

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200610060995.6

[43] 公开日 2007 年 12 月 5 日

[11] 公开号 CN 101083549A

[22] 申请日 2006.6.2

[21] 申请号 200610060995.6

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 许用梁 高建华 吴成庆

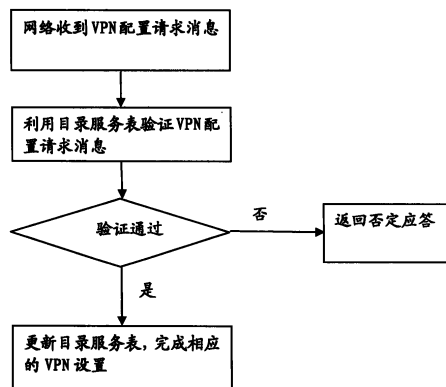
权利要求书 3 页 说明书 12 页 附图 2 页

[54] 发明名称

一种实现 VPN 配置服务的方法和系统

[57] 摘要

本发明公开了一种实现 VPN 配置服务的方法和系统。本发明方法中，网络收到 VPN 配置请求消息，利用目录服务表对所述 VPN 配置请求消息进行验证；验证通过后，更新所述目录服务表，完成所述 VPN 配置。本发明通过目录服务器和目录服务表配置 VPN 策略信息和 VPN 成员信息，当 VPN 网络发生动态变化时，查询目录服务表快速实现 VPN 成员的增加、删除等操作，以及 VPN 策略的动态变化，提高了 VPN 服务的效率；通过 VPN 策略信息的设置，将客户的 VPN 连接请求限定在封闭用户组内并且对客户的 VPN 连接请求进行相应的控制，从而实现了灵活的管理方式。



1、一种实现 VPN 配置服务的方法，其特征在于，

(1) 网络收到 VPN 配置请求消息，利用目录服务表对所述 VPN 配置请求消息进行验证；

(2) 验证通过后，更新所述目录服务表，完成所述 VPN 配置。

2、如权利要求 1 所述的方法，其特征在于，对所述 VPN 配置请求消息的验证由目录服务器完成，所述目录服务表保存在所述目录服务器上。

3、如权利要求 1 所述的方法，其特征在于，对所述 VPN 配置请求消息的验证由网络边缘设备完成，所述目录服务表保存在所述网络边缘设备上。

4、如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述 VPN 配置请求消息是添加 VPN 成员的请求消息，所述 VPN 配置请求消息包括 VPN 标识和 VPN 成员标识，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识是否存在于目录服务表中，若存在，则进一步验证所述 VPN 成员标识是否存在于所述 VPN 标识对应的表项中，若不存在，则验证通过，将所述 VPN 成员标识添加到目录服务表中；

或者，

验证所述 VPN 标识是否存在于目录服务表中，若存在，则进一步验证所述 VPN 成员标识是否存在于所述 VPN 标识对应的表项中，若不存在，则进一步验证是否符合目录服务表中基于所述 VPN 的策略信息，若符合，则验证通过，将所述 VPN 成员标识添加到目录服务表中。

5、如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述 VPN 配置请求消息是删除 VPN 成员的请求消息，所述 VPN 配置请求消息包括 VPN 标识和 VPN 成员标识，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识与所述 VPN 成员标识是否存在于目录服务表的一个表项中，若是，则进一步验证所述表项中的策略信息是否允许 VPN 成员动态退出，若是，则验证通过，删除目录服务表中的所述表项。

6、如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述 VPN 配置请求消息是修改 VPN 策略的请求消息，所述 VPN 配置请求消息包括 VPN 标识、VPN 成员标识和基于 CE 的策略信息，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识与所述 VPN 成员标识是否存在于目录服务表的一个表项中，若是，则进一步验证所述表项中的策略信息是否允许 VPN 成员动态修改 VPN 策略，若是，则验证通过，将目录服务表的所述表项中基于 CE 的策略信息更新为所述配置请求消息中的基于 CE 的策略信息。

7、如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述 VPN 配置请求消息是修改 VPN 策略的请求消息，所述 VPN 配置请求消息包括 VPN 标识、VPN 成员标识和基于 VPN 的策略信息，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识与所述 VPN 成员标识是否存在于目录服务表的一个表项中，若是，则进一步验证所述表项中的策略信息是否允许 VPN 成员动态修改 VPN 策略，若是，则验证通过，将目录服务表的所述表项中基于 VPN 的策略信息更新为所述配置请求消息中的基于 VPN 的策略信息。

8、如权利要求 1 或 2 或 3 所述的方法，其特征在于，进一步包括，客户之间需要建立 VPN 连接时，发送 VPN 连接请求消息，所述请求消息中包括 VPN 标识、源 VPN 成员标识和目的 VPN 成员标识，

网络根据所述目录服务表验证所述请求消息，

若验证通过，则建立 VPN 连接。

9、一种实现 VPN 配置服务的系统，包括客户边缘设备、网络边缘设备和网络内部设备，其中，一个网络边缘设备与一个或多个客户边缘设备相连，且与其他的网络边缘设备或网络内部设备相连，共同提供 VPN 服务，其特征在于，还包括目录服务器，所述目录服务器驻留在网络边缘设备或网络内部设备上；或者驻留在网络之外单独的计算机上，所述目录服务器上保存目录服务表，用于验证 VPN 配置请求消息。

10、如权利要求 9 所述的系统，其特征在于，所述目录服务器包括验

证程序模块、配置程序模块和存储器，其中，

验证程序模块根据所述目录服务表对所述 VPN 配置请求消息进行验证，
若验证通过，则发送配置消息给配置程序模块；

配置程序模块接收到所述配置消息后，更新目录服务表；

所述目录服务表存储于存储器中。

一种实现VPN配置服务的方法和系统

技术领域

本发明涉及VPN (Virtual Private Network, 虚拟专用网) 领域, 具体是一种实现VPN配置服务的方法和系统。

背景技术

VPN 网络通常由 CE 设备 (Customer Edge, 客户边缘设备)、PE 设备 (Provider Edge, 网络边缘设备) 和 P 设备 (Provider, 网络内部设备) 构成。其中 CE 设备是客户边缘节点, 是在同一个站点的 VPN 客户端点的出/入口; PE 设备是传送网络的边缘节点, 作为传送网络负责向客户提供 VPN 服务的边缘设备, 一个 PE 设备至少与一个 CE 设备相连, 并且至少和另外一个传送网络设备, 即 PE 或者 P 相连。P 设备是传送网络内部的传送设备, P 设备和传送网络内部其它的传送设备相连, 但不直接和 CE 设备相连。

现有技术一提供的 VPN 服务通常由网络管理系统, 即 NMS (Network Management System, 网络管理系统) 来实现, 如图 1 所示, 通过 NMS 完成 VPN 网络的配置和客户 VPN 连接业务的建立, 具体步骤如下:

- 1、在 NMS 中手动配置 VPN 信息, 包括 VPN 成员信息、VPN 策略信息等;
- 2、客户需要建立 VPN 连接时, 客户向 NMS 发送 VPN 连接请求消息;
- 3、NMS 根据预先配置的 VPN 信息验证客户请求, 验证通过后, 建立网络连接。

现有技术二是 IETF 草案 draft-ietf-vpn-bgp-auto-discovery-00, 其中描述了通过 BGP 协议 (Border Gateway Protocol, 边界网关协议) 实

现 VPN 成员的自动发现并提供 VPN 服务的方法。结合其中所描述的成员自动发现方法，网络提供 VPN 连接服务的具体步骤如下：

1、在 PE 设备上配置所接入的 CE 成员信息，并通过<CPI PPI>来标识该 VPN 成员，其中 CPI 为 CE 设备上接入网络设备的端口标识，PPI 为 PE 设备上连接该 CE 设备的端口标识；

2、PE 设备通过配置 VPN 成员信息后，通过 BGP 协议与该 VPN 中的其它 PE 设备进行交互，通过这种 BGP 的自动发现机制最终会在 VPN 中所有的 PE 设备中形成 VPN 成员信息表 PIT；

3、当某个 CE 设备需要和 VPN 中的其它成员之间通讯时，PE 设备根据 VPN 成员信息表 PIT 来验证客户 VPN 通讯请求，验证通过后，建立 VPN 网络连接。

在上述现有技术方案中，VPN 成员信息以及 VPN 策略信息都需要通过管理员在 NMS 或者 PE 设备上手动配置；当 VPN 成员发生动态变化时，对 VPN 网络配置信息的增加、删除和修改等操作的时延大，管理方式不灵活。

发明内容

本发明提供一种实现 VPN 配置服务的方法和系统，能够灵活配置 VPN 成员信息，并设置 VPN 策略信息，实现 VPN 成员的动态加入和退出处理。

本发明方法，包括如下步骤：

(1) 网络收到 VPN 配置请求消息，利用目录服务表对所述 VPN 配置请求消息进行验证；

(2) 验证通过后，更新所述目录服务表，完成所述 VPN 配置。

上述对 VPN 配置请求消息的验证由目录服务器完成，所述目录服务表保存在所述目录服务器上。

上述对 VPN 配置请求消息的验证也可由网络边缘设备完成，所述目录

服务表保存在所述网络边缘设备上。

其中，所述 VPN 配置请求消息是添加 VPN 成员的请求消息，所述 VPN 配置请求消息包括 VPN 标识和 VPN 成员标识，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识是否存在于目录服务表中，若存在，则进一步验证所述 VPN 成员标识是否存在于所述 VPN 标识对应的表项中，若不存在，则验证通过，将所述 VPN 成员标识添加到目录服务表中；

或者，

验证所述 VPN 标识是否存在于目录服务表中，若存在，则进一步验证所述 VPN 成员标识是否存在于所述 VPN 标识对应的表项中，若不存在，则进一步验证是否符合目录服务表中基于所述 VPN 的策略信息，若符合，则验证通过，将所述 VPN 成员标识添加到目录服务表中。

其中，所述 VPN 配置请求消息是删除 VPN 成员的请求消息，所述 VPN 配置请求消息包括 VPN 标识和 VPN 成员标识，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识与所述 VPN 成员标识是否存在于目录服务表的一个表项中，若是，则进一步验证所述表项中的策略信息是否允许 VPN 成员动态退出，若是，则验证通过，删除目录服务表中的所述表项。

其中，所述 VPN 配置请求消息是修改 VPN 策略的请求消息，所述 VPN 配置请求消息包括 VPN 标识、VPN 成员标识和基于 CE 的策略信息，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识与所述 VPN 成员标识是否存在于目录服务表的一个表项中，若是，则进一步验证所述表项中的策略信息是否允许 VPN 成员动态修改 VPN 策略，若是，则验证通过，将目录服务表的所述表项中基于 CE 的策略信息更新为所述配置请求消息中的基于 CE 的策略信息。

其中，所述 VPN 配置请求消息是修改 VPN 策略的请求消息，所述 VPN 配置请求消息包括 VPN 标识、VPN 成员标识和基于 VPN 的策略信息，所述步骤 (2) 具体包括步骤：

验证所述 VPN 标识与所述 VPN 成员标识是否存在于目录服务表的一个表项中，若是，则进一步验证所述表项中的策略信息是否允许 VPN 成员动态修改 VPN 策略，若是，则验证通过，将目录服务表的所述表项中基于 VPN 的策略信息更新为所述配置请求消息中的基于 VPN 的策略信息。

本发明方法进一步包括，客户之间需要建立 VPN 连接时，发送 VPN 连接请求消息，所述请求消息中包括 VPN 标识、源 VPN 成员标识和目的 VPN 成员标识，网络根据所述目录服务表验证所述请求消息，若验证通过，则建立 VPN 连接。

本发明还提供了一种实现 VPN 配置服务的系统，包括客户边缘设备、网络边缘设备和网络内部设备，其中，一个网络边缘设备与一个或多个客户边缘设备相连，且与其他的网络边缘设备或网络内部设备相连，共同提供 VPN 服务，还包括目录服务器，所述目录服务器驻留在网络内部的运营商边缘设备或运营商内部设备上；或者驻留在网络之外单独的计算机上，所述目录服务器上保存目录服务表，用于验证 VPN 配置请求消息。

其中，所述目录服务器包括 CPU 处理器、验证程序模块、配置程序模块和存储器，其中，

验证程序模块根据所述目录服务表对所述 VPN 配置请求消息进行验证，若验证通过，则发送配置消息给配置程序模块；

配置程序模块接收到所述配置消息后，更新目录服务表；

所述目录服务表存储于存储器中。

本发明基于目录服务实现对 VPN 的配置服务，VPN 成员信息以及 VPN 策略信息均由目录服务表存储，当客户请求对 VPN 配置信息进行改变时，通过查询目录服务表快速实现 VPN 成员的增加、删除，以及 VPN 策略信息的配置修改等操作，提高了 VPN 服务的效率，另外，可以通过设置 VPN 策略信息，将客户的 VPN 连接请求限定在封闭用户组内并且对客户的 VPN 连接请求进行控制。

附图说明

图 1 为现有技术中网管系统实现 VPN 服务的示意图;

图 2 为本发明中实现 VPN 配置服务的系统示意图;

图 3 为本发明中目录服务器的结构示意图;

图 4 为本发明中实现 VPN 配置服务的方法示意图。

具体实施方式

本发明通过目录服务来实现 VPN 配置服务。在本发明提供的系统中,网络包括目录服务器,该目录服务器可以驻留在网络之外单独的计算机上,也可以驻留在网络内部的某个传送设备,即 PE 设备或 P 设备上。目录服务器以目录形式维护一张 VPN ID 与 VPN 成员标识关系的列表,即目录服务表,通过目录服务实现 VPN 配置信息的自动注册和维护。通过 CE-PE 之间的交互处理传送客户用来维护 VPN 相关的信息,通过 PE 设备和目录服务器之间的交互来实现动态增加、删除、修改目录服务表中的 VPN 成员信息和 VPN 策略信息(包括基于 CE 的策略信息和基于 VPN 的策略信息)。当客户请求通过网络建立、删除或维护 VPN 连接时,首先通过查询目录服务表验证所述请求是否限定在对应的 VPN 成员之间以及请求的内容是否符合相应的 VPN 策略信息,所述 VPN 策略信息包括:请求的最大带宽值、SLA(Service Level Agreement,服务等级协议)属性值等,验证通过后,网络才会正确响应该请求,提供相应的 VPN 配置服务。从而实现 VPN 信息的灵活配置,达到快速提供 VPN 服务的目的。

上述目录服务表中所述的 VPN 成员标识可以有如下两种标识方法:

TNA (Transport Network Assigned Address, 传输网络分配地址) 地址: 也可以附加端口号, TNA 地址是传送网络为客户设备接入网络的物理链路所分配的全球唯一地址, 通过 TNA 地址, 运营商可以标识客户设备接入

网络的数据承载链路。当一个 TNA 地址对应多条数据承载链路时，通过 TNA 地址和端口号组合来标识客户设备接入网络的某一条数据承载链路。

<CPI, PPI>: 即<CPI, PPI>组合来标识 VPN 的某个特定的成员，其中 CPI 为 CE 设备接入 VPN 网络的端口标识，PPI 为 PE 设备连接 CE 设备的端口标识，这两个标识的组合可以唯一标识一个 VPN 成员。

下面以VPN中动态维护VPN成员过程为例对本发明方案做进一步的详细说明。

如图 2所示，是实现 VPN配置服务的系统示意图。其中，A 和 Z是同一个VPN网络的客户边缘设备CE，该CE设备可以是L1、L2或L3层设备，例如TDM交叉连接设备、二层交换设备和路由器等。网络节点 B 和 C 是该VPN网络中的网络边缘设备PE，这里的PE设备可以是一个TDM交换设备，一个OXC (Optic Cross Connect System, 光交叉连接系统) 设备，一个FXC (Fiber switch, 光纤交换) 设备，或者一个能够将以太帧信号映射到一层连接的以太网专线设备等。网络节点D 和 E 是网络内部设备P，P设备是一个一层的设备，可以是TDM交换设备、OXC设备或者FXC设备等。传送节点之间，即B、C、D、E之间通过 TDM 技术的线路连接，如 SDH 链路。节点 F 是目录服务器。整个网络的控制平面运行GMPLS协议，在A、B节点之间和D、Z节点之间是客户和网络接口UNI，通过UNI来进行通信的相关规范可参考UNI 1.0标准。UNI定义了几类地址，内部传送网络地址是指运营商网络内部节点的地址，可以用来作内部路由，以及网络管理的目的，但是这些地址不会暴露给客户；客户地址指客户网络对客户节点的编址，这些地址一般不会暴露给运营商；TNA地址是由网络分配给连接UNI-N (UNI Signaling Agent-Network, UNI信令Agent-网络) 和UNI-C (UNI Signaling Agent-Client, UNI信令Agent-客户) 的一条或多条数据承载链路的全球唯一地址。图2中，网络给节点A分配的TNA地址是101，给节点Z分配的TNA地址是102。

图 3 所示为目录服务器的基本结构。包括验证程序模块、配置程序模

块和存储器。其中，验证验证程序模块根据目录服务表对 VPN 配置请求消息进行验证，若验证通过，则发送配置消息给配置程序模块；配置程序模块接收到所述配置消息后，对 VPN 配置请求消息进行处理，具体包括：添加 VPN 成员、删除 VPN 成员、修改 VNN 策略等，更新目录服务表；所述目录服务表存储于存储器中。目录服务表可以采用表 1 所示的格式。

VPN ID	VPN成员标识 (TNA地址/端口号)	Per-CE Policy	Per-VPN Policy
1	101/10	Policy 11	Policy 1
1	102/10	Policy 12	
1	103	Policy 13	
2	201	Policy 21	Policy 2
2	202/11	Policy 22	
.....			

表1

当然，VPN成员标识可以仅仅是TNA地址，可以是TNA地址和端口号，也可采用<CPI,PPI>的标识方法，表1仅仅是本发明的一个示例，其不应过度地限制本发明的范围，本领域的一个普通技术人员应该认识到许多的变化、替换和更改，均在本发明的权利要求范围之内。

图4所示是本发明中提供VPN配置服务的方法示意图，具体步骤如下：

- (1)网络收到 VPN 配置请求消息，利用目录服务表对所述 VPN 配置请求消息进行验证；
 - (3)验证通过后，更新所述目录服务表，完成所述 VPN 配置；
- 否则，返回否定应答。

本发明方法中，在目录服务器中预先配置VPN ID和基于该VPN的部分或全部策略信息，包括：该VPN允许动态接入的最大成员节点数等。

通过目录服务对VPN成员的动态维护有两种实现方法，下面分别对这两

种方法进行详细描述。

实施例一：当CE设备发起VPN配置请求消息，即请求添加、删除VPN成员或修改VPN策略信息的时候，CE设备通过UNI接口向PE设备发出相应的请求消息，PE向目录服务器转发所述请求消息，目录服务器查询目录服务表验证所述请求消息，验证通过后，在目录服务器上更新相应的VPN信息，完成所述VPN配置。当两个CE设备之间需要通信的时候，PE设备根据CE设备发来的VPN连接请求消息查询目录服务器，对所述VPN连接请求消息进行验证，验证通过后，在上述请求的源和目的CE设备之间建立VPN连接，这样，源和目的CE设备只能在VPN确定的VPN成员之间以及相应VPN策略允许的前提下进行通讯。

下面结合图2对动态维护VPN成员的各种情形进行详细的阐述。

1、添加VPN成员，具体步骤如下：

(1) CE设备A 通过UNI接口向PE设备B发送添加VPN成员的请求消息，该请求消息包括VPN ID 1、VPN成员标识101、基于CE设备A的VPN策略信息Policy 11，如，允许的最大带宽值 BW_{max} 等，其中，VPN ID和VPN成员标识为必须要包含的信息，基于CE设备A的策略信息为可选信息；

(2) B 收到接入所述请求消息后，向目录服务器 F转发该请求消息；

(3) F 通过查询目录服务表，验证该请求消息是否合法，例如下述两种验证方法：

(a) 验证目录服务表中是否存在VPN ID 1，

(a1) 如果不存在，则返回否定应答，拒绝添加A为该VPN成员；

(a2) 如果目录服务表中存在VPN ID 1，则进一步判断VPN ID 1对应的表项中是否存在VPN成员标识101，

(a21) 若是，则返回否定应答，拒绝添加A，因为A已经存在于目录服务表中；

(a22) 若否，则验证通过，将VPN成员标识101以及请求消息中包含的其他VPN信息，如基于CE设备A的策略信息等添加到目录服务表的相应表项中，返回肯定应答。

(b) 验证目录服务表中是否存在VPN ID 1，

(b1) 如果不存在，则返回否定应答，拒绝添加A为该VPN成员；

(b2) 如果存在，则进一步判断VPN ID 1对应的表项中是否存在VPN成员标识101，

(b21) 若是，则返回否定应答，拒绝添加A，因为A已经存在于目录服务表中；

(b22) 若否，则进一步验证是否符合目录服务表中相应表项的基于VPN的策略信息，譬如，该表项中基于该VPN的策略信息Policy1中指定该VPN允许动态接入的最大成员节点数是3，

(b221) 如果该VPN中的已有成员数为0，1或2，则验证通过，将VPN成员标识101以及请求消息中包含的其他VPN信息，如基于CE设备A的策略信息等添加到目录服务表的相应表项中，返回肯定应答。

(b222) 如果该VPN中已有成员数为3，则拒绝添加A为该VPN成员，返回否定应答。

2、删除VPN成员，具体步骤如下：

(1) 当 A 向 B 发送删除VPN成员的请求消息，其中包含等待删除的VPN ID 1、VPN成员标识101；

(2) B 向 F 转发该请求消息，其中包含等待删除的VPN ID 1 和VPN成员标识 101；

(3) F 收到该请求消息后，验证该请求消息是否合法，即

验证目录服务表中是否存在VPN ID为1且VPN成员标识为101的表项，

(a) 如果该表项存在，则验证该表项中的策略信息是否允许VPN成员动态退出，

(a1) 若允许, 则验证通过, 首先发起删除与该节点相关的VPN连接, 并在对应的目录服务表项中删除对应的<VPN ID, VPN成员标识>项<1, 100/10>; 返回肯定应答;

(a2) 若不允许, 则返回否定应答。

(b) 若该表项不存在, 则返回否定应答。

3、修改VPN策略, 具体步骤如下:

(1) A 向 B发送修改VPN策略的请求消息, 其中包含VPN ID 1、VPN成员标识101、基于CE的策略信息或者基于VPN的策略信息;

(2) B 向 F 转发该请求消息, 其中包含VPN ID 1、VPN成员标识和基于CE的策略信息或者基于VPN的策略信息;

(3) F 接到该请求消息后, 验证VPN ID和VPN成员标识的合法性, 即验证目录服务表中是否存在VPN ID为1且VPN成员标识为101的表项,

(a) 若存在, 则进一步验证该表项中的策略信息是否允许VPN成员动态修改VPN策略,

(a1) 若否, 则返回否定应答;

(a2) 若是, 则验证通过, 将目录服务表中的策略信息更新为请求消息中包含的策略信息, 返回肯定应答

(b) 若不存在, 则返回否定应答。

4、建立VPN连接, 具体步骤如下:

(1) A 向 B 发送建立VPN连接请求消息, 其中包含等待建立连接的VPN ID 1 和源VPN成员标识101/10、目的VPN成员标识/102/10, 以及相关的请求参数, 如带宽、保护属性等;

(2) B 向目录服务器 F 转发该建立VPN连接请求消息;

(3) F 根据目录服务表验证VPN ID、源VPN成员标识和目的VPN成员标识, 并根据基于CE的策略信息和基于VPN的策略信息验证相关的请求参数,

若验证未通过, 则返回否定应答;

若验证通过，则建立A与Z之间的VPN连接，返回肯定应答。

综上，上述说明仅为单域的情况，多域的实现情况和单域类似。

本发明还提供了另外一个实施例，具体阐述如下。

实施例二：目录服务表不仅保存在目录服务器 F 上，同时也下载到各个PE设备，PE设备不需要保存所有VPN的目录服务表项，只需要保存自身所在的VPN相关的目录服务表项。

目录服务器F在下面三种情况下对PE设备的目录服务表进行更新：

(1) 通过网管系统设定的目录服务器更新时间间隔，目录服务器 F 会定时更新各个PE节点的目录服务表；

(2) 添加或删除VPN成员或者修改VPN策略信息时，目录服务器 F 会立即更新各个PE设备的目录服务表；

(3) 当PE设备向目录服务器 F 请求更新目录服务表的时候，目录服务器 F 会给该PE节点返回更新的目录服务表。

建立VPN连接时，PE节点只需要查询本身的目录服务表即可，不需要再向目录服务器发送请求。如图2所示，

添加VPN成员/删除VPN成员/修改VPN策略，具体步骤如下：

(1) CE设备A向PE设备B发送相应的VPN配置请求消息，其中包括相应的VPN信息，该过程与实施例一相同，只是请求的目的不是目录服务器 F，而是 B；

(2) PE设备B查询其目录服务表，对该请求消息进行验证，具体的验证过程同实施例一，

验证通过之后，完成相应的VPN配置；B 向 F 发送消息，更新 F 的目录服务表；

否则，返回否定应答。

(3) F 向其他相关 PE 发送更新目录服务表的消息。

CE 设备 A 与 Z 之间需要建立 VPN 连接时，步骤如下：

网络中的 PE 设备 B 收到来自 CE 设备 A 的 VPN 连接请求信息后, 查询 B 中的目录服务表, 验证该 VPN 连接请求消息,

验证通过后, 建立所述 VPN 连接;

否则, 返回否定应答。

以上所述, 仅为本发明较佳的具体实施方式, 但本发明的保护范围并不局限于此, 任何熟悉本技术领域的技术人员在本发明揭露的技术范围内, 可轻易想到的变化或替换, 都应涵盖在本发明的保护范围之内。因此, 本发明的保护范围应以权利要求的保护范围为准。

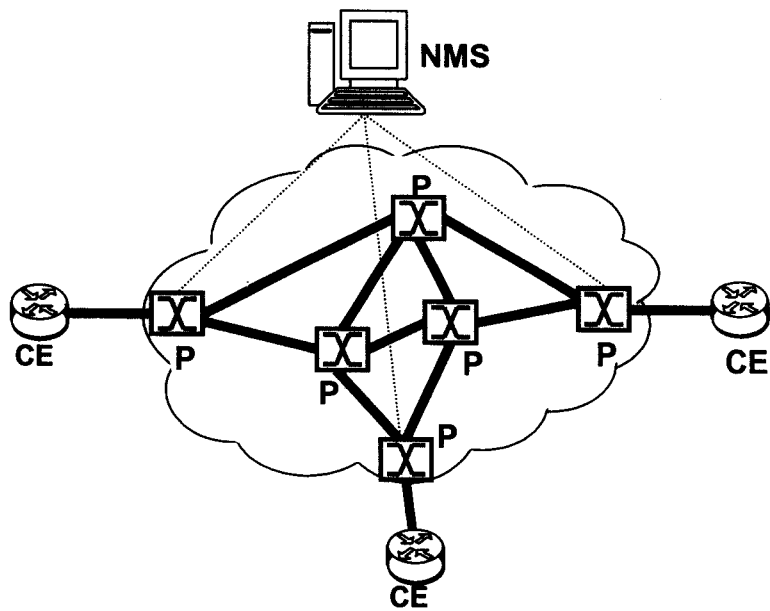


图 1

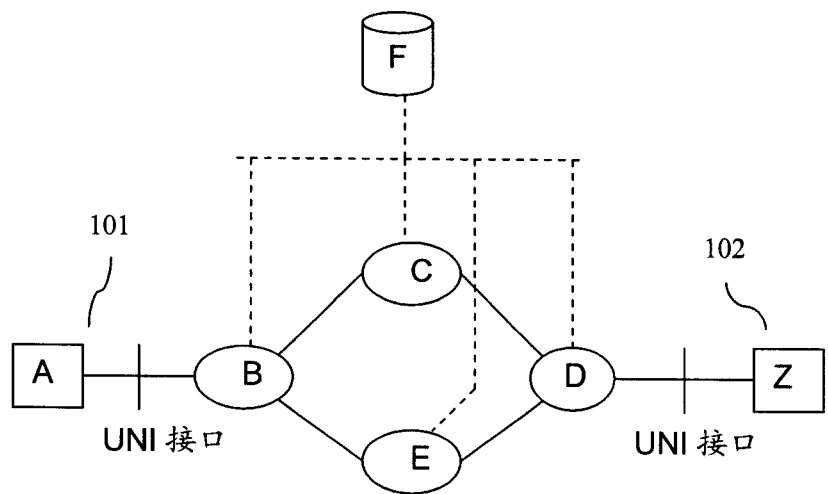


图 2

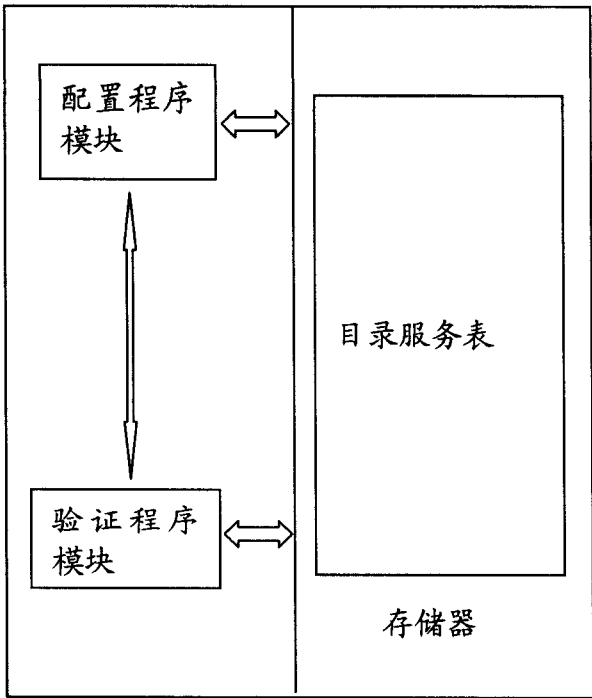


图 3

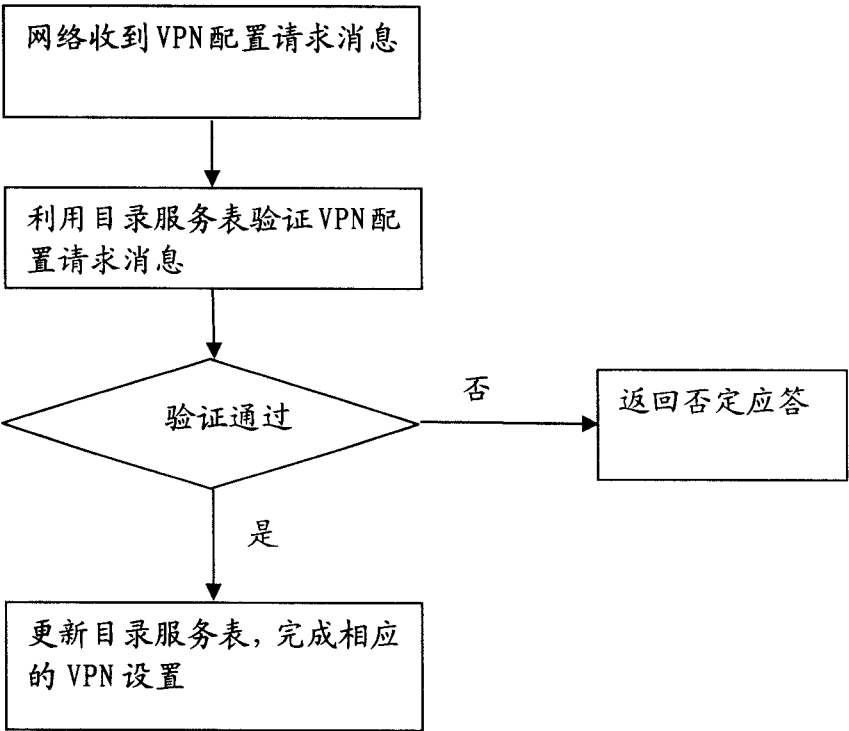


图 4