(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101599901 B
(45)授权公告日 2011.06.08

(21)申请号 200910088986.1

(22)申请日 2009.07.15

(73)专利权人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号华为杭州生产基地

(72)发明人 薛明 韩小平

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 王一斌 王琦

(51)Int.Cl.
H04L 12/56(2006.01)
H04L 12/66(2006.01)

(56)对比文件
US 7039687 B1,2006.05.02, 全文.
CN 1863127 A,2006.11.15, 全文.
CN 101355557 A,2009.01.28, 全文.
CN 1414753 A,2003.04.30, 全文.

审查员 谢正程

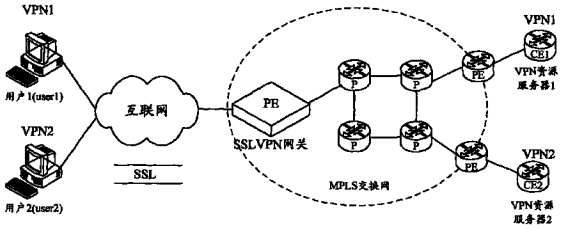
权利要求书 6 页 说明书 21 页 附图 7 页

(54)发明名称

远程接入 MPLS VPN 的方法、系统和网关

(57)摘要

本发明公开了一种远程接入 MPLS VPN 的方法、系统和网关，该网关同时作为 SSL VPN 网关和 PE。所述方法在 SSL VPN 网关中创建多个虚拟接口，一个 VPN 绑定一个虚拟接口并形成 VPN 实例；根据用户的认证授权信息区分不同 VPN 的用户，将用户的认证授权信息与相应 VPN 绑定；当 SSL VPN 网关接收用户 x 发来的报文时，根据用户 x 绑定的 VPN 实例为报文打上内外标签并转发。当 SSL VPN 网关接收到来自资源服务器的应答报文时，根据 VPN 标签查找相应 VPN 实例，根据查找到 VPN 实例将应答报文通过 SSL 连接转发给用户 x。这样，远程用户能够通过自身与 SSL VPN 网关之间的 SSL 连接，访问 MPLS VPN 中的 VPN 资源服务器。



CN 101599901 B

1. 一种远程接入多协议标记交换虚拟专用网络 MPLS VPN 的方法，其特征在于，远程用户通过自身与安全套接层虚拟专用网络 SSL VPN 网关之间的 SSL 连接访问 MPLS VPN 中的 VPN 资源服务器，所述 SSL VPN 网关同时作为 MPLS 交换网中的服务提供商边缘 PE 路由器，该方法包括：

A、在 SSL VPN 网关中创建多个虚拟接口，一个 VPN 绑定一个虚拟接口，根据 VPN 绑定的虚拟接口形成 VPN 实例；根据用户的认证授权信息区分不同 VPN 的用户，将用户的认证授权信息与相应 VPN 实例绑定；

B、用户 x 与 SSL VPN 网关之间进行信息交互，建立与远程接入相关的连接；

C、SSL VPN 网关接收用户 x 通过 SSL 连接发来的报文，根据用户 x 的认证授权信息绑定的 VPN 实例，为所接收报文添加 VPN 标签和 MPLS 转发标签，并通过 MPLS 交换网转发到 VPN 资源服务器；

D、SSL VPN 网关接收所述 VPN 资源服务器的返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例，根据查找到的 VPN 实例将应答报文通过所述 SSL 连接返回给用户 x。

2. 如权利要求 1 所述的方法，其特征在于，与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 1：目的地址为虚拟接口 V1 的 IP 地址，下一跳为内部环回接口地址；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；

当采用传输控制协议 TCP 或网页 WEB 方式接入 VPN 资源服务器时：

步骤 B 所述建立与远程接入相关的连接包括：当用户 x 请求访问 VPN 资源服务器 S1 时，建立用户 x 与 SSL VPN 网关之间的 SSL 连接；

为用户 x 建立虚拟接口 V1 与 VPN 资源服务器 S1 之间的 TCP 连接；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；在建立所述 TCP 连接过程中，根据用户 x 的认证授权信息绑定的 VPN 实例，为所述 TCP 连接的套接字 SOCKET 设置 VPN 实例标签索引；

所述步骤 C 包括：接收用户 x 通过 SSL 连接发来的报文，根据为用户 x 建立的 TCP 连接的信息，在 TCP 层为所接收报文添加 VPN 实例标签索引，再由 MPLS 模块根据 VPN 实例标签索引找到相应 VPN 实例，为报文添加 VPN 标签和 MPLS 转发标签，然后通过为用户 x 建立的 TCP 连接将报文转发给 VPN 资源服务器 S1；

所述步骤 D 包括：接收通过所述 TCP 连接返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例；根据所述应答报文的私网目的地址在查找到的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，则直接将所接收的应答报文转发到上层应用，该上层应用通过所述 SSL 连接将应答报文发送给用户 x。

3. 如权利要求 2 所述的方法，其特征在于，所述步骤 C 包括：

c1、报文通过 SSL 连接进入 SSLVPN 网关后，由位于 IP 层的 IP 模块去掉报文的公网 IP 头，将报文的数据部分经由 TCP 模块上送到位于应用层的 SSLVPN 业务模块；

c2、所述 SSLVPN 业务模块确定将所接收的报文通过为用户 x 建立的 TCP 连接转发；

c3、位于 TCP 层的 TCP 模块根据为用户 x 建立的 TCP 连接，为报文添加私网 IP 头，并且根据 SOCKET 的 VPN 实例标签索引在报文中记录 VPN 实例标签索引；

c4、位于 IP 层的 IP 模块通过路由查找确定由 MPLS 转发，并将报文发送给位于网络接口和 IP 层之间的 MPLS 模块；

c5、所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的 VPN 实例为报文添加 VPN 标签和 MPLS 转发标签并转发。

4. 如权利要求 3 所述的方法，其特征在于，所述步骤 D 包括 ：

d1、应答报文通过所述 TCP 连接进入 SSL VPN 网关后，位于网络接口和 IP 层之间的 MPLS 模块根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的报文及其所属 VPN 信息发送给位于 IP 层的 IP 模块 ；

d2、所述 IP 模块根据所述所属 VPN 信息获取相应 VPN 实例，并根据所述应答报文的私网目的地址在获取的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，然后直接将去掉私网 IP 头的应答报文经由 TCP 层转发到位于应用层的 SSL VPN 业务模块 ；

d3、所述 SSL VPN 业务模块确定将接收自所述 TCP 连接的应答报文通过所述 SSL 连接发送给用户 x，并将应答报文发送给所述 TCP 模块 ；

d4、所述 TCP 模块根据所述 SSL 连接的信息为报文添加公网 IP 头，由 IP 模块将报文通过所述 SSL 连接发送给用户 x。

5. 如权利要求 1 所述的方法，其特征在于，与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 2 ：目的地址为虚拟接口 V1 所在网段，下一跳为虚拟接口 V1 的 IP 地址 ；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口 ；

当采用 IP 方式接入 VPN 资源服务器时 ：

步骤 A 所述创建多个虚拟接口为 ：对应为每个 VPN 设置的地址池创建一个虚拟接口 ；对应的地址池和虚拟接口属于同一网段 ；

所述步骤 B 包括 ：SSL VPN 网关从为用户 x 所属 VPN 设置的地址池中为用户 x 分配虚地址 Add_x ；当用户 x 请求访问 VPN 资源服务器 S1 时，建立用户 x 与 SSL VPN 网关之间的 SSL 连接 ；

所述步骤 C 包括 ：接收用户 x 通过 SSL 连接发来的携带私网 IP 头的报文，其私网源地址为 Add_x ；根据用户 x 的认证授权信息绑定的 VPN 实例，在 IP 层为所接收报文添加 VPN 实例标签索引，再由 MPLS 模块根据 VPN 实例标签索引为报文添加 VPN 标签和 MPLS 转发标签，然后根据报文携带的私网 IP 头，通过直接 IP 转发方式将报文转发给 VPN 资源服务器 S1 ；

所述步骤 D 包括 ：接收返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例 ；根据所述应答报文的私网目的地址 Add_x 在查找到的 VPN 实例中匹配到所述路由转发表项 2，获得下一跳为虚拟接口 V1，则通过所述虚拟接口 V1 将应答报文经由所述 SSL 连接转发给用户 x。

6. 如权利要求 5 所述的方法，其特征在于，所述步骤 C 包括 ：

c1、报文通过所述 SSL 连接进入 SSL VPN 网关后，由 IP 层的 IP 模块去掉报文的公网 IP 头，将保留私网 IP 头和数据部分的报文发送到位于应用层的 SSL

VPN 业务模块 1，SSL VPN 业务模块 1 把报文发送给位于 IP 层的 SSL VPN 业务模块 2 ；

c2、所述 SSL VPN 业务模块 2 确定以直接 IP 转发方式转发报文，将报文发送给位于 IP 层的 VPN 标签处理模块 ；

c3、所述 VPN 标签处理模块根据用户 x 的认证授权信息绑定的 VPN 实例，在报文中记录 VPN 实例标签索引，然后将报文发给 IP 模块 ；

c4、所述 IP 模块通过路由查找确定由 MPLS 进行转发，并将报文发给位于网络接口和 IP 层之间的 MPLS 模块；

c5、所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的 VPN 实例为报文添加 VPN 标签和 MPLS 转发标签并转发。

7. 如权利要求 6 所述的方法，其特征在于，所述步骤 D 包括：

d1、应答报文进入 SSL VPN 网关后，位于网络接口和 IP 层之间的 MPLS 模块根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的报文及其所属 VPN 信息发送给 IP 层的 IP 模块；

d2、所述 IP 模块根据所述所属 VPN 信息获取相应 VPN 实例，并根据应答报文的私网目的地址 Add_x 在获取的 VPN 实例中匹配到所述路由转发表项 2，获得下一跳为虚拟接口 V1；

d3、位于 IP 层的 SSLVPN 业务模块 2 确定通过虚拟接口 V1 将应答报文经由所述 SSL 连接发送给用户 x，并将应答报文发送给位于应用层的 SSL VPN 业务模块 1，SSL VPN 业务模块 1 将应答报文发送给位于 TCP 层的 TCP 模块；

d4、所述 TCP 模块根据所述 SSL 连接的信息为应答报文添加公网 IP 头，由 IP 模块通过所述 SSL 连接将报文发送给用户 x。

8. 如权利要求 1 所述的方法，其特征在于，VPN 与虚拟接口绑定以及用户与 VPN 实例绑定后，进一步形成对应关系表，该对应关系表包括用户标识、用户的认证授权信息、虚拟接口和绑定的 VPN 实例的标签索引。

9. 如权利要求 1 所述的方法，其特征在于，所述认证授权信息为用户组、和 / 或虚拟域、和 / 或角色。

10. 如权利要求 1 所述的方法，其特征在于，所述虚拟接口为 SSL VPN 虚拟以太网接口或环回接口。

11. 一种网关，应用于远程用户通过自身与所述网关之间的 SSL 连接访问 MPLS VPN 中 VPN 资源服务器的系统，所述网关同时作为 SSL VPN 中的 SSLVPN 网关和 MPLS VPN 中的 PE 路由器；其特征在于，

所述网关包括配置单元、第一网络接口、第二网络接口、处理单元、VPN 实例存储单元和对应关系存储单元；

所述配置单元，用于创建多个虚拟接口、一个 VPN 绑定一个虚拟接口，根据 VPN 绑定的虚拟接口形成 VPN 实例，将形成的 VPN 实例存储在 VPN 实例存储单元中；根据用户的认证授权信息区别不同 VPN 的用户，将用户与相应的认证授权信息与相应 VPN 实例绑定；将建立的各种绑定关系存储在对应关系存储单元中；

所述对应关系存储单元，用于存储配置单元建立的绑定关系；

所述 VPN 实例存储单元，用于存储 VPN 实例；

第一网络接口，为所在网关和用户之间提供数据传输通道；

第二网络接口，为所在网关和 MPLS 交换网提供数据传输通道；

处理单元，用于与用户 x 进行信息交互，建立与远程接入相关的连接；当接收到用户 x 通过 SSL 连接发来的报文时，根据所述对应关系存储单元存储的绑定关系，从所述 VPN 实例存储单元获取用户 x 的认证授权信息绑定的 VPN 实例，采用获取的 VPN 实例为所接收报文添加 VPN 标签和 MPLS 转发标签，并通过 MPLS 交换网转发给 VPN 资源服务器；当接收到所述

VPN资源服务器返回的应答报文时，根据该应答报文携带的VPN标签在所述VPN实例存储单元中查找相应VPN实例，根据查找到的VPN实例将应答报文通过所述SSL连接返回给用户x。

12. 如权利要求11所述的网关，其特征在于，与用户x的认证授权信息绑定的VPN实例包括路由转发表项1：目的地址为虚拟接口V1的IP地址，下一跳为内部环回接口地址；所述虚拟接口V1为用户x所属VPN绑定的虚拟接口；

当采用TCP或WEB方式接入VPN资源服务器时，所述处理单元进一步用于：

在建立与远程接入相关的连接时，建立用户x与所在网关之间的SSL连接，为用户x建立虚拟接口V1与被请求访问的VPN资源服务器S1之间的TCP连接；在建立所述TCP连接过程中，根据用户x的认证授权信息绑定的VPN实例，为所述TCP连接的SOCKET设置VPN实例标签索引；

在接收到用户x通过所述SSL连接发来的报文时，根据为用户x建立的TCP连接的信息，在TCP层为所接收报文添加VPN实例标签索引，再由处理单元中的MPLS模块根据VPN实例标签索引找到相应VPN实例，为报文添加VPN标签和MPLS转发标签，然后通过为用户x建立的TCP连接将报文转发给VPN资源服务器S1；

在接收到通过所述TCP连接返回的应答报文时，根据应答报文携带的VPN标签查找相应VPN实例，根据所述应答报文的私网目的地址在查找到的VPN实例中匹配到所述路由转发表项1，获得下一跳为内部环回接口地址，则直接将所接收的应答报文转发到上层应用，该上层应用通过所述SSL连接将应答报文发送给用户x。

13. 如权利要求12所述的网关，其特征在于，所述处理单元包括位于应用层的SSL VPN业务模块和VPN标签处理模块、位于TCP层的TCP模块、位于IP层的IP模块，以及位于IP层与网络接口之间的MPLS模块；

所述SSL VPN业务模块，用于当用户x请求访问VPN资源服务器S1时，建立用户x与所在网关之间的SSL连接，为用户x建立虚拟接口V1与VPN资源服务器S1之间的TCP连接；

所述VPN标签处理模块，用于在建立所述TCP连接过程中，根据用户x的认证授权信息绑定的VPN实例，为所述TCP连接的SOCKET设置VPN实例标签索引；

当报文通过所述SSL连接进入所在网关后，所述IP模块去掉报文的公网IP头，将报文的数据部分经由TCP模块上送到SSL VPN业务模块；

所述SSL VPN业务模块进一步确定将所接收的报文通过为用户x建立的TCP连接转发，并将报文发送给所述TCP模块；

所述TCP模块根据为用户x建立的TCP连接，为报文添加私网IP头，并且根据SOCKET的VPN实例标签索引在报文中记录VPN实例标签索引，然后将报文发给所述IP模块；

所述IP模块进一步通过路由查找确定由MPLS转发，并将报文发送给MPLS模块；

所述MPLS模块根据报文携带的VPN实例标签索引查找相应VPN实例，为报文添加VPN标签和MPLS转发标签并转发；

当应答报文通过所述TCP连接进入所在网关后，所述MPLS模块进一步根据应答报文携带的VPN标签确定报文所属VPN，将去掉VPN标签的报文及其所属VPN信息发送给所述IP模块；

所述 IP 模块进一步根据所述所属 VPN 信息从所述 VPN 实例存储单元中获取相应 VPN 实例，并根据应答报文的私网目的地址在获取的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，然后直接将去掉私网 IP 头的报文经由 TCP 模块转发到所述 SSL VPN 业务模块；

所述 SSL VPN 业务模块进一步确定将接收自所述 TCP 连接的应答报文通过所述 SSL 连接发送给用户 x，并将应答报文发送给所述 TCP 模块；

所述 TCP 模块进一步根据所述 SSL 连接的信息为应答报文添加公网 IP 头，由 IP 模块将报文通过所述 SSL 连接发送给用户 x。

14. 如权利要求 11 所述的网关，其特征在于，与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 2：目的地址为虚拟接口 V1 所在网段，下一跳为虚拟接口 V1 的 IP 地址；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；

当采用 IP 方式接入 VPN 资源服务器时，所述配置单元在创建虚拟接口时，对应为每个 VPN 设置的地址池创建一个虚拟接口，对应的地址池和虚拟接口属于同一网段；

所述处理单元进一步用于：

在建立与远程接入相关的连接时，从为用户 x 所属 VPN 设置的地址池中为用户 x 分配虚地址 Add_x；建立用户 x 与所在网关之间的 SSL 连接；

在接收到用户 x 通过 SSL 连接发来的携带私网 IP 头的报文时，根据用户 x 的认证授权信息绑定的 VPN 实例，在 IP 层为所接收报文添加 VPN 实例标签索引，再由处理单元中的 MPLS 模块根据 VPN 实例标签索引为报文添加 VPN 标签和 MPLS 转发标签；所述私网 IP 头的源地址为 Add_x；

在接收到应答报文时，根据该应答报文携带的 VPN 标签查找相应 VPN 实例；根据所述应答报文的私网目的地址 Add_x 在查找到的 VPN 实例中匹配到所述路由转发表项 2，获得下一跳为虚拟接口 V1，则通过所述虚拟接口 V1 将应答报文经由所述 SSL 连接转发给用户 x。

15. 如权利要求 14 所述的网关，其特征在于，所述处理单元包括位于应用层的 SSL VPN 业务模块 1、位于 IP 层的 SSL VPN 业务模块 2 和 VPN 标签处理模块和 IP 模块，位于 TCP 层的 TCP 模块、以及位于 IP 层与网络接口之间的 MPLS 模块；

位于应用层的 SSL VPN 业务模块 1，用于从为用户 x 所属 VPN 设置的地址池中为用户 x 分配虚地址 Add_x；当用户 x 请求访问 VPN 资源服务器时，建立用户 x 与所在网关之间的 SSL 连接；

当报文通过所述 SSL 连接进入所在网关后，所述 IP 模块去掉报文的公网 IP 头，将保留私网 IP 头和数据部分的报文经由 TCP 模块发送到位于应用层的 SSL VPN 业务模块 1，SSL VPN 业务模块 1 把解析出来的报文直接发送给位于 IP 层的 SSL VPN 业务模块 2；

SSL VPN 业务模块 2 进一步确定以直接 IP 转发方式转发报文，将报文发送给 VPN 标签处理模块；

所述 VPN 标签处理模块根据所述对应关系存储单元保存的绑定关系，查找用户 x 的认证授权信息绑定的 VPN 实例，并在报文中记录相应 VPN 实例标签索引，然后将报文发送给所述 IP 模块；

所述 IP 模块通过路由查找确定由 MPLS 进行转发，并将报文发送给 MPLS 模块；

所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的

VPN 实例为报文添加 VPN 标签和 MPLS 转发标签并转发；

当应答报文通过第二网络接口进入所在网关后，所述 MPLS 模块进一步根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的应答报文及其所属 VPN 信息发送给所述 IP 模块；

所述 IP 模块进一步根据所述所属 VPN 信息从所述 VPN 实例存储单元中获取相应 VPN 实例，并根据应答报文的私网目的地址 Add_x 在获取的 VPN 实例中匹配上所述路由转发表项 2，获得下一跳为虚拟接口 V1；

位于 IP 层的 SSLVPN 业务模块 2 进一步确定通过虚拟接口 V1 将应答报文经由所述 SSL 连接发送给用户 x，并将应答报文发送给位于应用层的 SSL VPN 业务模块 1；SSL VPN 业务模块 1 将应答报文发送给位于 TCP 层的 TCP 模块；

所述 TCP 模块根据所述 SSL 连接的信息为应答报文添加公网 IP 头，由 IP 模块通过所述 SSL 连接将报文发送给用户 x。

16. 如权利要求 11 所述的网关，其特征在于，所述认证授权信息为用户组、和 / 或虚拟域、和 / 或角色。

17. 如权利要求 11 所述的网关，其特征在于，所述虚拟接口为 SSL VPN 以太网接口或环回接口。

18. 一种远程接入 MPLS VPN 的系统，其特征在于，该系统包括如权利要求 11 至 17 任意一项所述的网关。

远程接入 MPLS VPN 的方法、系统和网关

技术领域

[0001] 本发明涉及SSL VPN(Secure Socket Layer Virtual Private Network,安全套接层虚拟专用网络）技术和MPLS VPN(MPLS VPN,Multi-ProtocolLabel Switching Virtual Private Network,多协议标记交换虚拟专用网络）技术,具体涉及远程接入MPLS VPN的方法、系统和应用于该系统的网关。

背景技术

[0002] SSL VPN是一种采用SSL(Secure Socket Layer,安全套接层）加密连接实现远程访问的VPN(Virtual Private Network,虚拟专用网络）技术。图1A和图1B示出了SSL VPN的网络结构示意图。如图1A所示,远程主机与SSL VPN网关之间建立SSL连接,以加密方式在互联网上传送报文。SSLVPN网关终结了SSL连接,通过与内网的VPN资源服务器之间建立的TCP(Transmission Control Protocol,传输控制协议）连接或者通过直接IP转发,以明文方式传送远程主机发来的请求,并将服务器的应答通过SSL连接发给远程主机。

[0003] 用户远程接入的方式包括TCP接入方式、WEB(网页）接入方式和IP接入方式。TCP和WEB接入方式下的远程接入过程相同,而IP接入方式的远程接入过程略有不同。具体来说,在TCP/WEB(“/”表示“或”）接入方式下,远程访问过程包括以下步骤：

[0004] 步骤A、用户user1与SSL VPN网关之间进行信息交互,建立与远程接入相关的连接,具体包括：

[0005] a1、user1通过远程主机向SSL VPN网关请求登录认证;SSL VPN网关认证通过后,向用户user1返回用户资源页面,该用户资源页面包括用户user1允许访问的VPN资源信息；

[0006] a2、当user1请求访问VPN资源时,通过远程主机与SSL VPN网关建立SSL连接；在TCP/WEB接入方式下,网关需要维护双向连接对应关系表,即与用户主机之间的SSL连接和与VPN资源服务器之间的TCP连接,因此user1通过建立的SSL连接向SSL VPN网关发送用户ID(标识）和请求访问的VPN资源ID。用户ID用于识别用户,VPN资源ID用于指示被请求访问的资源。

[0007] a3、SSL VPN网关根据VPN资源ID,为user1建立SSL VPN网关与被请求访问的VPN资源所在VPN资源服务器1之间建立TCP连接并维护。其中,为user1建立的TCP连接的两端为:SSL VPN网关上物理出接口的私网地址172.1.1.1,以及VPN资源服务器1的私网地址10.3.1.1。

[0008] 步骤B、与远程接入相关的连接建立完成后,user1通过SSL连接向SSLVPN网关发送报文,SSL VPN网关将从SSL连接接收的报文通过为user1建立的TCP连接转发给VPN资源服务器1。

[0009] 由于在TCP/WEB接入方式下,user1不需要知道VPN资源服务器的地址,因此user1发给SSL VPN网关的报文仅携带公网IP头。user1发送的报文如图1A中的报文①,公网IP头中的公网源地址为user1使用的远程主机的公网地址60.191.123.24,公网目的

地址为 SSL VPN 网关的公网地址 220.189.204.90。

[0010] SSL VPN 网关的核心组成为 SSL VPN 业务单元，该单元分为 3 个模块，分别为 TCP 接入方式处理模块、WEB 接入方式处理模块和 IP 接入方式处理模块。其中 TCP 接入方式处理模块和 WEB 接入方式处理模块的报文转发流程类似，在此可以认为是一个模块，即 TCP/WEB 接入方式处理模块。该 TCP/WEB 接入方式处理模块工作在应用层，而 IP 接入方式处理模块同时工作在应用层和 IP 层。

[0011] 在 TCP/WEB 接入方式下，步骤 B 的转发过程具体包括子步骤 b1 ～ b3：

[0012] b1、报文通过 SSL 连接进入 SSL VPN 网关后，由 IP 层去掉公网 IP 头，将报文的数据部分经由 TCP 层上送到位于应用层的 TCP/WEB 接入方式处理模块；

[0013] b2、TCP/WEB 接入方式处理模块根据双向连接对应关系表确定将所接收的报文通过为 user1 建立的 TCP 连接转发，此时将报文发送给 TCP 层；

[0014] b3、TCP 层根据为 user1 建立的 TCP 连接 (172.1.1.1 至 10.3.1.1)，为报文添加私网 IP 头，其中私网 IP 头中的私网源地址和私网目的地址分别为 172.1.1.1 和 10.3.1.1，然后把报文传送给 IP 层。

[0015] b4、IP 层根据报文的目的地址进行路由查找，然后通过物理出接口 172.1.1.1 转发出去。转发出去的报文如图 1A 中的报文②，其中私网 IP 头中的私网源地址和私网目的地址分别为 172.1.1.1 和 10.3.1.1。

[0016] 步骤 C、SSL VPN 网关通过 TCP 连接接收 VPN 资源服务器 1 返回的应答报文，通过 SSL 连接返回给 user1。该步骤相当于步骤 B 的反向操作，先由 IP 层将应答报文的私网 IP 头去掉并经由 TCP 层上送到 TCP/WEB 接入方式处理模块，TCP/WEB 接入方式处理模块确定通过与 user1 之间的 SSL 连接返回应答报文，由 TCP 层为应答报文添加公网 IP 头，最后由 IP 层通过路由查找并转发出去。

[0017] 至此，完成了 TCP/WEB 接入方式下的远程接入。

[0018] 当用户 user1 在 IP 接入方式下进行远程接入时，需要创建为用户分配地址的地址池。接入过程仍包括上述步骤 A、B 和 C，但每个步骤的具体实现有所不同。具体来说，

[0019] 在步骤 A 中，SSL VPN 网关除了要返回用户资源页面，还需要从地址池中随机选择一个 IP 地址分配给用户 user1，作为用户 user1 访问 VPN 资源服务器的源地址也即虚地址。假设分配的虚地址为 10.1.1.2。当 user1 需要访问 VPN 资源时，仅建立 SSL 连接，不建立 TCP 连接，但 SSL VPN 网关需要维护用户、虚地址和 SSL 连接对应关系表，SSL VPN 网关不需要知道 user1 接下来要访问哪个 VPN 资源服务器。因此，user1 与 SSL VPN 网关交互信息时，只需通过建立的 SSL 连接向 SSL VPN 网关发送用户 ID 即可。

[0020] 在步骤 B 中，user1 仍通过 SSL 连接向 SSL VPN 网关发送报文，该报文中不仅包括前述的公网 IP 头，还包括私网 IP 头。user1 发送的报文如图 1B 的报文①，报文①的公网 IP 头与图 1A 相同，私网源地址为 user1 的虚地址 10.1.1.2，私网目的地址为被访问的 VPN 资源服务器的私网地址 10.3.1.1，该 VPN 资源服务器的私网地址是 user1 可以预先获知的。

[0021] 当 SSL VPN 网关接收到报文时，由 IP 层去掉公网 IP 头，并通过 TCP 层发送给 IP 接入方式处理模块，该处理模块确定直接根据私网 IP 头进行报文转发。去掉公网 IP 头的报文如图 1B 中的报文②。

[0022] 在步骤 C 中，SSL VPN 网关接收 VPN 资源服务器 1 返回的应答报文，由 IP 接入方

式处理模块根据用户、虚地址和 SSL 连接对应关系表确定通过与 user1 之间的 SSL 连接返回应答报文，然后由 TCP 层为报文添加公网 IP 头，由 IP 层查找路由并转发给 user1。

[0023] 至此，完成了 IP 接入方式下的远程接入。

[0024] MPLS L3VPN 是服务提供商 VPN 解决方案中一种基于 PE(ProviderEdge，提供商边缘）路由器的 L3（三层）VPN 技术，它使用 BGP(BorderGateway Protocol，边界网关协议）在 MPLS 交换网上发布 VPN 路由，使用标签转发在 MPLS 交换网上转发 MPLS 报文。图 2 为现有技术中 MPLSL3VPN 的组网结构示意图，如图 2 所示，MPLS L3VPN 模型由以下三部分组成：

[0025] CE(Customer Edge，用户网络边缘）设备，简称 CE，有接口直接与 P(Provider，服务提供商）路由器相连。CE 可以是路由器或交换机，也可以是一台主机。CE“感知”不到 VPN 的存在，也不需要必须支持 MPLS。

[0026] PE 路由器，简称 PE，是 MPLS 交换网的边缘设备，与 CE 直接相连。MPLS 网络中，所有 VPN 信息的处理都在 PE 上维护。PE 上存储有 VPN 路由转发实例 (VRF，VPN Routing & Forwarding Instance)，简称 VPN 实例。VPN 实例中包含路由转发表和 MPLS 标签转发表。其中，路由转发表包括两类路由，第一类路由为接收自 CE 设备的报文指示出接口，第二类路由为接收自 P 路由器的报文指示出接口。MPLS 标签转发表包括两类表项，第一类表项为各 VPN 的 VPN 标签（内层标签），第二类为转发表项，为接收自 CE 设备的报文指示下一跳 P 路由器信息和 MPLS 转发标签。

[0027] P 路由器，简称 P，是 MPLS 交换网的骨干路由器，不与 CE 直接相连，只需要具备基本 MPLS 转发能力，不用维护 VPN 信息。

[0028] 如图 2 所示，PE 路由器的不同物理接口连接不同 CE 设备，一个物理接口绑定一个 VPN，根据与 VPN 绑定的物理接口形成该 VPN 的 VPN 实例。当来自 CE 设备的报文从 PE 上的某一物理端口进入时，PE 路由器根据物理端口确定报文所属 VPN，采用报文所属 VPN 的 VPN 实例对报文进行转发处理。该转发处理操作包括：根据路由转发表查找报文的出接口，根据 MPLS 标签转发表查找报文的 VPN 标签（内层标签）、MPLS 转发标签（外层标签）以及下一跳 P 设备信息等等，根据查找到的信息为报文打上 VPN 标签和 MPLS 转发标签然后转发。当 PE 接收到来自 P 路由器的报文时，根据报文携带的 VPN 标签，查找相应 VPN 实例，通过与相应 VPN 实例绑定的物理接口将报文转发给 CE 设备。在现有技术中，PE 路由器还可以通过接入 VLAN（虚拟局域网）信息区分不同的 VPN 用户。

[0029] 当图 1A 和图 1B 中 SSL VPN 网关所连接的局域网采用 MPLS L3VPN 时，SSL VPN 网关如何与 MPLS L3VPN 中的设备连接，连接后如何将接收自 SSL 连接的报文转发到 MPLS 交换网中，使得远程用户能够通过 SSL 连接远程访问 MPLS VPN 中的 VPN 资源服务器，是亟待解决的问题，而且现有技术中还未提出相关的解决方案。

发明内容

[0030] 有鉴于此，本发明提供了一种远程接入 MPLS VPN 的方法，使得远程用户能够通过自身与 SSL VPN 网关之间的 SSL 连接，远程访问 MPLS VPN 中的 VPN 资源。

[0031] 远程用户通过自身与安全套接层虚拟专用网络 SSL VPN 网关之间的 SSL 连接访问 MPLS VPN 中的 VPN 资源服务器，所述 SSL VPN 网关同时作为 MPLS 交换网中的服务提供商边缘 PE 路由器。

[0032] 该方法包括：

[0033] A、在 SSL VPN 网关中创建多个虚拟接口，一个 VPN 绑定一个虚拟接口，根据 VPN 绑定的虚拟接口形成 VPN 实例；根据用户的认证授权信息区分不同 VPN 的用户，将用户的认证授权信息与相应 VPN 实例绑定；

[0034] B、用户 x 与 SSL VPN 网关之间进行信息交互，建立与远程接入相关的连接；

[0035] C、SSL VPN 网关接收用户 x 通过 SSL 连接发来的报文，根据用户 x 的认证授权信息绑定的 VPN 实例，为所接收报文添加 VPN 标签和 MPLS 转发标签，并通过 MPLS 交换网转发到 VPN 资源服务器；

[0036] D、SSL VPN 网关接收所述 VPN 资源服务器的返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例，根据查找到的 VPN 实例将应答报文通过所述 SSL 连接返回给用户 x。

[0037] 与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 1：目的地址为虚拟接口 V1 的 IP 地址，下一跳为内部环回接口地址；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；

[0038] 当采用传输控制协议 TCP 或网页 WEB 方式接入 VPN 资源服务器时：

[0039] 步骤 B 所述建立与远程接入相关的连接包括：当用户 x 请求访问 VPN 资源服务器 S1 时，建立用户 x 与 SSL VPN 网关之间的 SSL 连接；

[0040] 为用户 x 建立虚拟接口 V1 与 VPN 资源服务器 S1 之间的 TCP 连接；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；在建立所述 TCP 连接过程中，根据用户 x 的认证授权信息绑定的 VPN 实例，为所述 TCP 连接的套接字 SOCKET 设置 VPN 实例标签索引；

[0041] 所述步骤 C 包括：接收用户 x 通过 SSL 连接发来的报文，根据为用户 x 建立的 TCP 连接的信息，在 TCP 层为所接收报文添加 VPN 实例标签索引，再由 MPLS 模块根据 VPN 实例标签索引找到相应 VPN 实例，为报文添加 VPN 标签和 MPLS 转发标签，然后通过为用户 x 建立的 TCP 连接将报文转发给 VPN 资源服务器 S1；

[0042] 所述步骤 D 包括：接收通过所述 TCP 连接返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例；根据所述应答报文的私网目的地址在查找到的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，则直接将所接收的应答报文转发到上层应用，该上层应用通过所述 SSL 连接将应答报文发送给用户 x。

[0043] 所述步骤 C 包括：

[0044] c1、报文通过 SSL 连接进入 SSL VPN 网关后，由位于 IP 层的 IP 模块去掉报文的公网 IP 头，将报文的数据部分经由 TCP 模块上送到位于应用层的 SSL VPN 业务模块；

[0045] c2、所述 SSL VPN 业务模块确定将所接收的报文通过为用户 x 建立的 TCP 连接转发；

[0046] c3、位于 TCP 层的 TCP 模块根据为用户 x 建立的 TCP 连接，为报文添加私网 IP 头，并且根据 SOCKET 的 VPN 实例标签索引在报文中记录 VPN 实例标签索引；

[0047] c4、位于 IP 层的 IP 模块通过路由查找确定由 MPLS 转发，并将报文发送给位于网络接口和 IP 层之间的 MPLS 模块；

[0048] c5、所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的 VPN 实例为报文添加 VPN 标签和 MPLS 转发标签并转发。

[0049] 所述步骤 D 包括：

[0050] d1、应答报文通过所述 TCP 连接进入 SSL VPN 网关后，位于网络接口和 IP 层之间的 MPLS 模块根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的报文及其所属 VPN 信息发送给位于 IP 层的 IP 模块；

[0051] d2、所述 IP 模块根据所述所属 VPN 信息获取相应 VPN 实例，并根据所述应答报文的私网目的地址在获取的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，然后直接将去掉私网 IP 头的应答报文经由 TCP 层转发到位于应用层的 SSL VPN 业务模块；

[0052] d3、所述 SSL VPN 业务模块确定将接收自所述 TCP 连接的应答报文通过所述 SSL 连接发送给用户 x，并将应答报文发送给所述 TCP 模块；

[0053] d4、所述 TCP 模块根据所述 SSL 连接的信息为报文添加公网 IP 头，由 IP 模块将报文通过所述 SSL 连接发送给用户 x。

[0054] 与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 2：目的地址为虚拟接口 V1 所在网段，下一跳为虚拟接口 V1 的 IP 地址；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；

[0055] 当采用 IP 方式接入 VPN 资源服务器时：

[0056] 步骤 A 所述创建多个虚拟接口为：对应为每个 VPN 设置的地址池创建一个虚拟接口；对应的地址池和虚拟接口属于同一网段；

[0057] 所述步骤 B 包括：SSL VPN 网关从为用户 x 所属 VPN 设置的地址池中为用户 x 分配虚地址 Add_x；当用户 x 请求访问 VPN 资源服务器 S1 时，建立用户 x 与 SSL VPN 网关之间的 SSL 连接；

[0058] 所述步骤 C 包括：接收用户 x 通过 SSL 连接发来的携带私网 IP 头的报文，其私网源地址为 Add_x；根据用户 x 的认证授权信息绑定的 VPN 实例，在 IP 层为所接收报文添加 VPN 实例标签索引，再由 MPLS 模块根据 VPN 实例标签索引为报文添加 VPN 标签和 MPLS 转发标签，然后根据报文携带的私网 IP 头，通过直接 IP 转发方式将报文转发给 VPN 资源服务器 S1；

[0059] 所述步骤 D 包括：接收返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例；根据所述应答报文的私网目的地址 Add_x 在查找到的 VPN 实例中匹配到所述路由转发表项 2，获得下一跳为虚拟接口 V1，则通过所述虚拟接口 V1 将应答报文经由所述 SSL 连接转发给用户 x。

[0060] 所述步骤 C 包括：

[0061] c1、报文通过所述 SSL 连接进入 SSL VPN 网关后，由 IP 层的 IP 模块去掉报文的公网 IP 头，将保留私网 IP 头和数据部分的报文发送到位于应用层的 SSL VPN 业务模块 1，SSL VPN 业务模块 1 把报文发送给位于 IP 层的 SSL VPN 业务模块 2；

[0062] c2、所述 SSL VPN 业务模块 2 确定以直接 IP 转发方式转发报文，将报文发送给位于 IP 层的 VPN 标签处理模块；

[0063] c3、所述 VPN 标签处理模块根据用户 x 的认证授权信息绑定的 VPN 实例，在报文中记录 VPN 实例标签索引，然后将报文发给 IP 模块；

[0064] c4、所述 IP 模块通过路由查找确定由 MPLS 进行转发，并将报文发给位于网络接口

和 IP 层之间的 MPLS 模块；

[0065] c5、所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的 VPN 实例为报文添加 VPN 标签和 MPLS 转发标签并转发。

[0066] 所述步骤 D 包括：

[0067] d1、应答报文进入 SSL VPN 网关后，位于网络接口和 IP 层之间的 MPLS 模块根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的报文及其所属 VPN 信息发送给 IP 层的 IP 模块；

[0068] d2、所述 IP 模块根据所述所属 VPN 信息获取相应 VPN 实例，并根据应答报文的私网目的地址 Add_x 在获取的 VPN 实例中匹配到所述路由转发表项 2，获得下一跳为虚拟接口 V1；

[0069] d3、位于 IP 层的 SSL VPN 业务模块 2 确定通过虚拟接口 V1 将应答报文经由所述 SSL 连接发送给用户 x，并将应答报文发送给位于应用层的 SSLVPN 业务模块 1，SSL VPN 业务模块 1 将应答报文发送给位于 TCP 层的 TCP 模块；

[0070] d4、所述 TCP 模块根据所述 SSL 连接的信息为应答报文添加公网 IP 头，由 IP 模块通过所述 SSL 连接将报文发送给用户 x。

[0071] 较佳地，VPN 与虚拟接口绑定以及用户与 VPN 实例绑定后，进一步形成对应关系表，该对应关系表包括用户标识、用户的认证授权信息、虚拟接口和绑定的 VPN 实例的标签索引。

[0072] 所述认证授权信息为用户组、和 / 或虚拟域、和 / 或角色。

[0073] 所述虚拟接口为 SSL VPN 虚拟以太网接口或环回接口。

[0074] 本发明提供了一种网关，能够作为 SSL VPN 网关和 PE 路由器，使得远程用户能够通过自身与该网关之间的 SSL 连接，远程访问 MPLS VPN 中的 VPN 资源。

[0075] 所述网关同时作为 SSL VPN 中的 SSL VPN 网关和 MPLS VPN 中的 PE 路由器；

[0076] 所述网关包括配置单元、第一网络接口、第二网络接口、处理单元、VPN 实例存储单元和对应关系存储单元；

[0077] 所述配置单元，用于创建多个虚拟接口、一个 VPN 绑定一个虚拟接口，根据 VPN 绑定的虚拟接口形成 VPN 实例，将形成的 VPN 实例存储在 VPN 实例存储单元中；根据用户的认证授权信息区别不同 VPN 的用户，将用户与相应的认证授权信息与相应 VPN 实例绑定；将建立的各种绑定关系存储在对应关系存储单元中；

[0078] 所述对应关系存储单元，用于存储配置单元建立的绑定关系；

[0079] 所述 VPN 实例存储单元，用于存储 VPN 实例；

[0080] 第一网络接口，为所在网关和用户之间提供数据传输通道；

[0081] 第二网络接口，为所在网关和 MPLS 交换网提供数据传输通道；

[0082] 处理单元，用于与用户 x 进行信息交互，建立与远程接入相关的连接；当接收到用户 x 通过 SSL 连接发来的报文时，根据所述对应关系存储单元存储的绑定关系，从所述 VPN 实例存储单元获取用户 x 的认证授权信息绑定的 VPN 实例，采用获取的 VPN 实例为所接收报文添加 VPN 标签和 MPLS 转发标签，并通过 MPLS 交换网转发给 VPN 资源服务器；当接收到所述 VPN 资源服务器返回的应答报文时，根据该应答报文携带的 VPN 标签在所述 VPN 实例存储单元中查找相应 VPN 实例，根据查找到的 VPN 实例将应答报文通过所述 SSL 连接返回

给用户 x。

[0083] 其中，与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 1：目的地址为虚拟接口 V1 的 IP 地址，下一跳为内部环回接口地址；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；

[0084] 当采用 TCP 或 WEB 方式接入 VPN 资源服务器时，所述处理单元进一步用于：

[0085] 在建立与远程接入相关的连接时，建立用户 x 与所在网关之间的 SSL 连接，为用户 x 建立虚拟接口 V1 与被请求访问的 VPN 资源服务器 S1 之间的 TCP 连接；在建立所述 TCP 连接过程中，根据用户 x 的认证授权信息绑定的 VPN 实例，为所述 TCP 连接的 SOCKET 设置 VPN 实例标签索引；

[0086] 在接收到用户 x 通过所述 SSL 连接发来的报文时，根据为用户 x 建立的 TCP 连接的信息，在 TCP 层为所接收报文添加 VPN 实例标签索引，再由处理单元中的 MPLS 模块根据 VPN 实例标签索引找到相应 VPN 实例，为报文添加 VPN 标签和 MPLS 转发标签，然后通过为用户 x 建立的 TCP 连接将报文转发给 VPN 资源服务器 S1；

[0087] 在接收到通过所述 TCP 连接返回的应答报文时，根据应答报文携带的 VPN 标签查找相应 VPN 实例，根据所述应答报文的私网目的地址在查找到的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，则直接将所接收的应答报文转发到上层应用，该上层应用通过所述 SSL 连接将应答报文发送给用户 x。

[0088] 较佳地，所述处理单元包括位于应用层的 SSL VPN 业务模块和 VPN 标签处理模块、位于 TCP 层的 TCP 模块、位于 IP 层的 IP 模块，以及位于 IP 层与网络接口之间的 MPLS 模块；

[0089] 所述 SSL VPN 业务模块，用于当用户 x 请求访问 VPN 资源服务器 S 1 时，建立用户 x 与所在网关之间的 SSL 连接，为用户 x 建立虚拟接口 V1 与 VPN 资源服务器 S1 之间的 TCP 连接；

[0090] 所述 VPN 标签处理模块，用于在建立所述 TCP 连接过程中，根据用户 x 的认证授权信息绑定的 VPN 实例，为所述 TCP 连接的 SOCKET 设置 VPN 实例标签索引；

[0091] 当报文通过所述 SSL 连接进入所在网关后，所述 IP 模块去掉报文的公网 IP 头，将报文的数据部分经由 TCP 模块上送到 SSL VPN 业务模块；

[0092] 所述 SSL VPN 业务模块进一步确定将所接收的报文通过为用户 x 建立的 TCP 连接转发，并将报文发送给所述 TCP 模块；

[0093] 所述 TCP 模块根据为用户 x 建立的 TCP 连接，为报文添加私网 IP 头，并且根据 SOCKET 的 VPN 实例标签索引在报文中记录 VPN 实例标签索引，然后将报文发给所述 IP 模块；

[0094] 所述 IP 模块进一步通过路由查找确定由 MPLS 转发，并将报文发送给 MPLS 模块；

[0095] 所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，为报文添加 VPN 标签和 MPLS 转发标签并转发；

[0096] 当应答报文通过所述 TCP 连接进入所在网关后，所述 MPLS 模块进一步根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的报文及其所属 VPN 信息发送给所述 IP 模块；

[0097] 所述 IP 模块进一步根据所述所属 VPN 信息从所述 VPN 实例存储单元中获取相应

VPN 实例，并根据应答报文的私网目的地址在获取的 VPN 实例中匹配到所述路由转发表项 1，获得下一跳为内部环回接口地址，然后直接将去掉私网 IP 头的报文经由 TCP 模块转发到所述 SSL VPN 业务模块；

[0098] 所述 SSL VPN 业务模块进一步确定将接收自所述 TCP 连接的应答报文通过所述 SSL 连接发送给用户 x，并将应答报文发送给所述 TCP 模块；

[0099] 所述 TCP 模块进一步根据所述 SSL 连接的信息为应答报文添加公网 IP 头，由 IP 模块将报文通过所述 SSL 连接发送给用户 x。

[0100] 其中，与用户 x 的认证授权信息绑定的 VPN 实例包括路由转发表项 2：目的地址为虚拟接口 V1 所在网段，下一跳为虚拟接口 V1 的 IP 地址；所述虚拟接口 V1 为用户 x 所属 VPN 绑定的虚拟接口；

[0101] 当采用 IP 方式接入 VPN 资源服务器时，所述配置单元在创建虚拟接口时，对应为每个 VPN 设置的地址池创建一个虚拟接口，对应的地址池和虚拟接口属于同一网段；

[0102] 所述处理单元进一步用于：

[0103] 在建立与远程接入相关的连接时，从为用户 x 所属 VPN 设置的地址池中为用户 x 分配虚地址 Add_x；建立用户 x 与所在网关之间的 SSL 连接；

[0104] 在接收到用户 x 通过 SSL 连接发来的携带私网 IP 头的报文时，根据用户 x 的认证授权信息绑定的 VPN 实例，在 IP 层为所接收报文添加 VPN 实例标签索引，再由处理单元中的 MPLS 模块根据 VPN 实例标签索引为报文添加 VPN 标签和 MPLS 转发标签；所述私网 IP 头的源地址为 Add_x；

[0105] 在接收到应答报文时，根据该应答报文携带的 VPN 标签查找相应 VPN 实例；根据所述应答报文的私网目的地址 Add_x 在查找到的 VPN 实例中匹配到所述路由转发表项 2，获得下一跳为虚拟接口 V1，则通过所述虚拟接口 V1 将应答报文经由所述 SSL 连接转发给用户 x。

[0106] 较佳地，所述处理单元包括位于应用层的 SSL VPN 业务模块 1、位于 IP 层的 SSL VPN 业务模块 2 和 VPN 标签处理模块和 IP 模块，位于 TCP 层的 TCP 模块、以及位于 IP 层与网络接口之间的 MPLS 模块；

[0107] 位于应用层的 SSL VPN 业务模块 1，用于从为用户 x 所属 VPN 设置的地址池中为用户 x 分配虚地址 Add_x；当用户 x 请求访问 VPN 资源服务器时，建立用户 x 与所在网关之间的 SSL 连接；

[0108] 当报文通过所述 SSL 连接进入所在网关后，所述 IP 模块去掉报文的公网 IP 头，将保留私网 IP 头和数据部分的报文经由 TCP 模块发送到位于应用层的 SSL VPN 业务模块 1，SSL VPN 业务模块 1 把解析出来的报文直接发送给位于 IP 层的 SSL VPN 业务模块 2；

[0109] SSL VPN 业务模块 2 进一步确定以直接 IP 转发方式转发报文，将报文发送给 VPN 标签处理模块；

[0110] 所述 VPN 标签处理模块根据所述对应关系存储单元保存的绑定关系，查找用户 x 的认证授权信息绑定的 VPN 实例，并在报文中记录相应 VPN 实例标签索引，然后将报文发送给所述 IP 模块；

[0111] 所述 IP 模块通过路由查找确定由 MPLS 进行转发，并将报文发送给 MPLS 模块；

[0112] 所述 MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到

的 VPN 实例为报文添加 VPN 标签和 MPLS 转发标签并转发；

[0113] 当应答报文通过第二网络接口进入所在网关后，所述 MPLS 模块进一步根据应答报文携带的 VPN 标签确定报文所属 VPN，将去掉 VPN 标签的应答报文及其所属 VPN 信息发送给所述 IP 模块；

[0114] 所述 IP 模块进一步根据所述所属 VPN 信息从所述 VPN 实例存储单元中获取相应 VPN 实例，并根据应答报文的私网目的地址 Add_x 在获取的 VPN 实例中匹配上所述路由转发表项 2，获得下一跳为虚拟接口 V1；

[0115] 位于 IP 层的 SSL VPN 业务模块 2 进一步确定通过虚拟接口 V1 将应答报文经由所述 SSL 连接发送给用户 x，并将应答报文发送给位于应用层的 SSL VPN 业务模块 1；SSL VPN 业务模块 1 将应答报文发送给位于 TCP 层的 TCP 模块；

[0116] 所述 TCP 模块根据所述 SSL 连接的信息为应答报文添加公网 IP 头，由 IP 模块通过所述 SSL 连接将报文发送给用户 x。

[0117] 所述认证授权信息为用户组、和 / 或虚拟域、和 / 或角色。

[0118] 所述虚拟接口为 SSL VPN 以太网接口或环回接口。

[0119] 本发明还提供了一种远程接入 MPLS VPN 的系统，使得远程用户能够通过自身与 SSL VPN 网关之间的 SSL 连接，远程访问 MPLS VPN 中的 VPN 资源。该系统包括前述任意一种网关。

[0120] 根据以上技术方案可见，为了在只有一个物理接口的条件下实现 VPN 多实例即在同一台设备上区分不同的 VPN，本发明通过创建虚拟接口并绑定 VPN，使得每个 VPN 绑定一个虚拟接口，从而形成对应不同 VPN 的 VPN 实例，供转发报文时使用。

[0121] 而且，本发明采用用户的认证授权信息区分不同的 VPN 用户，从而在 SSL VPN 网关只为用户提供一个物理接口的限制下，实现了用户区分，进而采用相应的 VPN 实例进行报文转发，实现了远程用户访问 MPLS VPN 中 VPN 资源的方案。

附图说明

[0122] 图 1A 为现有技术中一种 SSL VPN 的网络结构示意图。

[0123] 图 1B 为现有技术中一种 SSL VPN 的网络结构示意图。

[0124] 图 2 为现有技术中 MPLS L3VPN 的组网结构示意图。

[0125] 图 3 为本发明实施例中 SSL VPN 网关同时作为 PE 路由器的组网示意图。

[0126] 图 4 为本发明实施例一中远程用户在 TCP/WEB 接入方式下通过 SSL 连接接入 MPLS VPN 的流程图。

[0127] 图 5 为本发明实施例二中远程用户在 IP 接入方式下通过 SSL 连接接入 MPLS VPN 的流程图。

[0128] 图 6 为本发明实施例中 SSL VPN 网关的结构示意图。

[0129] 图 7 为当采用 TCP/WEB 方式接入 VPN 资源服务器时，SSL VPN 网关的结构示意图。

[0130] 图 8 为当采用 IP 方式接入 VPN 资源服务器时，SSL VPN 网关的结构示意图。

具体实施方式

[0131] 本发明采用 SSL VPN 网关同时作为 MPLS L3VPN 中 PE 路由器，从而解决了 SSL VPN

网关与 MPLS L3VPN 的连接问题。下文的 MPLS VPN 均指 MPLS L3VPN。

[0132] 图 3 为本发明实施例中，SSL VPN 网关同时作为 PE 路由器的组网示意图。如图 3 所示，用户 1(user1) 属于 VPN1，用户 2(user2) 属于 VPN2，两个用户分别通过不同的远程主机访问 VPN 资源，CE1 和 CE2 为 VPN 资源服务器，VPN1 资源设置在 CE1 上，VPN2 资源设置在 CE2 上。远程主机与 SSL VPN 网关之间采用 SSL 连接传输数据，SSL VPN 网关同时作为 PE 路由器，与 MPLS 交换网中的 P 路由器相连。

[0133] SSL VPN 网关作为 PE 路由器与图 2 中的 PE 路由器有所不同，SSL VPN 网关对外只提供一个网络接口，即如图 3 所示 SSL VPN 网关对外，即对互联网和对 MPLS 交换网分别提供一个网络接口，因此 SSL VPN 网关无法像通常的 PE 路由器一样，将物理接口与 VPN 绑定，从而通过报文的入接口来区分不同的 VPN 用户，而且由于 SSL VPN 网关设置在互联网和局域网之间，接收自用户的报文已经经过互联网的传输，因此不携带接入 VLAN 信息，因此也不能通过报文携带的接入 VLAN 信息来区分不同的 VPN 用户。但是，SSL VPN 网关在用户登录认证时，维护了一些用户的认证授权信息，因此本发明实施例就利用用户的认证授权信息来区分不同的 VPN 用户。

[0134] 当然，SSL VPN 网关作为 PE 路由器还需要兼顾二者的功能，因此 SSLVPN 网关还需要承担 SSL 报文和 MPLS 报文相互转换任务，以及允许采用 SSL VPN 的三种接入方式之一或任意组合实现远程接入 MPLS VPN。

[0135] 为此，本发明提供了一种远程接入 MPLS VPN 的方法，该方法包括以下步骤：

[0136] A、在 SSL VPN 网关中创建多个虚拟接口，一个 VPN 绑定一个虚拟接口，根据 VPN 绑定的虚拟接口形成 VPN 实例，这里与虚拟接口绑定的 VPN 为 MPLS VPN，下面不再进行区分，统称为 VPN；根据用户的认证授权信息区分不同 VPN 的用户，从而将 SSL VPN 用户区分到不同的 MPLS VPN 中，然后将用户的认证授权信息与相应 VPN 绑定。

[0137] B、用户 x 与 SSL VPN 网关之间进行信息交互，建立与远程接入相关的连接。

[0138] C、SSL VPN 网关接收用户 x 通过 SSL 连接发来的报文，根据用户 x 的认证授权信息绑定的 VPN 实例，为所接收报文打上 VPN 标签和 MPLS 转发标签，并通过 MPLS 交换网转发到 VPN 资源服务器；

[0139] D、SSL VPN 网关接收 VPN 资源服务器返回的应答报文，根据该应答报文携带的 VPN 标签查找相应 VPN 实例，根据查找到的 VPN 实例将报文通过 SSL 连接返回给用户 x。

[0140] 由以上所述可见，本发明通过创建虚拟接口并绑定 VPN，使得每个 VPN 绑定一个虚拟接口，从而形成对应不同 VPN 的 VPN 实例，供转发报文时使用。鉴于 SSL VPN 网关只对用户提供一个物理接口，因此本发明结合 SSL

[0141] VPN 网关的特点，通过用户的认证授权信息区分不同的 VPN 用户，从而在 SSL VPN 网关只为用户提供一个物理接口的限制下，实现了用户区分，进而采用相应的 VPN 实例进行报文转发，实现了远程用户访问 MPLS VPN 中 VPN 资源的方案。

[0142] 下面结合附图并举实施例，对本发明进行详细描述。在以下实施例中，采用认证授权信息中的用户所属用户组区分不同的 VPN 用户，在实际网络中，还有不属于任何 VPN 的用户，称为公网用户，采用诸如用户组的认证授权信息也可以区分出这类用户。在其他实施例中，还可以采用认证授权信息中的用户组、虚拟域、角色这些参数之一或任意组合来区分不同的 VPN 用户。

[0143] 在本实施例中，首先，需要进行 MPLS VPN 和 SSLVPN 的相关配置。其中，MPLS VPN 的相关配置与常规的 MPLS VPN 配置相同，这里不赘述。SSL VPN 的相关配置具体包括以下步骤：

[0144] 1、在 SSL VPN 网关中创建多个地址池，每个地址池对应一个 VPN；地址池仅在 IP 接入方式下使用。

[0145] 2、对应每一个地址池创建一个虚拟接口，对应的地址池和虚拟接口属于同一网段，为每个虚拟接口绑定一个 VPN。其中，虚拟接口可以为 SSL VPN 虚拟以太网 (SVE，SSL VPN Virtual Ethernet) 接口，简称虚接口，也可以为环回 (Loopback) 接口。本实施例中，以 SVE 接口为例。

[0146] 3、根据与 VPN 绑定的虚接口，形成对应各 VPN 的 VPN 实例。每个 VPN 实例包括路由转发表和 MPLS 标签转发表。

[0147] 所述路由转发表包括两类路由，第一类路由是为接收自 VPN 资源服务器的报文指示出接口，第二类路由是为接收自用户的报文指示出接口。其中，第一类路由包括两条路由，一条路由在 TCP/WEB 接入方式下使用，另一条路由在 IP 接入方式下使用，下文会详细说明使用方法。

[0148] 所述 MPLS 标签转发表包括两类表项，第一类表项是 VPN 与 VPN 标签（内层标签）的映射关系，第二类表项为接收自用户的报文指示下一跳 P 路由器信息和 MPLS 转发标签。

[0149] 4、将虚接口授权给用户。在本发明实施例中，授权操作即为将虚接口和用户组绑定。由于在步骤 2 中虚接口与 VPN 绑定，因此经本步骤 4 后，用户组、虚接口和 VPN 实例三者形成了绑定关系。至于将哪个虚接口与哪个用户组绑定，还需要根据用户组允许访问的 VPN 资源确定，例如用户组 1 允许访问 VPN1 中的资源，则将 VPN1 对应的虚接口与用户组 1 绑定，本领域技术人员很容易理解该绑定关系的形成。

[0150] 经过以上几个步骤的配置在 SSL VPN 网关上形成如下表 1 示出的用户与 VPN 的对应关系表 (UVR，User to VPN relation table)，该 UVR 中记录了哪个用户对应哪个 VPN 以及与 VPN 绑定的虚接口。

[0151]

用户	所属用户组	虚接口	绑定的 VPN 实例 (VPN 实例标签索引)
user1	Vpn1group	SVE1/0	VPN1(VPN1 标签索引 :1)
user2	Vpn2group	SVE1/1	VPN2(VPN2 标签索引 :2)
user3	Pubgroup	无	PUBLIC(0)

[0152] 表 1

[0153] 如表 1 所示，UVR 表中包括如下字段：用户 ID、所属用户组、虚接口、绑定的 VPN 实例，表 1 中绑定的 VPN 实例字段中进一步包括 VPN 标签的索引。表 1 是根据图 3 中的组网结构形成的 UVR 表。其中，user1 属于用户组 Vpn1group，为该用户组 Vpn1group 绑定了虚接口 SVE1/0，与 SVE1/0 绑定的 VPN 实例为 VPN1 实例，VPN1 实例的标签索引为 1。uSer2 与 uSer1 类似。user3 为普通用户，不属于任何 VPN，因此如 UVR 表所示，user3 属于公网用户组 Pubgroup，没有为该公网用户组 Pubgroup 绑定任何虚接口和 VPN 实例，绑定的 VPN 实例

字段例如记为 PUBLIC(0)。

[0154] 经过以上几个步骤的配置，还在 SSL VPN 网关上形成对应不同 VPN 的 VPN 实例。下面列举对应 VPN1 和 VPN2 的 VPN 实例。以下描述的 VPN 实例仅将与本发明实施例密切相关的字段列出，省略了不相关的字段。

[0155] 首先，为 VPN 的路由转发表：

[0156]

vpn1 Route Information（路由信息）

Routing Table(路由表):vpn1 Route-Distinguisher(路由区分符):100:1

Destination/Mask(目的地址/掩码)	Nexthop(下一跳)	Interface(接口)
10.1.1.0/24	10.1.1.1	SVE1/0
10.1.1.1/32	127.0.0.1	InLoopBack0

VPN Routing Table（VPN 路由表）： Route-Distinguisher: 100:3

10.3.1.0/24	3.3.3.9	InLoopBack0

vpn2 Route Information

Routing Table: vpn2 Route-Distinguisher: 100:2

Destination/Mask	Nexthop	Interface
10.2.1.0/24	10.2.1.1	SVE1/1
10.2.1.1/32	127.0.0.1	InLoopBack0

VPN Routing Table: Route-Distinguisher: 100:4

10.4.1.0/24	3.3.3.9	InLoopBack0

[0157] 其中，在 VPN1 的路由转发表中，Routing Table（路由表）的内容为第一类路由，该第一类路由包括两条路由：

[0158] 第一条路由的目的地址为与 VPN1 绑定的虚接口 SVE1/0 以及相应地址池所在网段 10.1.1.0/24，下一跳为虚接口 SVE1/0 的 IP 地址 10.1.1.1。

[0159] 该条路由适用于 IP 接入方式，当来自 VPN 资源服务器的报文匹配 10.1.1.0/24 时，确定下一跳为 10.1.1.1 即虚接口 SVE1/0，则报文直接从虚接口 SVE1/0 转发出去。下面会详细说明 IP 接入方式下如何使用这条路由。

[0160] 第二条路由的目的地址为与 VPN1 绑定的虚接口 SVE1/0 的 IP 地址 10.1.1.1/32，下一跳指向内部环回（InLoopBack0）接口地址 127.0.0.1。

[0161] 该条路由适用于 TCP/WEB 接入方式，当来自 VPN 资源服务器的报文匹配 SVE1/0 的 IP 地址 10.1.1.1/32 时，确定下一跳为 127.0.0.1，即报文是发往本机的报文，此时 IP 层将报文直接经由 TCP 层上送到应用层的 SSL VPN 业务模块进行相应处理并转发。下面会详细

说明 TCP/WEB 接入方式下如何使用这条路由。

[0162] 在VPN1的路由转发表中，VPN Routing Table(VPN路由表)的内容为第二类路由。该第二类路由包括这样一条路由：其目的地址为 VPN 资源服务器所在网段 10.3.1.0/24，下一跳为 SSL VPN 网关通过 BGP 连接的对端 PE 设备地址，3.3.3.9 为对端 PE 设备的一个 loopback 接口地址。该条路由适用于任何接入方式，当来自用户的报文匹配 10.3.1.0/24 时，确定下一跳为 3.3.3.9。

[0163] VPN2 的 VPN 路由转发表设置与 VPN1 类似，这里不详细解释。

[0164] 其次，为 VPN 的 MPLS 标签转发表：

[0165]

Vpn-instance Name(VPN 实例名): vpn1 Route Distinguisher: 100:1

NO	FEC(转发等价类)	NEXTHOP	OUTER-LABEL(外层标签)
1	10.3.1.0/24	172.1.1.2	1026(vpn)

Vpn-instance Name: vpn2 Route Distinguisher: 100:2

NO	FEC	NEXTHOP	OUTER-LABEL
1	10.4.1.0/24	172.1.1.2	1026(vpn)

NO	VRFNAME(VRF 名)	INNER-LABEL(内层标签)
1	vpn1	1024
2	vpn2	1025

[0166] 其中，在 VPN1 的 MPLS 标签转发表中，VRFNAME(VRF 名) 和 INNER-LABEL(内层标签)的内容记载了各 VPN 的 VPN 标签；

[0167] Vpn-instance Name(VPN 实例名)的内容为转发表项，该转发表项的转发等价类 FEC 为 VPN 资源服务器所在网段 10.3.1.0/24，下一跳为从 SSL VPN 网关到 VPN 资源服务器经过的第一个 P 路由器的 IP 地址 172.1.1.2。该转发表项适用于任何接入方式，当来自用户的报文匹配 10.3.1.0/24 时，确定下一跳为 172.1.1.2，从而将报文转发到正确的 P 路由器。

[0168] 下面结合上述 UVR 和 VPN 实例，对 TCP/WEB 接入方式的远程接入过程以及 IP 接入方式的远程接入过程分别举实施例进行描述。

[0169] 实施例一：

[0170] 本实施例是远程用户 user1 在 TCP/WEB 接入方式下通过 SSL 连接接入 MPLS VPN 的实施例。该实施例中，假设 user1 所使用的远程主机的公网 IP 地址为 60.191.123.8，SSL VPN 网关的公网 IP 地址为 220.189.204.90，SSLVPN 网关中与 VPN1 绑定的虚接口 SVE1/0 的私网 IP 地址为 10.1.1.1，user1 允许访问的 VPN 资源所在网段为 10.3.1.0/24。为了描述

简便，下面将 user1 所使用的远程主机地址称为用户的地址，用户通过远程主机进行的操作均视为用户的操作。

[0171] 图 4 为本发明实施例一中远程用户在 TCP/WEB 接入方式下通过 SSL 连接接入 MPLS VPN 的流程图。如图 4 所示，该流程包括以下步骤：

[0172] 步骤 401：user1 向 SSL VPN 网关发送登录认证请求。

[0173] 步骤 402：SSL VPN 网关接收 user1 的登录认证请求，为 user1 进行登录认证处理，认证通过后，根据 user1 所属用户组确定 user1 所属 VPN，然后返回用户资源页面。该用户资源页面中携带 user1 允许访问的 VPN 资源信息。

[0174] 本实施例中，user1 属于用户组 Vpn1group，因此 user1 属于 VPN1。

[0175] 本步骤确定用户所属用户组和所属 VPN 的操作可以采用现有 SSL VPN 技术中的常规方式实现，也可以根据本发明设置的 UVR 表确定。

[0176] 步骤 403：当 user1 请求访问 VPN 资源服务器时，user1 与 SSL VPN 网关之间建立 SSL 连接，通过建立的 SSL 连接向 SSL VPN 网关发送用户 ID 和被请求访问的 VPN 资源 ID。

[0177] 步骤 404：SSL VPN 网关根据 user1 发来的 VPN 资源 ID，确定被请求访问的 VPN 资源所在 VPN 资源服务器的 IP 地址，这里假设为 10.3.1.1，同时在 UVR 表中查找与 user1 的用户组 Vpn1group 绑定的虚接口 SVE1/0，为 user1 建立虚接口 SVE1/0(10.1.1.1) 与被请求访问的 VPN 资源服务器 (10.3.1.1) 之间的 TCP 连接并维护双向连接对应关系表简称 ST 表。在 TCP 连接建立过程中，为 TCP 连接的 Socket 设置相应 VPN 实例标签索引。

[0178] 具体来说，SSL VPN 网关在确定被请求访问的 VPN 资源所在 VPN 资源服务器的 IP 地址后，在 UVR 表中查找 user1 所属 VPN 实例，这里为 VPN1，并为 socket 打上 VPN1 实例标签索引 1，然后向 10.3.1.1 发起 TCP 连接。TCP 层的 TCP 模块会根据 socket 的 VPN 实例标签索引给 TCP 连接请求报文打上 VPN 实例标签索引 1。其中，为报文打上 VPN 实例标签索引的操作并非在 IP 报文前面加上 VPN 实例标签索引而只是在报文属性中记录一下，在 MPLS 模块中才会真正在 IP 报文前面加上两层标签。

[0179] 然后，IP 模块根据报文的 VPN 实例标签索引 1 找到对应的 VPN1 实例，在查找到的 VPN1 实例中根据目的地址 10.3.1.1 查找转发路径，确定该报文由 MPLS 进行转发，将报文发给 MPLS 模块。MPLS 模块会根据报文的 VPN 实例标签索引 1 查找到 VPN1 的 VPN 标签 1024，以及根据 VPN 实例标签索引 1 和报文的目的地址 10.3.1.1，在 VPN1 实例的 MPLS 标签转发表中进行匹配，匹配上 VPN1 实例中 FEC 为 10.3.1.0/24 的 MPLS 标签转发表项，从而获得下一跳以及 MPLS 转发标签 1026；此时，MPLS 模块为 TCP 连接请求报文打上 VPN 标签 1024 及 MPLS 转发标签 1026 并根据下一跳将报文转发到对端资源服务器。由于该 VPN 实例绑定的接口为 SVE1/0，所以新建立的 TCP 连接的源地址为 SVE1/0 的 IP 地址，目的地址为 10.3.1.1。后续 user1 发来的报文将通过该 TCP 连接发送。

[0180] 步骤 405：user1 通过 SSL 连接向 SSL VPN 网关发送用户资源请求报文。该用户资源请求报文如图 4 中的报文①所示，报文①包括公网 IP 头、TCP 头和数据部分。为了突出报文在互联网和 MPLS 交换网中的变化，省略了 TCP 头的描述，但不影响转发流程的说明。

[0181] 其中，公网 IP 头的源地址和目的地址分别为 user1 的公网 IP 地址 60.191.123.8，和 SSL VPN 网关的公网 IP 地址 220.189.204.90。

[0182] 步骤 406：SSL VPN 网关接收到 user1 通过 SSL 连接发来的用户资源请求报文时，

根据 ST 表确定直接通过为 user1 建立的 TCP 连接进行转发。此时，TCP 层根据为 user1 建立的 TCP 连接的信息，为报文打上 VPN 实例标签索引，然后 MPLS 模块会根据报文的 VPN 实例标签索引打上 VPN 标签 1024 及转发所需要的 MPLS 转发标签 1026，并转发。

[0183] 本步骤具体由 SSL VPN 网关中的多个模块配合完成，这些模块包括位于应用层的 TCP/WEB 接入方式处理模块和 VPN 标签处理模块、位于 TCP 层的 TCP 模块、位于 IP 层的 IP 模块，以及位于 IP 层与网络接口之间的 MPLS 模块。其中 TCP/WEB 接入方式处理模块在建立与远程接入相关的连接时，建立并维护 ST 表。具体来说，本步骤 406 包括以下子步骤：

[0184] c1、报文通过自身与 user1 之间的 SSL 连接进入 SSL VPN 网关后，由 IP 模块去掉报文的公网 IP 头，将报文的数据部分经由 TCP 模块上送到 TCP/WEB 接入方式处理模块；

[0185] c2、TCP/WEB 接入方式处理模块根据 ST 表确定将所接收的报文通过为 user1 建立的 TCP 连接转发，将报文发送给 TCP 模块；

[0186] c3、TCP 模块根据建立的 TCP 连接信息为报文打上私网 IP 头，并且根据 socket 的 VPN 实例标签索引为报文打上 VPN 实例标签索引，然后将报文发给 IP 模块。其中，私网 IP 头的私网源地址和私网目的地址分别是 TCP 连接两端的地址，即私网源地址为虚接口 SVE1/0 的 IP 地址 10.1.1.1，私网目的地址为 user1 请求访问的 VPN 资源服务器的 IP 地址 10.3.1.1；

[0187] c4、IP 模块根据报文的 VPN 实例标签索引找到对应的 VPN 实例，在查找到的 VPN 实例中查找转发路径，确定该报文由 MPLS 进行转发，然后将报文发给 MPLS 模块；

[0188] c5、MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的 VPN 实例为报文打上 VPN 标签和 MPLS 转发标签，并转发。具体来说，MPLS 模块根据报文携带的 VPN 实例标签索引 1 得知报文属于 VPN1，从 VPN1 实例中获得 VPN 标签 1024，根据报文的私网目的地址在 MPLS 标签转发表中进行匹配，私网目的地址为 10.3.1.1 匹配上 FEC 为 10.3.1.0/24 的转发表项，获得下一跳 172.1.1.2 和 MPLS 转发标签 1026，进而给报文打上 VPN 标签 1024 和 MPLS 转发标签 1026，并根据下一跳 172.1.1.2 将报文转发到正确的 P 路由设备。

[0189] 经过本步骤 406 的处理，图 4 中的报文①转换成了报文②，报文②包括 MPLS 转发标签、VPN 标签、私网 IP 头和数据部分。其中，VPN 标签为内层标签用于区分报文所属 VPN，MPLS 转发标签为外层标签用于 MPLS 交换网的转发。

[0190] 步骤 407：MPLS 交换网通过报文携带的 MPLS 转发标签转发报文到对端的 PE 路由器。

[0191] 步骤 408：对端的 PE 路由器将报文转发给 VPN 资源服务器，并将 VPN 资源服务器的应答报文返回到 MPLS 交换网。

[0192] 步骤 409：与 SSL VPN 网关邻接的 P 路由器去掉应答报文的 MPLS 转发标签，然后把应答报文发送给 SSL VPN 网关。转发到 SSL VPN 网关的应答报文如图 4 示出的报文③。报文③包括 VPN 标签、私网 IP 头和数据部分。其中，私网 IP 头中的私网源地址为 10.3.1.1，私网目的地址为 10.1.1.1，VPN 标签为 1024。

[0193] 步骤 410：SSL VPN 网关根据应答报文携带的 VPN 标签查找相应的 VPN 实例，根据应答报文的私网目的地址在查找到的 VPN 实例中进行匹配，匹配上前述 VPN1 实例中的第二条路由转发表项，获得下一跳为内部环回接口地址 127.0.0.1，则直接将所接收应答报文转

发到上层应用，即应用层的 TCP/WEB 接入方式处理模块。TCP/WEB 接入方式处理模块处理完毕后，通过与 user1 之间的 SSL 连接将应答报文转发给 user1。

[0194] 具体来说，本步骤 410 包括以下子步骤：

[0195] d1、应答报文通过为 user1 建立的 TCP 连接进入 SSL VPN 网关后，MPLS 模块根据应答报文携带的 VPN 标签 1024 确定应答报文属于 VPN1，然后将去掉 VPN 标签的应答报文及其属于 VPN1 的信息发送给 IP 模块；

[0196] d2、IP 模块根据应答报文属于 VPN1 的信息获取 VPN1 实例，并根据报文的私网目的地址 10.1.1.1 在 VPN1 实例中进行路由匹配，VPN1 实例的具体内容已经在前文具体描述，这里匹配上 VPN1 实例中目的地址为 10.1.1.1/32 的路由转发表项，从匹配的路由转发表项中获取下一跳信息为内部环回接口地址 127.0.0.1，然后直接将去掉私网 IP 头的应答报文经由 TCP 模块转发到应用层的 TCP/WEB 接入方式处理模块；

[0197] d3、TCP/WEB 接入方式处理模块根据 ST 表确定将接收自 TCP 连接的应答报文通过 SSL 连接发送给 user1，此时将应答报文发送给 TCP 模块；

[0198] d4、TCP 模块根据所述 SSL 连接的信息为报文添加公网 IP 头，并转发给 IP 模块；

[0199] d5、IP 模块根据目的地址查找公网路由，从而通过 SSL 连接将报文发送给 user1。发送给 user1 的应答报文如图 4 中的报文④，报文④包括公网 IP 头和数据部分。

[0200] 至此，本流程结束。

[0201] 实施例二：

[0202] 本实施例是远程用户 user1 在 IP 接入方式下通过 SSL 连接接入 MPLSVPN 的实施例。该实施例中，假设 user1 所使用的远程主机的公网 IP 地址为 60.191.123.8，SSL VPN 网关的公网 IP 地址为 220.189.204.90，SSL VPN 网关中与 VPN1 绑定的虚接口 SVE1/0 的私网 IP 地址为 10.1.1.1，user1 允许访问的 VPN 资源所在网段为 10.3.1.0/24。

[0203] 图 5 为本发明实施例二中远程用户在 IP 接入方式下通过 SSL 连接接入 MPLS VPN 的流程图。如图 5 所示，该流程包括以下步骤：

[0204] 步骤 501：user1 向 SSL VPN 网关发送登录认证请求。

[0205] 步骤 502：SSL VPN 网关接收 user1 的登录认证请求，为 user1 进行登录认证处理，认证通过后，根据 user1 所属用户组 Vpn1group 确定 user1 属于 VPN1，然后返回用户资源页面。并且从为 user1 所属 VPN 设置的地址池中为 user1 随机分配而一个 IP 地址，作为 user1 的虚地址。本实施例假设分配给 user1 的虚地址为 10.1.1.2。

[0206] 步骤 503：当 user1 请求访问 VPN 资源服务器时，user1 与 SSL VPN 网关之间建立 SSL 连接，在 IP 接入方式下，SSL VPN 网关需要维护用户、虚地址和 SSL 连接对应关系表简称 UVS(User-Virtual IP-SSL，用户 - 虚 IP 地址 -SSL) 表。由于 IP 接入方式下，网关不需要与 VPN 资源服务器维持连接，因此 user1 仅需要通过建立的 SSL 连接向 SSL VPN 网关发送用户 ID。

[0207] 步骤 504：user1 通过 SSL 连接向 SSL VPN 网关发送用户资源请求报文。该用户资源请求报文如图 5 中的报文①所示，与实施例一不同之处在于，该报文①不仅包括公网 IP 头和数据部分，还包括私网 IP 头 (TCP 头仍省略)。

[0208] 其中，公网 IP 头的源地址和目的地址分别为 user1 的公网 IP 地址 60.191.123.8，和 SSL VPN 网关的公网 IP 地址 220.189.204.90。私网 IP 头的源地址和目的地址分别为

user1 的虚地址 10.1.1.2，和被请求访问的 VPN 资源服务器的私网 IP 地址 10.3.1.1。

[0209] 步骤 505 ：SSL VPN 网关接收到 user1 的用户资源请求报文时，通过 UVS 表可以确定报文来自用户 user1，进而通过查找 UVR 表确定 user1 所属 VPN，根据 user1 所属 VPN 的 VPN 实例，在 IP 层为所接收报文打上 VPN 实例标签索引，再由 MPLS 模块根据 VPN 实例标签索引为报文添加 VPN 标签和 MPLS 转发标签并转发。这里的转发是 MPLS 转发并发普通 IP 转发。

[0210] 本步骤具体由 SSL VPN 网关中的多个模块配合完成，这些模块包括位于应用层的 IP 接入方式处理模块 1、位于 IP 层的 IP 接入方式处理模块 2、VPN 标签处理模块和 IP 模块、位于 TCP 层的 TCP 模块、以及位于 IP 层与网络接口之间的 MPLS 模块。其中，位于应用层的 IP 接入方式处理模块 1 用于维护 SSL 连接以及 UVS 表，位于 IP 层的接入方式处理模块 2 用于处理转发，IP 接入方式处理模块 1 和 2 实际上是一个模块同时工作在应用层和 IP 层，为了理解方便将其分成了两个模块，这两个模块共享数据，数据到达 IP 接入方式处理模块 1 也就到了 IP 接入方式处理模块 2，反之依然。具体来说，本步骤 505 包括以下子步骤 ：

[0211] c1、报文通过自身与 user1 之间的 SSL 连接进入 SSL VPN 网关后，由 IP 模块去掉公网 IP 头，将保留私网 IP 头和数据部分的报文经由 TCP 模块发送给 IP 接入方式处理模块 1，IP 接入方式处理模块 1 把报文发送给 IP 接入方式处理模块 2 ；

[0212] c2、IP 接入方式处理模块 2 查找 UVS 表可以确定报文来自用户 user1，进而确定以直接 IP 转发方式转发报文，此时将报文发送给位于 IP 层的 VPN 标签处理模块 ；

[0213] c3、VPN 标签处理模块查找 UVR 表确定 user1 的 Vpn1group 绑定 VPN1 实例，并得到 VPN1 实例的 VPN 实例标签索引为 1，此时为解析出来的 IP 报文打上 VPN 实例标签索引 1，然后将报文转发给 IP 模块 ；

[0214] c4、IP 模块根据报文的目的地址进行路由查找，确定由 MPLS 进行转发，然后将报文发给 MPLS 模块 ；

[0215] c5、MPLS 模块根据报文携带的 VPN 实例标签索引查找相应 VPN 实例，根据查找到的 VPN 实例为报文打上 VPN 标签和 MPLS 转发标签并转发。该步骤与实施例一中的步骤 c5 相同。

[0216] 经过本步骤 505 的处理，图 5 中的报文①转换成了报文②，报文②包括 MPLS 转发标签、VPN 标签、私网 IP 头和数据部分。与实施例一不同的是，本实施例报文②中，私网源地址为 user1 的虚地址 10.1.1.2。

[0217] 步骤 506 ：MPLS 交换网通过报文携带的 MPLS 转发标签转发报文到对端的 PE 路由器。

[0218] 步骤 507 ：对端的 PE 路由器将报文转发给 VPN 资源服务器，并将 VPN 资源服务器的应答报文返回到 MPLS 交换网。

[0219] 步骤 508 ：与 SSL VPN 网关邻接的 P 路由器去掉应答报文的 MPLS 转发标签，然后把应答报文发送给 SSL VPN 网关。转发到 SSL VPN 网关的应答报文如图 5 示出的报文③。报文③包括 VPN 标签、私网 IP 头和数据部分。其中，私网 IP 头中的私网源地址为 10.3.1.1，私网目的地址为 10.1.1.2，VPN 标签为 1024。

[0220] 步骤 509 ：SSL VPN 网关根据应答报文的 VPN 标签找到相应的 VPN 实例，根据应答报文的私网目的地址 10.1.1.2 在查找到的 VPN 实例中进行匹配，匹配上前述 VPN1 实例中

的第一条路由转发表项，获得下一跳为虚接口 SVE1/0，则直接通过 SVE1/0 将应答报文经由 SSL 连接转发给 user1。

[0221] 具体来说，本步骤 509 包括以下子步骤：

[0222] d1、应答报文进入 SSL VPN 网关后，MPLS 模块根据应答报文携带的 VPN 标签确定应答报文属于 VPN1，然后将去掉 VPN 标签的应答报文及其属于 VPN1 的信息发送给 IP 模块；

[0223] d2、IP 模块根据应答报文属于 VPN1 的信息获取 VPN1 实例，并根据应答报文的私网目的地址 10.1.1.2 在 VPN1 实例中进行路由匹配，匹配上 VPN1 实例中目的地址为 10.1.1.0/24 的路由转发表项，从匹配的路由转发表项中获取下一跳信息为虚接口 SVE1/0 的 IP 地址 10.1.1.1，由于其目的地址并非本机内部接口地址，所以虚接口在收到报文会直接转发。

[0224] d3、虚接口的转发功能是由位于 IP 层的 IP 接入方式处理模块 2 来实现。IP 接入方式处理模块 2 根据应答报文中的私网目的地址即虚地址 10.1.1.2 以及 UVS 表确定将应答报文经由相应 SSL 连接发送给 user1(10.1.1.2)，此时将应答报文发送给位于应用层的 IP 接入方式处理模块 1，由 IP 接入方式处理模块 1 将报文发送给 TCP 模块。

[0225] d4、TCP 模块根据 SSL 连接的信息为应答报文添加公网 IP 头，并把报文转发给 IP 模块。

[0226] d5、IP 模块通过查找公网路由，从而将报文通过 SSL 连接发送给 user1。发送给 user1 的应答报文如图 5 中的报文④，报文④包括公网 IP 头、私网 IP 头和数据部分。

[0227] 至此，本流程结束。

[0228] 以上实施例一是支持 TCP 和 / 或 WEB 接入方式的方案，实施例二是支持 IP 接入方式的方案。在实际中，TCP、WEB 和 IP 三种接入方式可以并存，或者仅同时支持其中两种。

[0229] 对于公网用户 user3 的处理与现有 SSL VPN 网关的处理相同。具体包括：当 SSL VPN 网关接收到公网用户 user3 的用户资源请求报文时，查找 UVR 表确定 user3 属于用户组 Pubgroup，且没有绑定任何 VPN，此时确定接收到公共用户的报文，不进行打标签处理，直接通过公共路由也称全局路由向 VPN 资源服务器转发报文。同理，当 SSL VPN 网关接收到来自 VPN 资源服务器的报文且未携带 VPN 标签时，会通过全局路由送到上层经由 SSL 连接发送或者直接由虚接口经由 SSL 连接发送。

[0230] 为了实现上述方法，本发明提供了一种网关，该网关应用于这样一种系统，即远程用户通过自身与该网关之间的 SSL 连接，访问 MPLS VPN 中 VPN 资源服务器的系统，该网关同时作为 SSL VPN 中的 SSL VPN 网关和 MPLSVPN 中的 PE 路由器。本实施例中将该网关称为 SSL VPN 网关。

[0231] 图 6 为本发明实施例中 SSL VPN 网关的结构示意图。如图 6 所示，该 SSL VPN 网关包括配置单元（又称 WMI 单元）、第一网络接口、第二网络接口、处理单元、VPN 实例存储单元（又称 VRF 单元）和对应关系存储单元（又称 UVR 单元）。

[0232] WMI 单元，用于创建多个虚接口、一个 VPN 绑定一个虚接口，根据与 VPN 绑定的虚接口形成 VPN 实例，将形成的 VPN 实例存储在 VRF 单元中；根据用户的认证授权信息区别不同 VPN 的用户，将用户的认证授权信息与相应 VPN 实例绑定；将建立的各种绑定关系存储在 UVR 单元中。在创建虚接口时，WMI 单元对应为每个 VPN 设置的地址池创建一个虚接口，对应的地址池和虚接口属于同一网段，该地址池只在 IP 接入方式下使用。

[0233] 较佳地，WMI 单元还根据建立的各种绑定关系形成如表 1 示出的 UVR 表，保存到

UVR 单元中。该 WMI 单元形成的 VPN 实例包括路由转发表和 MPLS 标签转发表，这两个转发表的内容与方法实施例所述相同，这里不赘述。

[0234] UVR 单元，用于存储 WMI 单元建立的绑定关系。

[0235] VRF 单元，用于存储 VPN 实例。

[0236] 第一网络接口，为所在SSL VPN网关和用户之间提供数据传输通道，通过互联网与远程主机耦接。

[0237] 第二网络接口，为所在 SSL VPN 网关和 MPLS 交换网提供数据传输通道，通过 MPLS 交换网与 VPN 资源服务器耦接。

[0238] 处理单元，用于与 user1 进行信息交互，建立与远程接入相关的连接。当接收到 user1 通过 SSL 连接发来的报文时，根据 UVR 单元存储的绑定关系，从 VRF 单元获取 user1 所属用户组绑定的 VPN 实例，即 VPN1 实例，采用 VPN1 实例为所接收报文打上 VPN 标签 1024 和 MPLS 转发标签 1026，并通过 MPLS 交换网转发给 VPN 资源服务器；当接收到该 VPN 资源服务器返回的应答报文时，根据该应答报文携带的 VPN 标签 1024 在 VRF 单元中查找相应 VPN 实例，根据查找到的 VPN1 实例将应答报文通过与 user1 之间的 SSL 连接转发给 user1。

[0239] 当采用 TCP 或 WEB 方式接入 VPN 资源服务器时，所述处理单元进一步用于：在建立与远程接入相关的连接时，建立 user1 与所在 SSL VPN 网关之间的 SSL 连接，为 user1 建立虚接口 SVE1/0 与请求访问的 VPN 资源服务器 S 1 之间的 TCP 连接并维护 ST 表；在建立 TCP 连接过程中，根据 user1 的认证授权信息绑定的 VPN 实例，为建立的 TCP 连接的 Socket 打上相应 VPN 实例标签索引 1；

[0240] 在接收到 user1 通过所述 SSL 连接发来的报文时，根据为 user1 建立的 TCP 连接的信息，在 TCP 层为所接收报文打上 VPN 实例标签索引 1，再由处理单元中的 MPLS 模块根据 VPN 实例标签索引 1 找到相应 VPN1 实例，为报文添加 VPN 标签 1024 和 MPLS 转发标签 1026，然后通过为 user1 建立的 TCP 连接将报文转发给 VPN 资源服务器 S1；

[0241] 在接收到通过所述 TCP 连接返回的应答报文时，根据应答报文携带的 VPN 标签 1024 查找相应 VPN 实例，根据所述应答报文的私网目的地址 10.1.1.1 在查找到的 VPN1 实例中进行匹配，匹配到 VPN1 实例中的第二条路由转发表项，获得下一跳为内部环回接口地址 127.0.0.1，则直接将所接收的应答报文转发到上层应用，该上层应用通过所述 SSL 连接将应答报文发送给 user1。

[0242] 当采用 IP 方式接入 VPN 资源服务器时，所述 WMI 单元在创建虚接口时，对应为每个 VPN 设置的地址池创建一个虚接口，对应的地址池和虚接口属于同一网段。

[0243] 所述处理单元进一步用于，在建立与远程接入相关的连接时，从为 user1 所属 VPN 设置的地址池中为 user1 分配虚地址 10.1.1.2；建立 user1 与 SSLVPN 网关之间的 SSL 连接；

[0244] 在接收到 user1 通过 SSL 连接发来的携带私网 IP 头（私网源地址为 10.1.1.2）的报文时，根据 user1 所属用户组绑定的 VPN1 实例，在 IP 层为所接收报文打上 VPN 标签实例标签索引 1，再由处理单元中的 MPLS 模块根据 VPN 实例标签索引 1 为报文添加 VPN 标签 1024 和 MPLS 转发标签 1026；

[0245] 在接收到应答报文时，根据该应答报文携带的 VPN 标签 1024 查找相应 VPN 实例；根据所述应答报文的私网目的地址 10.1.1.2 在查找到的 VPN1 实例中匹配到第一条路由转

发表项，获得下一跳为虚接口 SVE1/0 的 IP 地址 10.1.1.1，则通过虚接口 SVE1/0 将应答报文经由所述 SSL 连接转发给 user1。

[0246] 下面对处理单元着重进行描述。

[0247] 处理单元包括 SSL VPN 业务模块、VPN 标签处理模块、TCP 模块、IP 模块和 MPLS 模块。其中，根据 SSL VPN 网关支持的接入方式，SSL VPN 业务模块具体包括 TCP/WEB 接入方式处理模块和 IP 接入方式处理模块中的一种或任意组合。

[0248] 图 7 示出了当采用 TCP/WEB 方式接入 VPN 资源服务器时，SSL VPN 网关中各组成模块的位置和连接关系。如图 7 所示，处理单元具体包括位于应用层的 TCP/WEB 接入方式处理模块和 VPN 标签处理模块、位于 TCP 层的 TCP 模块、位于 IP 层的 IP 模块和位于 IP 层与网络接口之间的 MPLS 模块。

[0249] 其中，TCP/WEB 接入方式处理模块，用于在 user1 请求登录认证时，向 user1 返回用户资源页面；当 user1 请求访问 VPN 资源服务器 S1 时，建立 user1 与所在 SSL VPN 网关之间的 SSL 连接，为 user1 建立虚接口 SVE1/0 与 VPN 资源服务器 S 1 之间的 TCP 连接并维护 ST 表。

[0250] 在建立 TCP 连接过程中，VPN 标签处理模块根据 user1 所属用户组息绑定的 VPN1 实例，为 TCP 连接的 socket 打上 VPN 实例标签索引 1。

[0251] 当报文通过 user1 与 SSL VPN 网关之间的 SSL 连接进入 SSL VPN 网关后，IP 模块去掉报文的公网 IP 头，将报文的数据部分经由 TCP 模块上送到 TCP/WEB 接入方式处理模块；

[0252] TCP/WEB 接入方式处理模块进一步根据 ST 表确定将所接收的报文通过为 user1 建立的 TCP 连接转发，将报文发送 TCP 模块；

[0253] TCP 模块根据为 user1 建立的 TCP 连接的信息为报文打上私网 IP 头，并且根据 socket 的 VPN 实例标签索引 1 为报文打上 VPN 实例标签索引 1，然后将报文发给 IP 模块；

[0254] IP 模块进行路由查找，即根据报文的 VPN 实例标签索引 1 找到对应的 VPN1 实例，并在 VPN 路由表和标签转发表中查找转发路径，从而确定由 MPLS 进行转发，然后将报文发给 MPLS 模块；

[0255] MPLS 模块根据报文携带的 VPN 实例标签索引 1 在 VRF 单元中查找相应 VPN1 实例，根据查找到的 VPN1 实例为报文打上 VPN 标签 1024 和 MPLS 转发标签 1026，然后转发出去。

[0256] 当应答报文通过 VPN 资源服务器 S1 与 SSL VPN 网关之间的 TCP 连接进入 SSL VPN 网关后，MPLS 模块根据应答报文携带的 VPN 标签 1024 确定报文所属 VPN，将去掉 VPN 标签的报文及其所属 VPN 信息发送给 IP 模块；

[0257] 所述 IP 模块根据所述所属 VPN 信息从 VRF 单元中获取相应 VPN 实例，并根据应答报文的私网目的地址 10.1.1.2 在获取的 VPN1 实例中进行匹配，匹配上 VPN1 实例中的第二条路由转发表项，获得下一跳为内部环回接口地址 127.0.0.1，然后直接将去掉私网 IP 头的报文经由 TCP 模块转发到 TCP/WEB 接入方式处理模块；

[0258] TCP/WEB 接入方式处理模块根据 ST 表确定将接收自所述 TCP 连接的应答报文通过与 user1 之间的 SSL 连接发送给 user1。此时，将应答报文发送给所述 TCP 模块；TCP 模块根据 SSL 连接的信息为应答报文添加公网 IP 头，并转发给 IP 模块；IP 模块通过查找公网路由，把报文发送给 user1。

[0259] 图 8 示出了当采用 IP 方式接入 VPN 资源服务器时，SSL VPN 网关中各组成模块的位置和连接关系。如图 8 所示，处理单元具体包括位于应用层的 IP 接入方式处理模块 1，位于 IP 层的 IP 接入方式处理模块 2 和 VPN 标签处理模块、位于 TCP 层的 TCP 模块、位于 IP 层的 IP 模块，以及位于 IP 层与网络接口之间的 MPLS 模块。

[0260] IP 接入方式处理模块 1，用于在 user1 请求登录认证时，向 user1 返回用户资源页面，且从为 user1 所属 VPN 设置的地址池中为 user1 分配虚地址 10.1.1.2；当 user1 请求访问 VPN 资源服务器时，建立 user1 与所在 SSL VPN 网关之间的 SSL 连接，并维护 UVS 表，该 UVS 表同时由 IP 接入方式处理模块 2 共享。

[0261] 当报文通过 user1 与 SSL VPN 网关之间的 SSL 连接进入 SSL VPN 网关后，所述 IP 模块去掉报文的公网 IP 头，将保留私网 IP 头和数据部分的报文经由 TCP 模块发送到位于应用层的 IP 接入方式处理模块 1，IP 接入方式处理模块 1 把报文发送到位于 IP 层的 IP 接入方式处理模块 2；私网源地址为 user1 的虚地址 10.1.1.2；

[0262] 所述 IP 接入方式处理模块 2 根据 UVS 表确定以直接 IP 转发方式转发报文，将报文发送给 VPN 标签处理模块；

[0263] VPN 标签处理模块根据 UVR 单元保存的绑定关系，确定 user1 所属用户组绑定的 VPN 为 VPN1，则为报文打上 VPN 实例标签索引 1，然后将报文通过所述 IP 模块；

[0264] IP 模块通过路由查找确定由 MPLS 进行转发，并将报文发送给 MPLS 模块；

[0265] MPLS 模块根据报文携带的 VPN 实例标签索引 1 查找相应 VPN 实例，根据查找到的 VPN1 实例为报文添加 VPN 标签 1024 和 MPLS 转发标签 1026 并转发。

[0266] 当应答报文通过第二网络接口进入 SSL VPN 网关后，所述 MPLS 模块根据应答报文携带的 VPN 标签 1024 确定报文所属 VPN，将去掉 VPN 标签的应答报文及其所属 VPN 信息发送给 IP 模块；

[0267] IP 模块根据所述所属 VPN 信息从 VRF 单元中获取相应 VPN 实例，并根据应答报文的私网目的地址，即 user1 的虚地址进行路由匹配，匹配上 VPN1 实例中的第一条路由转发表项，获得下一跳为 SVE1/0。然后根据匹配的路由转发表项把报文发送到虚接口 SVE1/0，虚接口 SVE1/0 的转发功能由位于 IP 层的 IP 接入方式处理模块 2 来实现，也就是说上述报文传送到 IP 接入方式处理模块 2；

[0268] IP 接入方式处理模块 2 根据 UVS 表确定通过虚接口 SVE1/0 将应答报文经由与 user1 之间的 SSL 连接转发，此时将应答报文发送给 TCP 模块；

[0269] TCP 模块根据 SSL 连接的信息为应答报文添加公网 IP 头，并转发给 IP 模块；

[0270] IP 模块通过查找公网路由，把报文发送给 user1。

[0271] 本发明还提供了一种远程接入 MPLS VPN 的系统，如图 3 所示，该系统包括用户使用的远程主机、互联网、SSL VPN 网关、MPLS VPN 网络以及 MPLS VPN 网络中的 VPN 资源服务器；远程主机通过自身与 SSL VPN 网关之间的 SSL 连接访问 MPLS VPN 中的 VPN 资源服务器；SSL VPN 网关同时作为 MPLS VPN 的 PE 路由器；其中，SSL VPN 网关可以采用前述实施例中的任意一种 SSL VPN 网关。

[0272] 综上所述，以上仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

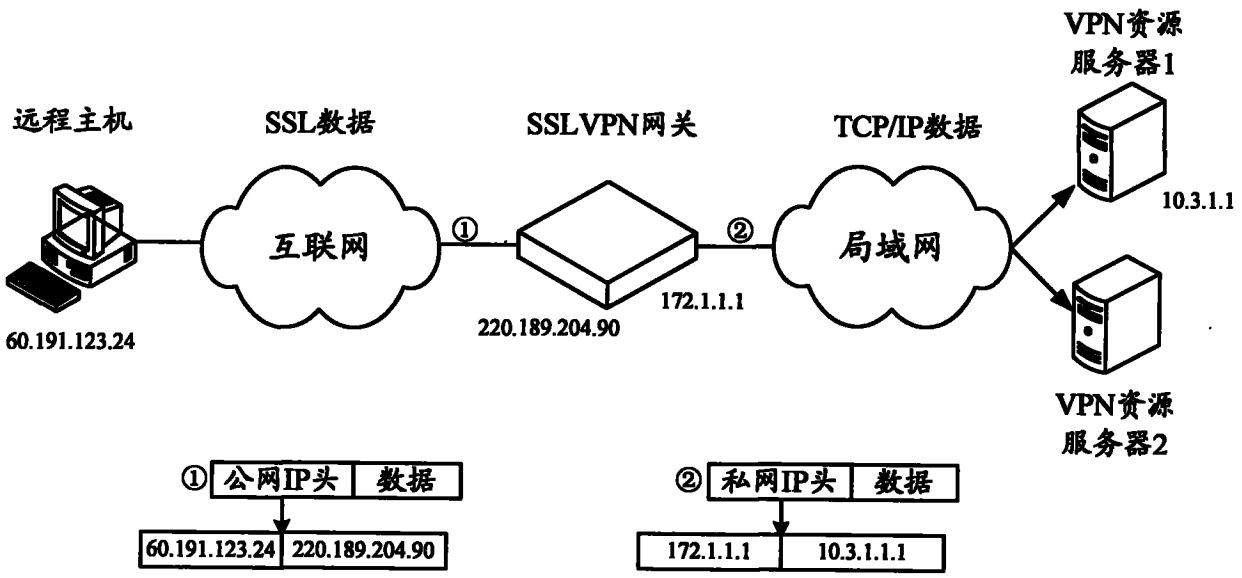

远程主机
SSL数据
SSLVPN网关
TCP/IP数据
VPN资源
服务器1
10.3.1.1
互联网
①
②
局域网
60.191.123.24
220.189.204.90
172.1.1.1
VPN资源
服务器2
①
公网IP头
数据
60.191.123.24
220.189.204.90
②
私网IP头
数据
172.1.1.1
10.3.1.1.1

图 1A

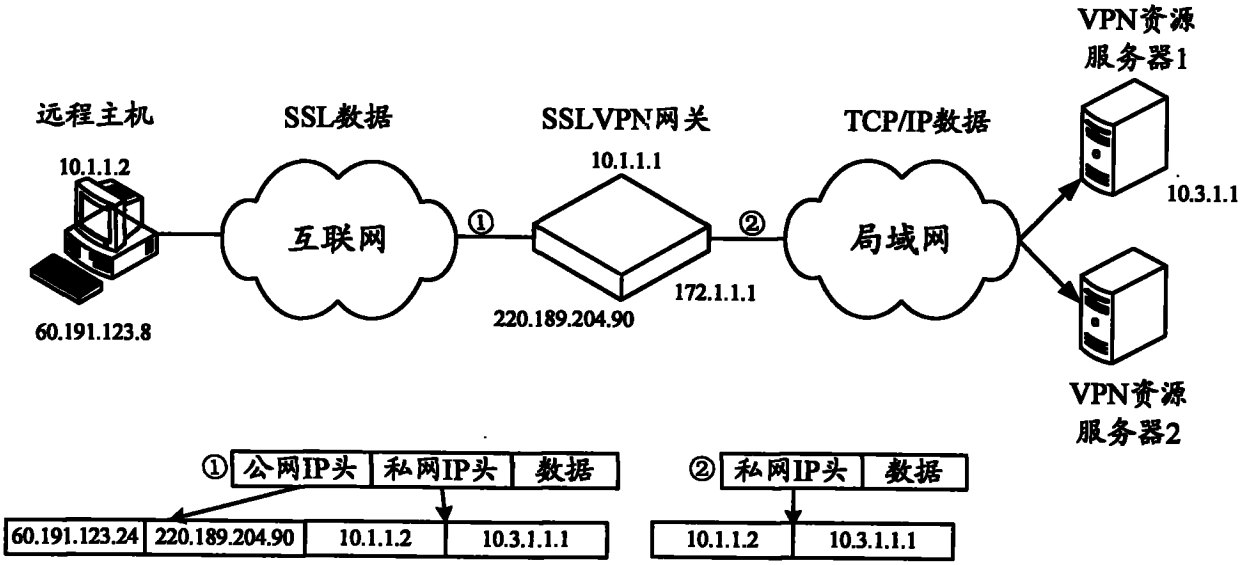

VPN资源
服务器1
远程主机
SSL数据
SSLVPN网关
TCP/IP数据
10.1.1.2
10.1.1.1
10.3.1.1
互联网
①
②
局域网
172.1.1.1
220.189.204.90
60.191.123.8
VPN资源
服务器2
①
公网IP头
私网IP头
数据
60.191.123.24
220.189.204.90
10.1.1.2
10.3.1.1.1
②
私网IP头
数据
10.1.1.2
10.3.1.1.1

图 1B

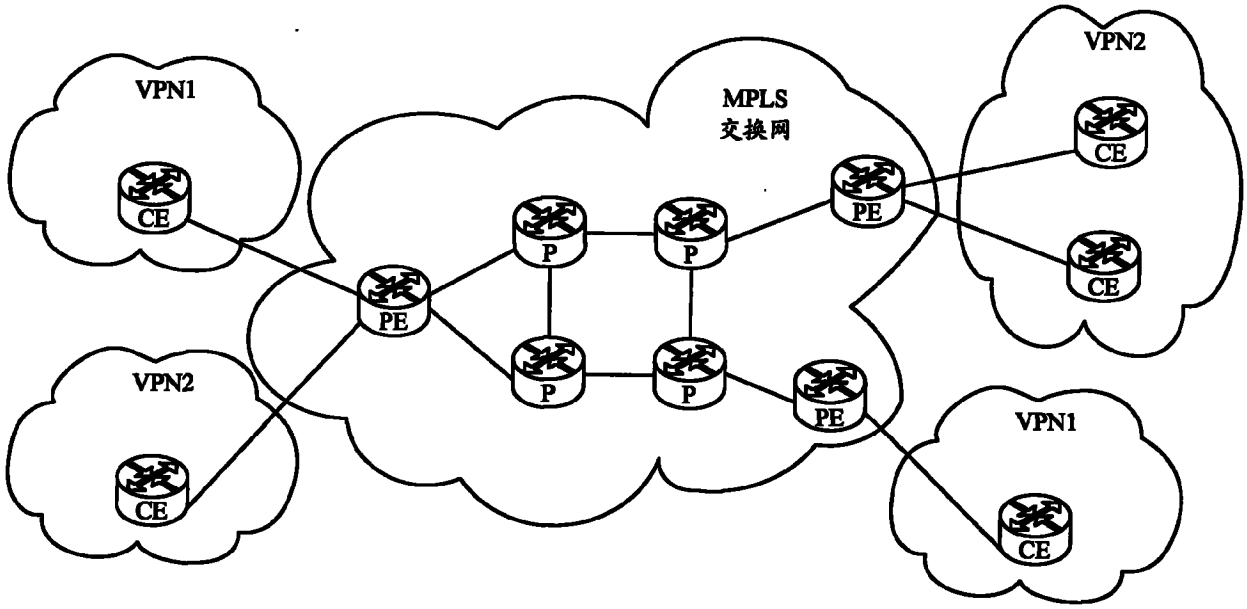

VPN1
CE
MPLS
交换网
P
P
PE
VPN2
CE
CE
PE
P
P
VPN2
CE
PE
VPN1
CE

图 2

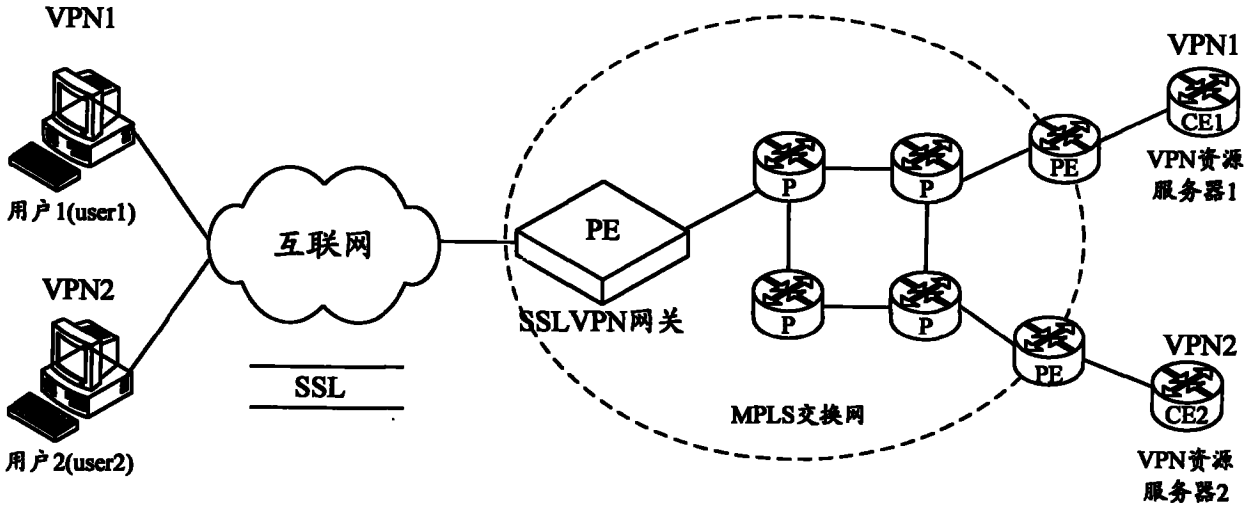

VPN1
用户 1(user1)
VPN2
用户 2(user2)
互联网
SSL
PE
SSLVPN网关
P
P
P
P
PE
PE
MPLS交换网
VPN1
CE1
VPN资源
服务器1
VPN2
CE2
VPN资源
服务器2

图 3

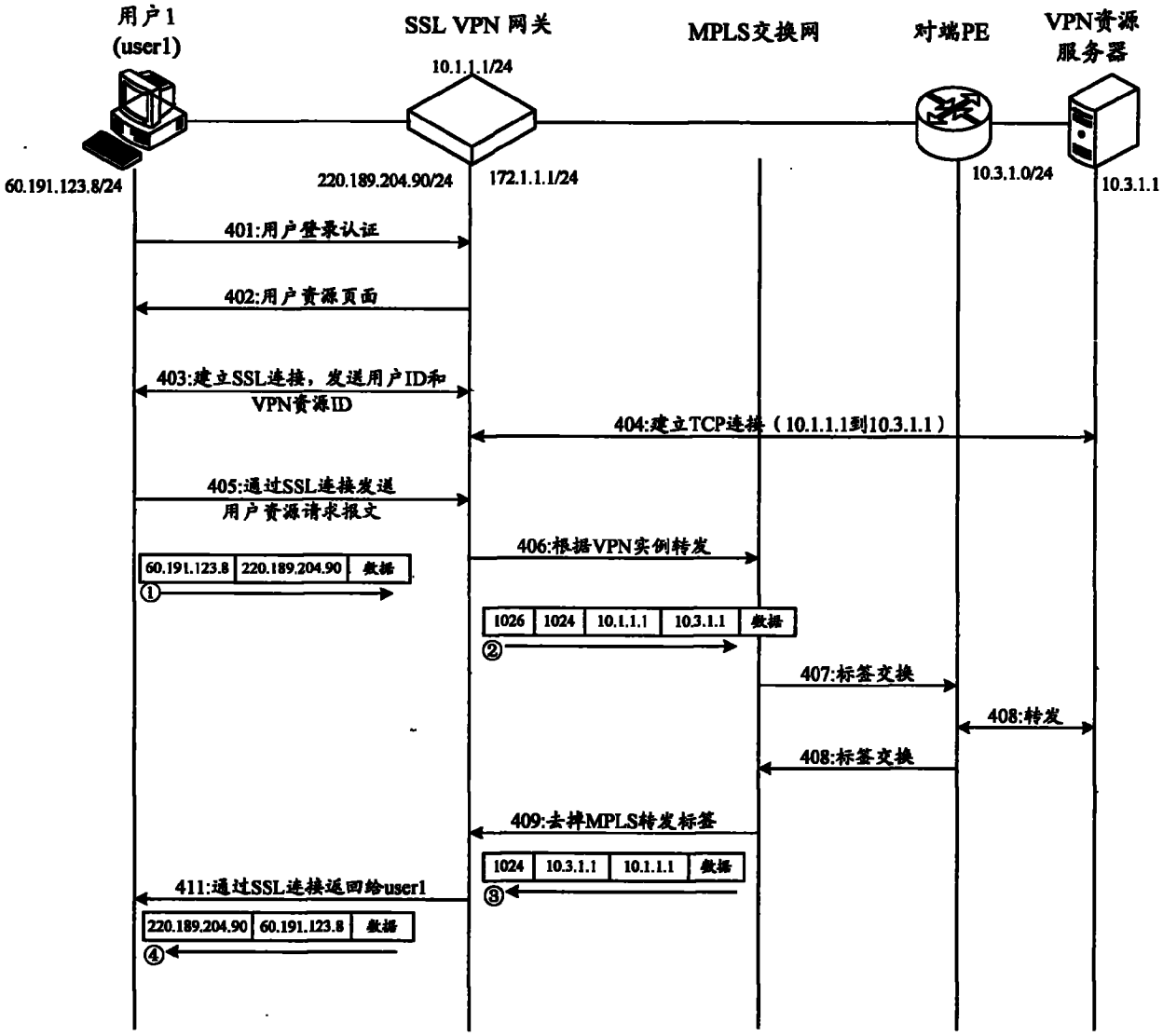

用户1
(user1)
SSL VPN 网关
10.1.1.1/24
MPLS交换网
对端PE
VPN资源
服务器
60.191.123.8/24
220.189.204.90/24
172.1.1.1/24
10.3.1.0/24
10.3.1.1
401:用户登录认证
402:用户资源页面
403:建立SSL连接，发送用户ID和
VPN资源ID
404:建立TCP连接（10.1.1.1到10.3.1.1）
405:通过SSL连接发送
用户资源请求报文
406:根据VPN实例转发
60.191.123.8
220.189.204.90
数据
①
1026
1024
10.1.1.1
10.3.1.1
数据
②
407:标签交换
408:转发
408:标签交换
409:去掉MPLS转发标签
1024
10.3.1.1
10.1.1.1
数据
③
411:通过SSL连接返回给user1
220.189.204.90
60.191.123.8
数据
④

图 4

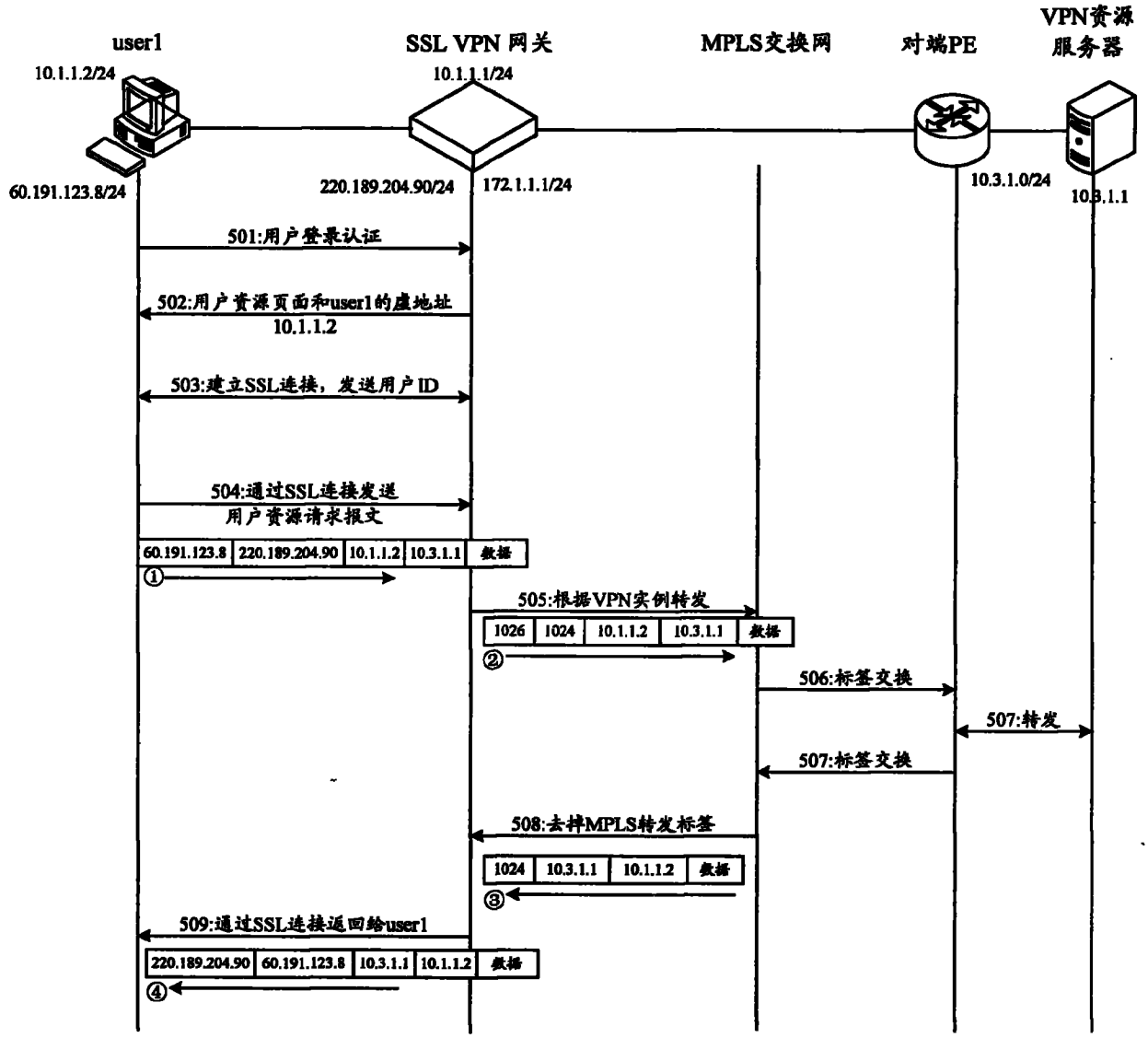

user1
10.1.1.2/24
60.191.123.8/24
SSL VPN 网关
10.1.1.1/24
220.189.204.90/24
172.1.1.1/24
MPLS交换网
对端PE
10.3.1.0/24
VPN资源
服务器
10.3.1.1
501:用户登录认证
502:用户资源页面和user1的虚地址
10.1.1.2
503:建立SSL连接，发送用户ID
504:通过SSL连接发送
用户资源请求报文
60.191.123.8
220.189.204.90
10.1.1.2
10.3.1.1
数据
①
505:根据VPN实例转发
1026
1024
10.1.1.2
10.3.1.1
数据
②
506:标签交换
507:转发
507:标签交换
508:去掉MPLS转发标签
1024
10.3.1.1
10.1.1.2
数据
③
509:通过SSL连接返回给user1
220.189.204.90
60.191.123.8
10.3.1.1
10.1.1.2
数据
④

图 5

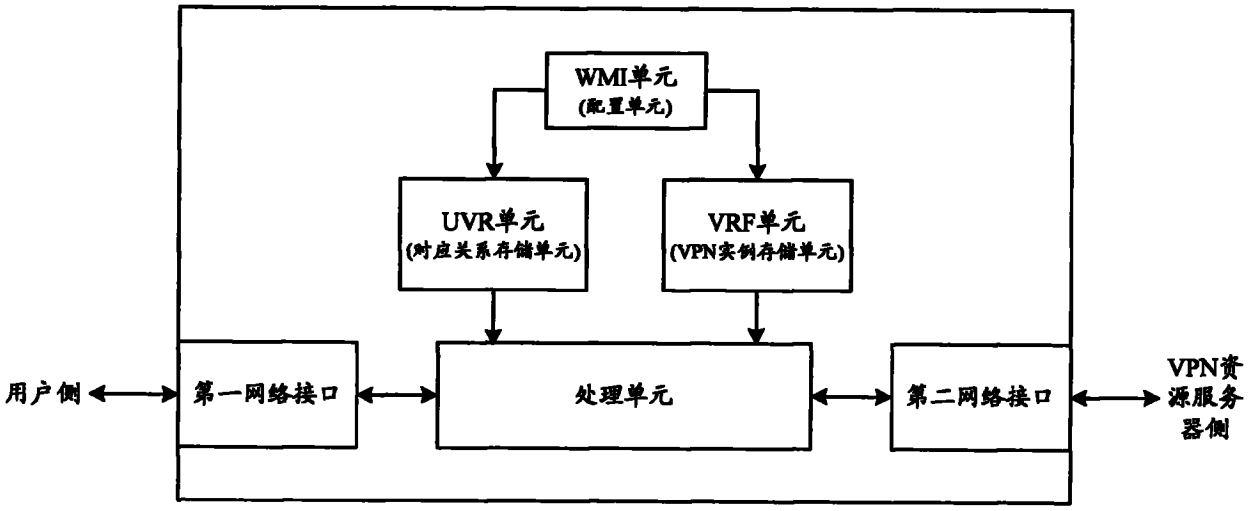

WMI单元
(配置单元)
UVR单元
(对应关系存储单元)
VRF单元
(VPN实例存储单元)
用户侧
第一网络接口
处理单元
第二网络接口
VPN资源服务器侧

图 6

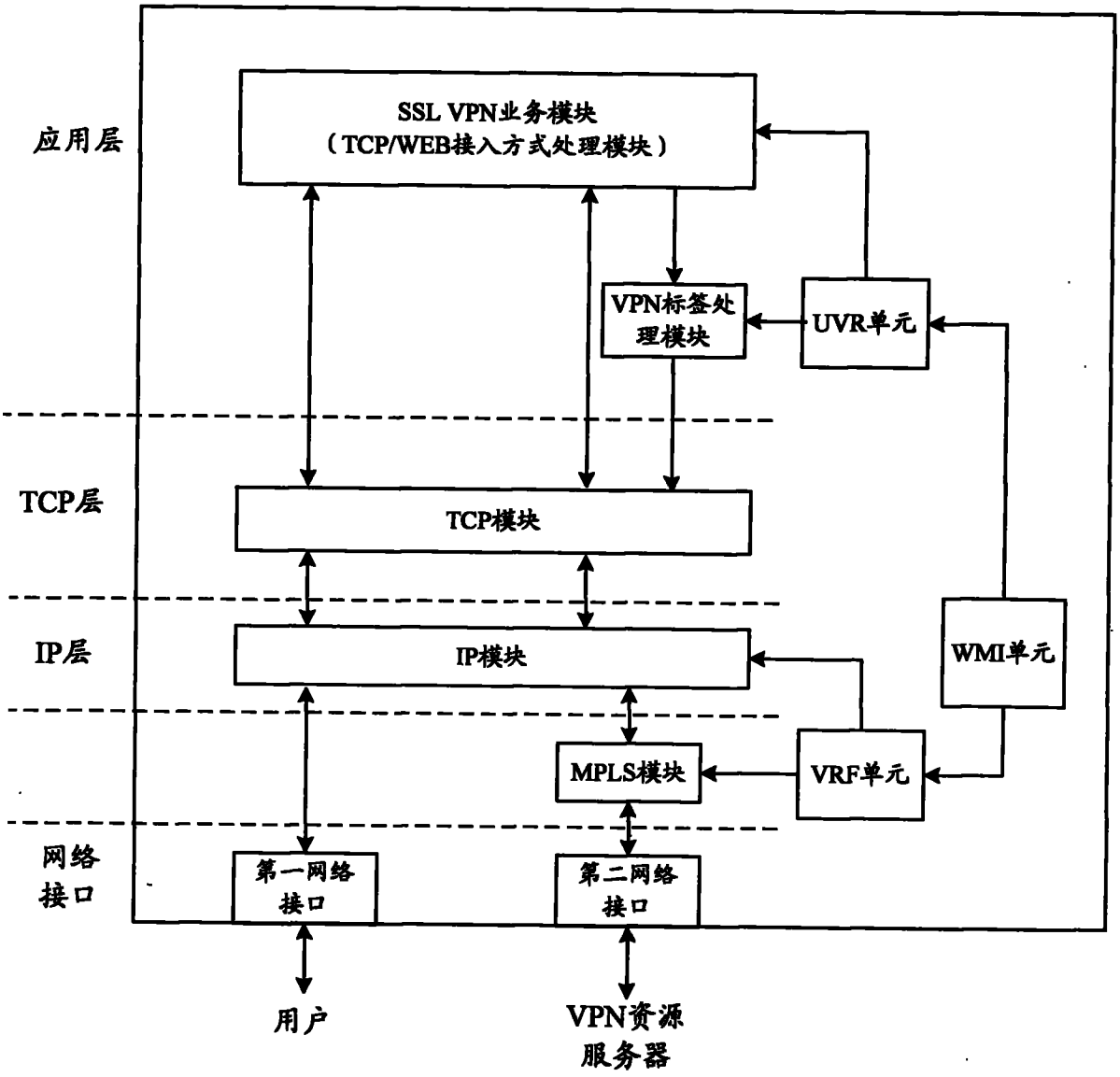

应用层
SSL VPN业务模块
（TCP/WEB接入方式处理模块）
VPN标签处理模块
UVR单元
TCP层
TCP模块
IP层
IP模块
WMI单元
MPLS模块
VRF单元
网络接口
第一网络接口
第二网络接口
用户
VPN资源服务器

图 7

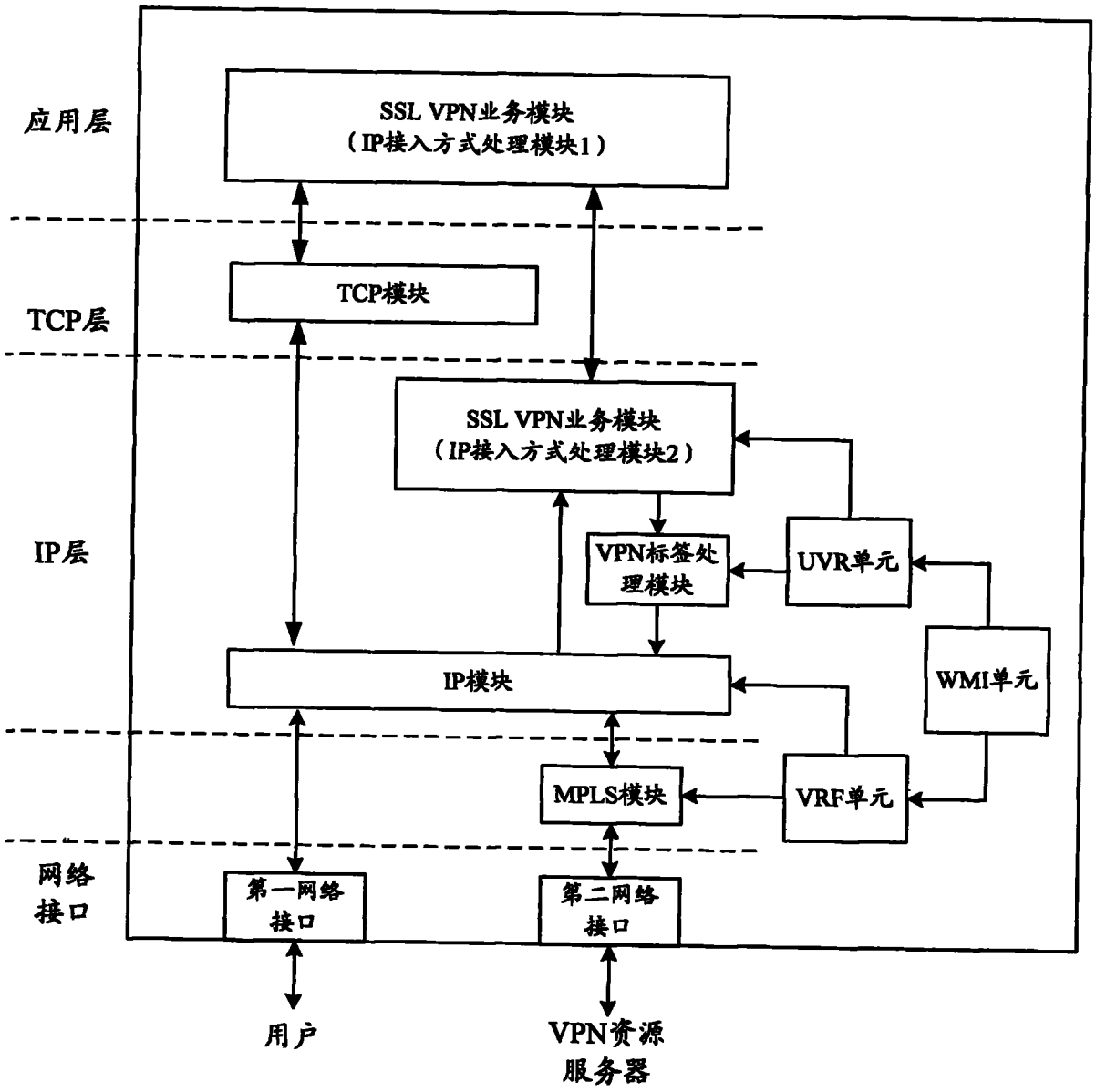

应用层
SSL VPN业务模块
（IP接入方式处理模块1）
TCP模块
TCP层
SSL VPN业务模块
（IP接入方式处理模块2）
IP层
VPN标签处理模块
UVR单元
WMI单元
IP模块
MPLS模块
VRF单元
网络接口
第一网络接口
第二网络接口
用户
VPN资源服务器

图 8