VPN-CRC to upstream VPN-CRCs, till the whole routing information (label stack) is sent to the ingress PE. When forwarding the data from a local site to a remote site, the ingress PE sets the EXP byte in all labels in the label stack in accordance with a descriptor of a traffic stream from a CE to a PE. In this way, all services from the local site to the remote site are transmitted along the route as calculated above; however, services of different types in the same direction will be distinguished by the EXP byte and transmitted in accordance with the MPLS-DiffServ mechanism.

Hereinafter the requirements for functions of PEs, ITRs, and CRs on the VPN bearer layer as shown in FIG. 4 are described.

The PE shall support static LSP configuration or dynamic LSP setup in CR-LDP/RSVP-TE, so as to implement pre-configuration and dynamic VPN-LBN adjustment; furthermore, the PE shall support stream classification, so as to set an EXP byte for the label stack received from the VPN-CRC. The PE stores the QoS routing information table, which mainly stores the following information: a VPN-ID, a local site, remote sites (a collection of destination address accessible in remote sites), and routes between the local site and the remote sites.

When an admission control response is received from the VPN-CRC, if the response is "admit access", the route and QoS information will be included in the response, and the ingress PE will log the information in the QoS information table. The ingress PE maintains the information for each QoS-VPN. In accordance with the VPN-ID index, the ingress PE logs an entry for each pair of sites (from a local site to a remote site) in the information of each QoS-VPN. The ingress PE performs queuing, scheduling, shaping, marking, policy-making, and MPLS encapsulation according to the QoS routing information table, and then performs, in the VPN-LBN, forwarding along the route determined in the label stack.

The Intermediate Transfer Router (ITR) shall support static LSP configuration or dynamic LSP setup through CR-LDP/RSVP-TE, so as to implement pre-configuration and dynamic adjustment of VPN-LBN; furthermore, the ITR shall support DiffServ-aware MPLS and stream processing by type of service.

The Core Router (CR) in the IP backbone network shall support only DiffSerV-aware MPLS and stream processing by type of service.

Hereinafter the method of isolation between QoS-VPNs by means of a VPN address is described.

A VPN address may include a globally unique VPN-ID in the VPN-LBN and private addresses related to L3/L2/L1 VPN, for example, an IPV4/IPV6/IPX address in L3 VPN, a data link address in L2 VPN, and a cross link ID in L1 VPN; in such a VPN address solution, addresses of sites in different QoS-VPNs may be overlapped. Since the VPN-ID is globally unique in the VPN-LBN, the resultant VPN address is also unique in the VPN-LBN.

With the QoS routing information table, information of different QoS-VPNs can be distinguished by VPN-IDs, and thereby isolation between QoS-VPNs can be implemented.

Hereinafter the routing and forwarding method is described.

QoS-VPN routes are maintained in the QoS routing information table in a PE, at a granularity of a site pair of a QoS-VPN, i.e., routes for all services from a local site to a remote site are identical. At the ingress PE, the route searching is performed in two stages: in the first stage, the home QoS-VPN of the local site is found in accordance with the VPN-ID as the index; in the second stage, the searching is oriented to the pair of local site and remote site in the QoS-VPN. What is associated with the remote site is an aggregated address in the remote site. When the destination address in the traffic stream matches the aggregated address associated with the remote site in the site pair, the searching is deemed as successful. After the two-stage searching is successful, the ingress PE determines routing information (an MPLS label stack specified by the VPN-CRC) for the traffic stream, and marks an EXP byte in a routing information label. If either of the searching at two stages fails, the ingress PE can reject the traffic stream.

Based on the MPLS technique, the QoS-VPN forwarding employs the label stack issued by the VPN-CRC and the EXP byte set by the ingress PE for the traffic stream, and also employs an MPLS-DiffServ mechanism in accordance with an outer layer label, so as to ensure the service bandwidth and forwarding priority, thereby ensuring QoS (bandwidth, time delay, jitter, packet loss rate) of the QoS-VPN.

Hereinafter the requirement for interfaces and signaling between devices is described, including interfaces and protocols between PEs and CEs, between a VPN-CRC and operator's routers (including a PE, an ITR, and a CR), and between VPN-CRCs.

The interface between a PE and a CE is used to transmit subscriber information, such as topology, an aggregated private address (e.g., a private IPv4/IPv6/IPX address in L3 VPN, a data link address in L2 VPN, or a cross link ID in L1 VPN) of the site connected to the CE, and a service request (including a stream ID).

The interface between the VPN-CRC and the PE enables the VPN-CRC to instruct the PE to process traffic streams of each site. It is necessary to define a corresponding protocol for the interface, for example, the protocol may be implemented by extending a COPS according to the structure described herein.

The protocol shall support the following functions:

(1) The ingress PE sends a service request (containing a VPN-ID, a local site ID, an export Route Target, a remote site ID, and a QoS requirement) to the VPN-CRC. The QoS requirement includes a service type and the corresponding bandwidth, a priority, time delay, jitter limit, a packet loss rate, MTU, etc. The QoS requirement for a site may be determined according to the SLA between the subscriber and the operator.

(2) The VPN-CRC determines whether there is connectivity between the local site and the remote site in accordance with the site IDs and the export Route Target contained in the service request (the VPN-CRC has to transmit the service request message to the corresponding VPN-CRC and the egress PE); if there is connectivity, the VPN-CRC will notify the result to the ingress PE, regardless of whether the admission control result from the VPN bearer control network is "reject" or "admit".

(3) If the admission control result is "admit", the VPN-CRC notifies the ingress PE of the route (a label stack representing a set of serial LSPs) associated with the site pair. The PE creates the record in the QoS routing information table for each site pair in each QoS-VPN.

(4) When a site is added to or deleted from the QoS-VPN or the connectivity between sites changes, the PE corresponding to the site where the change happened shall send an update message to the VPN-CRC of the current domain. The VPN-CRC transmits the message to an adjacent VPN-CRC and ultimately to the PE at the opposite end. Corresponding VPN-CRCs will update their membership information tables and connectivity information tables, and related PEs will update corresponding entries in the QoS routing information tables.

(5) The PE sends, to the VPN-CRC, the aggregated VPN address information of the site connected to the PE; then the VPN-CRC issues the information in the VPN bearer control network and ultimately to corresponding PEs. This function can be implemented by extending the existing BGP protocol. Finally, all PEs store, in the QoS routing information tables, the aggregated VPN addresses of QoS-VPN sites connected to them, so that when receiving a traffic stream, a PE can determine the route and EXP byte in accordance with the QoS routing information table and the stream ID.

Furthermore, the interface between a VPN-CRC and a PE, an ITR, or a CR in the domain shall support the following functions:

(1) It shall permit the VPN-CRC to configure MPLS Diffserv PHB for each type of service.

(2) It shall permit such routers as a PE, an ITR or a CR to report an LSP status to the VPN-CRC, i.e., when a link or router fails, the router shall report to the VPN-CRC of the current domain; the VPN-CRC issues the failure information in the VPN bearer control network, so that the VPN-CRCs recalculate resources for the reserved routes. If there is any route to be updated, the VPN-CRC shall send the new route to the corresponding ingress PE.

The interface between VPN-CRCs is used to implement resource allocation and routing for services between QoS-VPN sites across domains.

It is necessary to define a separate protocol for the interface, and the corresponding function can be accomplished by extending COPS or BGP.

The protocol shall support the following functions:

(1) It shall permit the VPN-CRC to request the downstream VPN-CRC to allocate bearer resources for services between QoS-VPNs across domains.

(2) It shall permit the VPN-CRC to notify the inter-domain QoS-VPN service identification information (a local site ID, a remote site ID, and a VPN-ID) to the downstream VPN-CRC.

(3) It shall permit the VPN-CRC to notify the QoS requirement of inter-domain QoS-VPN services (including a service type and bandwidth thereof, priority, time delay limit, jitter limit, packet loss rate limit, etc.) to the downstream VPN-CRC.

(4) It shall permit the VPN-CRC to request the adjacent VPN to release the bearer resources allocated for services between QoS-VPNs across domains.

(5) It shall permit the VPN-CRC to query other VPN-CRCs for the status of resource allocation for services between QoS-VPNs across domains.

(6) It shall permit the VPN-CRC to notify other VPN-CRCs of query responses.

(7) It shall permit the VPN-CRC to exchange service level specification (abbreviated as "SLS") and routing information with other VPN-CRCs.

Hereinafter the case of a hybrid QoS-VPN is described.

In some cases, some sites in the VPN have a QoS requirement while others don't have a QoS requirement; such a VPN is called a hybrid QoS-VPN. A hybrid QoS-VPN includes two parts: one part includes sites with a QoS requirement, and is called sub-QoS-VPN; the other part includes sites without a QoS requirement, and is called sub-VPN. For the sub-QoS-VPN, the above MPLS NBVPN scheme that ensures QoS by centralized resource control can be used for QoS assurance; for the sub-VPN, the QoS assurance can be implemented as instructed in relevant RFCs and drafts of IETF L3 VPN/L2 VPN workgroups. Route Target is used to determine the connectivity in the entire VPN (including the sub-QoS-VPN and the sub-VPN) by VPN-CRCs. In addition, QoS Route Target (route target with a QoS requirement) is introduced to maintain a connectivity information table of the sub-QoS-VPN. QoS Route Targets are in the same format as Route Targets. After Route Targets are compared to determine the general connectivity between sites, QoS Route Targets are continuously compared (if the service request from either of the two sites exists); if the comparison succeeds, it means the service between the two sites has a QoS requirement, and both of the sites belong to the sub-QoS-VPN. Otherwise, the two sites shall be included in the sub-VPN.

Hereinafter in-domain and inter-domain QoS-VPNs are described.

In-domain QoS-VPN routing and inter-domain routing are the foundation of resource management and admission control.

The VPN-CRC performs in-domain routing in the topology information table and the resource information table. A routing algorithm may be static, e.g., Time Dependent Routing (abbreviated as "TDR")/State Dependent Routing (abbreviated as "SDR"). Furthermore, the VPN-CPC shall maintain an inter-domain routing table for determining inter-domain LSPs in a QoS signaling protocol and find an adjacent downstream VPN-CRC.

The inter-domain routing table in the VPN-CRC can be configured manually or created automatically by running a dynamic routing protocol.

Hereinafter how cross-network providers provide a QoS-VPN is discussed.

To support a QoS-VPN across different networks of different providers, Autonomous System Boundary Routers (abbreviated as "ASBRs") thereof shall communicate with each other to transmit VPN service request signaling and VPN services. If VPN-CRCs are deployed in both networks and can communicate with each other, the VPN-CRCs only exchange and map inter-network SLAs; in this case, the VPN-CRCs only manage internal link resources, while the ASBRs manage inter-network link resources through specified SLAs and accomplish ingress PE functions that are available in the case of an operator internal QoS-VPN. If either of the networks is not provided with a VPN-CRC and but employs another QoS mechanism, the two ASBRs shall map the QoS requirement to each other, and the final QoS assurance level will depend on the VPN QoS implement mechanism of the other network provider.

Though the present invention is illustrated and described with reference to some preferred embodiments of the present invention, those of ordinary skilled in the art shall understand that diverse modifications can be made in forms and details to the present invention without departing from the spirit and scope of the present invention that are defined by the appended claims.

Drawings

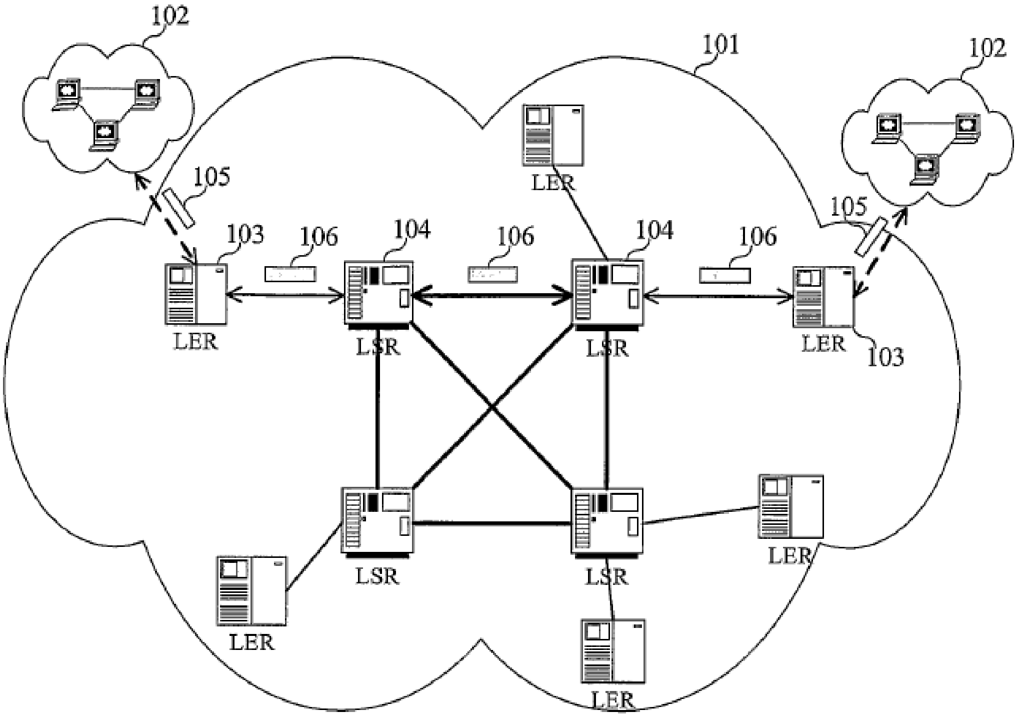


FIG. 1

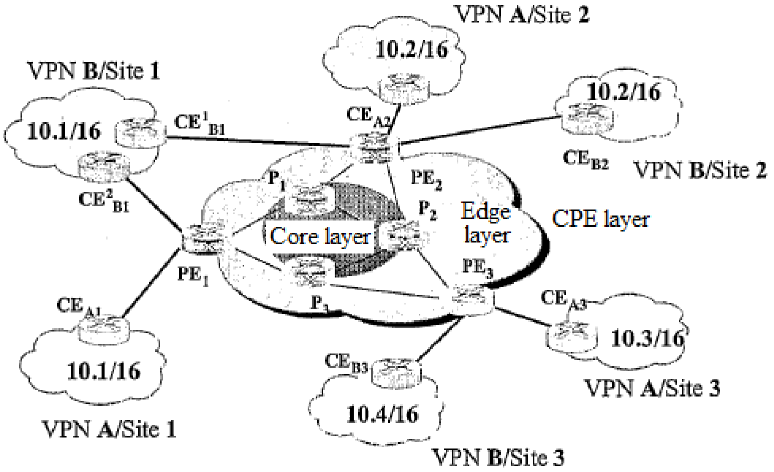


FIG. 2

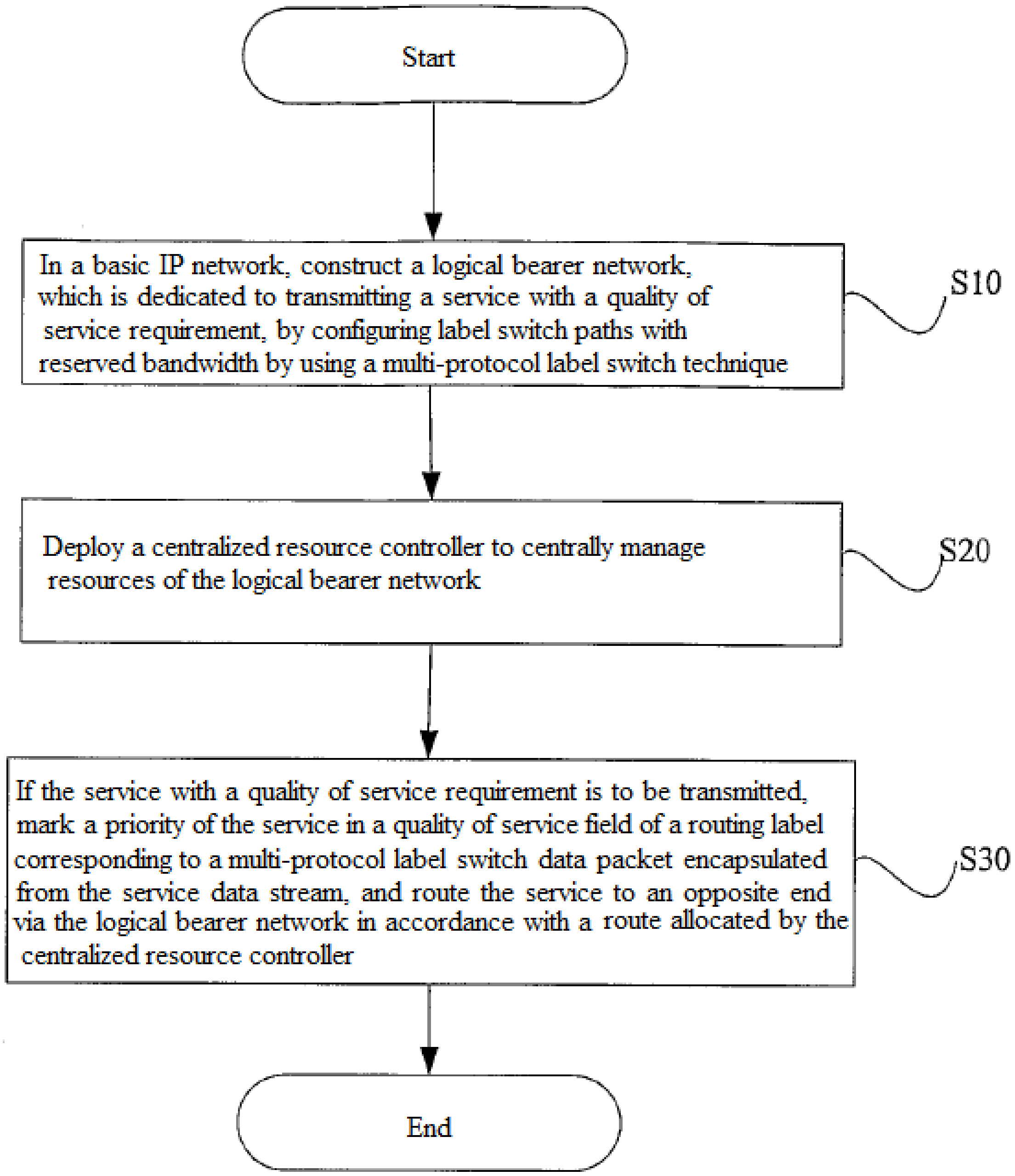

Start
In a basic IP network, construct a logical bearer network, which is dedicated to transmitting a service with a quality of service requirement, by configuring label switch paths with reserved bandwidth by using a multi-protocol label switch technique
S10
Deploy a centralized resource controller to centrally manage resources of the logical bearer network
S20
If the service with a quality of service requirement is to be transmitted, mark a priority of the service in a quality of service field of a routing label corresponding to a multi-protocol label switch data packet encapsulated from the service data stream, and route the service to an opposite end via the logical bearer network in accordance with a route allocated by the centralized resource controller
S30
End

FIG. 3A

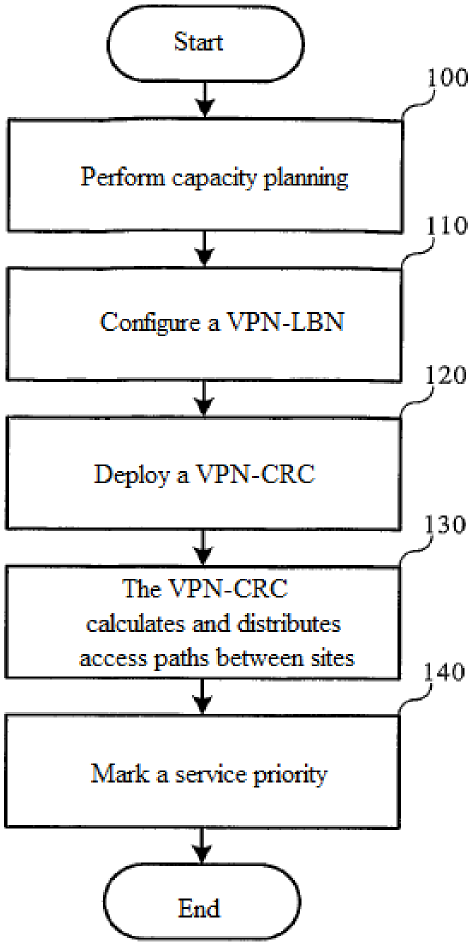

Start
100
Perform capacity planning
110
Configure a VPN-LBN
120
Deploy a VPN-CRC
130
The VPN-CRC calculates and distributes access paths between sites
140
Mark a service priority
End

FIG. 3B

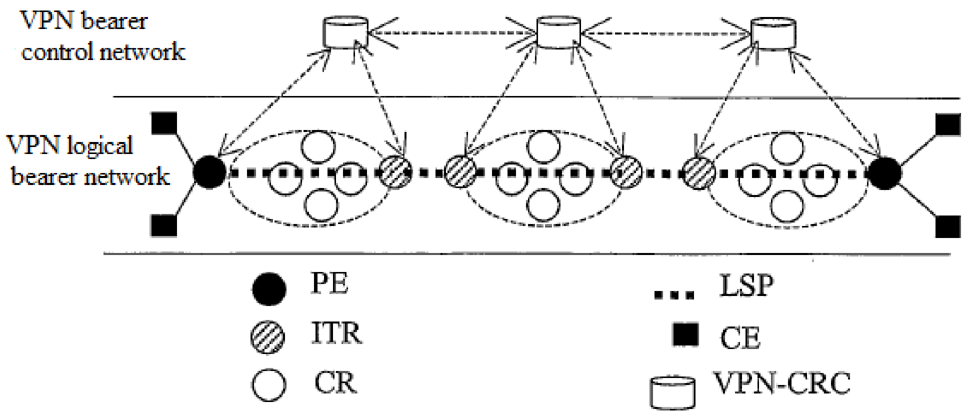

VPN bearer control network
VPN logical bearer network
PE
ITR
CR
LSP
CE
VPN-CRC

FIG. 4

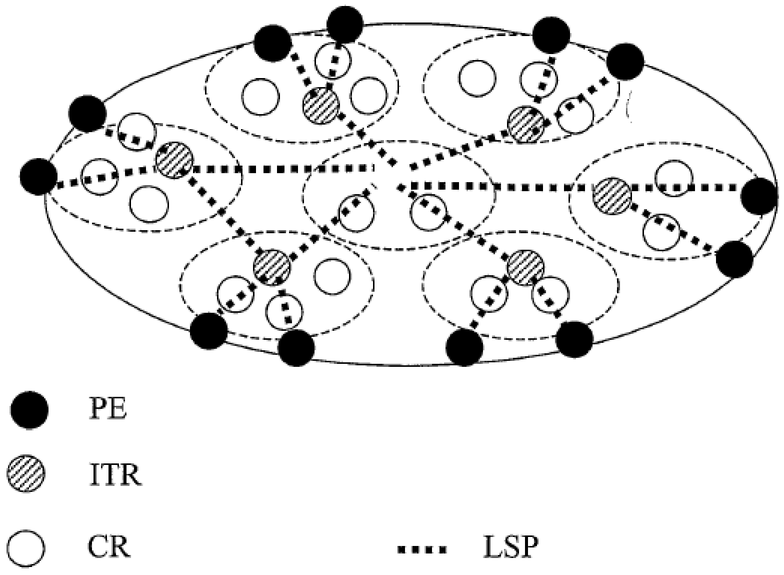

PE
ITR
CR
LSP

FIG. 5

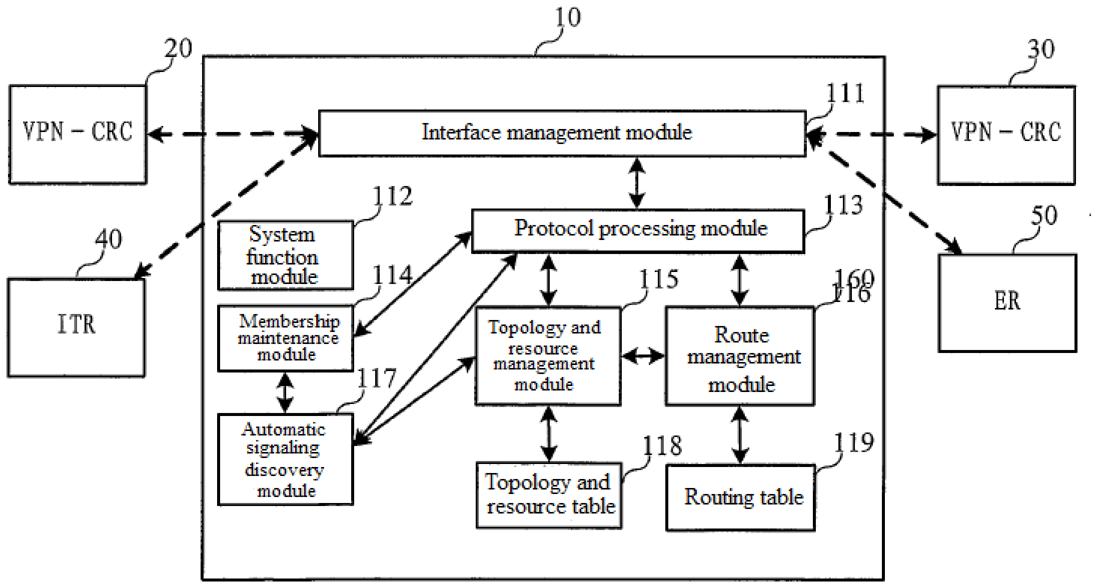

10
20
VPN－CRC
30
VPN－CRC
111
Interface management module
40
ITR
112
System function module
113
Protocol processing module
50
ER
114
Membership maintenance module
115
160
116
Topology and resource management module
Route management module
117
Automatic signaling discovery module
118
119
Topology and resource table
Routing table

FIG. 6