

通信方法、CP 设备及 NAT 设备

本申请要求于 2020 年 07 月 22 日提交的申请号为 202010712973.3、发明名称为“通信方法、CP 设备及 NAT 设备”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

本申请涉及通信技术领域，特别涉及一种通信方法、CP 设备及 NAT 设备。

背景技术

随着宽带用户数量的激增，公网的互联网协议（Internet Protocol, IP）地址（如公网互联网协议第四版（Internet Protocol version 4, IPv4）地址）面临资源不足的问题。有鉴于此，提供了网络地址转换（Network Address Translation, NAT）技术以及运营商级 NAT（Carrier Grade NAT, CGN）等执行 NAT 技术的 NAT 设备来解决这一问题。具体地，宽带网络网关（Broadband Network Gateway, BNG）等网关设备会为用户分配私网 IP 地址。NAT 设备会将私网 IP 地址转换为公网 IP 地址，以便通过转换后的公网 IP 地址支持用户访问公网。由于多个私网 IP 地址能够转换为同一个公网 IP 地址，从而有效解决了公网 IP 地址资源不足的问题。其中，由于 NAT 功能的部署会隐藏用户的私网 IP 地址，通常要求在部署 NAT 功能的同时实现溯源的功能。溯源是指能够根据用户的公网 IP 地址查询到用户的私网 IP 地址，以便根据私网 IP 地址锁定到具体用户。

从存在形态的角度来说，NAT 设备分为独立式 NAT 设备（如独立式 CGN 设备）和插卡式 NAT 设备（如 CGN 板卡）。独立式 NAT 设备的形态是一个独立的设备。独立式 NAT 设备通过线路和 BNG 等网关设备网络相连。插卡式 NAT 设备的形态是一个板卡，插卡式 NAT 设备插在 BNG 等网关设备的槽位上，从而与网关设备集成在一起。

在网关设备采用小型化设备（如迷你 BNG）实现的情况下，由于小型化设备不具备单独的槽位以插放插卡式 NAT 设备，NAT 的功能通常采用独立式 NAT 设备实现。在这一情况下，溯源功能通常是在流量转发阶段通过日志（Log）服务器实现的。具体地，当用户设备发送数据报文后，数据报文会被转发至 NAT 设备。NAT 设备接收数据报文，将数据报文中的源 IP 从私网 IP 地址转换为公网 IP 地址。同时，NAT 设备根据私网 IP 地址和公网 IP 地址生成 NAT 日志。NAT 设备将 NAT 日志发送至日志服务器。NAT 日志包括私网 IP 地址与公网 IP 地址之间的映射关系。当需要溯源时，日志服务器根据公网 IP 地址查询 NAT 日志，从 NAT 日志中得到公网 IP 地址对应的私网 IP 地址，从而在日志服务器上实现溯源。

目前基于独立式 NAT 设备进行溯源的方法依赖于日志服务器。因此，运营商需要投资建设日志服务器才能实现溯源的目的，这导致溯源的成本过高。

发明内容

本申请实施例提供了一种通信方法、CP 设备及 NAT 设备，有助于减少溯源的成本。所述技术方案如下。

第一方面,提供了一种通信方法,该方法应用于控制面(control plane, CP)和用户面(user plane, UP)分离的通信系统中,以CP设备执行该方法为例,所述CP设备为用户分配IP地址。CP设备将分配的IP地址下发给NAT设备,NAT设备在接收到CP设备下发的IP地址的触发条件下,为用户分配CP设备下发的IP地址所对应的公网IP地址,将公网IP地址上报给CP设备。CP设备根据NAT设备上报的公网IP地址,在计费报文中携带CP设备分配的IP地址以及NAT设备分配的公网IP地址,向远程用户拨号认证服务(remote authentication dial in user service, RADIUS)服务器发送计费报文,从而将CP设备分配的IP地址以及NAT设备分配的公网IP地址上报给RADIUS服务器,以便在RADIUS服务器上进行NAT溯源。

一方面,由于NAT溯源采用了RADIUS溯源的方式,能够通过复用RADIUS服务器进行溯源,摆脱了需要建设日志服务器才能溯源的限制,减少溯源的成本。另一方面,适于应用在NAT设备采用独立式NAT设备实现的场景,有助于解决NAT设备采用业务单板等插卡式NAT设备实现时会面临的UP槽位不足、NAT处理能力不足等问题。

可选地,所述第一IP地址包括私网IPv4地址或者互联网协议第六版(internet protocol version 6, IPv6)地址中的至少一项。

通过这种可选方式,CP设备通过分配私网IPv4地址以及向NAT设备下发私网IPv4地址,有助于支持NAT44(NAT IPv4-IPv4)场景下实现RADIUS溯源。CP设备通过分配IPv6地址以及向NAT设备下发IPv6地址,有助于支持轻量级双栈(dual stack lite, DS-Lite)场景等双栈网络中实现RADIUS溯源。

可选地,所述通信系统包括网关系统,所述网关系统为宽带网络网关BNG系统或者宽带远程接入服务器(virtual broadband remote access server, BRAS)系统。

通过这种可选方式,通过选用BNG系统中的CP或者BRAS系统中的CP实现本实施例方案,有助于复用BNG系统或者BRAS系统的网络架构,降低实现复杂度。

可选地,所述计费报文还包括端口块,所述端口块包括所述NAT设备为所述用户分配的至少一个端口号;所述CP设备从所述NAT设备接收第二IP地址,包括:所述CP设备从所述NAT设备接收所述用户的信息,所述用户的信息包括所述第一IP地址、所述第二IP地址和所述端口块的对应关系。

可选地,所述CP设备从所述NAT设备接收所述端口块之前,所述方法还包括:所述CP设备从所述RADIUS服务器接收端口块集合,所述端口块集合包括所述端口块;所述CP设备向所述NAT设备发送所述端口块集合。

通过这种可选方式,在运营商需要指定用户的端口块的范围的场景下,通过由RADIUS服务器向CP设备下发端口块集合,再由CP设备将端口块集合下发给NAT设备,从而指定NAT设备在端口块集合内分配端口块,因此满足了指定NAT端口块范围的需求。尤其是,CP通过将RADIUS指定的端口块集合和IP地址一起下发给NAT设备,使得通过RADIUS指定端口块范围的过程和触发NAT设备分配公网IP的过程得以同时执行,减少了通信开销和实现复杂度。

可选地,所述CP设备向RADIUS服务器发送计费报文之后,所述方法还包括以下至少一项:若所述用户下线,所述CP设备向所述NAT设备发送删除消息,所述删除消息用于指示所述NAT设备删除所述NAT设备上保存的所述用户的信息;若所述用户下线,所述CP设备删除所述CP设备上保存的所述用户的信息。

通过这种可选方式, CP 设备通过在用户下线时指示 NAT 设备删除用户的信息, 从而及时释放已下线的用户的信息在 NAT 设备上占用的存储空间, 节省了 NAT 设备的存储资源, 避免 NAT 设备上资源耗空的问题。CP 设备通过在用户下线时删除本地保存的用户的信息, 从而及时释放已下线的用户的信息在 CP 设备上占用的存储空间, 节省了 CP 设备的存储资源, 避免 CP 设备上资源耗空的问题。

可选地, 所述 NAT 设备包括互为备份关系的主 NAT 设备和备 NAT 设备, 所述 CP 设备从所述 NAT 设备接收第二 IP 地址, 包括: 所述 CP 设备从所述主 NAT 设备接收所述用户的信息。

通过这种可选方式, CP 设备通过将主 NAT 设备发来的用户的信息下发给备 NAT 设备, 使得备 NAT 设备获得了主 NAT 设备上保存的用户的信息。一方面, 实现了备 NAT 设备与主 NAT 设备之间用户的信息的同步, 从而能在主 NAT 设备故障时触发主备倒换, 实现业务正常运行。另一方面, 备 NAT 设备与主 NAT 设备不需要部署类似虚拟路由冗余协议(Virtual Router Redundancy Protocol, VRRP)的主备选举机制, 这样就不需要在主 NAT 设备与备 NAT 设备之间拉直连线, 简化配置和部署资源。

可选地, 所述 CP 设备从所述主 NAT 设备接收所述用户的信息之后, 所述方法还包括: 所述 CP 设备向所述备 NAT 设备发送所述用户的信息。

可选地, 所述方法还包括: 若所述主 NAT 设备处于故障状态, 所述 CP 设备向所述备 NAT 设备发送第一更新消息, 所述第一更新消息用于指示所述备 NAT 设备提高所述第二 IP 地址对应的路由优先级。

当主 NAT 设备发生故障时, CP 设备通过向备 NAT 设备下发第一更新消息, 从而通知备 NAT 设备调整公网地址对应的路由优先级, 由于备 NAT 设备的公网地址对应的路由优先级升高, 因此网络侧的流量会从主 NAT 设备切换至备 NAT 设备上, 使得备 NAT 设备升级为主 NAT 设备, 代替之前故障的主 NAT 设备处理网络侧的流量, 避免流量传输中断。此外, 由于流量的切换是 CP 设备引导的, 能够保证主 NAT 设备与备 NAT 设备不会存在流量绕行。尤其是, 该方法能够适用于 NAT44 场景, 有助于 NAT44 场景下实现双机备份。

可选地, 所述方法还包括: 若所述主 NAT 设备处于故障状态, 所述 CP 设备向所述备 NAT 设备发送第二更新消息, 所述第二更新消息用于指示所述备 NAT 设备提高第三 IP 地址对应的路由优先级, 所述第三 IP 地址为隧道端点的 IP 地址, 所述隧道端点包括所述主 NAT 设备或者所述备 NAT 设备。

当主 NAT 设备发生故障时, CP 设备通过向备 NAT 设备下发第一更新消息和第二更新消息, 从而通知备 NAT 设备调整公网地址对应的路由优先级以及隧道端点地址对应的路由优先级, 由于备 NAT 设备的公网地址对应的路由优先级升高, 因此网络侧的流量会从主 NAT 设备切换至备 NAT 设备, 由于备 NAT 设备的隧道端点地址对应的路由优先级升高, 因此用户侧的流量会从主 NAT 设备切换至备 NAT 设备, 使得备 NAT 设备升级为主 NAT 设备, 代替之前故障的主 NAT 设备处理网络侧的流量和用户侧的流量, 避免流量传输中断。此外, 由于流量的切换是 CP 设备引导的, 能够保证主 NAT 设备与备 NAT 设备不会存在流量绕行。尤其是, 该方法能够适用于 DS-Lite 场景, 有助于 DS-Lite 场景下实现双机备份。

第二方面, 提供了一种通信方法, 以该方法由 NAT 设备执行为例, 所述 NAT 设备从 CP

设备接收所述 CP 设备为用户分配的第一 IP 地址,所述 CP 设备是 CP 和 UP 分离的通信系统中的 CP 设备;所述 NAT 设备为所述用户分配第二 IP 地址,所述第二 IP 地址为公网 IP 地址;所述 NAT 设备向所述 CP 设备发送所述第二 IP 地址。NAT 设备分配公网 IP 地址后向 CP 设备上报该公网 IP 地址,以便 CP 设备在计费报文中携带 CP 设备分配的 IP 地址以及 NAT 设备分配的公网 IP 地址,向远程用户拨号认证服务(remote authentication dial in user service, RADIUS)服务器发送计费报文,从而将 CP 设备分配的 IP 地址以及 NAT 设备分配的公网 IP 地址上报给 RADIUS 服务器,以便在 RADIUS 服务器上进行 NAT 溯源。

一方面,由于 NAT 溯源采用了 RADIUS 溯源的方式,能够通过复用 RADIUS 服务器进行溯源,摆脱了需要建设日志服务器才能溯源的限制,减少溯源的成本。另一方面,适于应用在 NAT 设备采用独立式 NAT 设备实现的场景,有助于解决 NAT 设备采用业务单板等插卡式 NAT 设备实现时会面临的 UP 槽位不足、NAT 处理能力不足等问题。

可选地,所述 NAT 设备从 CP 设备接收所述 CP 设备为用户分配的第一 IP 地址之后,所述方法还包括:所述 NAT 设备为所述用户分配端口块,所述端口块包括至少一个端口号;所述 NAT 设备向所述 CP 设备发送所述端口块。

可选地,所述 NAT 设备为所述用户分配端口块之前,所述方法还包括:所述 NAT 设备从所述 CP 设备接收端口块集合;所述 NAT 设备为所述用户分配端口块,包括:所述 NAT 设备在所述端口块集合内,为所述用户分配端口块。

可选地,所述 NAT 设备为所述用户分配第二 IP 地址之后,所述方法还包括:所述 NAT 设备保存所述用户的信息,所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和所述端口块的对应关系。

可选地,所述 NAT 设备向所述 CP 设备发送所述第二 IP 地址,包括:所述 NAT 设备向所述 CP 设备发送所述用户的信息。

可选地,所述 NAT 设备向所述 CP 设备发送所述第二 IP 地址之后,所述方法还包括:所述 NAT 设备从所述 CP 设备接收删除消息;响应于所述删除消息,所述 NAT 设备删除所述用户的信息。

可选地,所述 NAT 设备为互为备份关系的主 NAT 设备和备 NAT 设备中的备 NAT 设备,所述 NAT 设备为所述用户分配第二 IP 地址之前,所述方法还包括:

所述备 NAT 设备从所述 CP 设备接收所述用户的信息,所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和端口块的对应关系,所述端口块包括至少一个端口号;所述 NAT 设备为所述用户分配第二 IP 地址,包括:在所述主 NAT 设备故障时,所述备 NAT 设备根据所述用户的信息为所述用户分配所述第二 IP 地址。

可选地,所述方法还包括:所述备 NAT 设备从所述 CP 设备接收第一更新消息;响应于所述第一更新消息,所述备 NAT 设备提高所述第二 IP 地址对应的路由优先级。

可选地,所述方法还包括:所述备 NAT 设备从所述 CP 设备接收第二更新消息;

响应于所述第二更新消息,所述备 NAT 设备提高第三 IP 地址对应的路由优先级,所述第三 IP 地址为隧道端点的 IP 地址,所述隧道端点包括所述主 NAT 设备或者所述备 NAT 设备。

第三方面,提供了一种 CP 设备,所述 CP 设备位于 CP 和 UP 分离的通信系统中,所述

CP 设备包括:

分配单元, 用于为用户分配第一 IP 地址;

发送单元, 用于向 NAT 设备发送所述第一 IP 地址;

接收单元, 用于从所述 NAT 设备接收第二 IP 地址, 所述第二 IP 地址为所述 NAT 设备为所述用户分配的公网 IP 地址;

所述发送单元, 还用于向 RADIUS 服务器发送计费报文, 所述计费报文包括所述第一 IP 地址和所述第二 IP 地址。

可选地, 所述第一 IP 地址包括私网 IPv4 地址或者 IPv6 地址中的至少一项。

可选地, 所述通信系统包括网关系统, 所述网关系统为 BNG 系统或者 BRAS 系统。

可选地, 所述计费报文还包括端口块, 所述端口块包括所述 NAT 设备为所述用户分配的至少一个端口号;

所述接收单元, 用于从所述 NAT 设备接收所述用户的信息, 所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和所述端口块的对应关系。

可选地, 所述接收单元, 还用于从所述 RADIUS 服务器接收端口块集合, 所述端口块集合包括所述端口块;

所述发送单元, 还用于向所述 NAT 设备发送所述端口块集合。

可选地, 所述发送单元, 还用于若所述用户下线, 向所述 NAT 设备发送删除消息, 所述删除消息用于指示所述 NAT 设备删除所述 NAT 设备上保存的所述用户的信息;

所述 CP 设备还包括: 删除单元, 用于若所述用户下线, 删除所述 CP 设备上保存的所述用户的信息。

可选地, 所述 NAT 设备包括互为备份关系的主 NAT 设备和备 NAT 设备, 所述接收单元, 用于从所述主 NAT 设备接收所述用户的信息。

可选地, 所述发送单元, 还用于向所述备 NAT 设备发送所述用户的信息。

可选地, 所述发送单元, 还用于若所述主 NAT 设备处于故障状态, 向所述备 NAT 设备发送第一更新消息, 所述第一更新消息用于指示所述备 NAT 设备提高所述第二 IP 地址对应的路由优先级。

可选地, 所述发送单元, 还用于若所述主 NAT 设备处于故障状态, 向所述备 NAT 设备发送第二更新消息, 所述第二更新消息用于指示所述备 NAT 设备提高第三 IP 地址对应的路由优先级, 所述第三 IP 地址为隧道端点的 IP 地址, 所述隧道端点包括所述主 NAT 设备或者所述备 NAT 设备。

在一些实施例中, 第三方面提供的 CP 设备中的单元通过软件实现, CP 设备中的单元是程序单元。在另一些实施例中, 第三方面提供的 CP 设备中的单元通过硬件或固件实现。

第四方面, 提供了一种 NAT 设备, 所述 NAT 设备包括:

接收单元, 用于从 CP 设备接收所述 CP 设备为用户分配的第一 IP 地址, 所述 CP 设备是 CP 和 UP 分离的通信系统中的 CP 设备;

分配单元, 用于为所述用户分配第二 IP 地址, 所述第二 IP 地址为公网 IP 地址;

发送单元, 用于向所述 CP 设备发送所述第二 IP 地址。

可选地, 所述分配单元, 还用于为所述用户分配端口块, 所述端口块包括至少一个端口

号;

所述发送单元,还用于向所述 CP 设备发送所述端口块。

可选地,所述接收单元,还用于从所述 CP 设备接收端口块集合;

所述分配单元,用于在所述端口块集合内,为所述用户分配端口块。

可选地,所述 NAT 设备还包括:保存单元,用于保存所述用户的信息,所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和所述端口块的对应关系。

可选地,所述发送单元,用于向所述 CP 设备发送所述用户的信息。

可选地,所述接收单元,还用于从所述 CP 设备接收删除消息;

所述 NAT 设备还包括:删除单元,用于响应于所述删除消息,所述 NAT 设备删除所述用户的信息。

可选地,所述 NAT 设备为互为备份关系的主 NAT 设备和备 NAT 设备中的备 NAT 设备,所述接收单元,还用于从所述 CP 设备接收所述用户的信息,所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和端口块的对应关系,所述端口块包括至少一个端口号;

所述分配单元,还用于在所述主 NAT 设备故障时,根据所述用户的信息为所述用户分配所述第二 IP 地址。

可选地,所述接收单元,还用于从所述 CP 设备接收第一更新消息;所述 NAT 设备还包括:提高单元,用于响应于所述第一更新消息,提高所述第二 IP 地址对应的路由优先级。

可选地,所述接收单元,还用于从所述 CP 设备接收第二更新消息;所述 NAT 设备还包括:提高单元,用于响应于所述第二更新消息,提高第三 IP 地址对应的路由优先级,所述第三 IP 地址为隧道端点的 IP 地址,所述隧道端点包括所述主 NAT 设备或者所述备 NAT 设备。

在一些实施例中,第四方面提供的 NAT 设备中的单元通过软件实现,NAT 设备中的单元是程序单元。在另一些实施例中,第四方面提供的 NAT 设备中的单元通过硬件或固件实现。

第五方面,提供了一种 CP 设备,该 CP 设备包括处理器和通信接口,该处理器用于执行指令,使得该 CP 设备执行上述第一方面或第一方面任一种可选方式所提供的通信方法,所述通信接口用于接收或发送报文。第五方面提供的 CP 设备的具体细节可参见上述第一方面或第一方面任一种可选方式,此处不再赘述。

第六方面,提供了一种 NAT 设备,该 NAT 设备包括处理器和通信接口,该处理器用于执行指令,使得该 NAT 设备执行上述第二方面或第二方面任一种可选方式所提供的通信方法,所述通信接口用于接收或发送报文。第六方面提供的 NAT 设备的具体细节可参见上述第二方面或第二方面任一种可选方式,此处不再赘述。

第七方面,提供了一种计算机可读存储介质,该存储介质中存储有至少一条指令,该指令由处理器读取以使 CP 设备执行上述第一方面或第一方面任一种可选方式所提供的通信方法。

第八方面,提供了一种计算机可读存储介质,该存储介质中存储有至少一条指令,该指令由处理器读取以使 NAT 设备执行上述第二方面或第二方面任一种可选方式所提供的通信

方法。

第九方面，提供了一种计算机程序产品，该计算机程序产品包括计算机指令，该计算机指令存储在计算机可读存储介质中。CP 设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该 CP 设备执行上述第一方面或第一方面任一种可选方式所提供的通信方法。

第十方面，提供了一种计算机程序产品，该计算机程序产品包括计算机指令，该计算机指令存储在计算机可读存储介质中。NAT 设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该 NAT 设备执行上述第一方面或第一方面任一种可选方式所提供的通信方法。

第十一方面，提供了一种芯片，当该芯片在 CP 设备上运行时，使得 CP 设备执行上述第一方面或第一方面任一种可选方式所提供的通信方法。

第十二方面，提供了一种芯片，当该芯片在 NAT 设备上运行时，使得 NAT 设备执行上述第二方面或第二方面任一种可选方式所提供的通信方法。

第十三方面，提供了一种通信系统，该通信系统包括 CP 设备以及 NAT 设备，该 CP 设备用于执行上述第一方面或第一方面任一种可选方式所述的方法，该 NAT 设备用于执行上述第二方面或第二方面任一种可选方式所述的方法。

第十四方面，提供了一种 CP 设备，该 CP 设备包括：中央处理器、网络处理器和物理接口。中央处理器用于执行如下操作：为用户分配第一 IP 地址。

网络处理器用于触发物理接口执行如下操作：向 NAT 设备发送所述第一 IP 地址；从所述 NAT 设备接收第二 IP 地址；向 RADIUS 服务器发送计费报文。

可选地，所述 CP 设备包括主控板和接口板，所述中央处理器设置在所述主控板上，所述网络处理器和所述物理接口设置在接口板上，所述主控板和所述接口板耦合。

在一种可能的实现方式中，主控板和接口板之间建立进程间通信协议（inter-process communication, IPC）通道，主控板和接口板之间通过 IPC 通道进行通信。

第十五方面，提供了一种 NAT 设备，该 NAT 设备包括：中央处理器、网络处理器和物理接口。中央处理器用于执行如下操作：为所述用户分配第二 IP 地址。

网络处理器用于触发物理接口执行如下操作：从 CP 设备接收第一 IP 地址；向所述 CP 设备发送第二 IP 地址。

可选地，所述 NAT 设备包括主控板和接口板，所述中央处理器设置在所述主控板上，所述网络处理器和所述物理接口设置在接口板上，所述主控板和所述接口板耦合。

在一种可能的实现方式中，主控板和接口板之间建立进程间通信协议（inter-process communication, IPC）通道，主控板和接口板之间通过 IPC 通道进行通信。

附图说明

- 图 1 是本申请实施例提供的一种 BNG 系统进行 NAT 的示意图；
- 图 2 是本申请实施例提供的一种通过独立式 CGN 设备和日志服务器进行 NAT 的示意图；
- 图 3 是本申请实施例提供的一种 RADIUS 溯源下与合法监听平台交互的流程图；
- 图 4 是本申请实施例提供的一种日志服务器溯源下与合法监听平台交互的流程图；
- 图 5 是本申请实施例提供的一种系统架构的示意图；
- 图 6 是本申请实施例提供的一种系统架构的示意图；
- 图 7 是本申请实施例提供的一种系统架构的示意图；
- 图 8 是本申请实施例提供的一种通信方法 200 的流程图；
- 图 9 是本申请实施例提供的一种 NAT44 场景下通信方法 300 的流程图；
- 图 10 是本申请实施例提供的一种 NAT44 场景下通信方法 400 的流程图；
- 图 11 是本申请实施例提供的一种 DS-Lite 场景下通信方法 500 的流程图；
- 图 12 是本申请实施例提供的一种 CGN 设备双机备份的示意图；
- 图 13 是本申请实施例提供的一种 DS-Lite 场景下 CGN 设备双机备份的示意图；
- 图 14 是本申请实施例提供的一种 UP 双机备份的示意图；
- 图 15 是本申请实施例提供的一种 CP 设备的结构示意图；
- 图 16 是本申请实施例提供的一种 NAT 设备的结构示意图；
- 图 17 是本申请实施例提供的一种 CP 设备的结构示意图；
- 图 18 是本申请实施例提供的一种 NAT 设备的结构示意图；
- 图 19 是本申请实施例提供的一种网络系统 1500 的结构示意图。

具体实施方式

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

下面先对本申请实施例涉及的一些术语相关概念进行介绍。

(1) 控制面和用户面分离 (control plane and user plane disaggregated, CU 分离)

随着软件定义网络 (software defined network, SDN) 技术和网络功能虚拟化 (network functions virtualization, NFV) 技术的发展，城域网由传统以网络为核心的架构向以数据中心为核心的网络架构演进。传统的网元设备也从专业化朝着通用化演进。传统网元设备从专业化朝着通用化演进主要解决两个解耦：控制与转发的解耦、软件与硬件的解耦。

有鉴于此，CU 分离技术应运而生，成为本领域的研究热点。CU 分离是指 CP 和 UP 解耦的网络架构。CU 分离包括而但不限于下述实现方式 A 和实现方式 B。

实现方式 A、控制面和转发面位于不同硬件设备上。

在采用实现方式 A 时，CP 设备和 UP 设备是两个单独且不同的设备。可选地，CP 设备与 UP 设备分布式在不同的地点。例如，CP 设备位于云端的数据中心，UP 设备根据需求部署在网络中合适的位置。通过这种方式，使得控制面和转发面的部署更加灵活。

实现方式 B、控制面和转发面位于同一个硬件设备上且功能分离。

在采用实现方式 B 时，CP 设备的物理实体和 UP 设备的物理实体为同一个设备。例如，

CP 设备与 UP 设备运行在同一个主机、同一个服务器或同一个终端中。

在一些实施例中，CP 设备和 UP 设备均通过虚拟化技术实现。CP 设备例如称为虚拟 CP (virtual CP, vCP)，UP 设备例如称为虚拟 UP (virtual UP, vUP)。例如，CP 设备为虚拟机，UP 设备为虚拟路由器或虚拟交换机。在一些实施例中，CP 设备和 UP 设备均是基于通用的物理服务器结合 NF) 技术实现的，CP 设备和 UP 设备是两个不同的虚拟网络功能 (virtualized network function, VNF)。例如，CP 设备和 UP 设备均是通过 X86 服务器虚拟化出的网元。

在另一些实施例中，CP 设备通过虚拟化技术实现，UP 设备通过传统的网络设备实现。UP 设备例如称为物理 UP (physical UP, pUP)。

本实施例对通信系统中 CP 设备与 UP 设备之间的数量关系不做限定。在一些实施例中，CP 设备与 UP 设备是一对多的关系，即，一个 CP 设备用于控制多个 UP 设备。在另一些实施例中，CP 设备与 UP 设备是一一对应的关系，即，一个 CP 设备用于控制一个 UP 设备。

本实施例对通信系统中 UP 设备的数量不做限定。可选地，CU 分离的通信系统包括多个 UP 设备。可选地，CU 分离的通信系统中多个 UP 设备分布在不同的地点。可选地，CU 分离的通信系统中多个 UP 设备基于分布式架构协同分担转发任务。

值得说明的一点是，“CU 分离”可以具有不同的名称。例如，不同标准、同一标准的不同版本、不同厂商、不同应用场景对“CU 分离”可以具有不同的称呼。例如，术语“CU 分离”有时也可以被称为“控制和转发分离”、“转控分离”、“控制面和用户面分离”、“控制和用户分离”等。

值得说明的一点是，“CP”可以具有不同的名称。例如，不同标准、同一标准的不同版本、不同厂商、不同应用场景对“CP”可以具有不同的称呼。例如，术语“CP”有时也可以被称为“CP 功能 (CP function, CPF)”或“CP 面”。本文中“CP”、“CPF”和“CP 面”可互换使用。术语“CP 设备”是指实现了 CP 功能的任意设备。

值得说明的一点是，“UP”可以具有不同的名称。例如，不同标准、同一标准的不同版本、不同厂商、不同应用场景对“UP”可以具有不同的称呼。例如，术语“UP”有时也可以被称为“UP 功能 (UP function, UPF)”或“UP 面”。本文中“UP”、“UPF”和“UP 面”可互换使用。术语“UP 设备”是指实现了 UP 功能的任意设备。

(2) BNG 系统

BNG 系统作为传统的宽带接入网关设备，用于承担将用户设备接入宽带网络的功能，在用户宽带接入业务和场景中非常重要。对 BNG 系统在用户接入上的主要的要求是用户认证、接入控制、流量调度等。BNG 主要负责认证以及互联网协议 (internet protocol, IP) 地址分配。在一些实施例中，认证过程基于远程用户拨号认证服务 (remote authentication dial in user service, RADIUS) 实现。例如，BNG 作为 RADIUS 客户端 (RADIUS client)，会和 RADIUS 服务器 (RADIUS server) 交互完成终端的认证。BNG 处理的协议栈包括而限于以太网承载 IP 协议 (internet protocol over ethernet, IPoE)、以太网承载点到点协议 (point-to-point protocol over ethernet, PPPoE)、802.1ad 协议、以太网协议和一些 802.3 物理层 (some 802.3 phy) 协议。

(3) CU 分离的 BNG 系统

随着各种互联网业务的层出不穷，对 BNG 系统支持的用户的会话数量要求不断提高、对用户接入带宽不断提高、尤其对 BNG 系统对外提供业务开放、可编程的能力的要求越来越高。

有鉴于这些需求，BNG 系统基于 SDN 或 NFV 的架构实现控制与转发的解耦以及软件与硬件的解耦，成为 CU 分离的 BNG 系统，从而具备 CU 分离的架构带来的优势，

例如，BNG 系统中的 CP 设备控制 BNG 系统中的多个 UP 设备，CP 设备调度多个 UP 设备处理流量的转发任务，CP 设备为多个 UP 分配资源，因此与单机实现 BNG 系统的方式相比，CU 分离架构下 BNG 系统的设备的利用率和可靠性都能得到大幅的提升。

值得说明的一点是，本申请实施例中“CU 分离的 BNG”可以具有不同的名称。例如，不同标准、同一标准的不同版本、不同厂商、不同应用场景对“CU 分离的 BNG”可以具有不同的称呼。例如，术语“CU 分离的 BNG”有时也可以被称为“分离的 BNG 系统(disaggregated BNG, DBNG)”，相应地，CU 分离的 BNG 中的 CP 设备可以被称为 DBNG-CP，CU 分离的 BNG 中的 UP 设备可以被称为 DBNG-UP。又如，术语“CU 分离的 BNG”有时也可以被称为“虚拟宽带网络网关 (virtual BNG, vBNG) 控制面和用户面分离的系统 (control plane and user plane disaggregated System, CU 系统)”，即“vBNG CU 系统”，相应地，CU 分离的 BNG 中的 CP 设备可以被称为 vBNG-CP，CU 分离的 BNG 中的 UP 设备可以被称为 vBNG-UP。又如，术语“CU 分离的 BNG”有时也可以被称为“虚拟宽带远程接入服务器 (virtual broadband remote access server, vBRAS) CU 系统”，即“vBRAS CU 系统”，相应地，CU 分离的 BNG 中的 CP 设备可以被称为 vBRAS-CP，CU 分离的 BNG 中的 UP 设备可以被称为 vBRAS-UP。本文中“DBNG”、“vBNG CU 系统”和“vBRAS CU 系统”可互换使用。

(4) 用户

本申请实施例中的用户包括而不限于客户前置设备 (customer premise equipment, CPE) 或者终端。在一些实施例中，至少一个终端接入至 CPE，CPE 接入至 BNG 系统。BNG 系统为用户分配 IP 地址是指 BNG 系统为 CPE 分配 IP 地址，CPE 为每个终端进一步分配 IP 地址。在另一些实施例中，BNG 系统为用户分配 IP 地址是指 BNG 系统为终端分配 IP 地址。

(5) 运营商级 NAT (carrier-grade NAT, CGN)

CGN 狭义上指大规模的 NAT，具体是指通过规模化部署互联网协议第四版 (internet protocol version 4, IPv4) 私有地址，以达到对目前公网 IPv4 地址的统计复用的技术。CGN 能够提高 IPv4 地址的利用率，从而可以在相当长的时间内解决 IPv4 地址耗尽问题，保证业务的平滑过渡，为互联网协议第六版 (internet protocol version 6, IPv6) 地址的部署争取时间。按 CGN 设备的存在形式而言，CGN 设备分为独立式 CGN 设备和插卡式 CGN 设备。

(6) 独立式 CGN 设备

独立式 CGN 设备是一个独立的设备，该设备专门承担 CGN 功能。独立式 CGN 设备例如旁挂在 BNG 系统上。例如，在上行流量转发的过程中，用户私网 IPv4 的流量引导到独立式 CGN 设备，独立式 CGN 设备进行 NAT 处理后，将 NAT 转换后的公网 IPv4 流量返回到 BNG 系统。在使用独立式 CGN 设备的情况下，地址转换用户管理例如分别在 CGN 和 BNG 系统上进行。

插卡式 CGN 设备是指承担 CGN 功能的一个单板插在其他功能的设备上。插卡式 CGN 设备占用设备的一个槽位。

(7) NAT44

NAT44 (NAT IPv4-IPv4) 是指将一个 IPv4 地址转换为另一个 IPv4 地址。例如，将私网 IPv4 地址转换为公网 IPv4 地址。

(8) 双栈 (dual stack, DS)

双栈是指在设备上既安装 IPv4 的协议栈, 又安装 IPv6 的协议栈, 从而实现分别与 IPv4 节点或 IPv6 节点间的信息互通。

(9) 轻量级双栈 (dual stack lite, DS-Lite)

DS-Lite 技术不存在不同地址族之间的转换。DS-Lite 本质上是在 IPv6 的网络中部署 IPv4-in-IPv6 隧道完成 IPv4 业务传输, 而 IPv6 业务则直接通过 IPv6 网络传输。例如, 路由型 CPE 作为 DS-Lite 的基本桥接宽带 (basic bridging broadband, B4), BNG 系统作为 IPv6 单栈节点, 在城域网部署 CGN, CGN 作为 DS-Lite 的地址族转换路由器 (address family transition router, AFTR)。CPE、BNG 系统和 CGN 之间是 IPv6 单栈 (IPv6-Only) 网络, CGN 和核心路由器 (core router, CR) 之间是双栈网络。由于使用 DS-Lite 时城域网只需要部署部分双栈, 是轻量级的双栈, 称为 DS-Lite 方案。

(10) B4

B4 具备双栈的能力, 在主机或者 CPE 设备上实现。其中, CPE 设备在运营商组网中为家庭网关。B4 向 AFTR 创建 IPv4-in-IPv6 的隧道。

(11) AFTR

AFTR 终结了 IPv4-in-IPv6 隧道, 并且实现了 NAT44 的功能。其中, AFTR 在运营商网络中为 CGN; 该 CGN 可为独立 CGN 设备, 也可以为插卡式 CGN。

(12) 地址溯源

CGN 特性的部署隐藏了私网用户的 IP 地址信息, 国家安全部门要求 CGN 部署具备可溯源的能力, 即可以根据公网地址和端口号查询到私网用户的 IP 地址, 进一步锁定具体用户。本申请的一些实施例中, 地址溯源采用 RADIUS 溯源的方式。

(13) RADIUS 溯源

RADIUS 溯源是指在 RADIUS 服务器上进行地址溯源。RADIUS 溯源例如通过发送计费报文的过程实现。例如, BNG 系统为用户分配公网 IP 地址以及端口块后, BNG 系统将公网 IP 地址以及端口块携带在计费报文中, BNG 系统通过向 RADIUS 服务器发送计费报文, 从而将公网 IP 地址以及端口块上报给 RADIUS 服务器。例如, 当用户上线时, BNG 系统向 RADIUS 服务器发送计费开始报文, RADIUS 服务器接收计费开始报文, 根据计费开始报文记录一次 RADIUS 日志; 当用户下线时, BNG 系统向 RADIUS 服务器发送计费结束报文, RADIUS 服务器接收计费结束报文, 根据计费结束报文记录一次 RADIUS 日志。RADIUS 服务器根据两次记录的 RADIUS 日志进行地址溯源。其中, 根据计费开始报文记录的 RADIUS 日志包括私网 IP 地址、公网 IP 地址、端口块、用户上线时间的对应关系。用户上线时间例如是计费开始报文中的计费开始时间。根据计费结束报文记录的 RADIUS 日志包括私网 IP 地址、公网 IP 地址、端口块、用户上线时间的对应关系。用户下线时间例如是计费结束报文中的计费结束时间。

(14) 端口块 (port block)

端口块也称端口范围 (port Range)。端口块包括 NAT 设备为用户分配的至少一个端口号。例如, BNG 系统为一个私网 IP 地址分配一个公网 IP 地址和一个端口段, 当对该私网 IP 地址进行 NAT 处理时, 均使用该公网 IP 地址和端口段中的端口号。

(15) 框间备份

框间备份是指一台设备中的 CPU 与另一台设备中的 CPU 互为备份关系。采用框间备份方案时，主 NAT 实例和备 NAT 实例是两个不同硬件设备上的 CPU。其中，NAT 实例是一个具体的 NAT 设备。例如，主 NAT 实例是 CGN 设备 1 上 1 号槽位的 0 号 CPU，备 NAT 实例是 CGN 设备 2 上 2 号槽位的 0 号 CPU。

(16) 框间温备

框间温备是指业务正常运行场景下，由主 NAT 设备进行业务处理，同时备 NAT 设备实时备份用户的信息。故障倒换场景下，主 NAT 设备发生故障，备 NAT 设备倒换为主 NAT 设备，根据预先备份的用户的信息进行业务的处理。

由于本申请实施例涉及 NAT 技术的应用，为了便于理解，下面对 NAT 技术的应用场景以及 NAT 技术在应用中的一些情况进行介绍。

由于公网的 IP 地址（如公网 IPv4 地址）数量有限，IP 地址耗尽已成为亟需解决的技术问题。有鉴于此，宽带拨号用户一般由 BNG 系统分配私网 IP 地址，并且用户的流量会被进行 NAT 地址转换，将用户的私网 IP 地址转换成公网 IP 地址。由于公网 IP 地址与用户之间为一对多的关系，达到了公网 IP 地址统计复用的功能，提高了公网 IP 地址的利用率，从而解决了公网 IP 地址数量有限的问题。NAT 技术在应用中时，面临以下情况一至情况二。

情况一、通过插卡式 CGN 设备以及 RADIUS 服务器实现溯源的情况

在一些实施例中，NAT 设备选择通过插卡式 CGN 设备实现。BNG 系统中的 UP 设备（如迷你 BNG 设备）插入插卡式 CGN 设备，实现 RADIUS 溯源。在这种情况下，由于 UP 设备和 CGN 设备集成在一起，NAT 地址转换是在 BNG 系统上进行的。例如，请参见附图 1，附图 1 示出了在 BNG 系统上进行 NAT 的过程，具体包括以下步骤 1 至步骤 5。

步骤 1、用户发送拨号请求，拨号请求用于向 BNG 系统申请 IP 地址。例如，在附图 1 中，拨号请求从终端传输至家庭网关（residential gateway, RGW），再由 RGW 传输至交换机（switch, SW）或光线路终端（optical line termination, OLT），再由 SW 或 OLT 传输至 BNG 系统。

步骤 2、BNG 系统接收拨号请求，向 RADIUS 服务器发起认证请求。

步骤 3、RADIUS 服务器接收认证请求，生成认证结果，向 BNG 系统回复认证结果。

步骤 4、BNG 系统根据配置向用户分配私网 IP 地址、用户的公网 IP 地址以及端口块。并且，BNG 系统向 RADIUS 服务器发送计费报文，通过 RADIUS 属性携带用户的公网 IP 地址以及端口块，从而实现用户的 NAT 溯源。

步骤 5、终端发送流量，流量转发至 BNG 系统。BNG 系统对流量进行 NAT 转换后，向公网侧发送转换后的流量，使得用户访问公网。例如，如附图 1 所示，流量的源 IP 地址为私网 IPv4 地址(10.1.1.1)，BNG 系统将私网 IPv4 地址(10.1.1.1)转换为公网 IPv4 地址(100.1.1.1)。

在 NAT 场景下应用情况一时，具有两个方面的缺陷。

一方面，时下海外存在很多二级运营商租用一级运营商的城域网，自己部署高挂的大容量框式 BNG 系统。但是，随着 CDN 的下沉以及出于便于维护的考虑，运营商希望将 BNG 下沉到边缘，选择采用迷你 BNG 设备实现 BNG 系统。由于 BNG 系统是小型化的，可以满足机房空间和功耗的要求。然而，由于比较大的框式 BNG 设备才有适于插入插卡式 CGN 设备的槽位，而迷你 BNG 设备没有单独的槽位插入插卡式 CGN 设备，造成插卡式 CGN 设备

只能放在比较大的框式 BNG 设备上实现。而迷你 BNG 设备自身线路处理板的 NAT 转发能力非常弱，不能满足 NAT 转换的要求。

另一方面，在迁移（steering）场景下，当 UP 设备插入了插卡式 CGN 设备后，如果 CP 设备将用户从原始 CP 设备迁移至目标 UP 设备，NAT 溯源信息需要被刷新。NAT 溯源信息刷新是指在目标 UP 设备上插入的插卡式 CGN 设备上保存迁移的用户的 NAT 溯源信息。具体地，目标 UP 设备上插入的插卡式 CGN 设备要为每一个迁移的用户分配公网 IP 地址以及端口块。并且，插卡式 CGN 设备要为每一个迁移的用户发送计费更新报文。然而，由于插卡式 CGN 设备只是个板卡，插卡式 CGN 设备的算力不足，难以承担大量用户迁移产生的 NAT 溯源信息刷新任务，造成刷新 NAT 溯源信息的速度非常慢，与 CP 设备下发用户表项的速率无法匹配，导致用户业务中断的时间会非常长。其中，Steering 场景也称用户在线动态迁移的场景，Steering 场景是指已上线的用户会从一个 UP 设备迁移到另外一个 UP 设备的情况。

情况二、通过独立式 CGN 设备以及日志服务器实现溯源的情况

独立式 CGN 设备高挂结合日志服务器的架构可以解决情况一中插卡式 CGN 设备具有的 NAT 转换能力不足的问题。例如，请参见附图 2，附图 2 示出了通过独立式 CGN 设备以及日志服务器进行 NAT 的过程，具体包括以下步骤 1 至步骤 5。

步骤 1、用户发送拨号请求，拨号请求用于向 BNG 系统申请 IP 地址。

步骤 2、BNG 系统接收拨号请求，向 RADIUS 服务器发起认证请求。

步骤 3、RADIUS 服务器接收认证请求，生成认证结果，向 BNG 系统回复认证结果。

步骤 4、BNG 系统根据配置向用户分配私网 IP 地址，并向 RADIUS 服务器发送计费报文，计费报文携带用户私网 IP 地址且不携带公网 IP 地址。

步骤 5、终端发送流量，流量转发至 CGN 设备。CGN 设备对流量进行 NAT 转换后，向公网侧发送转换后的流量，使得用户访问公网。在此步骤中，CGN 设备接收到流量后，会根据接收的流量建立 NAT 会话，并根据 NAT 会话生成 NAT 日志，将 NAT 日志发送给日志服务器，以便日志服务器根据 NAT 日志进行溯源。

在 NAT 场景下应用情况二时，具有两个方面的缺陷。

一方面，由上述步骤 5 可见，独立式 CGN 设备是在收到用户流量的触发下生成 NAT 会话，进而生成溯源使用的 NAT 日志。独立式 CGN 设备自身不会与 RADIUS 服务器交互，只能采用日志服务器进行地址溯源，无法保持原有的 RADIUS 溯源方式，运营商需要额外投资新建日志服务器，建设额外的日志服务器造成开销过大，成本过高。

另一方面，很多运营商部署了合法监听（lawful interception, LI）。合法监听功能是通过 RADIUS 服务器与合法监听设备交互实现的。合法监听设备例如包括合法监听网关（lawful interception gateway, LIG）以及监听中心（law enforcement agency, LEA）例如，参见附图 3，LEA 与 RADIUS 服务器交互，LEA 根据用户的公网 IP 地址以及端口块，查询用户的账号信息。LIG 根据用户账号信息，向 BNG 系统发起合法监听请求。

而参见附图 4，如果采用独立式 CGN 设备以及日志服务器进行溯源的方式，由于 NAT 溯源采用了日志服务器而非 RADIUS 服务器，因此运营商对应的合法监听设备也需要被重新改造，导致客户需要改造的设备比较多，增加了客户的建设和维护成本，无疑费用会非常大。而且，部分客户在用户上线时，具有由 RADIUS 服务器指定用户进行 NAT 时被分配的公网 IP 地址和端口块的需求。但是在采用日志服务器进行溯源的方式时，CGN 设备与 RADIUS

服务器无法交互, CGN 设备也就无法根据 RADIUS 服务器指定的公网 IP 地址分配公网 IP 地址, CGN 设备也就无法根据 RADIUS 服务器指定的端口块分配端口块。

有鉴于上述情况一和情况二存在的需求, 本申请的一些实施例, 提供一种对具有私网 IP 地址的用户进行 NAT 溯源的方案, 通过采用 CU 分离的 BNG 系统, 将 BNG 系统的 CP 设备作为统一的控制面, 由 CP 设备在管理 UP 设备的同时, 还管理独立式 CGN 设备。

针对情况一来说, 由于本申请的一些实施例采用了独立式 CGN 设备进行 NAT 处理, 独立式 CGN 设备的性能更强、容量更高, 解决了插卡式 CGN 设备的 NAT 能力不足的问题, 有助于支持对 CGN 设备性能要求高的 Steering 场景。并且, 摆脱了对 BNG 设备需要具备额外槽位的限制, 适于采用迷你 BNG 设备实现 BNG 系统的场景。

针对情况二来说, 本申请的一些实施例实现了 RADIUS 溯源的方式, 解决了使用独立式 CGN 设备时难以通过 RADIUS 服务器进行溯源的技术问题。一方面, 由于地址溯源是通过 RADIUS 服务器实现的, 而无需借助日志服务器, 从而摆脱了运营商进行溯源时在现网中增加日志服务器的限制。另一方面, 摆脱了运营商进行溯源时修改 LIG 设备的限制, 也就节省了修改 LIG 设备会带来的巨大工作量以及成本。另一方面, CP 设备能够通过与 RADIUS 服务器进行交互, 满足通过 RADIUS 服务器指定用户进行 NAT 时公网 IP 地址和端口范围的需求。

CP 设备对 CGN 设备的管理功能包括而但不限于以下管理功能一至管理功能五。

管理功能一、CP 设备将分配的用户 IP 地址(如私网 IPv4 地址或 IPv6 地址)下发给 CGN 设备。

管理功能二、在主 CGN 设备故障时, CP 设备将流量引导至备 CGN 设备。

管理功能三、CP 设备将主 CGN 设备上保存的用户表项同步至备 CGN 设备。

管理功能四、用户下线后, CP 设备清除 CGN 设备上的用户表项。

管理功能五、CP 设备为 CGN 设备指定分配的端口块的范围。

下面, 通过附图 5 示出的系统架构, 对 CP 设备统一管理 UP 设备以及 CGN 设备所基于的系统架构举例说明。通过附图 8 所示的方法 200、附图 9 所示的方法 300、附图 10 所示的方法 400、附图 11 所示的方法 500, 对 CP 设备如何实现管理功能一举例说明。通过附图 12 以及 S701 至 S708、S801 至 S804、附图 13 以及步骤 S901 至 S903 对 CP 设备如何实现管理功能二举例说明。通过 S601 至 S605, 对 CP 设备如何实现管理功能三举例说明。通过 S203 至 S223, 对 CP 设备如何实现管理功能四举例说明。通过 S201 至 S241, 对 CP 设备如何实现管理功能五举例说明。

参见附图 5, 本申请实施例提供了一种系统架构, 系统架构包括 CP 设备、UP 设备、接入网络设备、CPE 以及 NAT 设备。

CP 设备用于承担控制面的功能。在一些实施例中, CP 设备是 CU 分离的 BNG 系统中的 CP 设备, CP 设备承担 BNG 系统中控制面的功能。例如, CP 设备基于拨号协议处理用户的拨号请求。CP 设备与认证授权计费(authentication、authorization、accounting, AAA)交互, 进行用户认证、计费以及授权。其中, 当用户认证通过后, CP 设备将用户表项下发到用户接入的 UP 设备。UP 设备生成该用户的用户表项, 并向外发布路由。CP 设备包括以太网承

载点到点协议(point-to-point protocol over ethernet, PPPoE)模块或以太网承载 IP 协议(internet protocol over ethernet, IPoE) 模块、用户管理模块、AAA 模块、UP 管理模块、地址管理模块以及 RADIUS 模块。

在本申请的一些实施例中,由 CP 设备管理 UP 设备以及 NAT 设备(如独立式 CGN 设备)。例如,CP 设备通过用户管理模块管理 NAT 设备,CP 设备通过 UP 管理模块用户管理模块管理 NAT 设备。一个 CP 设备例如管理至少一个 UP 设备以及至少一个 NAT 设备。CP 设备与 UP 设备通过网络相连。CP 设备与 NAT 设备通过网络相连。

CP 设备例如通过虚拟化技术实现。例如,参见附图 6,CP 设备为 VNF,CP 设备是通过 X86 服务器虚拟化出的网元,CP 设备的物理实体为 X86 服务器。

UP 设备用于承担用户面的功能。在一些实施例中,UP 设备是 CU 分离的 BNG 系统中的 UP 设备,UP 设备承担 BNG 系统中用户面的功能。当用户请求上线时,UP 设备将用户的拨号请求通过业务通道上送至 CP 设备处理。CP 设备处理拨号请求后,向 UP 设备下发用户表项。UP 设备接收 CP 设备下发的用户表项,UP 设备在本地生成用户表项,UP 设备根据用户表项进行相关的业务策略执行和流量转发。并且,UP 设备向外发布路由。UP 设备包括多种实现方式。UP 设备通过网络与接入网络设备相连。

在一些实施例中,UP 设备通过虚拟化技术实现。例如,参见附图 6,UP 设备为 VNF,UP 设备是通过 X86 服务器虚拟化出的网元,UP 设备的硬件是 X86 服务器。在采用虚拟化技术实现 UP 设备时,UP 设备例如称为 vUP 设备(VNF)。在另一些实施例中,UP 设备为网络设备,UP 设备为 PNF。例如,UP 设备是硬件迷你 BNG 设备或框式 BNG 系统中的任一种。在采用网络设备实现 UP 设备时,UP 设备例如称为 pUP 设备(PNF)。接入网络设备包括但不限于接入节点(access node, AN)设备、SW 或 OLT 中的任一种。接入网络设备通过网络与 CPE 以及 UP 设备相连。接入网络设备用于将 CPE 汇聚至 UP 设备。接入网络设备还用于进行二层报文的转发,并对用户进行虚拟局域网(virtual LAN, VLAN)或 QinQ 的隔离。其中, QinQ 也称堆栈 VLAN(stacked VLAN)或双 VLAN(double VLAN)。

CPE 在运营商组网中为家庭网关(RGW,也称家庭终端)。CPE 用于接入家庭内的个人计算机(Personal Computer, PC)、手机。CPE 一般会进行 NAT 处理,向家庭内的 CP 设备、手机分配私网 IP 地址。此外,CPE 还进行 PPPoE、IPoE 协议拨号,向 BNG 系统获取 IP 地址,根据获取的 IP 地址进行网络访问。

NAT 设备用于进行 NAT 处理。例如,NAT 设备将用户的私网 IP 地址转换成公网 IP 地址以及端口块。又如,NAT 设备将用户的 IPv6 地址转换成公网 IP 地址以及端口块。在一些实施例中,NAT 设备为 CGN 设备。例如,NAT 设备为独立式 CGN 设备。独立式 CGN 设备包括多种实现方式。例如,独立式 CGN 设备是硬件设备,例如,独立式 CGN 设备是网络设备。又如,独立式 CGN 设备通过虚拟化技术实现。例如,独立式 CGN 设备是通过 X86 服务器虚拟化出的网元。在另一些实施例中,NAT 设备为 CGN 设备之外的其他具备 NAT 处理功能的设备。

参见附图 7,CP 设备与 UP 设备之间具有三种接口,三种接口分别是控制报文重定向接口(control packet redirect interface, CPRi)、管理接口(management interface, Mi)以及状态控制接口(state control interface, SCi)。

CPRi 采用基于 Vxlan 通用协议(Vxlan generic protocol encapsulation, Vxlan-GPE)接口

实现。UP 设备接收用户的接入报文，UP 设备会根据 CPRi 对应的报文封装格式，对接入报文进行封装，将封装后的接入报文上送至 CP 设备处理。

Mi 采用基于 XML 的网络配置协议 (Netconf) 接口实现。CP 设备采用 Mi 向 UP 设备下发配置，UP 设备采用 Mi 上报 UP 设备的运行状态。

SCi 采用转控分离协议 (control plane and user plane separated protocol, CUSP) 接口实现。CP 设备处理用户接入报文，完成用户的协议交互，用户上线后，CP 设备通过 SCi 向对应用户接入的 UP 设备下发用户的用户表项。

在本申请的一些实施例中，CP 设备在管理 CGN 设备时，同样采用 CPRi、Mi 以及 SCi 实现。例如，主 CGN 设备通过 SCi 向 CP 设备上报用户表项，CP 设备采用 SCi 向备 CGN 设备下发用户表项。

在一些实施例中，通信系统包括网关系统，网关系统为 BNG 系统或者 BRAS 系统。通过选用 BNG 系统中的 CP 或者 BRAS 系统中的 CP 实现本实施例方案，有助于复用 BNG 系统或者 BRAS 系统的网络架构，降低实现复杂度。可选地，采用 BNG 系统以及 BRAS 系统之外其他的 CU 分离通信系统中的 CP 实现 CP 设备。例如，采用 CU 分离的服务网关 (serving gateway, S-GW) 中的 CP 实现 CP 设备。又如，采用 CU 分离的分组数据网网关 (PDN gateway, PGW) 中的 CP 实现 CP 设备。又如，采用移动性管理功能 (access and mobility management function, AMF) 网元实现 CP 设备。又如，采用会话管理功能 (session management function, SMF) 网元实现 CP 设备。又如，采用 WT-456 固定、移动融合的通信系统中的接入网关功能 (access gateway function, AGF) 网元实现 CP 设备。

下面，以 UP 设备为迷你 BNG 设备、NAT 设备为独立式 CGN 设备、CP 设备分配的 IP 地址为私网 IPv4 地址的情况为例，对如何基于附图 5 示出的系统架构实现本申请实施例简要说明。

CP 设备同时管理迷你 BNG 设备和独立式 CGN 设备。用户从迷你 BNG 设备上线；CP 设备响应于上线请求，为用户分配私网 IPv4 地址后，同时将用户的私网 IPv4 地址下发给独立式 CGN 设备；独立式 CGN 设备从本地公网地址池中，为用户分配私网 IPv4 地址对应的公网 IPv4 地址以及端口块；独立式 CGN 设备将公网 IPv4 地址以及端口块上报给 CP 设备；CP 设备在计费报文中携带用户的公网 IPv4 地址以及端口块，将计费报文上报给 AAA，实现用户 RADIUS 溯源。

参见附图 8，附图 8 是本申请实施例提供的一种通信方法 200 的流程图。可选地，方法 200 由 CP 设备、NAT 设备以及 RADIUS 服务器执行。

示例性地，方法 200 包括 S210 至 S280。

S210、CP 设备为用户分配第一 IP 地址。

本实施例中，CP 设备和 NAT 设备会为同一个用户分配不同的 IP 地址。为了区分描述，将 CP 设备为用户分配的 IP 地址称为第一 IP 地址，将 NAT 设备为用户分配的 IP 地址称为第二 IP 地址。第一 IP 地址以及第二 IP 地址也称为用户的 IP 地址。

S220、CP 设备向 NAT 设备发送第一 IP 地址。

在一些实施例中，第一 IP 地址包括私网 IPv4 地址或者 IPv6 地址中的至少一项。

可选地, 第一 IP 地址为私网 IPv4 地址。例如, 在 NAT44 场景下, CP 设备为用户分配私网 IPv4 地址。NAT44 场景具体的处理流程请参考下述附图 9 所示的方法 300 或附图 10 所示的方法 400。CP 设备通过分配私网 IPv4 地址以及向 NAT 设备下发私网 IPv4 地址, 有助于支持 NAT44 场景下实现 RADIUS 溯源。可选地, 第一 IP 地址为 IPv6 地址。例如, 在 DS-Lite 场景下, CP 设备为用户分配 IPv6 地址。DS-Lite 场景具体的处理流程请参考下述附图 11 所示的方法 500。CP 设备通过分配 IPv6 地址以及向 NAT 设备下发 IPv6 地址, 有助于支持 DS-Lite 场景等双栈网络中实现 RADIUS 溯源。可选地, 第一 IP 地址包括私网 IPv4 地址以及 IPv6 地址。

CP 设备如何向 NAT 设备下发 IP 地址包括多种方式。在一些实施例中, CP 设备基于 CUSP 向 NAT 设备发送第一 IP 地址。例如, CP 设备生成并发送 CUSP 消息, CUSP 消息包括第一 IP 地址。在另一些实施例中, CP 设备基于 PFCP 向 NAT 设备发送第一 IP 地址。例如, CP 设备生成并发送 PFCP 消息, PFCP 消息包括第一 IP 地址。

S230、NAT 设备从 CP 设备接收 CP 设备为用户分配的第一 IP 地址。

S240、NAT 设备为用户分配第二 IP 地址。

第二 IP 地址为公网 IP 地址。例如, 第二 IP 地址为公网 IPv4 地址。在一些实施例中, NAT 设备从地址池中选择未被占用的公网 IP 地址, 作为分配的 IP 地址。

S250、NAT 设备向 CP 设备发送第二 IP 地址。

在一些实施例中, NAT 设备向 CP 设备发送第一 IP 地址和第二 IP 地址之间的对应关系, 以便 CP 设备知道 NAT 设备上报的公网 IP 地址是 NAT 设备为哪个用户的 IP 地址分配的。

在一些实施例中, NAT 设备收到 CP 设备下发的第一 IP 地址之后, NAT 设备不仅为用户分配公网 IP 地址, 还为用户分配端口块。相应地, NAT 设备不仅向 CP 设备上报公网 IP 地址, 还上报为用户分配的端口块。其中, 端口块包括至少一个端口号。

从步骤 S230 至步骤 S250 可见, 本实施例中 NAT 设备分配公网 IP 地址的触发方式与相关技术存在区别, 不是由收到流量的事件触发, 而是由 CP 设备下发 IP 地址的事件触发。

在一些实施例中, NAT 设备在本地保存分配的第二 IP 地址和端口块。例如, NAT 设备生成并保存用户的信息, 用户的信息包括第一 IP 地址、第二 IP 地址和端口块的对应关系。其中, 用户的信息的形式例如是用户表中的表项。例如, NAT 设备在用户表中新建用户表项, 在用户表项中保存第一 IP 地址、第二 IP 地址和端口块的对应关系, 该保存了第一 IP 地址、第二 IP 地址和端口块的对应关系的用户表项即为用户的信息。在一些实施例中, NAT 设备本地的用户表项除了包括第一 IP 地址、第二 IP 地址和端口块的对应关系之外, 还包括用户的其他信息, 例如用户标识等。

NAT 设备通过在本地保存用户的信息, 以便后续在数据报文转发阶段根据预先保存的用户的信息生成转发表项。在数据报文转发阶段, 当 NAT 设备接收到上行的数据报文时, 识别数据报文的源 IP 地址以及源端口号, 根据源 IP 地址查找用户的信息, 得到用户的信息中与源 IP 地址对应的 IP 地址以及源端口号对应的端口号, 将源 IP 地址转换为查找到的 IP 地址, 将源端口号转换为查找到的端口号, 从而进行 NAT。在一些实施例中, 数据报文的源 IP 地址是私网 IPv4 地址 (第一 IP 地址), 查找到的 IP 地址为第二 IP 地址, 换句话说, 将 CP 设备预先分配的私网 IPv4 地址转换为 NAT 设备预先分配的公网 IP 地址。在另一些实施例中, 例如在 DS-Lite 场景下, 数据报文是 IPv4-in-IPv6 的形式, 数据报文包括两个 IP 头, 外层的 IP

头是 IPv6 头，数据报文内层的 IP 头是 IPv4 头。外层的 IPv6 头属于隧道头。外层的 IPv6 头中的源 IP 地址是 CPE 的 IPv6 地址。CPE 的 IPv6 地址为 CP 设备分配的第一 IP 地址。内层的 IPv4 头中的源 IP 地址是 CPE 为终端分配的私网 IPv4 地址。NAT 设备会将 IPv4 头中的私网 IPv4 地址转换为公网 IPv4 地址。换句话说，将 CPE 预先分配的私网 IPv4 地址转换为 NAT 设备预先分配的公网 IP 地址。

在一些实施例中，NAT 设备向 CP 设备发送 NAT 设备本地的用户的信息，CP 设备从 NAT 设备接收用户的信息。通过这种方式，将 NAT 设备本地的用户表项同步给了 CP 设备。

S260、CP 设备从 NAT 设备接收第二 IP 地址，第二 IP 地址为 NAT 设备为用户分配的公网 IP 地址。

NAT 设备如何向 CP 设备上报 IP 地址和端口块包括多种方式。在一些实施例中，NAT 设备基于 CUSP 向 CP 设备发送第二 IP 地址和端口块。例如，NAT 设备生成并发送 CUSP 消息，CUSP 消息包括第二 IP 地址和端口块。在另一些实施例中，NAT 设备基于 PFCP 向 CP 设备发送第二 IP 地址和端口块。例如，NAT 设备生成并发送 PFCP 消息，PFCP 消息包括第二 IP 地址和端口块。

在一些实施例中，CP 设备在本地保存分配的第二 IP 地址和端口块。例如，CP 设备生成并保存用户的信息，用户的信息包括第一 IP 地址、第二 IP 地址和端口块的对应关系。其中，用户的信息的形式例如是用户表中的表项。例如，CP 设备在用户表中新建用户表项，在用户表项中保存第一 IP 地址、第二 IP 地址和端口块的对应关系，该保存了第一 IP 地址、第二 IP 地址和端口块的对应关系的用户表项即为用户的信息。在一些实施例中，CP 设备本地的用户表项还包括用户的授权信息，用户的授权信息例如服务质量（quality of service, QoS）信息、访问控制列表（access control lists, ACL）信息、媒体访问控制（media access control, Client MAC）地址等。

S270、CP 设备向 RADIUS 服务器发送计费报文。

CP 设备在生成计费报文时，会将 NAT 设备上报的公网 IP 地址（第二 IP 地址）以及 CP 设备分配的 IP 地址（第一 IP 地址）携带在计费报文中，使得计费报文包括第一 IP 地址和第二 IP 地址。此外，在 NAT 设备向 CP 设备上报端口块的情况下，CP 设备还会将 NAT 设备上报的端口块携带在计费报文中，使得计费报文包括第一 IP 地址和第二 IP 地址以及端口块。

计费报文包括而不限于计费开始报文或者计费结束报文中的至少一项。计费开始报文用于请求 RADIUS 服务器开始计费。计费结束报文用于请求 RADIUS 服务器结束计费。在一些实施例中，计费报文还包括端口块。在一些实施例中，计费报文还包括用户的上线时间或者用户的下线时间中的至少一项。用户的上线时间例如为计费开始报文中的计费开始时间。用户的下线时间例如为计费开始报文中的计费结束时间。第一 IP 地址、第二 IP 地址、端口块、用户的上线时间或者用户的下线时间可称为计费报文携带的用户的 NAT 溯源信息。在一些实施例中，计费报文包括至少一个 RADIUS 属性（Attribute）字段，RADIUS 属性字段包括第一 IP 地址、第二 IP 地址、端口块、用户的上线时间或者用户的下线时间中的至少一项。

CP 设备通过发送计费报文，从而将 NAT 溯源信息（第一 IP 地址、第二 IP 地址、端口块、用户上线时间、用户下线时间）上报给 RADIUS 服务器。

S280、RADIUS 服务器从计费报文获得第一 IP 地址和第二 IP 地址，保存第一 IP 地址和第二 IP 地址之间的对应关系。

RADIUS 服务器接收计费报文后, 会执行计费流程, 并将计费报文携带的 NAT 溯源信息保存在本地。当需要根据第一 IP 地址溯源时, 向 RADIUS 服务器发送溯源请求, 溯源请求包括第二 IP 地址。RADIUS 服务器接收溯源请求, 从溯源请求获得第二 IP 地址, 根据第二 IP 地址查询 NAT 溯源信息, 得到第一 IP 地址, 从而实现 RADIUS 溯源。

本实施例提供的方法, CP 设备将分配的 IP 地址下发给 NAT 设备, NAT 设备在接收到 CP 设备下发的 IP 地址的触发条件下, 为用户分配 CP 设备下发的 IP 地址所对应的公网 IP 地址, 将公网 IP 地址上报给 CP 设备。CP 设备根据 NAT 设备上报的公网 IP 地址, 在计费报文中携带 CP 设备分配的 IP 地址以及 NAT 设备分配的公网 IP 地址, 向 RADIUS 服务器发送计费报文, 从而将 CP 设备分配的 IP 地址以及 NAT 设备分配的公网 IP 地址上报给 RADIUS 服务器, 以便在 RADIUS 服务器上进行 NAT 溯源。一方面, 由于 NAT 溯源采用了 RADIUS 溯源的方式, 能够通过复用 RADIUS 服务器进行溯源, 摆脱了需要建设日志服务器才能溯源的限制, 减少溯源的成本。另一方面, 适于应用在 NAT 设备采用独立式 NAT 设备实现的场景, 有助于解决 NAT 设备采用业务单板等插卡式 NAT 设备实现时面临的 UP 槽位不足、NAT 处理能力不足等问题。

在一些实施例中, 当用户下线时, CP 设备清除 NAT 设备上保存的用户表项, 从而实现上文涉及的管理功能四。例如, 方法 200 具体包括以下步骤 S203 至 S223。

S203、若用户下线, CP 设备生成删除消息, 向 NAT 设备发送删除消息。

其中, 删除消息用于指示 NAT 设备删除 NAT 设备上保存的用户的信息。删除消息例如为 CUSP 消息。

S213、NAT 设备从 CP 设备接收删除消息。

S223、响应于删除消息, NAT 设备删除用户的信息。

CP 设备通过在用户下线时指示 NAT 设备删除用户的信息, 从而及时释放已下线的用户的信息在 NAT 设备上占用的存储空间, 节省了 NAT 设备的存储资源, 避免 NAT 设备上资源耗空的问题。

此外, 在一些实施例中, 若用户下线, CP 设备删除 CP 设备上保存的用户的信息, 使得 NAT 设备上保存的用户的信息和 CP 设备上保存的用户的信息被同步清除。例如, 在用户的信息的形式为用户表项的情况下, NAT 设备删除 NAT 设备上已下线的用户对应的用户表项, CP 设备删除 CP 设备上已下线的用户对应的用户表项, 从而完成 NAT 设备和 CP 设备同步清除用户表项的动作。CP 设备通过在用户下线时删除本地保存的用户的信息, 从而及时释放已下线的用户的信息在 CP 设备上占用的存储空间, 节省了 CP 设备的存储资源, 避免 CP 设备上资源耗空的问题。

在一些实施例中, 通过 RADIUS 服务器, 指定 NAT 时端口块所属的范围, 从而实现上文涉及的管理功能五。例如, 方法 200 具体包括以下步骤 S201 至 S241。

S201、RADIUS 服务器获得并向 CP 设备发送端口块集合。

其中, 端口块集合用于作为 NAT 设备分配的端口块的取值范围。端口块集合包括至少一个端口块。

S211、CP 设备从 RADIUS 服务器接收端口块集合。

S221、CP 设备向 NAT 设备发送端口块集合。

例如，CP 设备在向 NAT 设备下发第一 IP 地址时，还向 NAT 设备下发端口块集合，从而将第一 IP 地址和端口块集合一起传输至 NAT 设备上。

S231、NAT 设备从 CP 设备接收端口块集合。

S241、NAT 设备在端口块集合内，为用户分配端口块。

例如，NAT 设备从端口块集合中选择未被占用的端口块，将选择的端口块分配给用户。

在运营商需要指定用户的端口块的范围的场景下，通过由 RADIUS 服务器向 CP 设备下发端口块集合，再由 CP 设备将端口块集合下发给 NAT 设备，从而指定 NAT 设备在端口块集合内分配端口块，因此满足了指定 NAT 端口块范围的需求。尤其是，CP 通过将 RADIUS 指定的端口块集合和 IP 地址一起下发给 NAT 设备，使得通过 RADIUS 指定端口块范围的过程和触发 NAT 设备分配公网 IP 的过程得以同时执行，减少了通信开销和实现复杂度。

在一些实施例中，上述方法 200 中的第一 IP 地址为私网 IP 地址。具体地，当用户上线，由 CP 设备对用户的私网 IP 地址进行分配。同时，CP 设备下发用户私网 IP 地址以及相关信
息给 CGN 设备。CGN 设备从 CP 设备接收私网 IP 地址及相关信息后，为用户分配公网 IP
地址和端口块，将公网 IP 地址和端口块上报给 CP 设备。CP 设备在计费报文中增加用户公网
IP 地址和端口块，向 RADIUS 服务器发送计费报文，从而实现通过 RADIUS 服务器进行溯源。

请参见附图 9，附图 9 所示的方法 300 是对 NAT44 场景下如何实现方法 200 的举例说明。
换句话说，附图 9 所示的方法 300 关于 NAT44 场景下如何在采用独立式 CGN 设备的情况下
实现通过 RADIUS 服务器进行溯源。在附图 9 所示的方法 300 中，第一 IP 地址为私网 IPv4
地址，第二 IP 地址为公网 IPv4 地址，通信系统为 BNG 系统，NAT 设备为独立式 CGN 设备，
用户的信息保存在用户表中的用户表项中。

附图 9 所示的方法 300 包括以下 S301 至 S309。

S301、用户发送拨号请求。拨号请求用于向 BNG 系统申请 IP 地址。

S302、CP 设备接收拨号请求。CP 设备在拨号请求的触发下，向 RADIUS 服务器发起认
证请求。RADIUS 服务器认证通过后，CP 设备从私网地址池中，分配私网 IPv4 地址给用户。

S303、CP 设备将用户的私网 IPv4 地址下发给独立式 CGN 设备。

S304、独立式 CGN 设备从 CP 设备接收用户的私网 IPv4 地址。独立式 CGN 设备根据用
户的私网 IPv4 地址，在本地选择空闲的公网 IPv4 地址和端口块，将选择的公网 IPv4 地址和
端口块分配给用户。并且，独立式 CGN 设备在用户表中增加用户表项。新增的用户表项保存
了私网 IPv4 地址、公网 IPv4 地址和端口块的对应关系。

S305、独立式 CGN 设备将用户的私网 IPv4 地址、公网 IPv4 地址和端口块上报给 CP 设
备。

S306、CP 设备从独立式 CGN 设备接收用户的私网 IPv4 地址、公网 IPv4 地址和端口块。
CP 设备更新本地的用户表，在用户表中增加用户表项。新增的用户表项保存了公网 IPv4 地
址和端口块。

S307、CP 设备发送计费报文。计费报文例如是计费开始报文。计费报文携带用户的 NAT
溯源信息。NAT 溯源信息包括 CP 设备分配的私网 IPv4 地址、CGN 分配的公网 IPv4 地址以
及 CGN 分配的端口块。

S308、CP 设备向用户下发私网 IPv4 地址。

S309、CP 设备向 UP 设备下发对应的用户表项。

请参见附图 10, 附图 10 所示的方法 400 是对上述方法 300 的举例说明。在方法 400 中, BNG 系统中的 UP 设备为迷你 BNG 设备 (即附图 10 中的 mBNG)。CP 设备向 CGN 设备下发私网 IPv4 地址的动作通过 SCi 通道这种接口实现。CGN 设备向 CP 设备上报私网 IPv4 地址、公网 IPv4 地址和端口块的动作通过 SCi 通道这种接口实现。此外, 方法 400 还涉及与合法监听设备 (LIG 以及 LEA) 的交互流程。附图 10 所示的 NAT44 场景下的方法 400 包括以下 S401 至 S410。

S401、CPE 发送拨号请求。拨号请求也称用户上线请求。拨号请求例如是 PPPoE 拨号请求或动态主机配置协议 (dynamic host configuration protocol, DHCP) 拨号请求。CP 设备例如向二层网络广播拨号请求。迷你 BNG 设备 (UP 设备) 接收拨号请求。迷你 BNG 设备 (UP 设备) 通过 CPRi 通道, 将拨号请求上送至 CP 设备。

S402、CP 设备向 RADIUS 服务器发送认证请求。RADIUS 服务器认证通过后, RADIUS 服务器分配私网 IPv4 地址给用户。

S403、CP 设备通过 SCi 通道, 将用户的私网 IPv4 地址下发给 CGN 设备。

S404、CGN 设备分配公网 IPv4 地址以及端口块。并且, CGN 设备在用户表中增加用户表项。新增的用户表项保存了私网 IPv4 地址、公网 IPv4 地址和端口块的对应关系。

S405、CGN 设备通过 SCi 将用户私网 IPv4 地址、公网 IPv4 地址和端口块上报给 CP 设备。

S406、CP 设备向 RADIUS 服务器发送计费开始报文。计费开始报文携带用户的 NAT 溯源信息。NAT 溯源信息包括私网 IPv4 地址、公网 IPv4 地址和端口块。

S407、CP 设备向 CPE 下发私网 IPv4 地址。同时, CP 设备向迷你 BNG 设备下发用户表项。

S408、LIG 根据公网 IPv4 地址和端口块, 向 RADIUS 服务器请求用户的账号信息。用户的账号信息包括而不限于用户的名称、用户的账号和会话 ID 中的至少一项。具体地, 参见附图 10, LEA 向 LIG 发送合法监听请求 (LI request, LI 请求), 合法监听请求包括公网 IPv4 地址和端口块。LIG 接收 LI 请求, 使用公网 IPv4 地址, 从 RADIUS 服务器搜索用户的名称、账号和会话 ID。

S409、LIG 根据用户的账号信息, 向迷你 BNG 设备下发监听策略。监听策略例如为监听入口方向的报文或出口方向的数据报文。监听策略包括用户的账号以及会话 ID。监听策略例如为对迷你 BNG 设备的配置指令 (Configure command)。例如, 监听策略包括账号 1、会话 ID1 以及入口方向, 监听策略用于指示迷你 BNG 设备监听账号 1 的会话 ID1 的入口方向的数据报文。

S410、迷你 BNG 设备根据监听策略对用户的数据报文进行复制, 将复制出的数据报文转发至监听平台。

请参见附图 11, 附图 11 所示的方法 500 是对 DS-Lite 场景下如何实现方法 200 的举例说明。换句话说, 附图 11 所示的方法 500 关于 DS-Lite 场景下如何在采用独立式 CGN 设备的

情况下实现通过 RADIUS 服务器进行溯源。在附图 11 所示的方法 500 中,第一 IP 地址为 IPv6 地址,第二 IP 地址为公网 IPv4 地址,通信系统为 BNG 系统,用户的信息保存在用户表中的用户表项中。BNG 系统中的 UP 设备为迷你 BNG 设备(即附图 11 中的 mBNG)。

附图 11 所示的方法 500 包括以下 S501 至 S511。

S501、CPE 作为 DHCP 服务器,向终端分配私网 IPv4 地址。

S502、CPE 发送拨号请求。拨号请求也称用户上线请求。拨号请求例如是 PPPoE 拨号请求或 DHCP 拨号请求。CP 设备例如向二层网络广播拨号请求。迷你 BNG 设备(UP 设备)接收拨号请求。迷你 BNG 设备(UP 设备)通过 CPRi 通道,将拨号请求上送至 CP 设备。

S503、CP 设备向 RADIUS 服务器发送认证请求。RADIUS 服务器认证通过后,RADIUS 服务器分配 IPv6 地址给用户。

S504、CP 设备通过 SCi 将用户 IPv6 地址下发给 CGN 设备。

S505、CGN 设备根据用户 IPv6 地址分配公网 IPv4 地址以及端口块。并且,CGN 设备在用户表中增加用户表项。新增的用户表项保存了 IPv6 地址、公网 IPv4 地址和端口块的对应关系。

S506、CGN 设备通过 SCi 通道,将用户 IPv6 地址、公网 IPv4 地址以及端口块上报给 CP 设备。

S507、CP 设备向 RADIUS 服务器发送计费开始报文。计费开始报文携带用户的 NAT 溯源信息。NAT 溯源信息包括 IPv6 地址、公网 IPv4 地址和端口块。

S508、CP 设备向 CPE 下发 IPv6 地址。同时,CP 设备通过 SCi 通道,向迷你 BNG 设备下发用户表项。

S509、LIG 根据公网 IPv4 地址和端口块,向 RADIUS 服务器请求用户的账号信息。用户的账号信息包括而不限于用户的名称、用户的账号和会话 ID 中的至少一项。

S510、LIG 根据用户的账号信息向迷你 BNG 设备下发监听策略。

S511、迷你 BNG 设备根据监听策略对用户的数据报文进行复制,将复制出的数据报文转发至监听平台。

在一些实施例中,NAT 设备实现了可靠性方案,NAT 设备为互为备份关系的主 NAT 设备和备 NAT 设备中的备 NAT 设备。

在一些实施例中,NAT 设备的主备关系是 CP 设备配置的。例如,NAT 设备具有一个或多个 CPU,NAT 设备向 CP 设备发送 CPU 信息,CPU 信息指示 NAT 设备具有的 CPU 资源。CP 设备接收 CPU 信息,从 NAT 设备具有的一个或多个 CPU,选择第一 CPU 和第二 CPU。CP 设备向第一 CPU 发送配置指令,将第一 CPU 配置为主 NAT 设备,CP 设备向第二 CPU 发送配置指令,将第二 CPU 配置为备 NAT 设备。

在一些实施例中,CP 设备能够将主 NAT 设备上的用户表项同步至备 NAT 设备上,保证主 NAT 设备与备 NAT 设备之间的数据的一致性,使得主 NAT 设备故障时,备 NAT 设备能够根据获得的用户表项处理业务。下面,通过 S601 至 S605 对 CP 设备如何将主 NAT 设备上的用户表项同步至备 NAT 设备举例说明。

S601、主 NAT 设备向 CP 设备发送用户的信息,用户的信息包括第一 IP 地址、第二 IP 地址和端口块的对应关系。

S602、CP 设备从主 NAT 设备接收用户的信息。

S603、CP 设备向备 NAT 设备发送用户的信息。

S604、备 NAT 设备从 CP 设备接收用户的信息。

S605、在主 NAT 设备故障时，备 NAT 设备根据用户的信息为用户分配第二 IP 地址。

CP 设备通过将主 NAT 设备发来的用户的信息下发给备 NAT 设备，使得备 NAT 设备获得了主 NAT 设备上保存的用户的信息。一方面，实现了备 NAT 设备与主 NAT 设备之间用户的信息的同步，从而能在主 NAT 设备故障时触发主备倒换，实现业务正常运行。另一方面，备 NAT 设备与主 NAT 设备不需要部署类似 VRRP 的主备选举机制，这样就不需要在 CGN 之间拉直连线，简化配置和部署资源。

上述 S601 至 S605 适用的可靠性方案包括多种情况。例如，上述 S601 至 S605 应用在用户上线后两台 NAT 设备进行框间备份的情况。例如，上述 S601 至 S605 应用在用户上线后两台 NAT 设备之间实现 1:1 温备的情况，以下结合附图 12 举例说明。在附图 12 所示的方法中，两台 NAT 设备互为备份关系。两台 NAT 设备中一台 NAT 设备为主 NAT 设备，即主用 NAT 设备。两台 NAT 设备中另一台 NAT 设备为备 NAT 设备，即备用 NAT 设备。两台 NAT 设备例如是两台独立式 CGN 设备。其中，主 NAT 设备为主 CGN 设备，主 CGN 设备也称 CGN (M)；备 NAT 设备为备 CGN 设备，备 CGN 设备也称 CGN (S)。其中，CP 设备与主 CGN 设备、备 CGN 设备以及 UP 设备均通过 CPri、Mi、SCi 等接口通信。CP 设备与 RADIUS 服务器基于 RADIUS 协议通信。两台 NAT 设备例如称为两个 NAT 实例，两个 NAT 实例具有不同的实例 ID，一个 NAT 实例是主 CGN 设备的 NAT 实例，另一个 NAT 实例是备 CGN 设备的 NAT 实例。

附图 12 所示的 1:1 温备方法包括以下 S701 至 S708。

S701、用户上线后，CP 设备确定用户上线的 UP 设备的 ID。然后，CP 设备根据配置信息，确定 UP 设备的 ID 下绑定的主 CGN 设备和备 CGN 设备。

S702、CP 设备与 RADIUS 服务器交互后，CP 设备生成用户表项，下发用户表项给主 CGN 设备。

S703、主 CGN 设备从 CP 设备接收用户表项，完成用户表项分配。主 CGN 设备将分配的用户表项返回给 CP 设备。

S704、CP 设备从主 CGN 设备接收用户表项，给备 CGN 设备下发用户表项。在另一些实施例中，由主 CGN 设备向备 CGN 设备下发用户表项。

S705、CP 设备完成 RADIUS 溯源。

S706、CP 设备检测到主 CGN 设备故障。

在一些实施例中，主 CGN 设备是实现 CGN 功能的主 CPU，CP 设备检测主 CGN 设备故障是指检测到主 CPU 故障或者主 CPU 所在的业务板故障。

S707、CP 设备通过 CGN 设备绑定的 UP 设备 ID，确定主 CGN 设备与备 CGN 设备之间的备份关系。CP 设备根据主 CGN 设备与备 CGN 设备之间的备份关系以及主 CGN 设备，确定备 CGN 设备。

S708、CP 设备将流量引导到备 CGN 设备上，使得流量从主 CGN 设备切换至备 CGN 设备上。

在主备倒换过程中，CP 设备如何将流量引导至备 NAT 设备（备 CGN 设备）上包括多种方式，以下结合两类场景进行举例说明。

场景一、NAT44 场景下双机备份

在一些实施例中，CP 设备通过刷新备 NAT 设备上公网地址（第二 IP 地址）对应的路由优先级，实现 NAT44 场景下的流量切换。具体地，主 NAT 设备和备 NAT 设备上会保存同一个公网 IP 地址段。主 NAT 设备上保存的公网 IP 地址段的路由优先级高，备 NAT 设备上保存的公网 IP 地址段的路由优先级低。因此，在主 NAT 设备正常时，下行流量会路由转发至备 NAT 设备。在主 NAT 设备故障时，CP 设备与备 NAT 设备会交互执行以下步骤 S801 至 S804。其中，下行流量是指从 UP 设备发往用户设备的流量，下行流量也称网络侧流量或公网侧流量，下行流量中的源 IP 地址为公网 IP 地址。

S801、若主 NAT 设备处于故障状态，CP 设备生成第一更新消息。

S802、CP 设备向备 NAT 设备发送第一更新消息。

第一更新消息也称路由优先级更新命令。第一更新消息用于指示备 NAT 设备提高第二 IP 地址对应的路由优先级。其中，第二 IP 地址对应的路由优先级例如为第二 IP 地址所属的网段的路由优先级，该网段中的每个 IP 地址对应于同一个路由优先级。第二 IP 地址对应的路由优先级也称公网 IP 网段的路由优先级。

S803、备 NAT 设备从 CP 设备接收第一更新消息。

S804、响应于第一更新消息，备 NAT 设备提高第二 IP 地址对应的路由优先级。

当主 NAT 设备发生故障时，CP 设备通过向备 NAT 设备下发第一更新消息，从而通知备 NAT 设备调整公网地址对应的路由优先级，由于备 NAT 设备的公网地址对应的路由优先级升高，因此网络侧的流量会从主 NAT 设备切换至备 NAT 设备上，使得备 NAT 设备升级为主 NAT 设备，代替之前故障的主 NAT 设备处理网络侧的流量，避免流量传输中断。此外，由于流量的切换是 CP 设备引导的，能够保证主 NAT 设备与备 NAT 设备不会存在流量绕行。尤其是，该方法能够适用于 NAT44 场景，有助于 NAT44 场景下实现双机备份。

例如，参见附图 12，CGN1 和 CGN2 互为主备。CGN1 和 CGN2 中每个 CGN 可选地包括多个 CPU。CGN1 和 CGN2 分别将 CPU 资源上报给 CP 设备。CP 设备配置 CGN 的主备关系。其中，多对主备 CPU 实例和同一个 loopback 地址关联。主 CGN 的 loopback 地址对应的路由优先级高。此外，一对充当 CGN 的主备 CPU 共享一段公网地址，公网地址例如为 100.1.1.0/24。主 CPU 的公网地址所属的地址段的路由优先级高于备 CPU 的公网地址所属的地址段的路由优先级。当 CGN1（主 CGN）的 CPU 出现故障，CGN1 将故障事件上报给 CP 设备。CP 设备向 CGN2（备 CGN）下发调整路由优先级的命令，将备 CGN 的 CPU 的公网地址段优先级升高。当 CPU 故障后，CR 根据策略对 UNI 流量进行策略路由，将 UNI 流量重定向到 CGN1（原来的主 CGN）。然后，CR 再通过 CGN 之间的绕行隧道或者直连链路，将 UNI 流量转发至现在的主用 CGN2。NNI 流量由于公网地址段路由已经更新，所以 NNI 流量直接发到 CGN2。

场景二、DS-Lite 场景下双机备份

在一些实施例中，主 NAT 设备和备 NAT 设备上不仅会保存同一个公网 IP 地址段，还会为隧道端点配置同一个 IP 地址。在主 NAT 设备故障时，CP 设备通过刷新备 NAT 设备上公

网地址(第二 IP 地址)对应的路由优先级以及隧道端点的 IP 地址对应的优先级,实现 DS-Lite 场景下双机备份。例如,在主 NAT 设备故障时,CP 设备与备 NAT 设备会交互执行以下步骤 S901 至 S903,实现流量切换。

S901、若主 NAT 设备处于故障状态,CP 设备向备 NAT 设备发送第一更新消息和第二更新消息。

第一更新消息用于指示备 NAT 设备提高第二 IP 地址对应的路由优先级。第二更新消息用于指示备 NAT 设备提高第三 IP 地址对应的路由优先级。

第三 IP 地址为隧道端点的 IP 地址。隧道例如是 UP 设备与 NAT 设备之间的隧道。隧道例如是 DS-Lite 隧道。隧道端点例如是 NAT 设备。隧道端点包括主 NAT 设备或者备 NAT 设备。具体地,在主 NAT 设备正常时,隧道端点为主 NAT 设备。在主 NAT 设备故障时,隧道端点从原来的主 NAT 设备切换为备 NAT 设备。在一些实施例中,隧道端点对应于 NAT 设备上的回环(loopback)端口,第三 IP 地址为 loopback 地址。且,主 NAT 设备上第三 IP 地址对应的路由优先级高,备 NAT 设备上第三 IP 地址对应的路由优先级高。例如,请参见附图 13,CGN1 和 CGN2 和同一个 loopback 地址关联。CGN1 上隧道端点的 loopback 地址为 1.1.1.1/32,CGN2 的隧道端点的 loopback 地址也为 1.1.1.1/32。并且,CGN1 上隧道端点 IP 地址 1.1.1.1/32 的路由优先级高,CGN2 上隧道端点 IP 地址为 1.1.1.1/32 的路由优先级低。在这个例子中,loopback 地址 1.1.1.1/32 是对第三 IP 地址的举例说明。

此外,主 NAT 设备上保存的公网 IP 地址段的路由优先级高,备 NAT 设备上保存的公网 IP 地址段的路由优先级低。例如,请参见附图 13,附图 13 中的 CGN1 和 CGN2 是对互为备份关系的主 NAT 设备和备 NAT 设备的举例说明。在采用 CPU 实现 CGN 设备时,CGN1 和 CGN2 例如称为一对主备 CPU。CGN1 和 CGN2 上共享同一段公网 IP 地址。例如,CGN1 上公网 IP 地址段是 100.1.1.0/24。CGN2 上公网 IP 地址段也是 100.1.1.0/24。CGN1 上公网 IP 地址段 100.1.1.0/24 的路由优先级高,CGN2 上公网 IP 地址段 100.1.1.0/24 的路由优先级低。在这个例子中,公网 IP 地址段 100.1.1.0/24 是对第二 IP 地址所属的网段的举例说明。

S902、备 NAT 设备从 CP 设备接收第一更新消息和第二更新消息。

S903、响应于第一更新消息,备 NAT 设备提高第二 IP 地址对应的路由优先级。并且,响应于第二更新消息,备 NAT 设备提高第三 IP 地址对应的路由优先级。

例如,参见附图 13,当 CGN1(主 CGN 设备)的 CPU 出现故障时,CGN1 将 CPU 故障事件上报给 CP 设备。CP 设备向 CGN2(备 CGN 设备)下发第一更新消息和第二更新消息,从而将 CGN2(备 CGN 设备)的隧道端点 IP 地址的路由优先级提高。同时将 CGN2(备 CGN 设备)的公网地址段优先级升高。故障前 NNI 流量在 CGN1 与传输网络之间传输。故障后 NNI 流量在 CGN2 与传输网络之间传输。其中,NNI 是指 CGN 设备与 PSN(包封装网络)网络间的接口。NNI 流量也称公网侧流量,例如是 CGN 与之间传输的流量。故障前 UNI 流量在 CGN1 与 UP 设备之间传输。故障后 UNI 流量在 CGN2 与 UP 设备之间传输。其中,UNI 是指网络侧与用户侧间的通信接口,即 CGN 设备与用户设备之间的通信接口。UNI 流量也称用户侧流量,例如是用户设备与 CGN 之间传输的流量。

当主 NAT 设备发生故障时,CP 设备通过向备 NAT 设备下发第一更新消息和第二更新消息,从而通知备 NAT 设备调整公网地址对应的路由优先级以及隧道端点地址对应的路由优先级,由于备 NAT 设备的公网地址对应的路由优先级升高,因此网络侧的流量会从主 NAT 设

备切换至备 NAT 设备, 由于备 NAT 设备的隧道端点地址对应的路由优先级升高, 因此用户侧的流量会从主 NAT 设备切换至备 NAT 设备, 使得备 NAT 设备升级为主 NAT 设备, 代替之前故障的主 NAT 设备处理网络侧的流量和用户侧的流量, 避免流量传输中断。此外, 由于流量的切换是 CP 设备引导的, 能够保证主 NAT 设备与备 NAT 设备不会存在流量绕行。尤其是, 该方法能够适用于 DS-Lite 场景, 有助于 DS-Lite 场景下实现双机备份。

本申请的一些实施例提供了用户上线后两台 UP 设备之间如何实现 1:1 热备的方法, 以下结合附图 14 举例说明。在附图 14 所示的方法中, 两台 UP 设备之间互为备份关系。两台 UP 设备中一台 UP 设备为主 UP 设备, 即主用 UP 设备, 主 UP 设备也称 UP 设备 (M)。两台 UP 设备中另一台 UP 设备为备 UP 设备, 即备用 UP 设备, 备 UP 设备也称 UP 设备 (S)。两台 UP 设备例如是两台独立式 CGN 设备。其中, CP 设备与主 UP 设备、备 UP 设备均通过 CP Ri、Mi、SCi 等接口通信。在附图 14 所示的方法中, NAT 设备是独立式 CGN 设备。

附图 14 所示的 1:1 热备方法包括以下 S1001 至 S1004。

S1001、用户上线, CP 设备将用户表项同时下发至主 UP 设备和备 UP 设备。

S1002、终端发送流量。主 UP 设备从终端接收流量。主 UP 设备将流量转发至 CGN 设备。其中, 终端发送的流量也称上行流量。

S1003、CGN 设备从主 UP 设备接收流量, 根据流量生成 NAT 转换表项。从这一步骤可见, 本实施例中上行流量仍然要经过 CGN 设备。

S1004、当主 UP 设备故障时, 用户接入的 UP 设备从主 UP 设备切换至备 UP 设备。终端发送流量后, 备 UP 设备接收流量, 将流量转发至 CGN 设备。其中, 由于用户的私网 IPv4 地址没有发生变化, 所以 CGN 设备不感知 UP 设备故障情况。

附图 15 示出了 CP 设备的一种可能的结构示意图。附图 15 所示的 CP 设备 110 例如实现上述方法实施例中所涉及中 CP 设备的功能。

请参考附图 15, CP 设备 110 包括分配单元 1101、发送单元 1102 和接收单元 1103。CP 设备 110 中的各个单元全部或部分地通过软件、硬件、固件或者其任意组合来实现。CP 设备 110 中的各个单元用于执行上述方法 200 中 CP 设备各个相应的功能。具体地, 分配单元 1101 用于支持 CP 设备 110 执行 S210。发送单元 1102 用于支持 CP 设备 110 执行 S220、S270。接收单元 1103 用于支持 CP 设备 110 执行 S260。

在一些实施例中, 接收单元 1103、分配单元 1101 或发送单元 1102 还用于支持 CP 设备 110 执行本文所描述的技术中 CP 设备执行的其它过程。例如, 接收单元 1103 用于支持 CP 设备 110 执行方法 300、方法 400、方法 500 等实施例中 CP 设备执行的各种接收操作, 例如 S602、S704 等。分配单元 1101 用于支持 CP 设备 110 执行方法 200、方法 300、方法 400、方法 500 等实施例中 CP 设备执行的各种分配操作, 例如 S302、S403 等; 发送单元 1102 用于支持 CP 设备 110 执行方法 200、方法 300、方法 400、方法 500 等实施例中 CP 设备执行的各种发送操作, 例如 S303、S309、S402、S406、S503、S504、S507、S603、S702、S802、S901 或 S1001 等。具体执行过程请参考上述方法实施例中相应步骤的详细描述, 这里不再赘述。

本申请实施例中对单元的划分是示意性的, 仅仅为一种逻辑功能划分, 实际实现时可选

地有另外的划分方式。

在一些实施例中，CP 设备 110 中各个单元集成在一个处理单元中。例如，CP 设备 110 中各个单元集成在同一个芯片上。该芯片包括处理电路和与该处理电路内部连接通信的输入接口以及输出接口。分配单元 1101 通过芯片中的处理电路实现。接收单元 1103 通过芯片中的输入接口实现。发送单元 1102 通过芯片中的输出接口实现。例如，该芯片通过一个或多个现场可编程门阵列（英文全称：field-programmable gate array，英文简称：FPGA）、可编程逻辑器件（英文全称：programmable logic device，英文简称：PLD）、控制器、状态机、门逻辑、分立硬件部件、任何其它适合的电路、或者能够执行本申请通篇所描述的各种功能的电路的任意组合实现。

在另一些实施例中，CP 设备 110 各个单元单独物理存在。在另一些实施例中，CP 设备 110 一部分单元单独物理存在，另一部分单元集成在一个单元中。例如，在一些实施例中，分配单元 1101 和发送单元 1102 是同一个单元。在另一些实施例中，分配单元 1101 和发送单元 1102 是不同的单元。在一些实施例中，不同单元的集成采用硬件的形式实现，即，不同单元对应于同一个硬件。又如，不同单元的集成采用软件单元的形式实现。

在 CP 设备 110 中通过硬件实现的情况下，例如，CP 设备 110 中分配单元 1101 例如通过设备 1400 中的处理器 1401 实现。CP 设备 110 中接收单元 1103、发送单元 1102 例如通过设备 1400 中的通信接口 1404 实现。又如，CP 设备 110 中分配单元 1101 例如通过设备 1300 中的中央处理器 1311、中央处理器 1331 或者网络处理器 1332 中的至少一项实现。CP 设备 110 中接收单元 1103、发送单元 1102 例如通过设备 1300 中的物理接口卡 1333 或物理接口卡 1343 中的至少一项实现。

在 CP 设备 110 中通过软件实现的情况下，CP 设备 110 中各个单元例如为设备 1400 或设备 1300 中的处理器读取存储器中存储的程序代码后生成的软件。例如，CP 设备 110 为虚拟化设备。虚拟化设备包括而限于虚拟机、容器、Pod 中的至少一种。在一些实施例中，CP 设备 110 以虚拟机的形式，部署在硬件设备（如物理服务器）上。例如，基于通用的物理服务器结合网络功能虚拟化（Network Functions Virtualization, NFV）技术来实现 CP 设备 110。采用虚拟机的方式实现时，CP 设备 110 例如为虚拟主机、虚拟路由器或虚拟交换机。本领域技术人员通过阅读本申请即可结合 NFV 技术在通用物理服务器上虚拟出 CP 设备 110。在另一些实施例中，CP 设备 110 以容器（例如 docker 容器）的形式，部署在硬件设备上。例如，CP 设备 110 执行上述方法实施例的流程被封装在镜像文件中，硬件设备通过运行镜像文件来创建 CP 设备 110。在另一些实施例中，CP 设备 110 以 Pod 的形式，部署在硬件设备上。Pod 包括多个容器，每个容器用于实现 CP 设备 110 中的一个或多个单元。

附图 16 示出了 NAT 设备的一种可能的结构示意图。附图 16 所示的 NAT 设备 120 例如实现上述方法实施例中 NAT 设备（如 CGN 设备）的功能。

请参考附图 16，NAT 设备 120 包括接收单元 1201、分配单元 1202 和发送单元 1203。NAT 设备 120 中的各个单元全部或部分地通过软件、硬件、固件或者其任意组合来实现。NAT 设备 120 中的各个单元用于执行上述方法 200 中 NAT 设备各个相应的功能。具体地，接收单元 1201 用于支持 NAT 设备 120 执行 S230。分配单元 1202 用于支持 NAT 设备 120 执行 S24。发送单元 1203 用于支持 NAT 设备 120 执行 S250。

在一些实施例中,接收单元 1201、分配单元 1202 或发送单元 1203 还用于支持 NAT 设备 120 执行本文所描述的技术中 NAT 设备执行的其它过程或 CGN 设备执行的其它过程。例如,接收单元 1201 用于支持 NAT 设备 120 执行方法 300、方法 400、方法 500 等实施例中 NAT 设备执行的各种接收操作,如 S604, S703、S803、S902、S1003 中的至少一项。分配单元 1202 用于支持 NAT 设备 120 执行方法 300、方法 400、方法 500 等实施例中 NAT 设备执行的各种处理操作,如 S304、S404、S505、S605 中的至少一项;发送单元 1203 用于支持 NAT 设备 120 执行方法 300、方法 400、方法 500 等实施例中 NAT 设备执行的各种发送操作,如 S305、S601 中的至少一项。具体执行过程请参考方法 300、方法 400、方法 500 等实施例中相应步骤的详细描述,这里不再一一赘述。

本申请实施例中对单元的划分是示意性的,仅仅为一种逻辑功能划分,实际实现时可选地有另外的划分方式。

在一些实施例中,NAT 设备 120 中各个单元集成在一个处理单元中。例如,NAT 设备 120 中各个单元集成在同一个芯片上。该芯片包括处理电路和与该处理电路内部连接通信的输入接口以及输出接口。分配单元 1202 通过芯片中的处理电路实现。接收单元 1201 通过芯片中的输入接口实现。发送单元 1203 通过芯片中的输出接口实现。例如,该芯片通过一个或多个现场可编程门阵列(英文全称:field-programmable gate array,英文简称:FPGA)、可编程逻辑器件(英文全称:programmable logic device,英文简称:PLD)、控制器、状态机、门逻辑、分立硬件部件、任何其它适合的电路、或者能够执行本申请通篇所描述的各种功能的电路的任意组合实现。

在另一些实施例中,NAT 设备 120 各个单元单独物理存在。在另一些实施例中,NAT 设备 120 一部分单元单独物理存在,另一部分单元集成在一个单元中。例如,在一些实施例中,分配单元 1202 和发送单元 1203 是同一个单元。在另一些实施例中,分配单元 1202 和发送单元 1203 是不同的单元。在一些实施例中,不同单元的集成采用硬件的形式实现,即,不同单元对应于同一个硬件。又如,不同单元的集成采用软件单元的形式实现。

在 NAT 设备 120 中通过硬件实现的情况下,NAT 设备 120 中分配单元 1202 例如通过设备 1400 中的处理器 1401 实现。NAT 设备 120 中接收单元 1201、发送单元 1203 例如通过设备 1400 中的通信接口 1404 实现。又如,NAT 设备 120 中分配单元 1202 例如通过设备 1300 中的中央处理器 1311、中央处理器 1331 或者网络处理器 1332 中的至少一项实现。NAT 设备 120 中接收单元 1201、发送单元 1203 例如通过设备 1300 中的物理接口卡 1333 或物理接口卡 1343 中的至少一项实现。

在 NAT 设备 120 中通过软件实现的情况下,NAT 设备 120 中各个单元例如为设备 1400 或设备 1300 中的处理器读取存储器中存储的程序代码后生成的软件。例如,NAT 设备 120 为虚拟化设备。虚拟化设备包括而不限于虚拟机、容器、Pod 中的至少一种。在一些实施例中,NAT 设备 120 以虚拟机的形式,部署在硬件设备(如物理服务器)上。例如,基于通用的物理服务器结合网络功能虚拟化(Network Functions Virtualization, NFV)技术来实现 NAT 设备 120。采用虚拟机的方式实现时,NAT 设备 120 例如为虚拟主机、虚拟路由器或虚拟交换机。本领域技术人员通过阅读本申请即可结合 NFV 技术在通用物理服务器上虚拟出 NAT 设备 120。在另一些实施例中,NAT 设备 120 以容器(例如 docker 容器)的形式,部署在硬件设备上。例如,NAT 设备 120 执行上述方法实施例的流程被封装在镜像文件中,硬件设备

通过运行镜像文件来创建 NAT 设备 120。在另一些实施例中，NAT 设备 120 以 Pod 的形式，部署在硬件设备上。Pod 包括多个容器，每个容器用于实现 NAT 设备 120 中的一个或多个单元。

以上通过 CP 设备 110 和 NAT 设备 120，从逻辑功能的角度分别介绍了如何实现 CP 设备和 NAT 设备。以下通过设备 1300 或设备 1400，从硬件的角度介绍如何实现 CP 设备和 NAT 设备。附图 17 所示的设备 1300 或附图 18 所示的设备 1400 是对 CP 设备和 NAT 设备的硬件结构的举例说明。

设备 1300 或设备 1400 对应于上述各个方法实施例的 CP 设备或者 NAT 设备，设备 1300 或设备 1400 中的各硬件、模块和上述其他操作和/或功能分别为了实现方法实施例中 CP 设备或者 NAT 设备所实施的各种步骤和方法，关于设备 1300 或设备 1400 如何实现基于 RADIUS 的 NAT 溯源的详细流程，具体细节可参见上述各个方法实施例，为了简洁，在此不再赘述。其中，各个方法实施例的各步骤通过设备 1300 或设备 1400 处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块例如位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤，为避免重复，这里不再详细描述。

参见附图 17，附图 17 示出了本申请一个示例性实施例提供的设备 1300 的结构示意图，设备 1300 例如配置为 CP 设备或者 NAT 设备。设备 1300 包括：主控板 1310 和接口板 1330。

主控板也称为主处理单元(main processing unit, MPU)或路由处理卡(route processor card)，主控板 1310 用于对设备 1300 中各个组件的控制和管理，包括路由计算、设备管理、设备维护、协议处理功能。主控板 1310 包括：中央处理器 1311 和存储器 1312。

接口板 1330 也称为线路接口单元卡(line processing unit, LPU)、线卡(line card)或业务板。接口板 1330 用于提供各种业务接口并实现数据包的转发。业务接口包括但不限于以太网接口、POS(Packet over SONET/SDH)接口等，以太网接口例如是灵活以太网业务接口(Flexible Ethernet Clients, FlexE Clients)。接口板 1330 包括：中央处理器 1331、网络处理器 1332、转发表项存储器 1334 和物理接口卡(physical interface card, PIC) 1333。

接口板 1330 上的中央处理器 1331 用于对接口板 1330 进行控制管理并与主控板 1310 上的中央处理器 1311 进行通信。

网络处理器 1332 用于实现报文的转发处理。网络处理器 1332 的形态例如是转发芯片。具体而言，网络处理器 1332 用于基于转发表项存储器 1334 保存的转发表转发接收到的报文，如果报文的地址为设备 1300 的地址，则将该报文上送至 CPU（如中央处理器 1311）处理；如果报文的地址不是设备 1300 的地址，则根据该地址从转发表中查找到该目的地址对应的下一跳和出接口，将该报文转发到该目的地址对应的出接口。其中，上行报文的处理包括：报文入口口的处理，转发表查找；下行报文的处理：转发表查找等等。

物理接口卡 1333 用于实现物理层的对接功能，原始的流量由此进入接口板 1330，以及处理后的报文从该物理接口卡 1333 发出。物理接口卡 1333 也称为子卡，可安装在接口板 1330 上，负责将光电信号转换为报文并对报文进行合法性检查后转发给网络处理器 1332 处理。在

一些实施例中,中央处理器也可执行网络处理器 1332 的功能,比如基于通用 CPU 实现软件转发,从而物理接口卡 1333 中不需要网络处理器 1332。

可选地,设备 1300 包括多个接口板,例如设备 1300 还包括接口板 1340,接口板 1340 包括:中央处理器 1341、网络处理器 1342、转发表项存储器 1344 和物理接口卡 1343。

可选地,设备 1300 还包括交换网板 1320。交换网板 1320 也例如称为交换网板单元(switch fabric unit, SFU)。在网络设备有多个接口板 1330 的情况下,交换网板 1320 用于完成各接口板之间的数据交换。例如,接口板 1330 和接口板 1340 之间例如通过交换网板 1320 通信。

主控板 1310 和接口板 1330 耦合。例如。主控板 1310、接口板 1330 和接口板 1340,以及交换网板 1320 之间通过系统总线与系统背板相连实现互通。在一种可能的实现方式中,主控板 1310 和接口板 1330 之间建立进程间通信协议(inter-process communication, IPC)通道,主控板 1310 和接口板 1330 之间通过 IPC 通道进行通信。

在逻辑上,设备 1300 包括控制面和转发面,控制面包括主控板 1310 和中央处理器 1331,转发面包括执行转发的各个组件,比如转发表项存储器 1334、物理接口卡 1333 和网络处理器 1332。控制面执行路由器、生成转发表、处理信令和协议报文、配置与维护设备的状态等功能,控制面将生成的转发表下发给转发面,在转发面,网络处理器 1332 基于控制面下发的转发表对物理接口卡 1333 收到的报文查表转发。控制面下发的转发表例如保存在转发表项存储器 1334 中。在有些实施例中,控制面和转发面例如完全分离,不在同一设备上。

应理解,本申请实施例中接口板 1340 上的操作与接口板 1330 的操作一致,为了简洁,不再赘述。应理解,本实施例的设备 1300 可对应于上述各个方法实施例中的 CP 设备或者 NAT 设备,该设备 1300 中的主控板 1310、接口板 1330 和/或 1340 例如实现上述各个方法实施例中的 CP 设备或者 NAT 设备所具有的功能和/或所实施的各种步骤,为了简洁,在此不再赘述。

值得说明的是,主控板可能有一块或多块,有多块的时候例如包括主用主控板和备用主控板。接口板可能有一块或多块,网络设备的数据处理能力越强,提供的接口板越多。接口板上的物理接口卡也可以有一块或多块。交换网板可能没有,也可能有一块或多块,有多块的时候可以共同实现负荷分担冗余备份。在集中式转发架构下,网络设备可以不需要交换网板,接口板承担整个系统的业务数据的处理功能。在分布式转发架构下,网络设备可以有至少一块交换网板,通过交换网板实现多块接口板之间的数据交换,提供大容量的数据交换和处理能力。所以,分布式架构的网络设备的数据接入和处理能力要大于集中式架构的设备。可选地,网络设备的形态也可以是只有一块板卡,即没有交换网板,接口板和主控板的功能集成在该一块板卡上,此时接口板上的中央处理器和主控板上的中央处理器在该一块板卡上可以合并为一个中央处理器,执行两者叠加后的功能,这种形态设备的数据交换和处理能力较低(例如,低端交换机或路由器等网络设备)。具体采用哪种架构,取决于具体的组网部署场景,此处不做任何限定。

参见附图 18,附图 18 示出了本申请一个示例性实施例提供的设备 1400 的结构示意图,该设备 1400 可以配置为 CP 设备或者 NAT 设备。该设备 1400 可以是主机、服务器或个人计算机等。该设备 1400 可以由一般性的总线体系结构来实现。

设备 1400 包括至少一个处理器 1401、通信总线 1402、存储器 1403 以及至少一个通信接

口 1404。

处理器 1401 例如是通用中央处理器 (central processing unit, CPU)、网络处理器 (network processor, NP)、图形处理器 (Graphics Processing Unit, GPU)、神经网络处理器 (neural-network processing units, NPU)、数据处理单元 (Data Processing Unit, DPU)、微处理器或者一个或多个用于实现本申请方案的集成电路。例如, 处理器 1401 包括专用集成电路 (application-specific integrated circuit, ASIC)、可编程逻辑器件 (programmable logic device, PLD) 或其组合。PLD 例如是复杂可编程逻辑器件 (complex programmable logic device, CPLD)、现场可编程逻辑门阵列 (field-programmable gate array, FPGA)、通用阵列逻辑 (generic array logic, GAL) 或其任意组合。

通信总线 1402 用于在上述组件之间传送信息。通信总线 1402 可以分为地址总线、数据总线、控制总线等。为便于表示, 附图 18 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

存储器 1403 例如是只读存储器 (read-only memory, ROM) 或可存储静态信息和指令的其它类型的静态存储设备, 又如是随机存取存储器 (random access memory, RAM) 或者可存储信息和指令的其它类型的动态存储设备, 又如是电可擦可编程只读存储器 (electrically erasable programmable read-only Memory, EEPROM)、只读光盘 (compact disc read-only memory, CD-ROM) 或其它光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其它磁存储设备, 或者是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其它介质, 但不限于此。存储器 1403 例如是独立存在, 并通过通信总线 1402 与处理器 1401 相连接。存储器 1403 也可以和处理器 1401 集成在一起。

通信接口 1404 使用任何收发器一类的装置, 用于与其它设备或通信网络通信。通信接口 1404 包括有线通信接口, 还可以包括无线通信接口。其中, 有线通信接口例如可以为以太网接口。以太网接口可以是光接口, 电接口或其组合。无线通信接口可以为无线局域网 (wireless local area networks, WLAN) 接口, 蜂窝网络通信接口或其组合等。

在具体实现中, 作为一种实施例, 处理器 1401 可以包括一个或多个 CPU, 如附图 18 中所示的 CPU0 和 CPU1。

在具体实现中, 作为一种实施例, 设备 1400 可以包括多个处理器, 如附图 18 中所示的处理器 1401 和处理器 1405。这些处理器中的每一个可以是一个单核处理器 (single-CPU), 也可以是一个多核处理器 (multi-CPU)。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据 (如计算机程序指令) 的处理核。

在具体实现中, 作为一种实施例, 设备 1400 还可以包括输出设备和输入设备。输出设备和处理器 1401 通信, 可以以多种方式来显示信息。例如, 输出设备可以是液晶显示器 (liquid crystal display, LCD)、发光二极管 (light emitting diode, LED) 显示设备、阴极射线管 (cathode ray tube, CRT) 显示设备或投影仪 (projector) 等。输入设备和处理器 1401 通信, 可以以多种方式接收用户的输入。例如, 输入设备可以是鼠标、键盘、触摸屏设备或传感设备等。

在一些实施例中, 存储器 1403 用于存储执行本申请方案的程序代码 1410, 处理器 1401 可以执行存储器 1403 中存储的程序代码 1410。也即是, 设备 1400 可以通过处理器 1401 以及存储器 1403 中的程序代码 1410, 来实现方法实施例提供的方法。

本申请实施例的设备 1400 可对应于上述各个方法实施例中的 CP 设备或者 NAT 设备，并且，该设备 1400 中的处理器 1401、通信接口 1404 等可以实现上述各个方法实施例中的 CP 设备或者 NAT 设备所具有的功能和/或所实施的各种步骤和方法。为了简洁，在此不再赘述。

参见附图 19，本申请实施例提供了一种通信系统 1500，系统 1500 包括：CP 设备 1501 和 NAT 设备 1502。可选的，CP 设备 1501 为如附图 15 所示的 CP 设备 1100 或附图 17 所示的设备 1300 或附图 18 所示的设备 1400，NAT 设备 1502 为如附图 16 的 NAT 设备 1200 或附图 17 所示的设备 1300 或附图 18 所示的设备 1400。

本领域普通技术人员可以意识到，结合本文中所公开的实施例中描述的各方法步骤和单元，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各实施例的步骤及组成。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参见前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，该单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口、装置或单元的间接耦合或通信连接，也可以是电的，机械的或其它的形式连接。

该作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本申请实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

该集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分，或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例中方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

本申请中术语“第一”“第二”等字样用于对作用和功能基本相同的相同项或相似项进行区分，应理解，“第一”、“第二”之间不具有逻辑或时序上的依赖关系，也不对数量和执行顺序进行限定。还应理解，尽管以下描述使用术语第一、第二等来描述各种元素，但这些元素不

应受术语的限制。这些术语只是用于将一元素与另一元素区别分开。例如，在不脱离各种示例的范围的情况下，第一 IP 地址可以被称为第二 IP 地址，并且类似地，第二 IP 地址可以被称为第一 IP 地址。第一 IP 地址和第二 IP 地址都可以是 IP 地址，并且在某些情况下，可以是单独且不同的 IP 地址。

本申请中术语“至少一个”的含义是指一个或多个。本文中术语“系统”和“网络”经常可互换使用。

还应理解，术语“若”或“如果”可被解释为意指“当...时”(“when”或“upon”)或“响应于确定”或“响应于检测到”。类似地，根据上下文，短语“如果确定...”或“如果检测到[所陈述的条件或事件]”可被解释为意指“在确定...时”或“响应于确定...”或“在检测到[所陈述的条件或事件]时”或“响应于检测到[所陈述的条件或事件]”。

以上描述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机程序指令。在计算机上加载和执行该计算机程序指令时，全部或部分地产生按照本申请实施例中的流程或功能。该计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。

该计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，该计算机程序指令可以从一个网站站点、计算机、服务器或数据中心通过有线或无线方式向另一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质（例如软盘、硬盘、磁带）、光介质（例如，数字视频光盘（digital video disc, DVD）、或者半导体介质（例如固态硬盘）等。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，该程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

权 利 要 求 书

1.一种通信方法，其特征在于，应用于控制面 CP 和用户面 UP 分离的通信系统中的 CP 设备，所述方法包括：

所述 CP 设备为用户分配第一互联网协议 IP 地址；

所述 CP 设备向网络地址转换 NAT 设备发送所述第一 IP 地址；

所述 CP 设备从所述 NAT 设备接收第二 IP 地址，所述第二 IP 地址为所述 NAT 设备为所述用户分配的公网 IP 地址；

所述 CP 设备向远程用户拨号认证系统 RADIUS 服务器发送计费报文，所述计费报文包括所述第一 IP 地址和所述第二 IP 地址。

2.根据权利要求 1 所述的方法，其特征在于，所述第一 IP 地址包括私网互联网协议第四版 IPv4 地址或者互联网协议第六版 IPv6 地址中的至少一项。

3.根据权利要求 1 或 2 所述的方法，其特征在于，所述通信系统包括网关系统，所述网关系统为宽带网络网关 BNG 系统或者宽带远程接入服务器 BRAS 系统。

4.根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述计费报文还包括端口块，所述端口块包括所述 NAT 设备为所述用户分配的至少一个端口号；

所述 CP 设备从所述 NAT 设备接收第二 IP 地址，包括：所述 CP 设备从所述 NAT 设备接收所述用户的信息，所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和所述端口块的对应关系。

5.根据权利要求 4 所述的方法，其特征在于，所述 CP 设备从所述 NAT 设备接收所述端口块之前，所述方法还包括：

所述 CP 设备从所述 RADIUS 服务器接收端口块集合，所述端口块集合包括所述端口块；

所述 CP 设备向所述 NAT 设备发送所述端口块集合。

6.根据权利要求 4 至 5 中任一项所述的方法，其特征在于，所述 CP 设备向远程用户拨号认证系统 RADIUS 服务器发送计费报文之后，所述方法还包括以下至少一项：

若所述用户下线，所述 CP 设备向所述 NAT 设备发送删除消息，所述删除消息用于指示所述 NAT 设备删除所述 NAT 设备上保存的所述用户的信息；

若所述用户下线，所述 CP 设备删除所述 CP 设备上保存的所述用户的信息。

7.根据权利要求 4 至 6 中任一项所述的方法，其特征在于，所述 NAT 设备包括互为备份关系的主 NAT 设备和备 NAT 设备，所述 CP 设备从所述 NAT 设备接收第二 IP 地址，包括：所述 CP 设备从所述主 NAT 设备接收所述用户的信息。

8.根据权利要求7所述的方法,其特征在于,所述CP设备从所述主NAT设备接收所述用户的信息之后,所述方法还包括:

所述CP设备向所述备NAT设备发送所述用户的信息。

9.根据权利要求7所述的方法,其特征在于,所述方法还包括:

若所述主NAT设备处于故障状态,所述CP设备向所述备NAT设备发送第一更新消息,所述第一更新消息用于指示所述备NAT设备提高所述第二IP地址对应的路由优先级。

10.根据权利要求9所述的方法,其特征在于,所述方法还包括:

若所述主NAT设备处于故障状态,所述CP设备向所述备NAT设备发送第二更新消息,所述第二更新消息用于指示所述备NAT设备提高第三IP地址对应的路由优先级,所述第三IP地址为隧道端点的IP地址,所述隧道端点包括所述主NAT设备或者所述备NAT设备。

11.一种通信方法,其特征在于,应用于网络地址转换NAT设备,所述方法包括:

所述NAT设备从控制面CP设备接收所述CP设备为用户分配的第一互联网协议IP地址,所述CP设备是CP和用户面UP分离的通信系统中的CP设备;

所述NAT设备为所述用户分配第二IP地址,所述第二IP地址为公网IP地址;

所述NAT设备向所述CP设备发送所述第二IP地址。

12.根据权利要求11所述的方法,其特征在于,所述NAT设备从控制面CP设备接收所述CP设备为用户分配的第一互联网协议IP地址之后,所述方法还包括:

所述NAT设备为所述用户分配端口块,所述端口块包括至少一个端口号;

所述NAT设备向所述CP设备发送所述端口块。

13.根据权利要求12所述的方法,其特征在于,所述NAT设备为所述用户分配端口块之前,所述方法还包括:所述NAT设备从所述CP设备接收端口块集合;

所述NAT设备为所述用户分配端口块,包括:所述NAT设备在所述端口块集合内,为所述用户分配端口块。

14.根据权利要求12所述的方法,其特征在于,所述NAT设备为所述用户分配第二IP地址之后,所述方法还包括:

所述NAT设备保存所述用户的信息,所述用户的信息包括所述第一IP地址、所述第二IP地址和所述端口块的对应关系。

15.根据权利要求14所述的方法,其特征在于,所述NAT设备向所述CP设备发送所述第二IP地址,包括:

所述NAT设备向所述CP设备发送所述用户的信息。

16.根据权利要求14或15中任一项所述的方法,其特征在于,所述NAT设备向所述CP

设备发送所述第二 IP 地址之后，所述方法还包括：

所述 NAT 设备从所述 CP 设备接收删除消息；

响应于所述删除消息，所述 NAT 设备删除所述用户的信息。

17.根据权利要求 11 所述的方法，其特征在于，所述 NAT 设备为互为备份关系的主 NAT 设备和备 NAT 设备中的备 NAT 设备，所述 NAT 设备为所述用户分配第二 IP 地址之前，所述方法还包括：

所述备 NAT 设备从所述 CP 设备接收所述用户的信息，所述用户的信息包括所述第一 IP 地址、所述第二 IP 地址和端口块的对应关系，所述端口块包括至少一个端口号；

所述 NAT 设备为所述用户分配第二 IP 地址，包括：

在所述主 NAT 设备故障时，所述备 NAT 设备根据所述用户的信息为所述用户分配所述第二 IP 地址。

18.根据权利要求 17 所述的方法，其特征在于，所述方法还包括：

所述备 NAT 设备从所述 CP 设备接收第一更新消息；

响应于所述第一更新消息，所述备 NAT 设备提高所述第二 IP 地址对应的路由优先级。

19.根据权利要求 17 或 18 所述的方法，其特征在于，所述方法还包括：

所述备 NAT 设备从所述 CP 设备接收第二更新消息；

响应于所述第二更新消息，所述备 NAT 设备提高第三 IP 地址对应的路由优先级，所述第三 IP 地址为隧道端点的 IP 地址，所述隧道端点包括所述主 NAT 设备或者所述备 NAT 设备。

20.一种控制平面 CP 设备，其特征在于，所述 CP 设备位于 CP 和用户平面 UP 分离的通信系统中，所述 CP 设备包括：

分配单元，用于为用户分配第一互联网协议 IP 地址；

发送单元，用于向网络地址转换 NAT 设备发送所述第一 IP 地址；

接收单元，用于从所述 NAT 设备接收第二 IP 地址，所述第二 IP 地址为所述 NAT 设备为所述用户分配的公网 IP 地址；

所述发送单元，还用于向远程用户拨号认证系统 RADIUS 服务器发送计费报文，所述计费报文包括所述第一 IP 地址和所述第二 IP 地址。

21.一种网络地址转换 NAT 设备，其特征在于，所述 NAT 设备包括：

接收单元，用于从控制面 CP 设备接收所述 CP 设备为用户分配的第一互联网协议 IP 地址，所述 CP 设备是 CP 和用户面 UP 分离的通信系统中的 CP 设备；

分配单元，用于为所述用户分配第二 IP 地址，所述第二 IP 地址为公网 IP 地址；

发送单元，用于向所述 CP 设备发送所述第二 IP 地址。

22.一种通信系统，其特征在于，所述通信系统包括如权利要求 20 所述的 CP 设备以及如

权利要求 21 所述的 NAT 设备。

23.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令，所述指令由处理器读取以使控制平面 CP 设备和用户面 UP 分离的通信系统中的 CP 设备执行如权利要求 1 至权利要求 10 中任一项所述的方法。

24.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令，所述指令由处理器读取以使网络地址转换 NAT 设备执行如权利要求 11 至权利要求 19 中任一项所述的方法。