

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 8 月 31 日 (31.08.2017)



(10) 国际公布号
WO 2017/143903 A1

- (51) 国际专利分类号:
H04L 12/46 (2006.01) H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2017/072904
- (22) 国际申请日: 2017 年 2 月 4 日 (04.02.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610100415.5 2016 年 2 月 23 日 (23.02.2016) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 谢莹 (XIE, Ying); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。王昕 (WANG, Xin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

(54) Title: METHOD, DEVICE AND SYSTEM FOR ACCESS CONTROL

(54) 发明名称: 接入控制方法、装置及系统

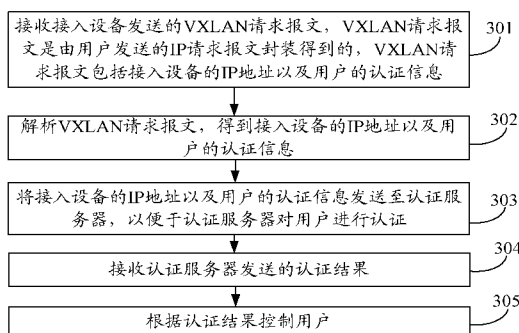


图3

- 301 Receive a VXLAN request message sent by an access device, the VXLAN request message being obtained by encapsulating an IP request message that is sent by a user, the VXLAN request message comprising the IP address of the access device and authentication information of the user
- 302 Parse the VXLAN request message, so as to obtain the IP address of the access device and the authentication information of the user
- 303 Send the IP address of the access device and the authentication information of the user to an authentication server, so as to facilitate user-authentication by the authentication server
- 304 Receive an authentication result sent by the authentication server
- 305 Control the user according to the authentication result

(57) Abstract: Disclosed in the present invention are a method, a device and a system for access control, which belong to the field of communications. Said method comprises: receiving a virtual extensible local area network (VXLAN) request message sent by an access device; parsing the VXLAN request message, so as to obtain the IP address of the access device and authentication information of a user; sending the IP address of the access device and the authentication information of the user to an authentication server, so as to facilitate user-authentication by the authentication server; receiving an authentication result sent by the authentication server; and controlling the user according to the authentication result. The present invention accomplishes user-authentication according to the access information of the user in a VXLAN environment.

(57) 摘要: 本发明公开了一种接入控制方法、装置及系统, 属于通信领域。所述方法包括: 接收接入设备发送的虚拟可扩展局域网 VXLAN 请求报文; 解析 VXLAN 请求报文, 得到接入设备的 IP 地址以及用户的认证信息; 将接入设备的 IP 地址以及用户的认证信息发送至认证服务器, 以便于认证服务器对用户进行认证; 接收认证服务器发送的认证结果; 根据认证结果控制用户。本发明实现了 VXLAN 场景下根据用户的接入信息对用户的认证。

WO 2017/143903 A1

接入控制方法、装置及系统

本申请要求于 2016 年 2 月 23 日提交中国专利局、申请号为 201610100415.5、发明名称为“接入控制方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信领域，特别涉及一种接入控制方法、装置及系统。

10 背景技术

随着通信技术的发展，出现了一种虚拟可扩展局域网（英文：virtual extensible local area network；简称：VXLAN），VXLAN 是三层网络虚拟化（network virtualization over layer 3；简称：NVo3）中的一种网络虚拟化技术，通过将虚拟机（英文：virtual machine；简称：VM）或物理服务器发出的数据包封装在用户数据报协议（英文：User Datagram Protocol；简称：UDP）报文中，并使用物理网络的因特网协议（英文：Internet Protocol；简称：IP）地址或媒体访问控制（英文：media access control；简称：MAC）地址作为报文头进行封装，然后在 IP 网络上传输，到达目的地后由隧道终结点解封封装并将数据发送给目标 VM 或物理服务器。即，用户能够通过 VXLAN 与另一个网络中的对端用户通信。如图 1 所示，VXLAN 包括接入设备 01 和业务路由器（英文：Service Router；简称：SR）02，且接入设备 01 和 SR 02 均为 VXLAN 的边缘设备，称为网络虚拟边缘（英文：network virtualization edge；简称：NVE），每个 NVE 上配置了 VXLAN 隧道终端（英文：VXLAN Tunneling End Point；简称：VTEP）。

在传统的园区接入或者城域以太网宽带接入场景中，SR-02 需要根据用户的物理位置信息，对用户进行认证、计费、授权，并在用户上线后需要对用户 IP 业务报文做安全绑定检查。具体来说，由接入设备 01 在动态主机配置协议（英文：Dynamic Host Configuration Protocol，简称：DHCP）报文中插入携带用户的物理位置信息的 DHCP 82 选项或者在以太网承载 PPP 协议（英文：Point-to-Point Protocol Over Ethernet，简称：PPPoE）报文中插入携带用户的接入信息（例如物理位置，环路标识等）的 PPPoE+ 选项，并将 DHCP 报文或者 PPPoE 报文发送给 SR-02，然后 SR-02 将 DHCP 报文或者 PPPoE 报文中携带的用户物理位置信息，以及用户名和/或密码、虚拟局域网（英文：virtual local area network；简称：VLAN）标识、SR 用于接收 DHCP 报文或者 PPPoE 报文的端口中的一个或多个发送到认证服务器 1 对用户进行认证，认证成功后，用户才可以访问网络。

然而，在 VXLAN 网络中，配置了 VTEP 的接入设备通过等价多路径（英文：equal-cost multi-path routing；简称：ECMP）的方式向配置了 VTEP 的 SR 发送 VXLAN 报文，这样，就无法确定 SR 实际会通过哪个端口接收 VXLAN 报文，因此，无法预先在认证服务器中配置用于认证的信息，进而无法实现在 VXLAN 场景下根据用户的接入信息对用户进行认证。

发明内容

为了解决 VXLAN 场景下无法实现根据用户的接入信息对用户进行认证的问题，本发明提供了一种接入控制方法、装置及系统。所述技术方案如下：

第一方面，提供了一种接入控制方法，用于虚拟可扩展局域网 VXLAN 中的业务路由器，所述 VXLAN 还包括接入设备，所述方法包括：

接收所述接入设备发送的 VXLAN 请求报文，所述 VXLAN 请求报文是由用户发送的因特网协议 IP 请求报文封装得到的，所述 VXLAN 请求报文包括所述接入设备的 IP 地址以及所述用户的认证信息；

解析所述 VXLAN 请求报文，得到所述接入设备的 IP 地址以及所述用户的认证信息；

将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服务器，以便于所述认证服务器对所述用户进行认证；

接收所述认证服务器发送的认证结果；

根据所述认证结果控制所述用户。

由于接入设备将用户发送的 IP 请求报文进行封装得到 VXLAN 请求报文，并将 VXLAN 请求报文发送至业务路由器，并由该业务路由器对 VXLAN 请求报文进行解析得到接入设备的 IP 地址以及用户的认证信息，然后将接入设备的 IP 地址和用户的认证信息发送至认证服务器对用户进行认证。由于在 VXLAN 中，每个用户对应的接入设备是唯一的，因此，能够预先在认证服务器中配置用于认证的用户对应的接入设备的 IP 地址以及用户的认证信息，从而实现 VXLAN 场景下根据用户的接入信息对用户进行认证。

进一步的，由于在 VLAN 中用户认证的过程中，需要接入设备在 IP 请求报文中加插 DHCP option 82 或 PPPoE option+才能确定用户的物理位置信息，所以用户认证的过程较复杂。本发明中，在进行认证的过程中，接入设备直接封装用户发送的 IP 请求报文，且 VXLAN 请求报文包括接入设备的 IP 地址，且接入设备的 IP 地址可以间接的反映用户的物理位置信息，所以本发明中用户认证的过程较简单。

现有技术中，由于用户名和密码能够被用户篡改，所以用户认证的可靠性较低；本发明中对接入设备的 IP 地址进行认证，由于 VXLAN 请求报文中的外层源 IP 地址为接入设备添加的，无法被用户篡改，因此，用户认证的可靠性较高。

可选的，所述根据所述认证结果控制所述用户，包括：

在所述认证结果指示认证成功时，允许所述用户接入网络；

在所述认证结果指示认证失败时，禁止所述用户接入网络。

可选的，所述方法还包括：

在所述认证结果指示认证成功时，根据所述认证结果生成本地认证绑定表项，所述本地认证绑定表项包括所述接入设备的 IP 地址以及所述用户的认证信息。

可选的，所述方法还包括：

接收 VXLAN 业务报文，所述 VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

解析所述 VXLAN 业务报文，得到所述 IP 业务报文以及所述 VXLAN 业务报文的 VXLAN 头中外层源 IP 地址；

根据所述本地认证绑定表项处理所述 IP 业务报文。

可选的, 所述根据所述本地认证绑定表项处理所述 IP 业务报文, 包括:

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址相同时, 转发所述 IP 业务报文;

5 在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址不
相同时, 禁止转发所述 IP 业务报文。

进一步的, 由于在认证结果指示认证成功时, 根据认证结果生成包括接入设备的 IP 地址以及用户的认证信息的本地认证绑定表项, 使得业务路由器在接收到 VXLAN 业务报文后, 解析 VXLAN 业务报文, 得到 IP 业务报文以及 VXLAN 业务报文中的外层源 IP 地址 (即封装 IP 业务报文的接入设备的 IP 地址), 并根据本地认证绑定表项处理 IP 业务报
10 文。即通过判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相同, 来确定 IP 业务报文是否安全。在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同时, 确定 IP 业务报文安全, 转发 IP 业务报文; 在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不相同, 确定 IP 业务报文不安全, 禁止转发 IP 业务报文, 保证了网络的安全性。又由于 VXLAN 业务报文中的外层源 IP 地址
15 为接入设备添加的, 无法被用户篡改, 因此, 安全绑定检查的可靠性较高。

可选的, 将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服务器, 包括:

生成包括所述接入设备的 IP 地址以及所述用户的认证信息的认证报文;

将所述认证报文发送至所述认证服务器。

20 可选的, 所述认证服务器为远程认证拨号用户服务器 RADIUS,
所述认证报文的 87 号属性字段包括所述接入设备的 IP 地址。

第二方面, 提供了一种接入控制装置, 用于虚拟可扩展局域网 VXLAN, 所述 VXLAN 还包括接入设备, 所述接入控制装置包括:

25 第一接收模块, 用于接收所述接入设备发送的 VXLAN 请求报文, 所述 VXLAN 请求报
文是由用户发送的因特网协议 IP 请求报文封装得到的, 所述 VXLAN 请求报文包括所述接入设备的 IP 地址以及所述用户的认证信息;

第一解析模块, 用于解析所述 VXLAN 请求报文, 得到所述接入设备的 IP 地址以及所述用户的认证信息;

30 发送模块, 用于将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服
务器, 以便于所述认证服务器对所述用户进行认证;

第二接收模块, 用于接收所述认证服务器发送的认证结果;

控制模块, 用于根据所述认证结果控制所述用户。

可选的, 所述控制模块还用于:

在所述认证结果指示认证成功时, 允许所述用户接入网络;

35 在所述认证结果指示认证失败时, 禁止所述用户接入网络。

可选的, 所述接入控制装置还包括:

生成模块, 用于在所述认证结果指示认证成功时, 根据所述认证结果生成本地认证绑定表项, 所述本地认证绑定表项包括所述接入设备的 IP 地址以及所述用户的认证信息。

可选的，所述接入控制装置还包括：

第三接收模块，用于接收 VXLAN 业务报文，所述 VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

第二解析模块，用于解析所述 VXLAN 业务报文，得到所述 IP 业务报文以及所述 VXLAN 业务报文的 VXLAN 头中外层源 IP 地址；

处理模块，用于根据所述本地认证绑定表项处理所述 IP 业务报文。

可选的，所述处理模块还用于：

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址相同时，转发所述 IP 业务报文；

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址不

相同时，禁止转发所述 IP 业务报文。

可选的，所述发送模块还用于：

生成包括所述接入设备的 IP 地址以及所述用户的认证信息的认证报文；

将所述认证报文发送至所述认证服务器。

可选的，所述认证服务器为远程认证拨号用户服务器 RADIUS，

所述认证报文的 87 号属性字段包括所述接入设备的 IP 地址。

第三方面，提供了一种接入控制系统，所述接入控制系统包括：虚拟可扩展局域网 VXLAN 和认证服务器，所述 VXLAN 包括：接入设备和业务路由器，

所述业务路由器包括：第二方面所述的接入控制装置。

第四方面，提供了一种接入控制装置，用于虚拟可扩展局域网 VXLAN，所述 VXLAN 还包括接入设备，所述接入控制装置包括：至少一个处理器、至少一个网络接口、存储器和至少一个通信总线，所述处理器用于执行所述存储器中存储的程序，所述程序包括：

接收所述接入设备发送的 VXLAN 请求报文，所述 VXLAN 请求报文是由用户发送的因特网协议 IP 请求报文封装得到的，所述 VXLAN 请求报文包括所述接入设备的 IP 地址以及所述用户的认证信息；

解析所述 VXLAN 请求报文，得到所述接入设备的 IP 地址以及所述用户的认证信息；

将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服务器，以便于所述认证服务器对所述用户进行认证；

接收所述认证服务器发送的认证结果；

根据所述认证结果控制所述用户。

可选的，所述根据所述认证结果控制所述用户，包括：

在所述认证结果指示认证成功时，允许所述用户接入网络；

在所述认证结果指示认证失败时，禁止所述用户接入网络。

可选的，所述程序还包括：

在所述认证结果指示认证成功时，根据所述认证结果生成本地认证绑定表项，所述本地认证绑定表项包括所述接入设备的 IP 地址以及所述用户的认证信息。

可选的，所述程序还包括：

接收 VXLAN 业务报文，所述 VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

解析所述 VXLAN 业务报文,得到所述 IP 业务报文以及所述 VXLAN 业务报文的 VXLAN 头中外层源 IP 地址;

根据所述本地认证绑定表项处理所述 IP 业务报文。

可选的,所述根据所述本地认证绑定表项处理所述 IP 业务报文,包括:

5 在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址相同时,转发所述 IP 业务报文;

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址不
相同时,禁止转发所述 IP 业务报文。

10 可选的,将所述接入设备的 IP 地址以及所述用户的认证信息发送至所述认证服务器,包括:

生成包括所述接入设备的 IP 地址以及所述用户的认证信息的认证报文;

将所述认证报文发送至所述认证服务器。

可选的,所述认证服务器为远程认证拨号用户服务器 RADIUS,
所述认证报文的 87 号属性字段包括所述接入设备的 IP 地址。

15 第五方面,提供了一种接入控制系统,所述接入控制系统包括:虚拟可扩展局域网 VXLAN 和认证服务器,所述 VXLAN 包括:接入设备和业务路由器,

所述业务路由器包括:第四方面所述的接入控制装置。

综上所述,本发明提供了一种接入控制方法、装置及系统,在接入控制方法中,接入设备将用户发送的 IP 请求报文进行封装得到 VXLAN 请求报文,并将 VXLAN 请求报文
20 发送至业务路由器,并由该业务路由器对 VXLAN 请求报文进行解析得到接入设备的 IP 地址以及用户的认证信息,然后将接入设备的 IP 地址和用户的认证信息发送至认证服务器对用户进行认证。由于在 VXLAN 中,每个用户对应的接入设备是唯一的,因此,能够预先在认证服务器中配置用于认证的用户对应的接入设备的 IP 地址以及用户的认证信息,从而实现 VXLAN 场景下根据用户的接入信息对用户进行认证。

25 进一步的,由于在认证结果指示认证成功时,根据认证结果生成包括接入设备的 IP 地址以及用户的认证信息的本地认证绑定表项,使得业务路由器在接收到 VXLAN 业务报文后,解析 VXLAN 业务报文,得到 IP 业务报文以及 VXLAN 业务报文中的外层源 IP 地址(即封装 IP 业务报文的接入设备的 IP 地址),并根据本地认证绑定表项处理 IP 业务报文。即通过判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相
30 同,来确定 IP 业务报文是否安全。在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同时,确定 IP 业务报文安全,转发 IP 业务报文;在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不相同时,确定 IP 业务报文不安全,禁止转发 IP 业务报文,保证了网络的安全性。又由于 VXLAN 请求报文和 VXLAN 业务报文中的外层源 IP 地址均为接入设备添加的,无法被用户篡改,因此,用户认证以及安全
35 绑定检查的可靠性均较高。

附图说明

为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍。

图 1 为现有技术提供的一种 VXLAN 的结构示意图；

图 2 为本发明实施例提供的一种接入控制方法的应用场景示意图；

图 3 为本发明实施例提供的一种接入控制方法的方法流程图；

图 4-1 为本发明实施例提供的另一种接入控制方法的方法流程图；

5 图 4-2 为本发明实施例提供的一种 VXLAN 请求报文的结构示意图；

图 4-3 为本发明实施例提供的一种发送 IP 业务报文的方法流程图；

图 5-1 为本发明实施例提供的一种接入控制装置的结构示意图；

图 5-2 为本发明实施例提供的另一种接入控制装置的结构示意图；

图 5-3 为本发明实施例提供的又一种接入控制装置的结构示意图；

10 图 6 为本发明实施例提供的一种接入控制系统的结构示意图；

图 7 为本发明实施例提供的再一种接入控制装置的结构示意图。

具体实施方式

15 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

图 2 为本发明实施例提供的一种接入控制方法的应用场景示意图。如图 2 所示，VXLAN 2 包括：接入设备 21、业务路由器 22。其中，接入设备 21 可以为接入交换机或者接入路由器，该业务路由器可以为宽带网络网关（英文：broadband network gateway；简称：BNG）或宽带远程接入服务器（英文：broadband remote access server；简称：BRAS），或其他具有认证功能的网关。用户能够登录在用户设备 3 上，用户设备 3 接入接入设备 21，接入设备 21 接入业务路由器 22，业务路由器 22 可以同时接入认证服务器 1 和网络（图 2 中未示出）。示例的，该网络可以为与用户设备 3 进行通信的其他用户设备所在的目标网络，或者接入该目标网络的核心网络。认证服务器 1 可以为远程认证拨号用户服务器（英文：Remote Access Dial-In User Service；简称：RADIUS）。

25

如图 3 所示，本发明实施例提供了一种接入控制方法，该接入控制方法可以用于图 2 中的业务路由器 22，该接入控制方法可以包括：

步骤 301、接收接入设备发送的 VXLAN 请求报文，VXLAN 请求报文是由用户发送的 IP 请求报文封装得到的，VXLAN 请求报文包括接入设备的 IP 地址以及用户的认证信息。

30 步骤 302、解析 VXLAN 请求报文，得到接入设备的 IP 地址以及用户的认证信息。

步骤 303、将接入设备的 IP 地址以及用户的认证信息发送至认证服务器，以便于认证服务器对用户进行认证。

步骤 304、接收认证服务器发送的认证结果。

步骤 305、根据认证结果控制用户。

35 其中，步骤 305 可以包括：在认证结果指示认证成功时，允许用户接入网络；在认证结果指示认证失败时，禁止用户接入网络。

为了实现本发明，需要预先在认证服务器上配置认证规则，每条认证规则包括接入设备的 IP 地址以及至少一种用户信息，用户信息为能够唯一标识一个用户的信息，例如，用户名、密码等。此外，每条认证规则还可以包括用户的 VXLAN 标识等其他信息。

综上所述，由于本发明实施例提供的接入控制方法中，接入设备将用户发送的 IP 请求报文进行封装得到 VXLAN 请求报文，并将 VXLAN 请求报文发送至业务路由器，并由该业务路由器对 VXLAN 请求报文进行解析得到接入设备的 IP 地址以及用户的认证信息，然后将接入设备的 IP 地址和用户的认证信息发送至认证服务器对用户进行认证。由于在 VXLAN 中，每个用户对应的接入设备是唯一的，因此，能够预先在认证服务器中配置用于认证的用户对应的接入设备的 IP 地址以及用户的认证信息，从而实现 VXLAN 场景下根据用户的接入信息对用户进行认证。

可选的，该接入控制方法还可以包括：

在所述认证结果指示认证成功时，根据所述认证结果生成本地认证绑定表项，所述本地认证绑定表项包括所述接入设备的 IP 地址以及所述用户的认证信息。

可选的，该接入控制方法还可以包括：

接收 VXLAN 业务报文，所述 VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

解析所述 VXLAN 业务报文，得到所述 IP 业务报文以及所述 VXLAN 业务报文的 VXLAN 头中外层源 IP 地址；

根据所述本地认证绑定表项处理所述 IP 业务报文。

可选的，所述根据所述本地认证绑定表项处理所述 IP 业务报文，包括：

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址相同时，转发所述 IP 业务报文；

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址不相同时，禁止转发所述 IP 业务报文。

可选的，步骤 303 可以包括：

生成包括所述接入设备的 IP 地址以及所述用户的认证信息的认证报文；

将所述认证报文发送至所述认证服务器。

可选的，所述认证服务器为远程认证拨号用户服务器 RADIUS，所述认证报文的 87 号属性字段包括所述接入设备的 IP 地址。

综上所述，由于本发明实施例提供的接入控制方法中，接入设备将用户发送的 IP 请求报文进行封装得到 VXLAN 请求报文，并将 VXLAN 请求报文发送至业务路由器，并由该业务路由器对 VXLAN 请求报文进行解析得到接入设备的 IP 地址以及用户的认证信息，然后将接入设备的 IP 地址和用户的认证信息发送至认证服务器对用户进行认证。由于在 VXLAN 中，每个用户对应的接入设备是唯一的，因此，能够预先在认证服务器中配置用于认证的用户对应的接入设备的 IP 地址以及用户的认证信息，从而实现 VXLAN 场景下根据用户的接入信息对用户进行认证。

进一步的，由于在认证结果指示认证成功时，根据认证结果生成包括接入设备的 IP 地址以及用户的认证信息的本地认证绑定表项，使得业务路由器在接收到 VXLAN 业务报文后，解析 VXLAN 业务报文，得到 IP 业务报文以及 VXLAN 业务报文中的外层源 IP 地址（即封装 IP 业务报文的接入设备的 IP 地址），并根据本地认证绑定表项处理 IP 业务报文。即通过判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相同，来确定 IP 业务报文是否安全。在外层源 IP 地址与本地认证绑定表项中记录的接入

设备的 IP 地址相同时，确定 IP 业务报文安全，转发 IP 业务报文；在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不不同时，确定 IP 业务报文不安全，禁止转发 IP 业务报文，保证了网络的安全性。又由于 VXLAN 请求报文和 VXLAN 业务报文中的外层源 IP 地址均为接入设备添加的，无法被用户篡改，因此，用户认证以及安全绑定检查的可靠性均较高。

如图 4-1 所示，本发明实施例提供了另一种接入控制方法，该接入控制方法以用户为合法用户为例进行解释说明，该接入控制方法可以包括：

步骤 401、用户设备向接入设备发送 IP 请求报文。

10 用户设备接入接入设备，接入设备接入业务路由器，业务路由器可以同时接入认证服务器和网络，示例的，该网络可以为与该用户设备进行通信的其他用户设备所在的目标网络，或者接入该目标网络的核心网络，该目标网络可以为因特网（英文：Internet）。

用户可以在用户设备上输入用户名和密码，使得用户设备生成包括用户的认证信息（例如，用户名和密码）的 IP 请求报文，并将生成的 IP 请求报文发送至用户设备接入的接入设备。示例的，用户名和密码可以是预先分配给用户的，用户设备生成的 IP 请求报文的具体结构可以参考在 VLAN 中用户设备生成的 IP 请求报文的具体结构，本发明实施例在此不作赘述。

步骤 402、接入设备封装 IP 请求报文，得到 VXLAN 请求报文。

20 接入设备在接收到用户设备发送的 IP 请求报文后，接入设备可以采用将 MAC 地址封装在 UDP 中的封装方式封装该 IP 请求报文，从而得到 VXLAN 请求报文，且该 VXLAN 请求报文可以包括该接入设备的 IP 地址、用户的认证信息（例如，用户名和密码）以及该接入设备所在的 VXLAN 的标识。

图 4-2 为本发明实施例提供的一种 VXLAN 请求报文的结构示意图，如图 4-2 所示，该 VXLAN 请求报文可以依次包括：外层 Ethernet 头（英文：outer Ethernet header）封装部分、外层 IP 头（英文：outer IP header）封装部分、外层 UDP 头（英文：outer UDP header）封装部分、VXLAN 头（英文：VXLAN header）封装部分以及 IP 请求报文。

Outer Ethernet header 封装部分可以依次包括：目的 MAC 地址（英文：MAC DA）字段、源 MAC 地址（英文：MAC SA）字段、VLAN 类型（英文：VLAN type）字段、VLAN 标识（英文：VLAN identifier；简称：VLAN ID）字段和以太网类型（英文：Ethernet type）字段。其中，MAC DA 字段表示：目的虚拟机所属 VTEP 上路由表中直连的下一跳 MAC 地址；MAC SA 字段表示：发送 VXLAN 请求报文的虚拟机所属 VTEP 的 MAC 地址；当 IP 请求报文中携带 VLAN Tag（标签）时，VLAN Type 字段的取值为 0x8100；当 Ethernet Type 字段对应的协议报文为 IP 协议报文时，Ethernet Type 字段的取值为 0x0800。

35 Outer IP header 封装部分可以依次包括：前空闲字段、协议（英文：protocol）字段、后空闲字段、源 IP 地址（英文：IP SA）字段和目的 IP 地址（英文：IP DA）字段。其中，IP SA 字段表示接入设备的 IP 地址；IP DA 字段表示业务路由器的 IP 地址。

Outer UDP header 封装部分可以依次包括：源端口（英文：source port）字段、目的端口（英文：destport）字段、UDP 长度（英文：UDP length）字段和 UDP 校验和（英文：UDP checksum）字段。其中，destport 字段所指示的端口号可以为 4789，source

port 字段所指示的源端口号可以通过对 IP 请求报文采用哈希算法进行计算得来。

VXLAN header 封装部分依次包括：VXLAN 标记（英文：VXLAN flags）字段、前预留（英文：reserved）字段、VXLAN 标识（英文：VXLAN identifier；简称：VNI）字段和后 reserved 字段，其中，VNI 字段可以包括接入设备所在的 VXLAN 的标识。

- 5 IP 请求报文依次包括：内层以太网头（英文：inner Ethernet header）字段、内层 IP 头（英文：inner IP header）字段和有效载荷（英文：payload）字段。其中，Payload 字段包括用户输入的用户名和密码。

步骤 403、接入设备向业务路由器发送 VXLAN 请求报文。

- 10 接入设备在将用户设备发送的 IP 请求报文进行封装并得到 VXLAN 请求报文后，接入设备可以将包含接入设备的 IP 地址、VXLAN 的标识以及用户的认证信息的 VXLAN 请求报文发送至业务路由器。

步骤 404、业务路由器解析 VXLAN 请求报文，得到接入设备的 IP 地址、VXLAN 的标识以及用户的认证信息。

- 15 业务路由器在接收到 VXLAN 请求报文后，可以解析该 VXLAN 请求报文，得到该 VXLAN 请求报文中包括的接入设备的 IP 地址、用户名、密码和 VXLAN 的标识。例如，从 VXLAN 请求报文中的 Outer IP header 封装部分得到接入设备的 IP 地址，从 VXLAN 请求报文中的 VXLAN header 封装部分得到接入设备所在的 VXLAN 的标识，从 VXLAN 请求报文中的 IP 请求报文得到用户名和密码。

- 20 步骤 405、业务路由器生成包含接入设备的 IP 地址、VXLAN 的标识以及用户的认证信息的认证报文。

- 示例的，当认证服务器可以为 RADIUS 时，该业务路由器可以根据 RADIUS 协议、接入设备的 IP 地址、用户名、密码和 VXLAN 的标识，生成包括接入设备的 IP 地址、用户名、密码和 VXLAN 的标识的认证报文，具体的，生成的认证报文的具体结构可以参考现有技术中根据 RADIUS 协议生成的认证报文的具体结构。示例的，该认证报文的第 87 号属性字段可以包括接入设备的 IP 地址，该 87 号属性字段可以为网络附属存储端口标识（英文：network attached storage port identifier；简称：NAS-Port-Id）字段。

步骤 406、业务路由器向认证服务器发送认证报文。

- 30 由于业务路由器接入认证服务器，所以业务路由器可以将该认证报文发送至认证服务器，认证服务器可以为 RADIUS，需要说明的是，认证服务器还可以为除 RADIUS 外的其他认证服务器，本发明实施例对此不做限定。

步骤 407、认证服务器对认证报文进行认证。

- 35 具体的，认证服务器上可以预先配置有认证规则，每条认证规则包括接入设备的 IP 地址以及至少一种用户信息，用户信息为能够唯一标识一个用户的信息，例如，用户名、密码等。此外，每条认证规则还可以包括用户的 VXLAN 标识等其他信息。示例的，认证服务器上可以设置有助于记录认证规则的认证表项。

认证表项可以如表 1 所示，该认证表项中记录了两条认证规则。其中，第一条认证规则包括：ZHANGSAN（用户名）、110（密码）、A1（接入设备的 IP 地址）以及 VXLAN-B1（接入设备所在的 VXLAN 的标识）。第二条认证规则包括：LISI（用户名）、120（密码）、A2（接入设备的 IP 地址）以及 VXLAN-B2（接入设备所在的 VXLAN 的标识）。

表 1

用户名	密码	接入设备的 IP 地址	接入设备所在的 VXLAN 的标识
ZHANGSAN	110	A1	VXLAN-B1
LISI	120	A2	VXLAN-B2

认证服务器在接收到认证报文后,认证服务器能够获取认证报文中的接入设备的 IP 地址、用户名、密码和 VXLAN 的标识,并在认证服务器上的认证表项中查找该认证表项中是否存在一条认证规则同时包括该认证报文中的接入设备的 IP 地址、用户名、密码和 VXLAN 的标识。如果该认证表项中存在一条认证规则同时包括该认证报文中的接入设备的 IP 地址、用户名、密码和 VXLAN 的标识,则该认证服务器可以确定认证成功,并生成用于指示认证结果为认证成功的第一报文。如果该认证表项中不存在一条认证规则同时包括该认证报文中的接入设备的 IP 地址、用户名、密码和 VXLAN 的标识,则该认证服务器可以确定认证失败,并生成用于指示认证结果为认证失败的第二报文。

由于本发明实施例以用户为合法用户为例,所以认证服务器上的认证表项中存在一条认证规则同时包括该认证报文中的接入设备的 IP 地址、用户名、密码以及 VXLAN 标识,认证服务器可以生成用于指示认证结果为认证成功的第一报文。

步骤 408、认证服务器向业务路由器发送认证结果。

认证服务器在对该认证报文进行认证后,认证服务器可以将认证结果发送至业务路由器。示例的,该认证服务器可以将用于指示认证结果为认证成功的第一报文发送至业务路由器。

步骤 409、业务路由器控制用户设备接入目标网络。

由于本发明实施例中的用户为合法用户,所以,步骤 408 中认证服务器发送给业务路由器的认证结果指示认证成功,该业务路由器允许用户接入网络,并可以控制用户设备接入网络,以及通知用户认证成功且已接入网络。

需要说明的是,若认证结果指示认证成功,则在步骤 409 之后,该业务路由器可以根据认证结果生成本地认证绑定表项,该本地认证绑定表项可以包括认证成功的接入设备的 IP 地址以及用户的认证信息。示例的,该本地认证绑定表项可以如表 2 所示,表 2 中记录了第一用户的认证信息 C1 与接入设备的 IP 地址 A1 的对应关系,以及第二用户的认证信息 C2 与接入设备的 IP 地址 A2 的对应关系。可选的,表 2 中的用户的认证信息 C1 或 C2 可以包括用户名、密码、用户的 IP 地址等信息。

表 2

用户的认证信息	接入设备的 IP 地址
C1	A1
C2	A2

步骤 410、用户设备通过接入设备和业务路由器向网络发送 IP 业务报文。

在业务路由器控制用户设备接入网络后,用户设备可以生成 IP 业务报文,并通过接入设备和业务路由器将 IP 业务报文发送至目标网络。

如图 4-3 所示,步骤 410 可以包括:

步骤 4101、用户设备向接入设备发送 IP 业务报文。

在用户设备接入网络后，用户设备可以根据需要生成 IP 业务报文，并将生成的 IP 业务报文发送至用户设备接入的接入设备，该 IP 业务报文可以包括用户的至少一种认证信息，该至少一种认证信息可以包括用户的 IP 地址。需要说明的是，用户设备生成的 IP 业务报文的具体结构，可以参考在现有技术中用户设备生成的 IP 业务报文的具体结构，本发明实施例在此不作赘述。

步骤 4102、接入设备封装 IP 业务报文，得到 VXLAN 业务报文。

示例的，接入设备在接收到用户设备发送的 IP 业务报文后，接入设备可以采用将 MAC 地址封装在 UDP 中的封装方式封装该 IP 业务报文，得到 VXLAN 业务报文。需要说明的是，步骤 4102 中接入设备封装 IP 业务报文的具体方式可以参考步骤 402 中接入设备封装 IP 请求报文的具体方式，本发明实施例在此不做赘述。

步骤 4103、接入设备向业务路由器发送 VXLAN 业务报文。

接入设备在将用户设备发送的 IP 业务报文进行封装并得到 VXLAN 业务报文后，接入设备可以将 VXLAN 业务报文发送至业务路由器。

步骤 4104、业务路由器解析 VXLAN 业务报文，得到外层源 IP 地址以及 IP 业务报文。

业务路由器在接收到 VXLAN 业务报文后，可以解析该 VXLAN 业务报文，得到该 VXLAN 业务报文中的信息，如从 VXLAN 业务报文中的 Outer IP header 封装部分得到外层源 IP 地址，从 VXLAN 业务报文中的 IP 业务报文得到用户的 IP 地址。

步骤 4105、业务路由器判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相同。

一方面，在步骤 401 中用户设备发送至接入设备的 IP 请求报文中可以包括用户的 IP 地址，在步骤 404 中，业务路由器解析 VXLAN 请求报文还可以得到用户的 IP 地址。在步骤 408 之后，即在业务路由器接收到的认证结果指示认证成功之后，业务路由器建立的本地认证绑定表项中的认证信息中可以包括用户的 IP 地址。

另一方面，在步骤 401 中用户设备发送至接入设备的 IP 请求报文中可以不包括用户的 IP 地址，在步骤 404 中，业务路由器解析 VXLAN 请求报文无法得到用户的 IP 地址。在步骤 407 中，若认证成功，则认证服务器可以给用户分配一个 IP 地址，具体的，认证服务器发送至业务路由器的认证结果中可以包括分配给用户的 IP 地址。在步骤 408 中业务路由器接收到认证结果后，业务路由器可以将分配给用户的 IP 地址发送至用户设备，使得步骤 4101 中用户设备发送至接入设备的 IP 业务报文包括用户的 IP 地址，进一步的，该业务路由器还可以将分配给用户的 IP 地址存储在本地认证绑定表项中的认证信息中。

在步骤 4105 中，业务路由器可以根据步骤 4104 中解析得到的 IP 业务报文中的用户的认证信息（如用户的 IP 地址），在本地认证绑定表项中查找用户的 IP 地址对应的接入设备的 IP 地址，并判断步骤 4104 中解析得到的外层源 IP 地址与该本地认证绑定表项中的接入设备的 IP 地址是否相同，若外层源 IP 地址与该本地认证绑定表项中的接入设备的 IP 地址相同，则确定该 VXLAN 业务报文中的 IP 业务报文安全；若外层源 IP 地址与该本地认证绑定表项中的接入设备的 IP 地址不同，则确定该 VXLAN 业务报文中的 IP 业务报文不安全。

步骤 4106、在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同时，业务路由器向网络转发 IP 业务报文。

若外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同，则业务路由器可以确定解析得到的 IP 业务报文安全，并将解析得到的 IP 业务报文转发至网络，
5 示例的，可以将该 IP 业务报文转发至目标网络，或者将该 IP 业务报文转发至接入目标网络的核心网络，进而由核心网络将该 IP 业务报文转发至目标网络。

若用户为非法用户，则步骤 408 中认证服务器发送给业务路由器的认证结果指示认证失败，该业务路由器可以禁止用户接入网络，并通知用户认证失败。

需要说明的是，若用户为非法用户，一方面，在该业务路由器禁止用户接入网络后，
10 该非法用户仍然可以控制用户设备生成 IP 业务报文，并将生成的 IP 业务报文发送至接入设备，由接入设备封装用户设备生成的 IP 业务报文，得到 VXLAN 业务报文，并将 VXLAN 业务报文发送至业务路由器；另一方面，步骤 401 中用户设备可以不生成 IP 请求报文，而直接生成 IP 业务报文，并将生成的 IP 业务报文发送至接入设备，由接入设备封装 IP 业务报文得到 VXLAN 业务报文，并将 VXLAN 业务报文发送至业务路由器。

15 业务路由器在接收到 VXLAN 业务报文后，可以解析该 VXLAN 业务报文，并判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相同。由于用户为非法用户，所以外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不相同，该业务路由器可以确定 VXLAN 业务报文中的 IP 业务报文不安全，并禁止转发 IP 业务报文，保证了网络的安全性。

20 现有技术中，由于在 VLAN 中用户认证的过程中，需要接入设备在 IP 请求报文中加插 DHCP option82 或 PPPoE option+才能确定用户的物理位置信息，所以用户认证的过程较复杂。本发明中，在进行认证的过程中，接入设备直接封装用户发送的 IP 请求报文，且 VXLAN 请求报文包括接入设备的 IP 地址，且接入设备的 IP 地址可以间接的反映用户的物理位置信息，所以本发明中用户认证的过程较简单。且现有技术中，对用户输入的用户名和密码进行认证，由于用户名和密码能够被用户篡改，所以用户认证的可靠性较低；本发明中对接入设备的 IP 地址进行认证，由于 VXLAN 请求报文中的外层源 IP
25 地址为接入设备添加的，无法被用户篡改，因此，用户认证的可靠性较高。

综上所述，由于本发明实施例提供的接入控制方法中，接入设备将用户发送的 IP 请求报文进行封装得到 VXLAN 请求报文，并将 VXLAN 请求报文发送至业务路由器，并由
30 该业务路由器对 VXLAN 请求报文进行解析得到接入设备的 IP 地址以及用户的认证信息，然后将接入设备的 IP 地址和用户的认证信息发送至认证服务器对用户进行认证。由于在 VXLAN 中，每个用户对应的接入设备是唯一的，因此，能够预先在认证服务器中配置用于认证的用户对应的接入设备的 IP 地址以及用户的认证信息，从而实现 VXLAN 场景下根据用户的接入信息对用户进行认证。

35 进一步的，由于在认证结果指示认证成功时，根据认证结果生成包括接入设备的 IP 地址以及用户的认证信息的本地认证绑定表项，使得业务路由器在接收到 VXLAN 业务报文后，解析 VXLAN 业务报文，得到 IP 业务报文以及 VXLAN 业务报文中的外层源 IP 地址（即封装 IP 业务报文的接入设备的 IP 地址），并根据本地认证绑定表项处理 IP 业务报文。即通过判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相

同，来确定 IP 业务报文是否安全。在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同时，确定 IP 业务报文安全，转发 IP 业务报文；在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不相同，确定 IP 业务报文不安全，禁止转发 IP 业务报文，保证了网络的安全性。又由于 VXLAN 请求报文和 VXLAN 业务报文中的外层源 IP 地址均为接入设备添加的，无法被用户篡改，因此，用户认证以及安全绑定检查的可靠性均较高。

如图 5-1 所示，本发明实施例提供了一种接入控制装置 50，该接入控制装置 50 可以用于 VXLAN，VXLAN 还可以包括接入设备，该接入控制装置 50 可以包括：

第一接收模块 501，用于接收接入设备发送的 VXLAN 请求报文，VXLAN 请求报文是由用户发送的因特网协议 IP 请求报文封装得到的，VXLAN 请求报文包括接入设备的 IP 地址以及用户的认证信息。

第一解析模块 502，用于解析 VXLAN 请求报文，得到接入设备的 IP 地址以及用户的认证信息。

发送模块 503，用于将接入设备的 IP 地址以及用户的认证信息发送至认证服务器，以便于认证服务器对用户进行认证。

第二接收模块 504，用于接收认证服务器发送的认证结果。

控制模块 505，用于根据认证结果控制用户。

可选的，控制模块 505 还可以用于：

在认证结果指示认证成功时，允许用户接入网络；

在认证结果指示认证失败时，禁止用户接入网络。

如图 5-2 所示，在图 5-1 所示的基础上，该接入控制装置 50 还可以包括：

生成模块 506，用于在认证结果指示认证成功时，根据认证结果生成本地认证绑定表项，本地认证绑定表项包括接入设备的 IP 地址以及用户的认证信息。

如图 5-3 所示，在图 5-2 的基础上，该接入控制装置 50 可以包括：

第一接收模块 501，用于接收接入设备发送的 VXLAN 请求报文，VXLAN 请求报文是由用户发送的因特网协议 IP 请求报文封装得到的，VXLAN 请求报文包括接入设备的 IP 地址以及用户的认证信息。

第一解析模块 502，用于解析 VXLAN 请求报文，得到接入设备的 IP 地址以及用户的认证信息。

发送模块 503，用于将接入设备的 IP 地址以及用户的认证信息发送至认证服务器，以便于认证服务器对用户进行认证。

第二接收模块 504，用于接收认证服务器发送的认证结果。

控制模块 505，用于根据认证结果控制用户。

生成模块 506，用于在认证结果指示认证成功时，根据认证结果生成本地认证绑定表项，本地认证绑定表项包括接入设备的 IP 地址以及用户的认证信息。

第三接收模块 507，用于接收 VXLAN 业务报文，VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

第二解析模块 508，用于解析 VXLAN 业务报文，得到 IP 业务报文以及所述 VXLAN

业务报文的 VXLAN 头中外层源 IP 地址；

处理模块 509，用于根据本地认证绑定表项处理 IP 业务报文。

可选的，处理模块 509 还可以用于：

在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同时，转发 IP 业务报文；

在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不相同时，禁止转发 IP 业务报文。

可选的，发送模块 503 还可以用于：

生成包括接入设备的 IP 地址以及用户的认证信息的认证报文；

将认证报文发送至认证服务器。

可选的，认证服务器为远程认证拨号用户服务器 RADIUS，认证报文的 87 号属性字段包括接入设备的 IP 地址。

由于本发明实施例提供的接入控制装置中，第一接收模块接收的接入设备发送的 VXLAN 请求报文中包括接入设备的 IP 地址以及用户的认证信息，使得第一解析模块解析得到接入设备的 IP 地址以及用户的认证信息，然后发送模块将接入设备的 IP 地址和用户的认证信息发送至认证服务器对用户进行认证。由于在 VXLAN 中，每个用户对应的接入设备是唯一的，因此，能够预先在认证服务器中配置用于认证的用户对应的接入设备的 IP 地址以及用户的认证信息，从而实现对 VXLAN 场景下根据用户的接入信息对用户进行认证。

进一步的，由于在认证结果指示认证成功时，根据认证结果生成包括接入设备的 IP 地址以及用户的认证信息的本地认证绑定表项，使得业务路由器在接收到 VXLAN 业务报文后，解析 VXLAN 业务报文，得到 IP 业务报文以及 VXLAN 业务报文中的外层源 IP 地址（即封装 IP 业务报文的接入设备的 IP 地址），并根据本地认证绑定表项处理 IP 业务报文。即通过判断外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址是否相同，来确定 IP 业务报文是否安全。在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址相同时，确定 IP 业务报文安全，转发 IP 业务报文；在外层源 IP 地址与本地认证绑定表项中记录的接入设备的 IP 地址不相同时，确定 IP 业务报文不安全，禁止转发 IP 业务报文，保证了网络的安全性。又由于 VXLAN 请求报文和 VXLAN 业务报文中的外层源 IP 地址均为接入设备添加的，无法被用户篡改，因此，用户认证以及安全绑定检查的可靠性均较高。

如图 6 所示，本发明实施例提供了一种接入控制系统 60，该接入控制系统 60 可以包括：VXLAN 2 和认证服务器 1，VXLAN 2 可以包括：接入设备 21 和业务路由器 22，该业务路由器 22 可以包括图 5-1、图 5-2 或图 5-3 所示的接入控制装置。

图 7 描述了本发明实施例提供的再一种接入控制装置的结构，该接入控制装置可以用于 VXLAN，VXLAN 还包括：接入设备，该接入控制装置包括至少一个处理器 701（例如 CPU），至少一个网络接口 702 或者其他通信接口，存储器 703，和至少一个通信总线 704，用于实现这些装置之间的通信。处理器 701 用于执行存储器 703 中存储的可执行模块，

例如计算机程序。存储器 703 可能包括高速随机存取存储器（英文：random access memory，简称：RAM），也可能还包括非易失性存储器（英文：non-volatile memory），例如至少一个磁盘存储器。通过至少一个网络接口 702（可以是有线或者无线）实现该接入控制装置与至少一个其他网元之间的通信，可以使用互联网，广域网，本地网，城域网等。

在一些实施方式中，存储器 703 存储了程序 7031，程序 7031 可以被处理器 701 执行以实现图 3 或图 4-1 所示的方法。

需要说明的是，本发明实施例提供的接入控制方法步骤的先后顺序可以进行适当调整，步骤也可以根据情况进行相应增减，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，可轻易想到变化的方法，都应涵盖在本发明的保护范围之内，因此不再赘述。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的接入控制装置和接入控制系统的具体工作过程，可以参考前述接入控制方法实施例中的对应过程，在此不再赘述。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，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，均应包括在本发明的保护范围之内。

权利要求

1、一种接入控制方法，其特征在于，用于虚拟可扩展局域网 VXLAN 中的业务路由器，所述 VXLAN 还包括接入设备，所述方法包括：

5 接收所述接入设备发送的 VXLAN 请求报文，所述 VXLAN 请求报文是由用户发送的因特网协议 IP 请求报文封装得到的，所述 VXLAN 请求报文包括所述接入设备的 IP 地址以及所述用户的认证信息；

 解析所述 VXLAN 请求报文，得到所述接入设备的 IP 地址以及所述用户的认证信息；

10 将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服务器，以便于所述认证服务器对所述用户进行认证；

 接收所述认证服务器发送的认证结果；

 根据所述认证结果控制所述用户。

15 2、根据权利要求 1 所述的方法，其特征在于，所述根据所述认证结果控制所述用户，包括：

 在所述认证结果指示认证成功时，允许所述用户接入网络；

 在所述认证结果指示认证失败时，禁止所述用户接入网络。

3、根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

20 在所述认证结果指示认证成功时，根据所述认证结果生成本地认证绑定表项，所述本地认证绑定表项包括所述接入设备的 IP 地址以及所述用户的认证信息。

4、根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

25 接收 VXLAN 业务报文，所述 VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

 解析所述 VXLAN 业务报文，得到所述 IP 业务报文以及所述 VXLAN 业务报文的 VXLAN 头中外层源 IP 地址；

 根据所述本地认证绑定表项处理所述 IP 业务报文。

30 5、根据权利要求 4 所述的方法，其特征在于，所述根据所述本地认证绑定表项处理所述 IP 业务报文，包括：

 在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址相同时，转发所述 IP 业务报文；

35 在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址不
 相同时，禁止转发所述 IP 业务报文。

6、根据权利要求 1 至 5 任一所述的方法，其特征在于，将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服务器，包括：

 生成包括所述接入设备的 IP 地址以及所述用户的认证信息的认证报文；

将所述认证报文发送至所述认证服务器。

7、根据权利要求 6 所述的方法，其特征在于，所述认证服务器为远程认证拨号用户服务器 RADIUS，

5 所述认证报文的 87 号属性字段包括所述接入设备的 IP 地址。

8、一种接入控制装置，其特征在于，用于虚拟可扩展局域网 VXLAN，所述 VXLAN 还包括接入设备，所述接入控制装置包括：

10 第一接收模块，用于接收所述接入设备发送的 VXLAN 请求报文，所述 VXLAN 请求报文是由用户发送的因特网协议 IP 请求报文封装得到的，所述 VXLAN 请求报文包括所述接入设备的 IP 地址以及所述用户的认证信息；

第一解析模块，用于解析所述 VXLAN 请求报文，得到所述接入设备的 IP 地址以及所述用户的认证信息；

15 发送模块，用于将所述接入设备的 IP 地址以及所述用户的认证信息发送至认证服务器，以便于所述认证服务器对所述用户进行认证；

第二接收模块，用于接收所述认证服务器发送的认证结果；

控制模块，用于根据所述认证结果控制所述用户。

20 9、根据权利要求 8 所述的接入控制装置，其特征在于，所述控制模块还用于：在所述认证结果指示认证成功时，允许所述用户接入网络；在所述认证结果指示认证失败时，禁止所述用户接入网络。

10、根据权利要求 9 所述的接入控制装置，其特征在于，所述接入控制装置还包括：生成模块，用于在所述认证结果指示认证成功时，根据所述认证结果生成本地认证
25 绑定表项，所述本地认证绑定表项包括所述接入设备的 IP 地址以及所述用户的认证信息。

11、根据权利要求 10 所述的接入控制装置，其特征在于，所述接入控制装置还包括：
30

第三接收模块，用于接收 VXLAN 业务报文，所述 VXLAN 业务报文是由用户发送的 IP 业务报文封装得到的；

第二解析模块，用于解析所述 VXLAN 业务报文，得到所述 IP 业务报文以及所述 VXLAN 业务报文的 VXLAN 头中外层源 IP 地址；

处理模块，用于根据所述本地认证绑定表项处理所述 IP 业务报文。
35

12、根据权利要求 11 所述的接入控制装置，其特征在于，所述处理模块还用于：在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址相同时，转发所述 IP 业务报文；

在所述外层源 IP 地址与所述本地认证绑定表项中记录的所述接入设备的 IP 地址不

相同时，禁止转发所述 IP 业务报文。

13、根据权利要求 8 至 12 任一所述的接入控制装置，其特征在于，所述发送模块还用于：

- 5 生成包括所述接入设备的 IP 地址以及所述用户的认证信息的认证报文；
 将所述认证报文发送至所述认证服务器。

14、根据权利要求 13 所述的接入控制装置，其特征在于，所述认证服务器为远程认证拨号用户服务器 RADIUS，

- 10 所述认证报文的 87 号属性字段包括所述接入设备的 IP 地址。

15、一种接入控制系统，其特征在于，所述接入控制系统包括：虚拟可扩展局域网 VXLAN 和认证服务器，所述 VXLAN 包括：接入设备和业务路由器，

 所述业务路由器包括：权利要求 8 至 14 任一所述的接入控制装置。

15

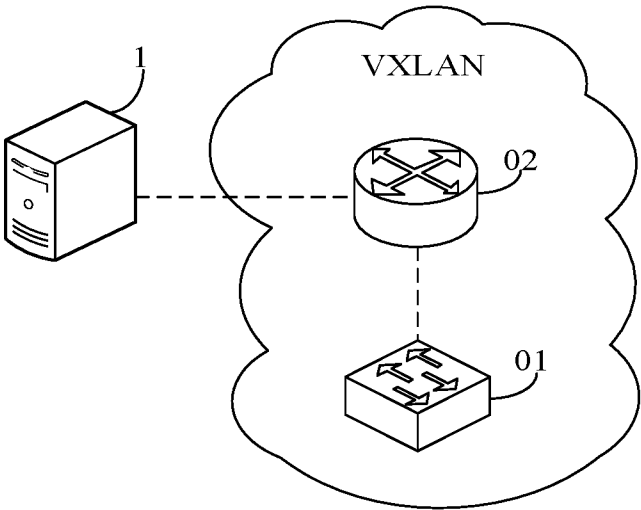


图 1

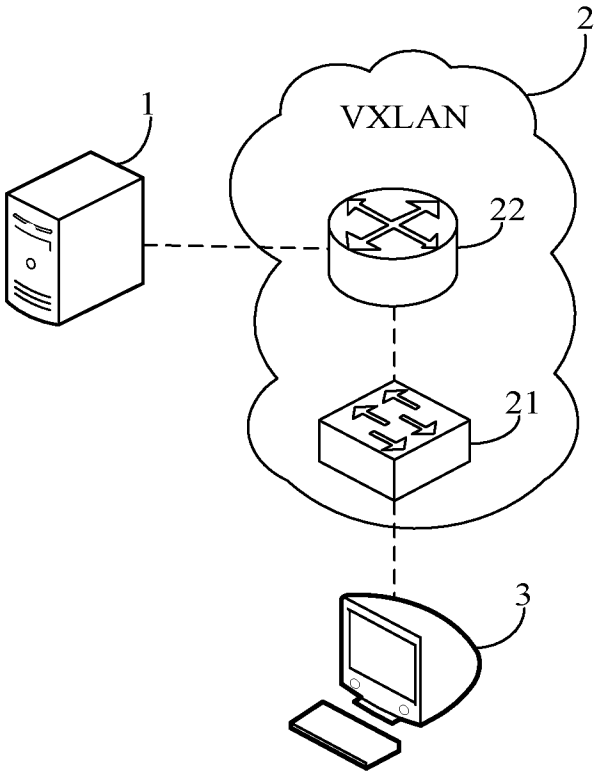


图 2

2/6

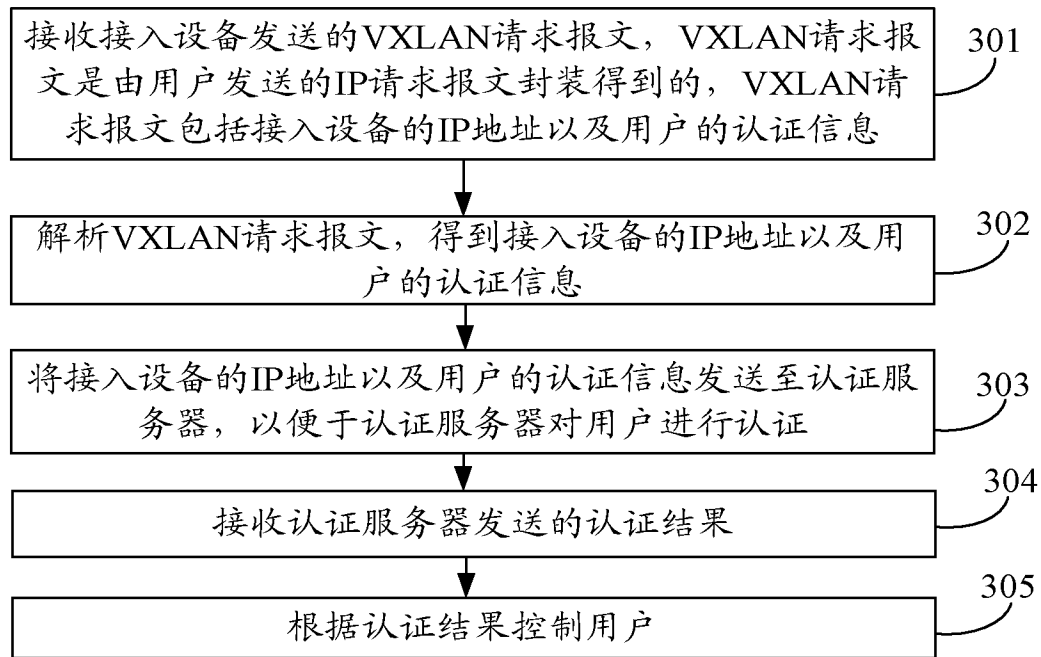


图 3

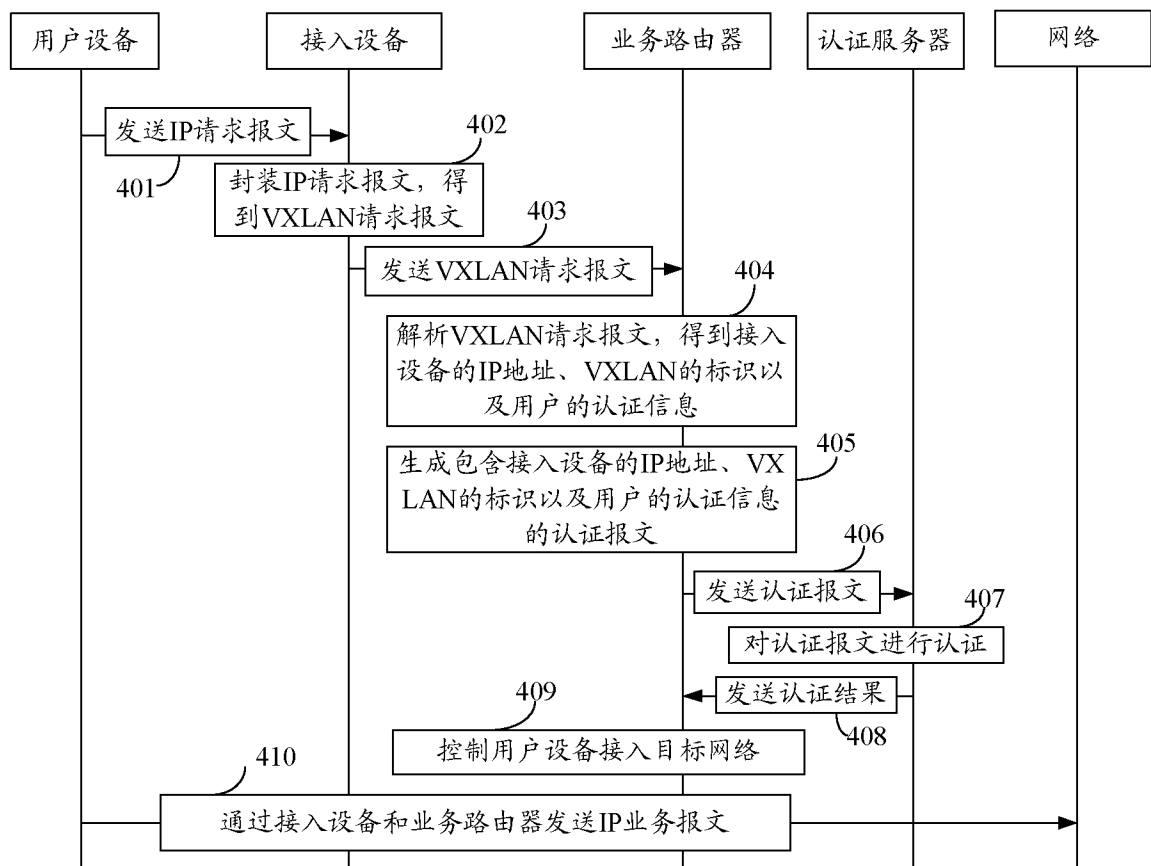


图 4-1

3/6

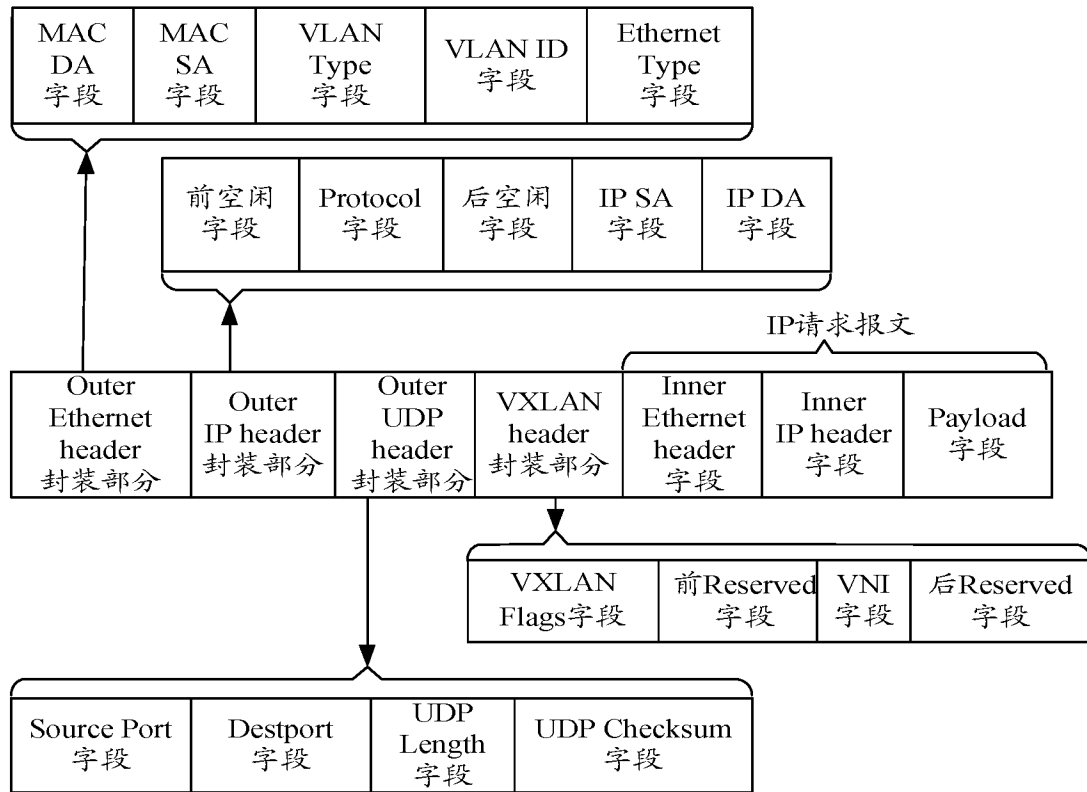


图 4-2

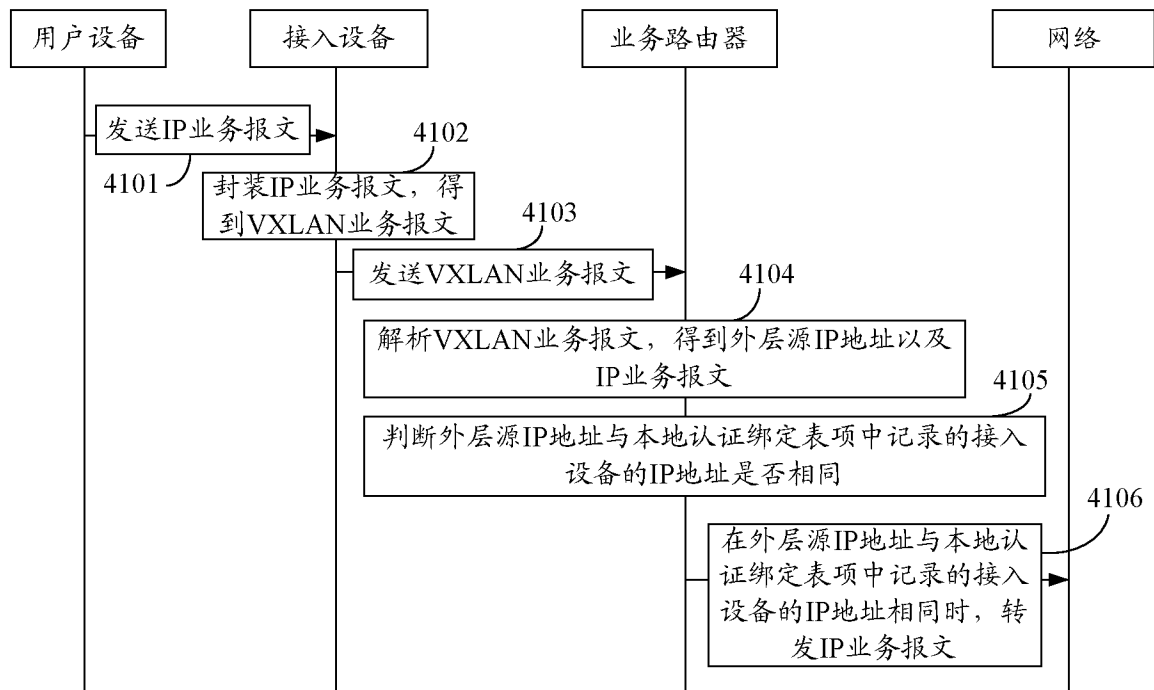


图 4-3

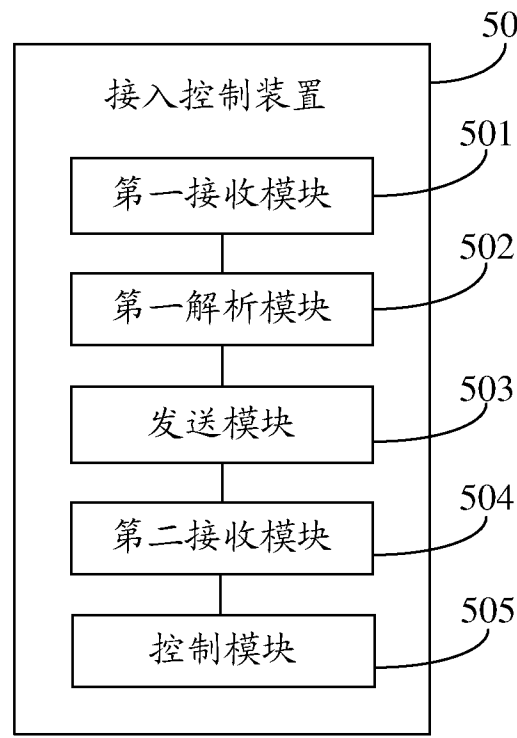


图 5-1

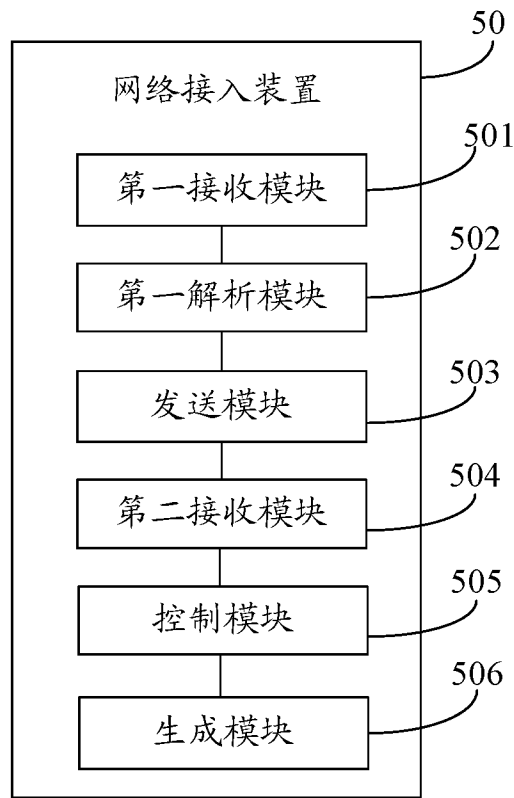


图 5-2

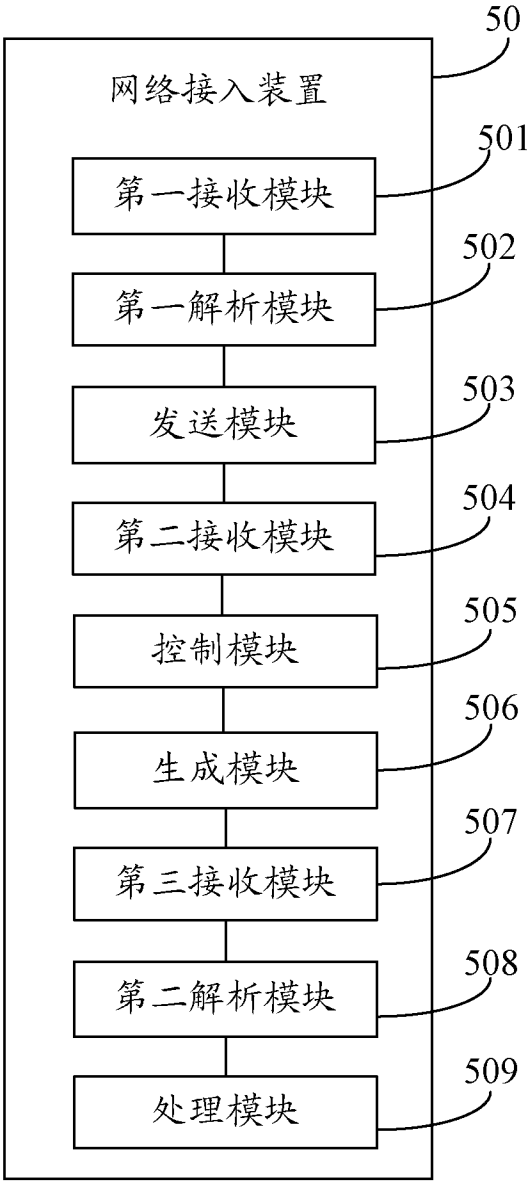


图 5-3

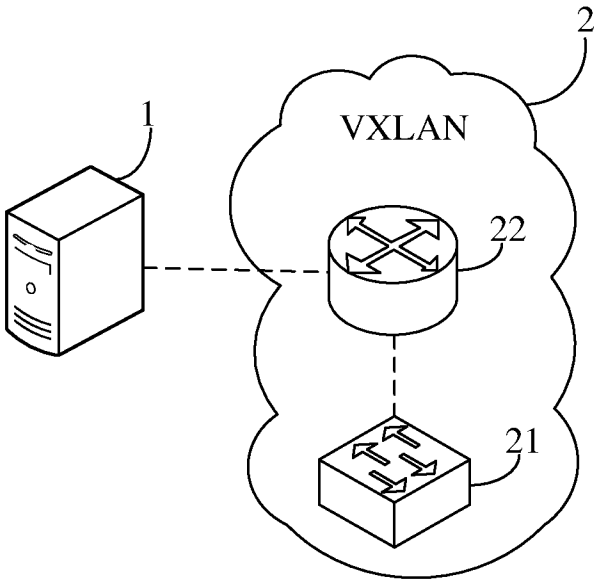


图 6

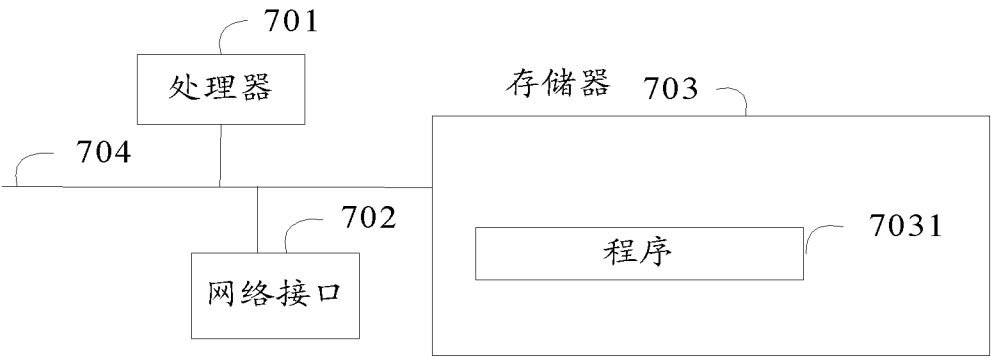


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/072904

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/46 (2006.01) i; H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: extensible VLAN, VXLAN, VLAN, LAN, BRAS, BNG, Ethernet, IP, ethernet, service, access, router, AP, node, switch, RADIUS, authentication, request, point, bind, IP address, server, service route, access router, access device, access node, access switch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102857517 A (HUAWEI TECHNOLOGIES CO., LTD.) 02 January 2013 (02.01.2013) description, paragraphs [0052]-[0130]	1-15
Y	CN 101436934 A (FUJIAN STAR-NET NETWORK CO., LTD.) 20 May 2009 (20.05.2009) description, page 5, line 10 to page 7, line 24, and figure 1	1-15
A	CN 103209159 A (CHINA TELECOM CORPORATION LTD.) 17 July 2013 (17.07.2013) the whole document	1-15
A	CN 101043331 A (HUAWEI TECHNOLOGIES CO., LTD.) 26 September 2007 (26.09.2007) the whole document	1-15

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 31 March 2017	Date of mailing of the international search report 24 April 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer BI, Yachao Telephone No. (86-10) 62413310

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/CN2017/072904

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101789906 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 28 July 2010 (28.07.2010) the whole document	1-15
A	US 2016036771 A1 (ARUBA NETWORKS INC.) 04 February 2016 (04.02.2016) the whole document	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/072904

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102857517 A	02 January 2013	None	
CN 101436934 A	20 May 2009	None	
CN 103209159 A	17 July 2013	None	
CN 101043331 A	26 September 2007	None	
CN 101789906 A	28 July 2010	None	
US 2016036771 A1	04 February 2016	None	

A. 主题的分类 H04L 12/46 (2006.01) i; H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT, CNKI, WPI, EPODOC: 虚拟可扩展局域网, 可扩展虚拟局域网, 扩展 VLAN, 虚拟局域网, 局域网, 以太网, VXLAN, VLAN, LAN, 宽带远程接入服务器, BRAS, 宽带网络网关, BNG, 业务路由器, 接入路由器, 接入设备, 接入节点, 接入点, 接入交换机, 接入, 认证, 请求, IP 地址, 绑定, ethernet, service, access, router, AP, node, switch, RADIUS, authentication, request, point, bind, IP address, server		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 102857517 A (华为技术有限公司) 2013年 1月 2日 (2013 - 01 - 02) 说明书第[0052]-[0130]段	1-15
Y	CN 101436934 A (福建星网锐捷网络有限公司) 2009年 5月 20日 (2009 - 05 - 20) 说明书第5页第10行至第7页第24行, 图1	1-15
A	CN 103209159 A (中国电信股份有限公司) 2013年 7月 17日 (2013 - 07 - 17) 全文	1-15
A	CN 101043331 A (华为技术有限公司) 2007年 9月 26日 (2007 - 09 - 26) 全文	1-15
A	CN 101789906 A (杭州华三通信技术有限公司) 2010年 7月 28日 (2010 - 07 - 28) 全文	1-15
A	US 2016036771 A1 (ARUBA NETWORKS INC.) 2016年 2月 4日 (2016 - 02 - 04) 全文	1-15
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2017年 3月 31日		国际检索报告邮寄日期 2017年 4月 24日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 毕雅超 电话号码 (86-10) 62413310

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/072904

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	102857517	A	2013年 1月 2日	无	
CN	101436934	A	2009年 5月 20日	无	
CN	103209159	A	2013年 7月 17日	无	
CN	101043331	A	2007年 9月 26日	无	
CN	101789906	A	2010年 7月 28日	无	
US	2016036771	A1	2016年 2月 4日	无	