

(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
2019 年 12 月 19 日 (19.12.2019)



(10) 国际公布号
WO 2019/237683 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2018/119058

(22) 国际申请日: 2018 年 12 月 4 日 (04.12.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810614712.0 2018年6月14日 (14.06.2018) CN

(71) 申请人: 烽火通信科技股份有限公司 (FIBERHOME TELECOMMUNICATION TECHNOLOGIES CO., LTD) [CN/CN]; 中国湖北省武汉市东湖高新技术开发区高新四路6号, Hubei 430000 (CN)。

(72) 发明人: 李和松 (LI, Hesong); 中国湖北省武汉市东湖高新技术开发区高新四路6号, Hubei 430000 (CN)。许赛群 (XU, Saiqun); 中国湖北省武汉市东湖高新技术开发区高新四路6号, Hubei 430000 (CN)。王晔 (WANG, Ye); 中国湖北省武汉市东湖高新技术开发区高新四

路6号, Hubei 430000 (CN)。王颖 (WANG, Ying); 中国湖北省武汉市东湖高新技术开发区高新四路6号, Hubei 430000 (CN)。

(74) 代理人: 武汉智权专利代理事务所 (特殊普通合伙) (WUHAN ZHI QUAN PATENT AGENCY); 中国湖北省武汉市东湖高新技术开发区珞喻路727号星光无限4栋21层2103室, Hubei 430000 (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, 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,

(54) Title: PROTOCOL PACKET, AND METHOD FOR MANAGING VIRTUAL CLIENT TERMINAL DEVICE

(54) 发明名称: 一种协议报文以及虚拟客户终端设备的管理方法

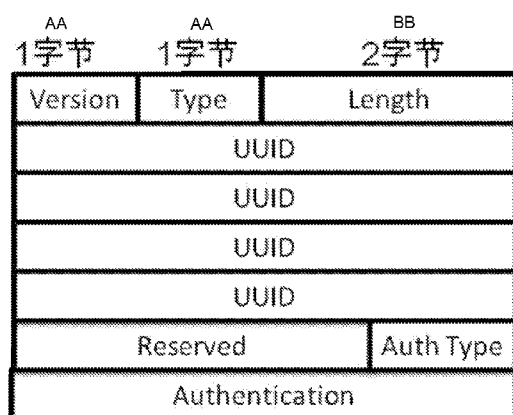


图 3

AA One byte

BB Two bytes

(57) Abstract: Disclosed are a protocol packet, and a method for managing a virtual client terminal device, which are used for communication between a network controller and the virtual client terminal device VCPE, and relate to the technical field of communications. A payload part of the protocol packet has a common header, wherein the common header comprises a field for indicating a universally unique identifier (UUID) of the VCPE, and the UUID is generated when the VCPE is started for the first time. In the present invention, the UUID of the VCPE serves as a unique identifier for the network controller to remotely manage the VCPE and is a basis for online and later service configuration management of the VCPE, such that large-scale deployment of the VCPE can be quickly and reliably realized.

(57) 摘要: 本发明公开了一种协议报文以及虚拟客户终端设备的管理方法, 用于网络控制器与虚拟客户终端设备VCPE之间的通信, 涉及通信技术领域。协议报文的净荷部分具有公共头部, 公共头部包括用于指示VCPE的通用唯一识别码UUID的字段, UUID是VCPE首次启动时生成的。本发明采用VCPE的UUID作为网络控制器对VCPE进行远程管理的唯一标识, 成为VCPE上线以及后期业务配置管理的依据, 从而快速、可靠地实现VCPE的大规模部署。

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))。

一种协议报文以及虚拟客户终端设备的管理方法

技术领域

本发明涉及通信技术领域，具体是涉及一种协议报文以及虚拟客户终端设备的管理方法。

背景技术

在软件定义网络（Software Defined Network，SDN）/网络功能虚拟化（Network Function Virtualization，NFV）技术的驱动下，通信行业迎来了云化的浪潮。通过将传统通信设备的硬件和软件解耦，并利用 SDN 的思想实现集中化的管理和业务开通，可极大地提高网络运营商的运维成本，同时最大程度地挖掘网络的附加值。图 1 所示为一种虚拟用户驻地设备（Virtual Customer Premise Equipment，VCPE）现网部署，包括业务编排器、网络控制器和分别连接多个用户的虚拟客户终端设备的 VCPE，业务编排器进行业务的策略下发和管理，对网络控制器进行统一管理，网络控制器对 VCPE 进行上线管理和身份认证等管理。其中，VCPE 是软件定义广域网（Software Defined-Wide Area Network，SD-WAN）解决方案中最引人注目的商业模式，可以使网络运营商将服务进一步延伸至用户出口的同时，也将用户特别是中小型企业从繁琐的网络管理中解脱出来，是一个典型的双赢模式。然而，由于用户具有分散性的特点，如何实现大规模 VCPE 的远程管理和业务开通，是 VCPE 走向实用化需要解决的关键问题。

发明内容

针对现有技术中存在的缺陷，本发明的目的在于提供一种协议报

文以及虚拟客户终端设备的管理方法,采用 VCPE 的 UUID 作为网络控制器对 VCPE 进行远程管理的唯一标识,成为 VCPE 上线以及后期业务配置管理的依据,从而快速、可靠地实现 VCPE 的大规模部署。

本发明提供一种协议报文,用于网络控制器与虚拟客户终端设备 VCPE 之间的通信:

所述协议报文的净荷部分具有公共头部,所述公共头部包括用于指示所述 VCPE 的通用唯一识别码 UUID 的字段,所述 UUID 是所述 VCPE 首次启动时生成的。

在上述技术方案的基础上,所述公共头部为类型长度值 TLV,包括协议版本号、消息类型、消息总长度和认证加密字段。

在上述技术方案的基础上,所述消息类型包括认证请求、认证应答、心跳和节点信息上报。

在上述技术方案的基础上,所述消息类型还包括服务端口通告和会话关闭,服务端口通告报文包括 IP 类型、网络控制器的 IP 地址和服务端口信息,用于通知所述 VCPE 向网络控制器主动发起控制连接。

在上述技术方案的基础上,所述认证加密字段包括认证类型和对应的密码信息,所述认证类型包括简单密码认证和 MD5 认证,所述密码信息为明文密码或者全 0。

在上述技术方案的基础上,所述公共头部还包括保留字段,用于自定义功能,自定义功能包括告警上报和拓扑自动发现。

在上述技术方案的基础上,所述协议报文为 TCP 报文或者 UDP 报文。

本发明还提供一种使用上述协议报文的虚拟客户终端设备的管理方法,其包括:

网络控制器根据所述 VCPE 发出的用户认证请求进行用户身份校验，认证通过后，将业务编排器下发的业务配置信息转发给所述 VCPE，其中，所述用户认证请求和业务配置消息均由所述 VCPE 的 UUID 的协议报文承载。

在上述技术方案的基础上，所述公共头部为类型长度值 TLV，包括协议版本号、消息类型、消息总长度和认证加密字段，基于所述消息类型，所述协议报文包括认证请求报文、认证应答报文、心跳报文和节点信息上报报文；

当所述 VCPE 首次启动以及所述 VCPE 的 IP 地址发生变化时，向网络控制器发出带有所述用户认证请求的认证请求报文，所述用户认证请求包括用户名、密码和所述 VCPE 的 IP 地址；

网络控制器提取所述用户认证请求并进行认证，以及返回带有认证结果的认证应答报文。

在上述技术方案的基础上，所述协议报文还包括服务端口通告报文，服务端口通告报文包括 IP 类型、网络控制器的 IP 地址和服务端口信息，用于通知所述 VCPE 向网络控制器主动发起控制连接；

当网络控制器收到所述 VCPE 发出的所述认证请求报文时，对比所述 VCPE 的 IP 地址以及所述协议报文的源 IP 地址，如果不一致，则向所述 VCPE 发出所述服务端口通告报文。

与现有技术相比，本发明的优点如下：

(1) 实现 VCPE 设备上线管理：由于 VCPE 本质上是一个软件功能实体，采用 VCPE 的 UUID，使得网络控制器对 VCPE 进行远程管理需要一个类似于物理设备序列号作为 VCPE 的唯一标识，作为 VCPE 上线以及后期业务配置管理的依据，在此基础上制定出一套完善的 VCPE 管理协议报文，从而快速、可靠地实现 VCPE 的大规模部

署，具有成本低、可扩展性好、适应性强、易于实现和部署等优点。

(2) 实现 VCPE 设备的身份认证：VCPE 的设备安全认证是产品成熟度的关键衡量因素，由于 VCPE 部署的分散性和开放性的特点，对 VCPE 进行身份认证是涉及业务安全的关键性问题，合理的认证方案极大地提高了 VCPE 的可用性，避免整个业务网络的瘫痪。

(3) 解决 VCPE 迁移的重认证问题：在 NFV 的实际应用中，软件迁移是最为常见的需求，本发明实施例能够在 VCPE 发生迁移、IP 地址变化的情况下对 VCPE 进行可靠的重认证，且重认证可以由 VCPE 或者网络控制器发起，进一步提高 VCPE 的可用性和管理效率。

(4) 解决 NAT 穿越问题：在现网的部署场景中，很多中小型企业出口并没有公网地址，而是处于运营商 NAT 网关的背后，且私网地址是动态获取的，本发明实施例使得 VCPE 可以主动发起控制连接，从而有效地解决了 VCPE 实用化过程中的这种特殊问题。

附图说明

图 1 是一种 VCPE 现网部署示意图；

图 2 是本发明第一实施例协议报文的结构示意图；

图 3 是本发明第一实施例协议报文的公共头部示意图；

图 4 是本发明第一实施例协议报文的消息类型；

图 5 是本发明第二实施例协议报文的各消息类型所对应的协议数据；

图 6 是本发明第三实施例中，VCPE 的上线管理流程图；

图 7 是本发明第三实施例网络控制器协议状态机；

图 8 是本发明第六实施例 NAT 穿越下的命令行通道建立流程图。

具体实施方式

下面结合附图及具体实施例对本发明作进一步的详细描述。

本发明提供一种协议报文，用于网络控制器与虚拟客户终端设备 VCPE 之间的通信，协议报文的净荷部分具有公共头部，公共头部包括用于指示 VCPE 的通用唯一识别码（Universally Unique Identifier, UUID）的字段，UUID 是 VCPE 首次启动时生成的，并存储在 VCPE 的配置文件中作为 VCPE 的唯一标识，生成 UUID 可以利用 uuidgen.exe 等工具。

由于 VCPE 本质上是一个软件功能实体，采用 VCPE 的 UUID，使得网络控制器对 VCPE 进行远程管理需要一个类似于物理设备序列号作为 VCPE 的唯一标识，作为 VCPE 上线以及后期业务配置管理的依据，在此基础上制定出一套完善的 VCPE 管理协议报文，从而快速、可靠地实现 VCPE 的大规模部署，具有成本低、可扩展性好、适应性强、易于实现和部署等优点。

参见图 2 所示，本发明第一实施例提供一种协议报文，协议报文包括报文头部和净荷部分，其中，协议报文的净荷部分具有公共头部和协议数据，公共头部的格式参见图 3 所示，公共头部为类型长度值 TLV（Type、Length、Value），公共头部包括协议版本号（Version）、消息类型（Type）、消息总长度（Length）、以及用于指示 VCPE 的通用唯一识别码 UUID 的字段，UUID 是 VCPE 首次启动时生成的。

公共头部还包括认证加密字段，认证加密字段包括认证类型（Auth Type）和对应的密码信息（Authentication），认证类型包括简单密码认证和 MD5 认证，密码信息为明文密码或者全 0。

公共头部还包括保留字段（Reserved），用于自定义功能，自定义功能包括告警上报和拓扑自动发现。

参见图 3 所示，对各字段描述如下：

- (1) 协议版本号 Version: 可自定义, 1 字节;
- (2) 消息类型 Type: 1 字节, 定义的消息类型参见图 4 所示, 包括认证请求 (Type1)、认证应答 (Type2)、心跳 (连接保活, Type3)、节点信息上报 (Type4)、服务端口通告 (Type5) 和会话关闭 (Type6)。可按实际需要进行扩展;
- (3) 消息总长度 Length: 消息包括本公共头部和数据部分;
- (4) UUID: 16 字节, VCPE 的唯一标志;
- (5) 保留字段 Reserved: 3 字节, 留作实际需要进行扩展;
- (6) 认证类型 Auth Type: 0 表示不认证, 1 表示简单密码认证, 2 表示消息摘要算法第五版 (Message Digest Algorithm, MD5) 认证;
- (7) 密码信息 Authentication: 为简单密码认证时携带的是明文密码, 不认证或者 MD5 时全 0;

当 AuthType 为 2 时, 表示 MD5 认证, 在报文的协议数据尾部有额外 16 字节的 MD5 的校验字段。

由上面的描述可知, 该协议报文的净荷部分具有公共头部, 采用的是 TLV 的格式, 因此具有良好的扩展性, 可以满足后期多样化的需求。

本发明第二实施例提供一种协议报文, 在本发明第一实施例的基础上, 消息类型 Type 的具体定义可以如图 5 所示, 图 5 描述的内容均为协议数据, 根据公共头部中的 Type 值进行区分, 具体说明如下:

认证请求 (Type1) 包括用户名长度 (UserName Len)、用户名 (UserName)、密码长度 (Password Len)、密码 (Password), VCPE 的 IP 地址长度 (IP Len) 和 VCPE 的 IP 地址 (My IP)。

认证应答 (Type2) 包括认证结果 (Result) 和保留字符 (Reserved)。

由网络控制器发往 VCPE，用于对 VCPE 的用户认证请求给予应答，当认证成功时，Result 字段为 0，当认证失败时，Result 字段返回 1；需要重认证时，Result 字段填 2。

心跳（连接保活，Type3）包括魔术字（Magic number），魔术字用于心跳报文的校验，也可作为保留字段用作扩展用途。

节点信息上报（Type4）包括子类型（Sub Type）、子长度（Sub Length）和子值（Sub Value）。

服务端口通告（Type5）用于网络控制器通知 VCPE 向网络控制器主动发起控制连接，包括 IP 类型（IP Type）、网络控制器的 IP 地址长度（IP Len）、网络控制器的 IP 地址（IP）和服务端口信息，服务端口信息包括端口类型（Port Type）、端口长度（Port Len）和端口号（Port）。

其中，IP 类型=1 时，IPv4；IP 类型=2 时，IPv6。端口类型=1：TCP；端口类型=2：UDP。

会话关闭（Type6）包括关闭连接（关闭）和保留字（Reserve），关闭为 1 个字节，保留字（Reserve）为 7 个字节，用于其他功能扩展。

协议报文为传输控制协议（Transmission Control Protocol，TCP）报文或者用户数据报协议（User Datagram Protocol，UDP）报文。参见图 2 所示，协议报文的报文头部包括 IP 头部以及 TCP/UDP 头部，公共头部的定义并没有强制要求承载协议使用 TCP 还是 UDP，但是考虑到 TCP 本身对资源的消耗以及最大限度地提高网络控制器的管理能力，优选使用 UDP，实践表明，使用 UDP 承载上面定义的认证协议具有开发周期短，资源消耗低等特点。

VCPE 支持 IPv4/IPv6 双栈，可以在 IPv4 和 IPv6 网络中部署。

实现 VCPE 设备的身份认证：VCPE 的设备安全认证是产品成熟度的关键衡量因素，由于 VCPE 部署的分散性和开放性的特点，对 VCPE 进行身份认证是涉及业务安全的关键性问题，合理的认证方案极大地提高了 VCPE 的可用性，避免整个业务网络的瘫痪。

本发明第三实施例提供使用上述第二实施例协议报文的虚拟客户终端设备的管理方法，其包括：

网络控制器根据 VCPE 发出的用户认证请求进行用户身份校验，认证通过后，将业务编排器下发的业务配置信息转发给 VCPE，其中，用户认证请求和业务配置消息均由 VCPE 的 UUID 的协议报文承载。

基于消息类型，协议报文包括认证请求报文、认证应答报文、心跳报文和节点信息上报报文。

当 VCPE 首次启动时，向网络控制器发出带有用户认证请求的认证请求报文，用户认证请求包括用户名、密码和 VCPE 的 IP 地址。

网络控制器提取用户认证请求并进行认证，以及返回带有认证结果的认证应答报文。

VCPE 的上线管理流程参见图 6 所示，每个 VCPE 可以作为一个实例，认证服务器与网络控制器可以集成在一起，也可进行功能分离。为了提高网络控制器管理的网络规模，优选使用独立的验证、授权、计费（Authentication、Authorization、Accounting，AAA）服务器作为认证服务器，网络控制器通过远程用户拨号认证服务（Remote Authentication Dial In User Service，Radius）或者终端访问控制器访问控制系统（Terminal Access Controller Access Control System，TACACS）协议与认证服务器进行交互，可以满足规模商用的需求。

S1 管理员为即将开通的 VCPE 分配用户名，密码以及位置代码，并存储在认证服务器数据库内；

S2 管理员通过邮件或者短信的方式将用户名，密码以及位置代码等信息告知设备开通人员；

S3 开通人员通过配置文件或者 WEB 客户端将用户名、密码以及位置代码等信息写入到 VCPE 配置文件，位置代码为网络控制器对全网 VCPE 的一个唯一编号，通过位置代码可以获取 VCPE 的地理位置信息；

S4 VCPE 首次启动时生成 UUID，并保存在配置文件中；VCPE 通过动态主机配置协议 (Dynamic Host Configuration Protocol, DHCP) 或者静态指定的 IP 地址与控制器互通，将用户名、密码、位置代码和本地管理 IP 地址等通过私有认证报文发送到网络控制器，必要时进行数据加密或者完整性校验。

S5 网络控制器提取 VCPE 认证请求报文中的用户名，密码，UUID 以及位置信息，并发送到认证服务器进行认证，认证服务器根据本地数据库进行用户身份校验，同时向控制器返回认证结果；

S6 网络控制器接收认证服务器返回的认证结果，如果认证通过，则为合法的 VCPE，将 VCPE 的信息上报编排器；如果认证不通过，则丢弃 VCPE 的认证请求，并通过日志进行记录；

S7 业务编排器通过界面向通过认证的 VCPE 下发业务配置数据；

S8 网络控制器以 UUID 为标识，将业务编排器下发的配置转化成设备协议并下发给各 VCPE 实例。

VCPE 认证过程中，网络控制器协议状态机参见图 7 所示。

启动状态 (Init): 网络控制器收到 VCPE 认证请求报文，向 AAA 服务器发送认证请求。

未认证状态 (Unauthorized): AAA 服务器认证不通过，返回结果，等待再次认证。

认证状态 (Authorized): AAA 服务器认证通过, 获取拓扑信息, 并会和包活。

会话超时后, 从认证状态 (Authorized) 转换为未认证状态 (Unauthorized); 认证超时后, 从未认证状态 (Unauthorized) 转换为启动状态 (Init)。

本发明实施例实现 VCPE 设备的身份认证: VCPE 的设备安全认证是产品成熟度的关键衡量因素, 由于 VCPE 部署的分散性和开放性的特点, 对 VCPE 进行身份认证是涉及业务安全的关键性问题, 合理的认证方案极大地提高了 VCPE 的可用性, 避免整个业务网络的瘫痪。

本发明第四实施例提供虚拟客户终端设备的管理方法, 在本发明第三实施例的基础上, 用于对迁移的 VCPE 进行重认证, 具体包括:

当 VCPE 的 IP 地址发生变化时, 重复上述图 6 中的过程, 向网络控制器重新发出带有用户认证请求的认证请求报文, 网络控制器提取用户认证请求并进行认证, 以及返回带有认证结果的认证应答报文。

本发明第五实施例提供虚拟客户终端设备的管理方法, 在本发明第三实施例的基础上, 用于网络控制器主动要求 VCPE 进行重认证, 具体包括: 网络控制器向 VCPE 发出认证应答报文, 认证应答报文中消息类型为认证应答 (Type2), 其中, Result 字段填 2, 表示需要重认证。

本发明第四实施例和第五实施例解决 VCPE 迁移的重认证问题: 在 NFV 的实际应用中, 软件迁移是最为常见的需求, 本发明实施例能够在 VCPE 发生迁移、IP 地址变化的情况下对 VCPE 进行可靠的重认证, 且重认证可以由 VCPE 或者网络控制器发起, 进一步提高

VCPE 的可用性和管理效率。

本发明第六实施例提供虚拟客户终端设备的管理方法，在本发明第三实施例的基础上，用于解决 NAT 穿越问题，包括：

当网络控制器收到 VCPE 发出的认证请求报文时，对比 VCPE 的 IP 地址以及协议报文的源 IP 地址，如果不一致，则向 VCPE 发出服务端口通告报文。

由上面 Type1 类型消息的描述可知，当控制器接收到认证请求报文，对比报文净荷部分的管理 IP 以及报文的源 IP，如果两个 IP 不一致，则 VCPE 处于 NAT 网关背后，网络控制器无法主动发起控制连接。此时网络控制器会启动一个随机端口作为侦听服务端，并将端口信息通过该消息通告给 VCPE。VCPE 收到该消息后，可主动向网络控制器的指定端口发起控制连接。由该消息的结构可知，已经充分地考虑 IPv4 和 IPv6，以及 TCP/UDP 的兼容性问题。

参见图 8 所示，VCPE 包括 UDP 认证模块和命令行界面（Command Line Interface，CLI），在 NAT 穿越下的命令行通道建立过程中，网络控制器、认证模块和命令行界面 CLI 的交互过程如下：

S201 UDP 认证模块向网络控制器发送认证请求报文。

S202 网络控制器根据认证请求报文，对比 UDP 头的源 IP 和净荷部分中的 VCPE 的 IP 字段，如果不一致，则 VCPE 处于 NAT 网关背后，网络控制器动态分配 TCP 端口号启动服务端，同时发送 Type 5 的服务端口通告报文告知 VCPE。

S203 UDP 认证模块向网络控制器的服务端口主动发起连接。

S204 UDP 认证模块向命令行界面 CLI 动态建立 TCP 连接。

S205 网络控制器向建立的 TCP 连接发送命令行数据。

S206 UDP 认证模块透传命令行数据到命令行界面 CLI。

S207 命令行界面 CLI 返回数据。

S208 UDP 认证模块透传返回数据到网络控制器。

S209 网络控制器命令行发送完毕后，发送 Type6 的关闭连接报文到 UDP 认证模块。

S210 UDP 认证模块关闭连接。

由图中可以看出，在 NAT 穿越的情景下，UDP 认证模块其实是作为控制连接的代理发挥作用的。

在现网的部署场景中，很多中小型企业出口并没有公网地址，而是处于运营商 NAT 网关的背后，且私网地址是动态获取的。VCPE 的控制连接一般由控制器主动发起，如典型的命令行配置通道情况下，VCPE 往往作为远程终端协议 Telnet/安全外壳协议 (Secure Shell, SSH) 的服务端，网络控制器通过客户端主动连接 VCPE。然而，当 VCPE 处于 NAT 网关背后时，网络控制器不能主动发起到 VCPE 的控制连接。本发明实施例使得 VCPE 可以主动发起控制连接，从而有效地解决了 VCPE 实用化过程中的这种特殊问题。

本发明不局限于上述实施方式，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本发明的保护范围之内。本说明书中未作详细描述的内容属于本领域专业技术人员公知的现有技术。

权 利 要 求 书

1. 一种协议报文，用于网络控制器与虚拟客户终端设备 VCPE 之间的通信，其特征在于：

所述协议报文的净荷部分具有公共头部，所述公共头部包括用于指示所述 VCPE 的通用唯一识别码 UUID 的字段，所述 UUID 是所述 VCPE 首次启动时生成的。

2. 如权利要求 1 所述的协议报文，其特征在于：所述公共头部为类型长度值 TLV，包括协议版本号、消息类型、消息总长度和认证加密字段。

3. 如权利要求 2 所述的协议报文，其特征在于：所述消息类型包括认证请求、认证应答、心跳和节点信息上报。

4. 如权利要求 2 所述的协议报文，其特征在于：所述消息类型还包括服务端口通告和会话关闭，服务端口通告报文包括 IP 类型、网络控制器的 IP 地址和服务端口信息，用于通知所述 VCPE 向网络控制器主动发起控制连接。

5. 如权利要求 2 所述的协议报文，其特征在于：所述认证加密字段包括认证类型和对应的密码信息，所述认证类型包括简单密码认证和 MD5 认证，所述密码信息为明文密码或者全 0。

6. 如权利要求 1 所述的协议报文，其特征在于：所述公共头部还包括保留字段，用于自定义功能，自定义功能包括告警上报和拓扑自动发现。

7. 如权利要求 1 所述的协议报文，其特征在于：所述协议报文为 TCP 报文或者 UDP 报文。

8. 一种使用权利要求 1 至 7 任一项所述的协议报文的虚拟客户终端设备的管理方法，其特征在于，其包括：

网络控制器根据所述 VCPE 发出的用户认证请求进行用户身份校验，认证通过后，将业务编排器下发的业务配置信息转发给所述 VCPE，其中，所述用户认证请求和业务配置消息均由所述 VCPE 的 UUID 的协议报文承载。

9. 如权利要求 8 所述的虚拟客户终端设备的管理方法，其特征在于：所述公共头部为类型长度值 TLV，包括协议版本号、消息类型、消息总长度和认证加密字段，基于所述消息类型，所述协议报文包括认证请求报文、认证应答报文、心跳报文和节点信息上报报文；

当所述 VCPE 首次启动以及所述 VCPE 的 IP 地址发生变化时，向网络控制器发出带有所述用户认证请求的认证请求报文，所述用户认证请求包括用户名、密码和所述 VCPE 的 IP 地址；

网络控制器提取所述用户认证请求并进行认证，以及返回带有认证结果的认证应答报文。

10. 如权利要求 9 所述的虚拟客户终端设备的管理方法，其特征在于：所述协议报文还包括服务端口通告报文，服务端口通告报文包括 IP 类型、网络控制器的 IP 地址和服务端口信息，用于通知所述 VCPE 向网络控制器主动发起控制连接；

当网络控制器收到所述 VCPE 发出的所述认证请求报文时，对比所述 VCPE 的 IP 地址以及所述协议报文的源 IP 地址，如果不一致，则向所述 VCPE 发出所述服务端口通告报文。

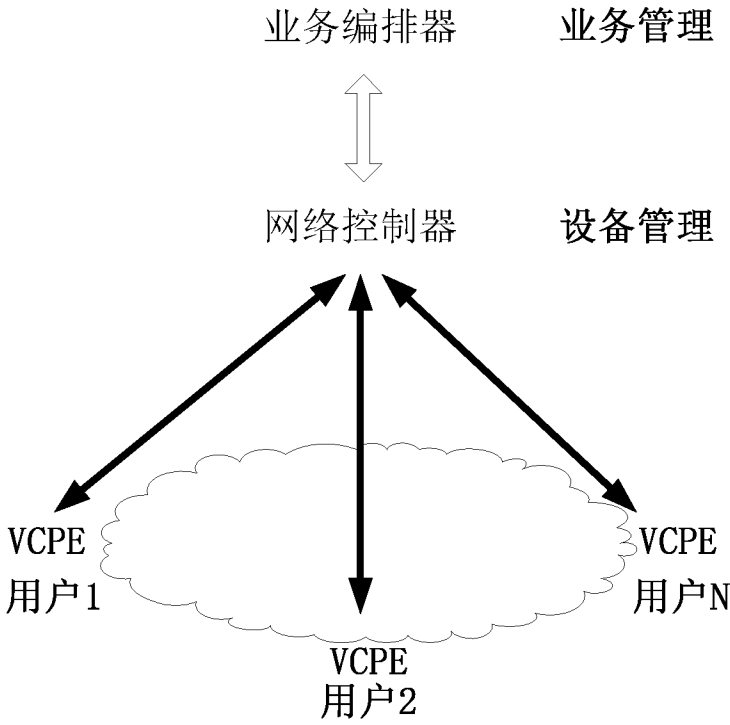


图 1

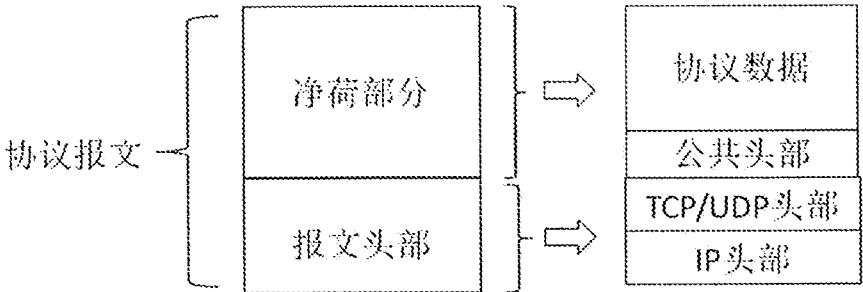


图 2

1字节	1字节	2字节
Version	Type	Length
UUID		
UUID		
UUID		
UUID		
Reserved		Auth Type
Authentication		

图 3

Type 类型值	描述
1	认证请求
2	认证应答
3	连接保活
4	节点信息上报
5	服务端口通告
6	会话关闭

图 4

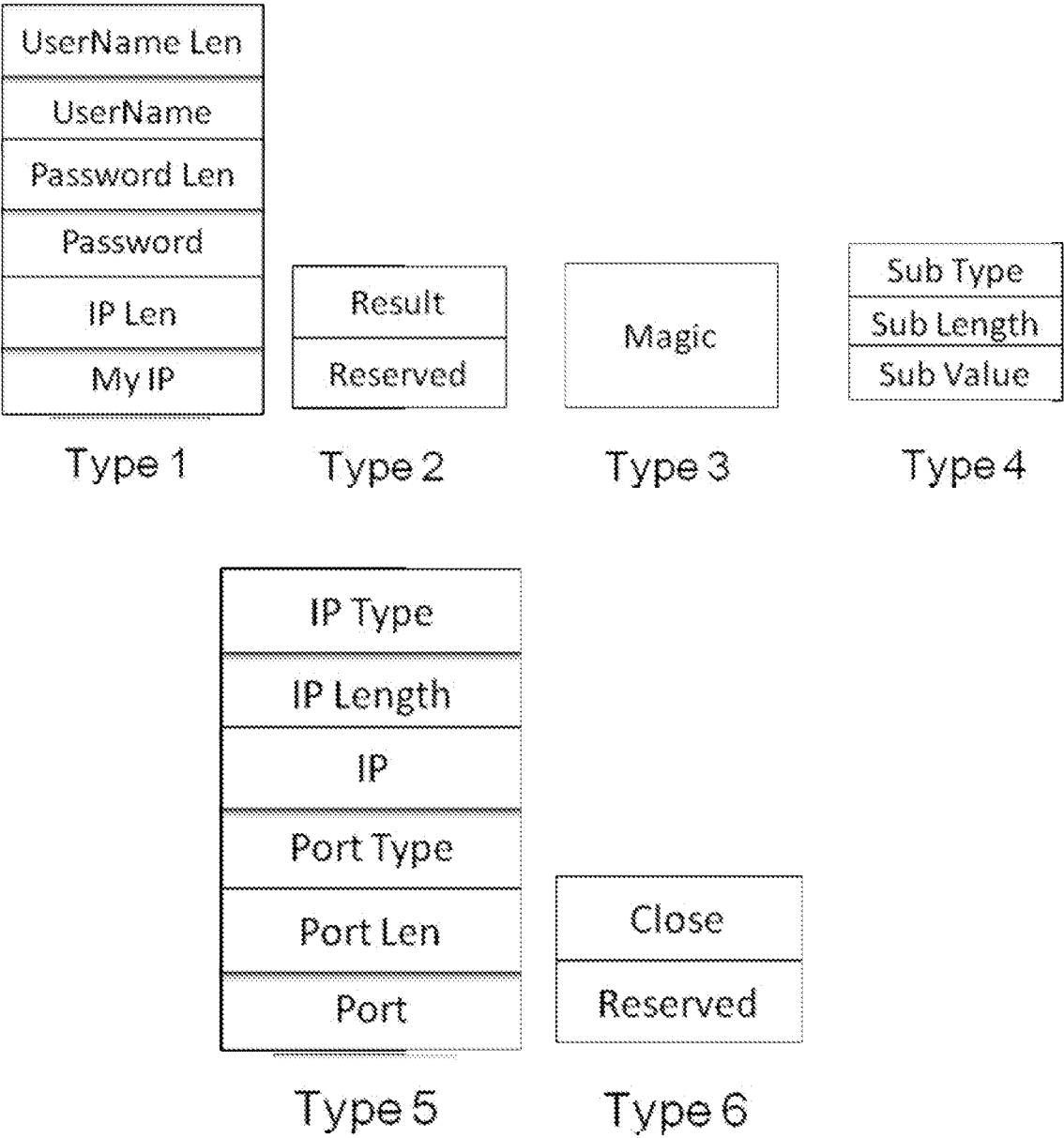


图 5

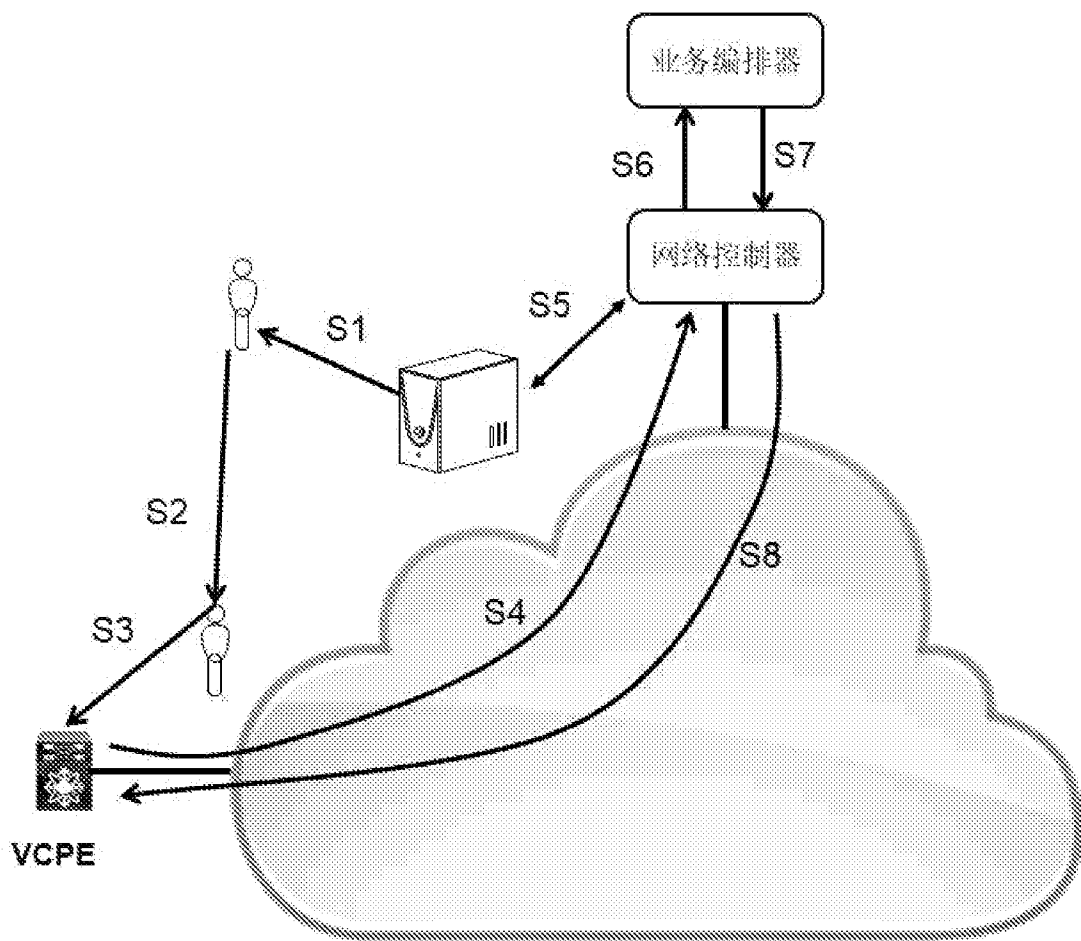


图 6

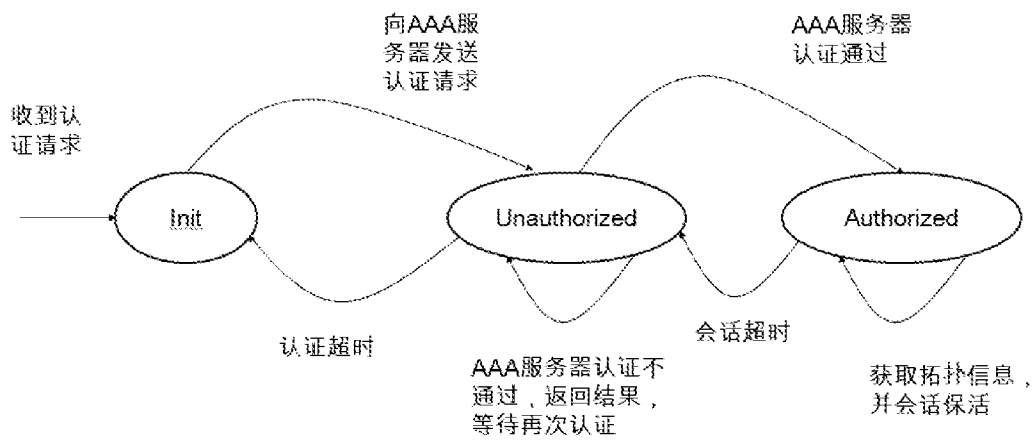


图 7

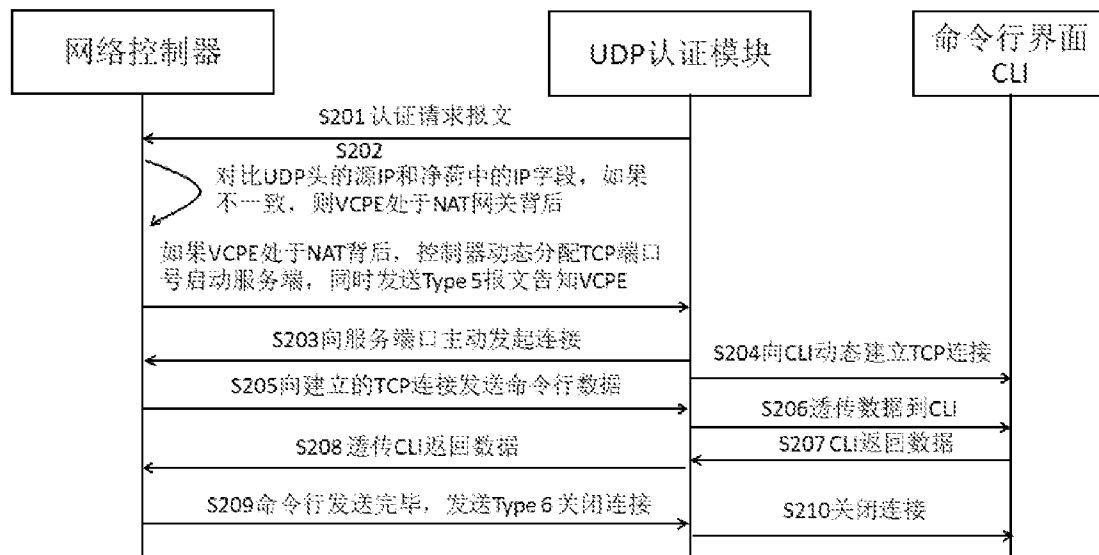


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/119058

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(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)

CNKI, CNPAT, WPI, EPODOC, IEEE: 协议, 报文, 头部, 虚拟客户端, 虚拟用户驻地, 标识, 唯一, 识别码, 首次, 第一次, 启动, 开启, protocol, message, head, VCPE, ID, unique, identifier, UUID, first, start

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106533883 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 22 March 2017 (2017-03-22) description, paragraphs [0029]-[0077]	1-10
A	CN 105959188 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 September 2016 (2016-09-21) entire document	1-10
A	CN 105681055 A (ZTE CORPORATION) 15 June 2016 (2016-06-15) entire document	1-10
A	WO 2017107963 A1 (BEIJING QIHOO TECHNOLOGY CO., LTD.) 29 June 2017 (2017-06-29) 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

14 February 2019

Date of mailing of the international search report

27 February 2019

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC (ISA/CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/119058

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106533883	A	22 March 2017	None			
CN	105959188	A	21 September 2016	None			
CN	105681055	A	15 June 2016	WO	2016078291	A1	26 May 2016
WO	2017107963	A1	29 June 2017	CN	105553832	A	04 May 2016

国际检索报告

国际申请号

PCT/CN2018/119058

A. 主题的分类

H04L 12/24(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))

CNKI, CNPAT, WPI, EPDOC, IEEE: 协议, 报文, 头部, 虚拟客户端, 虚拟用户驻地, 标识, 唯一, 识别码, 首次, 第一次, 启动, 开启, protocol, message, head, VCPE, ID, unique, identifier, UUID, first, start

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
X	CN 106533883 A (中国联合网络通信集团有限公司) 2017年 3月 22日 (2017 - 03 - 22) 说明书第[0029]-[0077]段	1-10
A	CN 105959188 A (华为技术有限公司) 2016年 9月 21日 (2016 - 09 - 21) 全文	1-10
A	CN 105681055 A (中兴通讯股份有限公司) 2016年 6月 15日 (2016 - 06 - 15) 全文	1-10
A	WO 2017107963 A1 (北京奇虎科技有限公司) 2017年 6月 29日 (2017 - 06 - 29) 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

2019年 2月 14日

国际检索报告邮寄日期

2019年 2月 27日

ISA/CN的名称和邮寄地址

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

受权官员

陈文静

传真号 (86-10)62019451

电话号码 86-(10)-53961739

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/119058

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	106533883	A	2017年 3月 22日	无			
CN	105959188	A	2016年 9月 21日	无			
CN	105681055	A	2016年 6月 15日	WO	2016078291	A1	2016年 5月 26日
WO	2017107963	A1	2017年 6月 29日	CN	105553832	A	2016年 5月 4日