(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
2020 年 6 月 4 日 (04.06.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/108531 A1

(51) 国际专利分类号:
H04L 12/46 (2006.01)

(21) 国际申请号: PCT/CN2019/121267

(22) 国际申请日: 2019 年 11 月 27 日 (27.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811426641.8 2018年11月27日 (27.11.2018) CN

(71) 申请人: 新华三技术有限公司 (**NEW H3C TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国浙江省杭州市滨江区长河路 466 号, Zhejiang 310052 (CN)。

(72) 发明人: 程剑锋 (**CHENG, Jianfeng**); 中国北京市朝阳区广顺南大街8号院1号楼利星行中心A座640室, Beijing 100102 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (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, JO, 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,

WO 2020/108531 A1

(54) **Title:** PACKET FORWARDING

(54) 发明名称: 报文转发

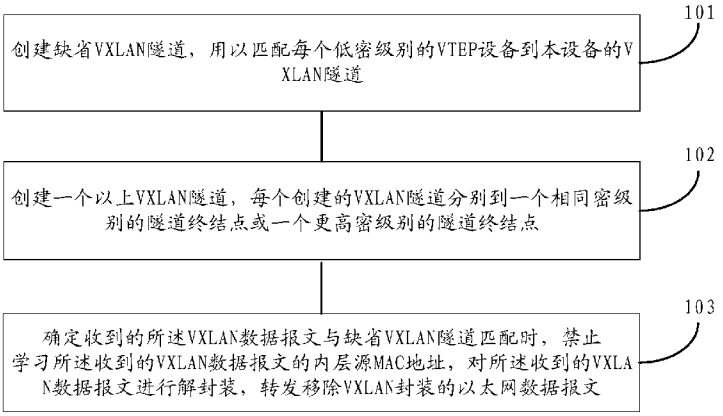

图 1

101 Establish a default VXLAN tunnel for matching a VXLAN tunnel from each VTEP device of a low encryption level to the present device
102 Establish more than one VXLAN tunnel, each established VXLAN tunnel connecting to a tunnel endpoint of the same encryption level or a tunnel endpoint of a higher encryption level, respectively
103 When it is determined that the received VXLAN data packet matches the default VXLAN tunnel, prohibit from learning an inner source MAC address of the received VXLAN data packet, decapsulate the received VXLAN data packet, and forward an Ethernet data packet having the VXLAN encapsulation removed

(57) **Abstract:** The present application provides a packet forwarding method and apparatus. According to one example of the method, a VTEP establishes a default VXLAN tunnel and more than one VXLAN tunnel. The default VXLAN tunnel established by the VTEP device is used for matching a VXLAN tunnel from each VTEP device of a low encryption level to the present device. Each VXLAN tunnel established by the VTEP device connects to a tunnel endpoint of the same encryption level or a tunnel endpoint of a higher encryption level, respectively. When determining that the received VXLAN data packet matches the default VXLAN tunnel, the VTEP device prohibits from learning an inner source MAC address of the received VXLAN data packet, decapsulates the received VXLAN

[见续页]

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))。

data packet, and forwards an Ethernet data packet having the VXLAN encapsulation removed.

(57) 摘要：本申请提供一种报文转发方法及装置。根据该方法一个示例，VTEP创建缺省VXLAN隧道和一个以上VXLAN隧道。该VTEP设备创建的缺省VXLAN用以匹配每个低密级别的VTEP设备到本设备的VXLAN隧道；该VTEP设备创建的每个VXLAN隧道分别到一个相同密级别的隧道终结点或一个更高密级别的隧道终结点。该VTEP设备确定收到的VXLAN数据报文与缺省VXLAN隧道匹配时，禁止学习收到的VXLAN数据报文的内层源MAC地址，对收到的VXLAN数据报文进行解封装，转发移除VXLAN封装的以太网数据报文。

报文转发

技术领域

[01] 本申请涉及网络通信技术领域，尤其涉及一种报文转发方法及装置。

背景技术

[02] 虚拟扩展局域网（VXLAN: Virtual Extensible Local Area Network）是一种将二层报文用三层协议进行封装的技术，具体包括：引入一个用户数据包协议（UDP: User Datagram Protocol）格式的外层隧道，作为数据路径层，而原有的报文数据作为净荷来传输。VXLAN 网络的涉密信息的保护是需要解决网络保护问题。

附图说明

[03] 图 1 是本申请实施例提供的一种报文转发方法的流程示意图；

[04] 图 2 是本申请实施例提供的具体应用场景的架构示意图；

[05] 图 3 是本申请实施例提供的另一种具体应用场景的架构示意图；

[06] 图 4 是本申请实施例提供的一种报文转发装置的结构示意图；

[07] 图 5 是本申请实施例提供的一种报文转发装置的结构示意图；

[08] 图 6 是本申请实施例提供的一种报文转发设备的结构示意图。

具体实施方式

[09] 为了使本技术领域的人员更好地理解本申请实施例中的技术方案，并使本申请实施例的上述目的、特征和优点能够更加明显易懂，下面结合附图对本申请实施例中技术方案作进一步详细的说明。

[10] 在 VXLAN（Virtual Extensible Local Area Network，虚拟可扩展局域网）的网络中存在高密级别的设备或者网络和低密级别的设备或者网络，为了保证网络的安全，需要确保低密级别的设备或者网络的数据能流向高密级别的设备或者网络，并且高密级别的设备或者网络的数据不能向低密级别的设备或者网络的数据。但是，VTEP 会将通过接入电路（Attachment Circuit）收到的广播数据报文、未知单播数据报文以及组播数

据报文，在同一个 VXLAN 网络进行广播。这样，来自高密级别设备的数据报文会通过 VTEP 广播到同一个 VXLAN，导致泄密。

[11] 图 1 为本申请实施例提供的一种报文转发方法的流程示意图。如图 1 所示，该报文转发方法可以包括以下处理。

[12] 处理 101，创建缺省 VXLAN 隧道，用以匹配每个低密级别的 VTEP 设备到本设备的 VXLAN 隧道。

[13] 处理 102，创建一个以上 VXLAN 隧道，每个创建的 VXLAN 隧道分别到一个相同密级别的隧道终结点或一个更高密级别的隧道终结点。

[14] 处理 103，确定收到的 VXLAN 数据报文与缺省 VXLAN 隧道匹配时，禁止学习收到的 VXLAN 数据报文的内层源 MAC 地址，对收到的 VXLAN 数据报文进行解封装，转发移除 VXLAN 封装的以太网数据报文。

[15] 本申请实施例中，为了确保 VXLAN 网络中低密级别的设备或者网络的数据能流向高密级别的设备或者网络，低密级别的 VTEP 可以正常创建 VXLAN 隧道用以向高密级别的 VTEP 设备发送数据报文，而高密级别的 VTEP 设备创建缺省 VXLAN 隧道，用以隔离向同一个 VXLAN 内的低密级别的 VTEP 设备发送数据报文。

[16] VTEP 设备可以接收低密级别的 VTEP 设备的通过 VXLAN 隧道发送给本设备的 VXLAN 数据报文。需要说明的是，在本申请实施例中，当 VTEP 设备确定接收到的 VXLAN 数据报文的外层目的 IP 地址不是本设备的 IP 地址时，不需要进行 VXLAN 隧道终结。VTEP 设备可以根据该 VXLAN 数据报文的外层目的 IP 地址查找 underlay（下层）的三层转发表项进行转发。或这，当 VTEP 设备根据收到 VXLAN 数据报文的外层源 IP 地址和目的 IP 地址匹配到连接相同保密级或更高保密级 VTEP 的 VXLAN 隧道时 TEP 设备可以对 VXLAN 数据报文解除 VXLAN 封装后转发，学习 MAC 地址，执行常规的 VXLAN 转发。具体地，VTEP 设备确定收到的 VXLAN 数据报文的目的 IP 地址为本设备的 IP 地址，进行 VXLAN 隧道终结；确定收到的 VXLAN 数据报文的源 IP 地址是本设备连接相同保密级或更高保密级 VTEP 的 VXLAN 隧道的目的 IP 地址，则确定接收的 VXLAN 数据报文的外层源 IP 地址和目的 IP 地址匹配到连接相同保密级或更高保密级 VTEP 的 VXLAN 隧道。

[17] 本图 1 所示实施例中，为了保证高密级别的设备或者网络的数据不能流向低密级别的设备或者网络，VTEP 创建 VXLAN 隧道连接相同密级别的 VTEP 或更高密级别的 VTEP 的 VXLAN 隧道；并且 VTEP 不学习来自低密级别 VTEP 的数据报文的 MAC 地址，避免保密

级别收到的数据报文发往低己密级别的 VTEP，以保证数据转发安全。

[18] 为了避免向低密级别 VTEP 发送 VXLAN 数据报文，VTEP 将来自低密级别 VTEP 的 VXLAN 数据报文匹配缺省 VXLAN 隧道，不进行 MAC 地址学习，还能进一步节省存储 MAC 地址表项的硬件资源。

[19] 为了使本领域技术人员更好地理解本申请实施例提供的技术方案，下面结合具体应用场景对本申请实施例提供的技术方案进行说明。

[20] 图 2 为本申请实施例提供的一种具体应用场景的架构示意图。图 2 中，Server（服务器）110 和 Server 120 是相同密级别的低密级别的服务器，Server 130 和 Server 140 为相同密级别的高密级别的服务器，Server 110，Server 120，Server 130 以及 Server 140 分别通过 VTEP 210，VTEP 220，VTEP 230 以及 VTEP 240 接入三层核心网络。VTEP 210 和 VTEP 220 是低密级别的 VTEP 设备，VTEP 230 和 VTEP 240 是高密级别的 VTEP 设备。

[21] 在图 2 所示的实施例中，VTEP 230 和 VTEP 240 之间创建了用以交互数据报文的 VXLAN 隧道。VTEP 230 创建到 VTEP 240 的 VXLAN 隧道 34；VXLAN 隧道 34 的源 IP 地址和目的 IP 地址分别为 VTEP 230 的 IP 地址 IP 230，VTEP 240 的 IP 地址 IP 240。VTEP 240 创建到 VTEP 230 的 VXLAN 隧道 43；VXLAN 隧道 43 的源 IP 地址为 VTEP 240 的 IP 地址 IP 240，目的 IP 地址为 VTEP 230 的 IP 地址 IP 230。

[22] VTEP 210 和 VTEP 220 之间可创建了用以交互数据报文的 VXLAN 隧道（图中未示）。VTEP 210 创建到 VTEP 220 的 VXLAN 隧道源 IP 地址和目的 IP 地址分别为 VTEP210 的 IP 地址 IP210 以及 VTEP 220 的 IP 地址 IP 220 。VTEP 220 创建到 VTEP 210 的 VXLAN 隧道，该 VXLAN 隧道的 IP 地址和目的 IP 地址分别为 VTEP 220 的 IP 地址 IP 220 以及 VTEP 210 的 IP 地址 IP 210。

[23] VTEP 210 创建到 VTEP 240 的 VXLAN 隧道 14；VXLAN 隧道 14 的源 IP 地址为 VTEP210 的 IP 地址 IP 210，目的 IP 地址为 VTEP 240 的 IP 地址 IP 240。VTEP 220 创建到 VTEP 240 的 VXLAN 隧道（图中未示出），用以向 VTEP240 发送 VXLAN 封装的数据报文。VTEP 240 创建缺省 VXLAN 隧道 10，设置 VXLAN 隧道 10 的出端口为不存在；该缺省 VXLAN 隧道 10 的源 IP 地址为 VTEP 240 的 IP 地址，目的 IP 地址为空（null），即不存在。VTEP 240 设置 VXLAN 隧道 10 不学习 MAC 地址，设置 VXLAN 隧道 10 的出端口为不存在的物理端口。VTEP 240 创建该缺省 VXLAN 隧道 10 的源 IP 地址创建的缺省 VXLAN 隧道 10 用以匹配低密级别 VTEP 向 VTEP 240 发送 VXLAN 数据报文的 VXLAN 隧道，

包括VXLAN隧道14以及VTEP 220上连接VTEP 240的VXLAN隧道。

[24] VTEP 210和VTEP 220可以分别创建到VTEP 230的VXLAN隧道（图中未示），用以向VTEP230发送VXLAN数据报文。VTEP 230可以创建缺省VXLAN隧道(图中未示)；其中源IP地址和目的IP地址分别为VTEP 230的IP地址以及空（null）。VTEP 230的缺省VXLAN隧道用以匹配低密级别VTEP210和220到VTEP 230的VXLAN隧道。

[25] 在该实施例中，分别以VTEP 210和VTEP 240发出的数据报文的传输为例。

[26] 请参见图3,VTEP240创建VSI A,设置VSI A绑定VXLAN_ID1,VTEP240将Server 140与VTEP 240之间的AC 4绑定该VSI A;VTEP210创建VSI A,设置VSI A绑定VXLAN_ID1,VTEP 210设置Server 110接入VTEP 210的AC 1绑定VSI A，设置VXLAN隧道14与VSI A绑定。

[27] 属于来自Server 110的流量的以太网数据报文200到达VTEP 210。VTEP 210根据接收到以太网数据报文200的VLAN信息（identifier）和入端口信息（port identifier）识别AC 1。VTEP_210在AC 1关联的VSI A的转发表中，确定以太网数据报文200的目的MAC地址对应的出端口为VXLAN隧道14。VTEP210对以太网数据报文200进行VXLAN封装；其中，外层源IP地址为VTEP 210的IP地址，外层目的IP地址为VTEP 240的IP地址； VNI是VXLAN_ ID1。VTEP210将VXLAN封装数据报文201通过VXLAN隧道14的出端口发送。

[28] VTEP 240通过VXLAN隧道14接收到VXLAN封装数据报文201，获取VXLAN头的外层目的IP地址，识别获取的外层目的IP地址为本设备的IP地址，但是本设备不存在与该VXLAN封装头中的源IP地址和目的IP地址匹配的VXLAN隧道，即不存在源IP地址为该VXLAN封装头中的目的IP地址，目的IP地址为该VXLAN封装头中的源IP地址的VXLAN隧道。VTEP 240确定这些收到VXLAN封装的数据报文与缺省VXLAN隧道匹配。具体地，VTEP240确定VXLAN封装数据报文201的外层目的IP地址为本设备IP地址，终结VXLAN隧道。VTEP 240检查已创建的VXLAN隧道的目的IP地址与收到的VXLAN封装数据报文201的外层源IP地址是否一致。VTEP 240确定每个已创建的VXLAN隧道的目的IP地址与收到的VXLAN封装数据报文201的外层源IP地址不一致，检查是否创建了本设备VTEP 240的IP地址为源IP地址的缺省VXLAN隧道。VTEP 240确定创建了以本设备VTEP 240的IP地址为源IP地址的缺省VXLAN隧道10，确定收到该VXLAN封装的数据报文201的VXLAN隧道匹配缺省VXLAN隧道 10。VTEP_240移除VXLAN数据报文201的VXLAN封装,根据VXLAN数据报文201的VXLAN封装携带的VXLAN_ID(VXLAN ID1)

确定对应的VSI A。VTEP 240的缺省VXLAN隧道 10被配置为不学习MAC地址，VTEP 240禁止学习VXLAN数据报文201的内层MAC地址关联于VXLAN隧道 14。

[29] VTEP 204在该VSI A的转发表中查找到移除VXLAN封装的以太网数据报文200的目的MAC地址映射的AC_4。VTEP 240通过查找到的AC4将以太网数据报文200发送到Server 140。

[30] 来自服务器140的组播数据报文、广播以太网数据报文或者未知单播以太网数据报文202到达VTEP 240。VTEP 240根据收到组播数据报文、广播以太网数据报文或者未知单播以太网数据报文的VLAN标识和入端口标识识别AC 4。VTEP 240在AC 4关联的VSI A内查找广播转发表，为VSI_A的每个VXLAN隧道复制一份，从而在VSI A进行广播。VTEP240通过VXLAN隧道 43，将这些需要在VSI A内广播的广播以太网数据报文或者未知单播以太网数据报文封装为VXLAN广播数据报文203，并发送到相同密级别的VTEP230。由于VTEP240的缺省VXLAN隧道10的出端口为空，即不存在的物理端口。VTEP 240丢弃为VXLAN隧道 10复制的报文。这样，来自高密级别的服务器的数据报文需要在VSI内广播时,VTEP240只会向VSI内相同保密级别或者更高密级别的VTEP广播，而通过缺省VXLAN隧道 10丢弃了发往低密级别的VTEP210和220的VXLAN广播数据报文。

[31] 需要说明的是，在本申请实施例中，相同密级别的VTEP 210与VTEP 220之间的VXLAN数据报文转发以及相同密级别VTEP 230与VTEP 240之间的VXLAN数据报文转发按已有方案执行，包括：VTEP240学习来自VTEP230的VXLAN数据报文的内层MAC地址与外层源IP的映射;VTEP230学习来自VTEP220的VXLAN数据报文的内层MAC地址与外层源IP的映射；VTEP240向VTEP230发送需要在VXLAN网络内广播的VXLAN数据报文；VTEP230向VTEP240发送需要在VXLAN网络内广播的VXLAN数据报文等已有转发方案。

[32] 通过以上描述可以看出，在本申请实施例提供的技术方案中，实现了高密级别的VTEP设备过滤发往低密级别的VTEP设备的数据报文，有益于保证数据的安全。

[33] 图4为本申请实施例提供的一种报文转发装置400的示意图。该装置400可以应用于图2和图3所示的例子中的VTEP设备240或230。如图4所示，该报文转发装置400可以包括： 创建模块410，接收模块420，确定模块430，解封装模块440，转发模块450以及学习模块460。

[34] 创建模块 410，用于创建缺省 VXLAN 隧道以及创建一个以上 VXLAN 隧道。创建模块 410 创建的缺省隧道用以匹配每个低密级别的 VTEP 设备到本设备的 VXLAN 隧道。每个由创建模块 410 创建的 VXLAN 隧道分别到一个相同密级别的隧道终结点或一个更高密级别的隧道终结点。

[35] 接收模块 420，接收 VXLAN 数据报文。

[36] 确定模块 430，用于确定收到的 VXLAN 数据报文与缺省 VXLAN 隧道匹配。

[37] 解封装模块 440，用于解封装收到的 VXLAN 数据报文。

[38] 学习模块 460，用于禁止学习确定模块 430 确定的匹配缺省 VXLAN 隧道的 VXLAN 数据报文的内层源 MAC 地址。

[39] 确定模块 430 确定匹配缺省 VXLAN 隧道的 VXLAN 数据报文由解封装模块 440 解封装之后，由转发模块 450 转发移除 VXLAN 封装的以太网数据报文。

[40] 图 4 所示例子中，应用了报文转发装置 400 的 VTEP 创建 VXLAN 隧道连接相同密级别的 VTEP 或更高密级别的 VTEP 的 VXLAN 隧道；并且该 VTEP 不学习来自低密级别 VTEP 的数据报文的 MAC 地址，避免向低密级别的 VTEP 发送数据报文，保证数据转发安全。有益于保证了数据的安全性。

[41] 在图 5 所示的例子中，报文转发装置 400 还可进一步包括封装模块 470。

[42] 接收模块 420，用于接收以太网数据报文。确定模块 430，还用于确定收到的以太网数据报文需要在 VXLAN 网络内广播，丢弃通过缺省 VXLAN 隧道发送的一份以太网数据报文。封装模块 470，还用于通过每个创建的 VXLAN 隧道对一份以太网数据报文进行 VXLAN 封装。转发模块 450 还用于通过创建模块 410 创建的每个的 VXLAN 隧道发送一份 VXLAN 封装的以太网数据报文，用以向相同密级别的 VTEP 或者更高密级别的 VTEP 发送 VXLAN 数据报文。

[43] 确定模块 430，还用于确定收到的 VXLAN 数据报文的 VXLAN 封装头中的外层目的 IP 地址为本设备的 IP 地址；确定收到的 VXLAN 数据报文的 VXLAN 封装头中的外层源 IP 地址与每个创建的 VXLAN 隧道的目的 IP 地址不一致；确定收到的 VXLAN 数据文与缺省 VXLAN 隧道匹配。

[44] 确定模块 430，还用于根据收到以太网数据报文的虚拟局域网 VLAN 信息和入端口信息确定对应的接入电路 AC；在 AC 关联的虚拟交换实例 VSI 内查找转发表，确定在

VXLAN 网络内通过缺省 VXLAN 隧道和每个创建的 VXLAN 隧道广播的收到的以太网数据报文。

[45] 创建模块 410 创建的缺省 VXLAN 隧道的源 IP 地址为本设备的 IP 地址，缺省 VXLAN 隧道的目的 IP 为空；缺省 VXLAN 隧道的出方向为不存在的物理端口。

[46] 图 4 和图 5 所示的报文转发装置 400 可以通过软件实现（例如，存储于存储器并且由处理器运行的机器可读指令）、硬件实现（例如专用集成电路 ASIC 的处理器），或者由软件和硬件共同实现。

[47] 图 6 所示为本公开提供的一个 VTEP 例子。图 6 中，该 VTEP600 包括：转发单元 610、处理器 620 以及连接处理器 620 的存储有机器可执行指令的机器可读存储介质 630 存储单元 630。转发单元 610、处理器 620 以及存储单元 630 之间可经由系统总线通信。

[48] 转发单元 610 例如可以是硬件转发芯片且具有多个物理接口（图中未示）。进一步，转发单元 610 可包括图 4 和图 5 所示的接收模块 420，确定模块 430，解封装模块 440，封装模块 470，转发模块 450 以及学习模块 460。

[49] 处理器 620 通过读取并执行机器可读存储介质 630 中机器可执行指令，用以执行可执行图 4 以及图 5 中创建模块 410 的处理。

[50] 图 6 所示例子中的 VTEP 创建 VXLAN 隧道连接相同密级别的 VTEP 或更高密级别的 VTEP 的 VXLAN 隧道；并且该 VTEP 不学习来自低密级别 VTEP 的数据报文的 MAC 地址，避免向低密级别的 VTEP 发送数据报文，进一步保证了数据的安全性。

[51] 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以位于一个物理硬件，或者也可以分布到多个物理硬件，可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[52] 本领域技术人员在考虑说明书及实践这里公开的申请后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

权利要求书

1. 一种数据报文转发方法，其特征在于，

创建缺省 VXLAN 隧道，用以匹配每个低密级别的 VTEP 设备到本设备的 VXLAN 隧道；

创建一个以上 VXLAN 隧道，每个所述创建的 VXLAN 隧道分别到一个相同密级别的隧道终结点或一个更高密级别的隧道终结点；

确定收到的所述 VXLAN 数据报文与缺省 VXLAN 隧道匹配时，对所述收到的 VXLAN 数据报文进行解封装，禁止学习所述收到的 VXLAN 数据报文的内层源 MAC 地址，转发移除 VXLAN 封装的以太网数据报文。

2. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：确定收到的以太网数据报文需要在 VXLAN 网络内广播，丢弃所述通过所述缺省 VXLAN 隧道发送的一份所述以太网数据报文；通过每个所述创建的 VXLAN 隧道对一份所述以太网数据报文进行 VXLAN 封装，通过每个所述创建的 VXLAN 隧道发送一份 VXLAN 封装的以太网数据报文。

3. 根据权利要求 1 所述的方法，其特征在于，所述确定收到的所述 VXLAN 数据报文与缺省 VXLAN 隧道匹配，包括：

确定所述收到的 VXLAN 数据报文的 VXLAN 封装头中的外层目的 IP 地址为本设备的 IP 地址；

确定所述收到的 VXLAN 数据报文的 VXLAN 封装头中的外层源 IP 地址与每个所述创建的 VXLAN 隧道的目的 IP 地址不一致；

确定所述收到的 VXLAN 数据文与所述缺省 VXLAN 隧道匹配。

4. 根据权利要求 2 所述的方法，其特征在于，确定收到的以太网数据报文需要在 VXLAN 网络内广播之前，所述方法还包括：

根据所述收到以太网数据报文的虚拟局域网 VLAN 信息和入端口信息确定对应的接入电路 AC；

在所述 AC 关联的虚拟交换实例 VSI 内查找转发表，确定在所述 VXLAN 网络内通过所述缺省 VXLAN 隧道和每个所述创建的 VXLAN 隧道广播的所述收到的以太网数据报文。

5. 根据权利要求 1 所述的方法，其特征在于，所述缺省 VXLAN 隧道的源 IP 地址为本设备的 IP 地址，所述缺省 VXLAN 隧道的目的 IP 为空；所述缺省 VXLAN 隧道的出方向为不存在的物理端口。

6. 一种报文转发装置，其特征在于，

创建模块，用于创建缺省 VXLAN 隧道以及创建一个以上 VXLAN 隧道；其中，所述缺

省隧道用以匹配每个低密级别的 VTEP 设备到本设备的 VXLAN 隧道；每个所述创建的VXLAN 隧道分别到一个相同密级别的隧道终结点或一个更高密级别的隧道终结点；

接收模块，接收 VXLAN 数据报文；

确定模块，用于确定收到的所述 VXLAN 数据报文与缺省 VXLAN 隧道匹配；

解封装模块，用于解封装所述收到的 VXLAN 数据报文；

学习模块，用于禁止学习所述收到的 VXLAN 数据报文的内层源 MAC 地址；

转发模块，转发移除 VXLAN 封装的以太网数据报文。

7. 根据权利要求 6 所述的装置，其特征在于，所述装置还包括封装模块；

所述接收模块，用于接收以太网数据报文；

所述确定模块，还用于确定收到的以太网数据报文需要在 VXLAN 网络内广播，丢弃所述通过所述缺省 VXLAN 隧道发送的一份所述以太网数据报文；

所述封装模块，还用于通过每个所述创建的 VXLAN 隧道对一份所述以太网数据报文进行 VXLAN 封装；

所述转发模块，还用于通过每个所述创建的 VXLAN 隧道发送一份 VXLAN 封装的以太网数据报文。

8. 根据权利要求 6 所述的装置，其特征在于，

所述确定模块，还用于确定所述收到的 VXLAN 数据报文的 VXLAN 封装头中的外层目的 IP 地址为本设备的 IP 地址；确定所述收到的 VXLAN 数据报文的 VXLAN 封装头中的外层源 IP 地址与每个所述创建的 VXLAN 隧道的目的 IP 地址不一致；确定所述收到的 VXLAN 数据文与所述缺省 VXLAN 隧道匹配。

9. 根据权利要求 7 所述的装置，其特征在于，

所述确定模块还用于，根据所述收到以太网数据报文的虚拟局域网 VLAN 信息和入端口信息确定对应的接入电路 AC；在所述 AC 关联的虚拟交换实例 VSI 内查找转发表，确定在所述 VXLAN 网络内通过所述缺省 VXLAN 隧道和每个所述创建的 VXLAN 隧道广播的所述收到的以太网数据报文。

10. 根据权利要求 6 所述的装置，其特征在于，所述创建模块创建的所述缺省 VXLAN 隧道的源 IP 地址为本设备的 IP 地址，所述缺省 VXLAN 隧道的目的 IP 为空；所述缺省 VXLAN 隧道的出方向为不存在的物理端口。

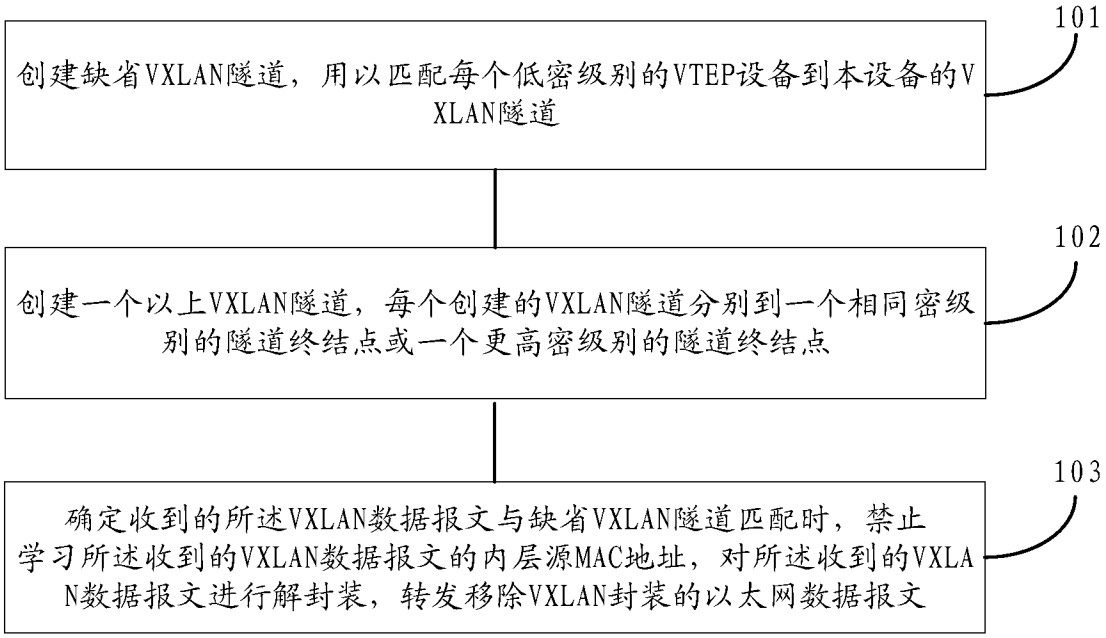
101
创建缺省VXLAN隧道，用以匹配每个低密级别的VTEP设备到本设备的VXLAN隧道
102
创建一个以上VXLAN隧道，每个创建的VXLAN隧道分别到一个相同密级别的隧道终结点或一个更高密级别的隧道终结点
103
确定收到的所述VXLAN数据报文与缺省VXLAN隧道匹配时，禁止学习所述收到的VXLAN数据报文的内层源MAC地址，对所述收到的VXLAN数据报文进行解封装，转发移除VXLAN封装的以太网数据报文

图 1

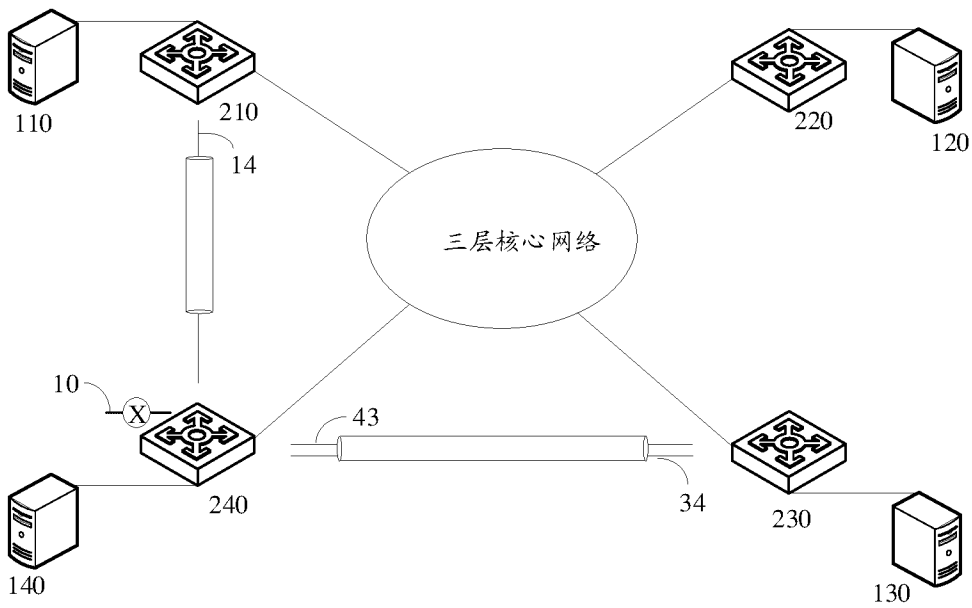
110
210
14
三层核心网络
220
120
10
X
43
240
34
230
140
130

图 2

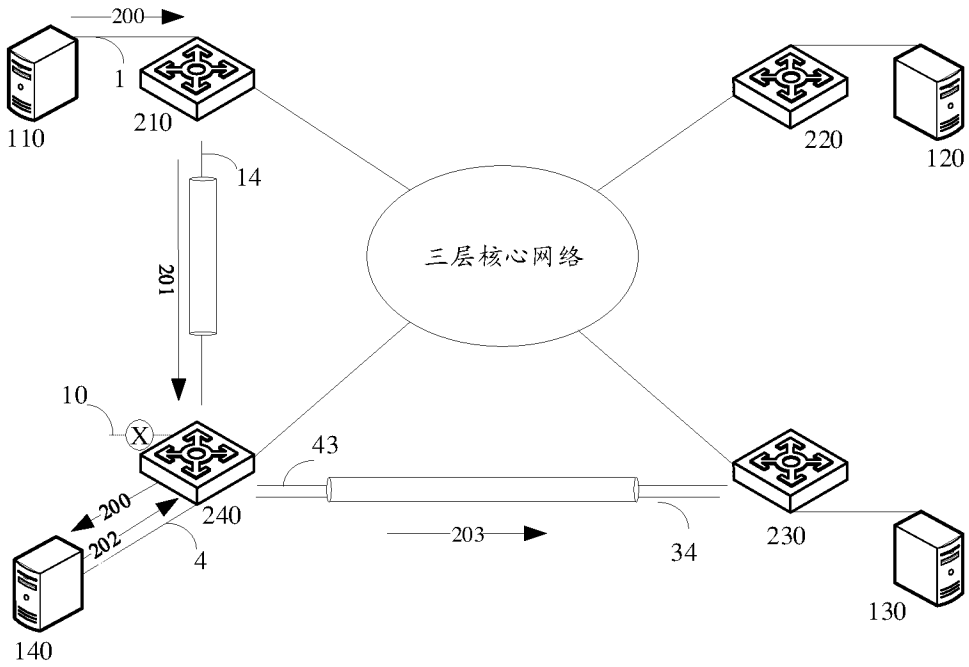
200
1
110
210
14
201
三层核心网络
220
120
10
X
43
200
202
240
4
203
34
230
130
140

图 3

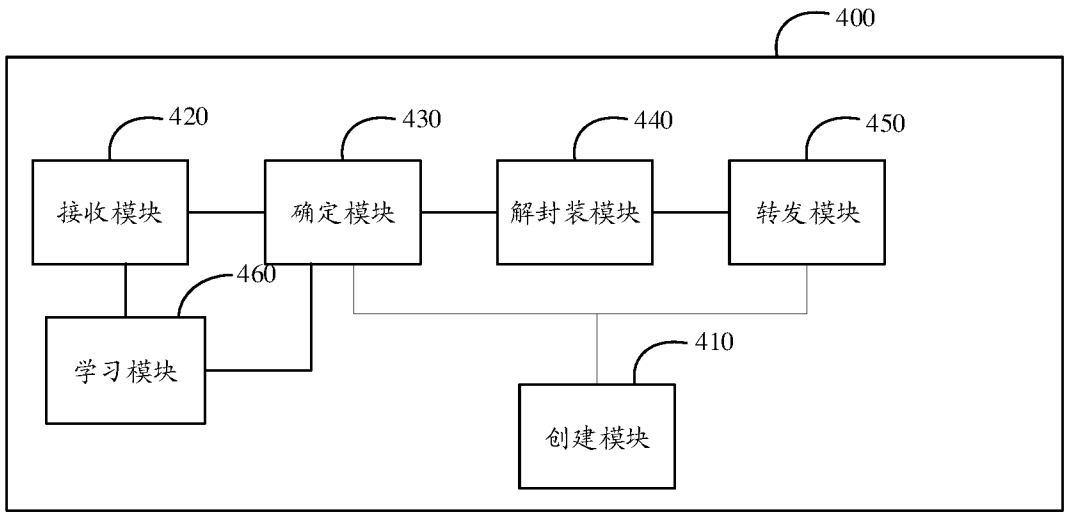
400
420
430
440
450
接收模块
确定模块
解封装模块
转发模块
460
学习模块
410
创建模块

图 4

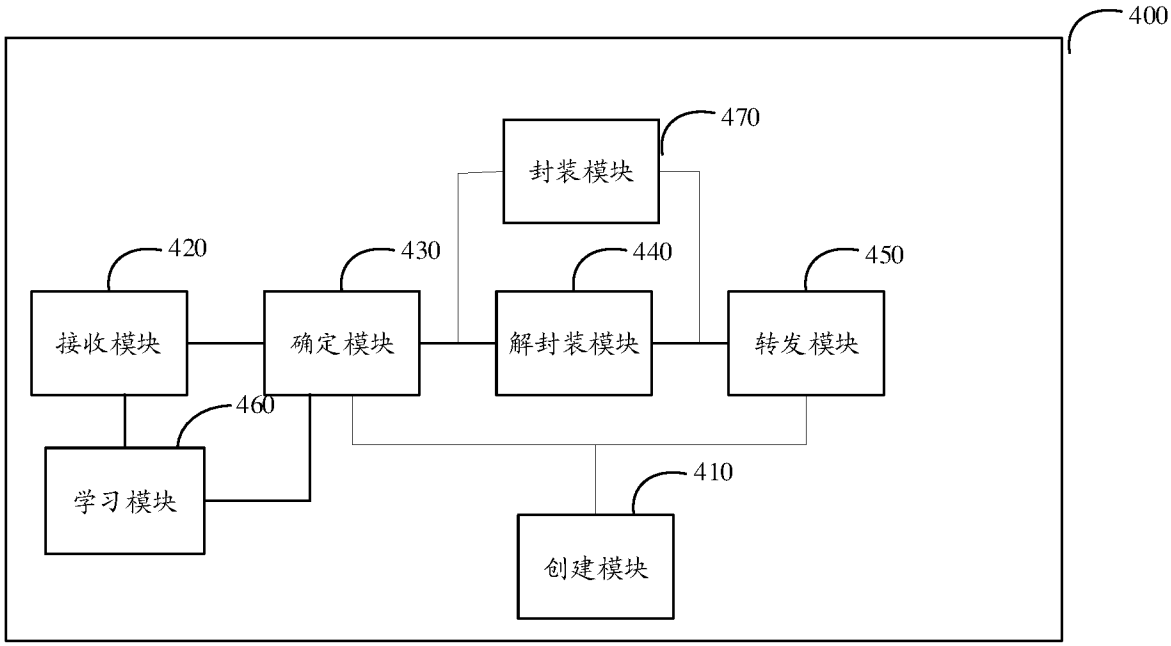
400
封装模块
470
420
430
440
450
接收模块
确定模块
解封装模块
转发模块
460
学习模块
410
创建模块

图 5

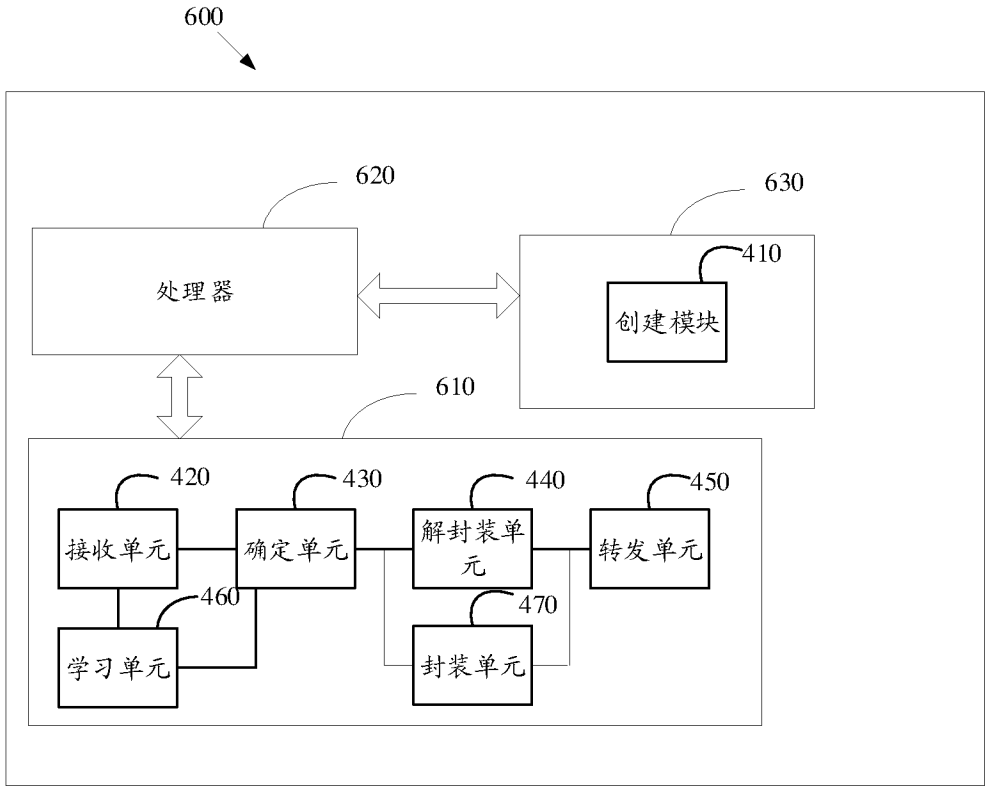
600
620
630
处理器
410
创建模块
610
420
430
440
450
接收单元
确定单元
解封装单元
转发单元
460
470
学习单元
封装单元

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/121267

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/46(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)

CNTXT; CNABS; CNKI; SIPOABS; DWPI: 高, 密, 安全, 隐私, 低, 单向, 传输, 传送, 发送, 转发, 泄密, 保密, 网络, VXLAN, 缺省隧道, high, safe, private, low, one way, transmit, send, forward, reveal, leakage, secret, network, default, tunnel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 101127680 A (HU, Deyong) 20 February 2008 (2008-02-20) description, page 1, line 2 to page 3, line 29, and figure 1	1-10
Y	henaulxyxa上传 (Non-official translation: Henaulxyxa Upload). "17-VXLAN配置指导-VXLAN配置 (Non-official translation: 17-VXLAN Configuration Guide-VXLAN Configuration)" *百度文库 (Baidu Library)*, 22 August 2015 (2015-08-22), text, section 1.3	1-10
A	CN 103491072 A (BEIJING INSTITUTE OF INFORMATION AND CONTROL) 01 January 2014 (2014-01-01) entire document	1-10
A	US 2014003434 A1 (AVAYA INC. et al.) 02 January 2014 (2014-01-02) entire document	1-10

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2020	**18 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/121267

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 101127680 A	20 February 2008	None	
CN 103491072 A	01 January 2014	CN 103491072 B	15 March 2017
US 2014003434 A1	02 January 2014	US 9451056 B2	20 September 2016

国际检索报告

国际申请号
PCT/CN2019/121267

A. 主题的分类

H04L 12/46(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））

CNTXT;CNABS;CNKI;SIPOABS;DWPI:高，密，安全，隐私，低，单向，传输，传送，发送，转发，泄密，保密，网络，VXLAN，缺省隧道，high, safe, private, low, one way, transmit, send, forward, reveal, leakage, secret, network, default, tunnel

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 101127680 A (胡德勇) 2008年 2月 20日 (2008-02-20) 说明书第1页第2行-第3页第29行，图1	1-10
Y	henaulxyxa上传. ″《17-VXLAN配置指导-VXLAN配置》″ 《百度文库》, 2015年 8月 22日 (2015-08-22), 正文第1.3节	1-10
A	CN 103491072 A (北京信息控制研究所) 2014年 1月 1日 (2014-01-01) 全文	1-10
A	US 2014003434 A1 (AVAYA INC等) 2014年 1月 2日 (2014-01-02) 全文	1-10

☐ 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	国际检索报告邮寄日期
2020年 1月 22日	2020年 2月 18日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	刘永喆
传真号 (86-10)62019451	电话号码 86-(010)-62412024

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/121267

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 101127680 A	2008年 2月 20日	无	
CN 103491072 A	2014年 1月 1日	CN 103491072 B	2017年 3月 15日
US 2014003434 A1	2014年 1月 2日	US 9451056 B2	2016年 9月 20日