(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106685847 B
(45)授权公告日 2020.01.17

(21)申请号 201510752291.4

(22)申请日 2015.11.06

(65)同一申请的已公布的文献号
申请公布号 CN 106685847 A

(43)申请公布日 2017.05.17

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 徐亦斌 孙兵

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 罗振安

(51)Int.Cl.
H04L 12/823(2013.01)

(56)对比文件
US 8666786 B1,2014.03.04,
US 8516556 B2,2013.08.20,
CN 100484130 C,2009.04.29,
CN 1522020 A,2004.08.18,
CN 104579994 A,2015.04.29,

审查员 舒维莹

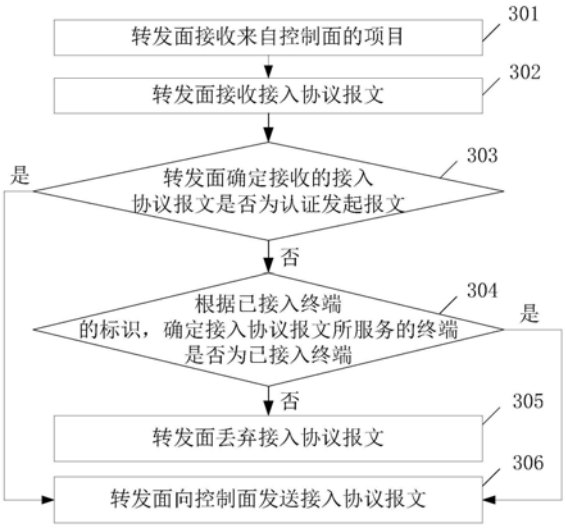
权利要求书4页 说明书9页 附图2页

(54)发明名称

一种报文处理方法、装置及设备

(57)摘要

本发明公开了一种报文处理方法、装置及设备，属于通信技术领域。所述方法包括：转发面接收来自所述转发面的控制面的项目；所述项目包括已接入终端的标识；接收接入协议报文；当所述转发面确定所述接入协议报文不是认证发起报文时，所述转发面根据所述已接入终端的标识，确定所述接入协议报文所服务的终端是否为所述已接入终端，其中，所述认证发起报文为用于发起对所述认证发起报文所服务的终端的认证过程的认证报文；当所述接入协议报文不是认证发起报文，并且所述接入协议报文所服务的终端不是所述已接入终端时，所述转发面丢弃所述接入协议报文。本发明可以提升用户体验。



CN 106685847 B

1.一种报文处理方法,其特征在于,所述方法包括:

转发面接收来自所述转发面的控制面的项目,所述项目包括已接入终端的标识,所述已接入终端是指已发起认证过程且还未完成认证的终端,或者是已完成认证且在线的终端;

所述转发面接收接入协议报文;

当所述转发面确定所述接入协议报文不是认证发起报文时,所述转发面根据所述已接入终端的标识,确定所述接入协议报文所服务的终端是否为所述已接入终端,其中,所述认证发起报文为用于发起对所述认证发起报文所服务的终端的认证过程的认证报文;

当所述接入协议报文不是认证发起报文,并且所述接入协议报文所服务的终端不是所述已接入终端时,所述转发面丢弃所述接入协议报文。

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:

当所述转发面确定所述接入协议报文是认证发起报文时,所述转发面将所述接入协议报文放入新接入终端报文队列;

当所述转发面确定所述接入协议报文不是认证发起报文且所述转发面确定所述接入协议报文所服务的终端是所述已接入终端时,所述转发面将所述接入协议报文放入已接入终端报文队列;

所述转发面按照所述新接入终端报文队列和所述已接入终端报文队列各自的优先级,调度所述新接入终端报文队列和所述已接入终端报文队列,其中,所述新接入终端报文队列的优先级不同于所述已接入终端报文队列的优先级。

3.根据权利要求2所述的方法,其特征在于,所述项目还包括已接入终端的认证状态,所述认证状态为未完成认证或完成认证,所述已接入终端报文队列包括认证中报文队列和认证完成报文队列,所述认证中报文队列的优先级不同于所述认证完成报文队列的优先级;

所述转发面将所述接入协议报文放入已接入终端报文队列,包括:

所述转发面确定所述接入协议报文所服务的终端的认证状态;

当所述接入协议报文所服务的终端的认证状态为未完成认证时,所述转发面将所述接入协议报文放入所述认证中报文队列;

当所述接入协议报文所服务的终端的认证状态为完成认证时,所述转发面将所述接入协议报文放入所述认证完成报文队列。

4.根据权利要求1至3任意一项所述的方法,其特征在于,所述项目还包括已接入终端的认证状态,所述认证状态为未完成认证或完成认证,所述方法还包括:

当所述转发面确定所述接入协议报文不是认证发起报文且所述转发面确定所述接入协议报文所服务的终端是所述已接入终端时,所述转发面确定所述接入协议报文所服务的终端的认证状态;

当所述接入协议报文所服务的终端的认证状态为未完成认证,并且所述转发面确定所述接入协议报文为在线报文时,丢弃所述接入协议报文;

当所述接入协议报文所服务的终端的认证状态为完成认证,并且所述转发面确定所述接入协议报文为除认证发起报文之外的认证报文时,丢弃所述接入协议报文。

5.根据权利要求1至3任意一项所述的方法,其特征在于,所述方法还包括:

所述转发面接收所述控制面发送的指示，所述指示用于指示认证状态为未完成认证的已接入终端的数量高于预设数量；

所述转发面限制向所述控制面发送所述认证发起报文的速率。

6.一种报文处理装置，其特征在于，所述装置包括：

接收单元，用于接收来自控制面的项目和接收接入协议报文；所述项目包括已接入终端的标识，所述已接入终端是指已发起认证过程且还未完成认证的终端，或者是已完成认证且在线的终端；

处理单元，用于当确定所述接入协议报文不是认证发起报文时，根据所述已接入终端的标识，确定所述接入协议报文所服务的终端是否为所述已接入终端，其中，所述认证发起报文为用于发起对所述认证发起报文所服务的终端的认证过程的认证报文；当所述接入协议报文不是认证发起报文，并且所述接入协议报文所服务的终端不是所述已接入终端时，丢弃所述接入协议报文。

7.根据权利要求6所述的装置，其特征在于，所述处理单元还用于：

当确定所述接入协议报文是认证发起报文时，将所述接入协议报文放入新接入终端报文队列；

当确定所述接入协议报文不是认证发起报文且确定所述接入协议报文所服务的终端是所述已接入终端时，将所述接入协议报文放入已接入终端报文队列；

按照所述新接入终端报文队列和所述已接入终端报文队列各自的优先级，调度所述新接入终端报文队列和所述已接入终端报文队列，其中，所述新接入终端报文队列的优先级不同于所述已接入终端报文队列的优先级。

8.根据权利要求7所述的装置，其特征在于，所述项目还包括已接入终端的认证状态，所述认证状态为未完成认证或完成认证，所述已接入终端报文队列包括认证中报文队列和认证完成报文队列，所述认证中报文队列的优先级不同于所述认证完成报文队列的优先级；

所述处理单元用于，

当确定所述接入协议报文不是所述认证发起报文且确定所述接入协议报文所服务的终端是所述已接入终端时，确定所述接入协议报文所服务的终端的认证状态；

当所述接入协议报文所服务的终端的认证状态为未完成认证时，将所述接入协议报文放入所述认证中报文队列；

当所述接入协议报文所服务的终端的认证状态为完成认证时，将所述接入协议报文放入所述认证完成报文队列。

9.根据权利要求6至8任意一项所述的装置，其特征在于，所述项目还包括已接入终端的认证状态，所述认证状态为未完成认证或完成认证，所述处理单元还用于：

当确定所述接入协议报文不是认证发起报文且确定所述接入协议报文所服务的终端是所述已接入终端时，确定所述接入协议报文所服务的终端的认证状态；

当所述接入协议报文所服务的终端的认证状态为未完成认证，并且确定所述接入协议报文为在线报文时，丢弃所述接入协议报文；

当所述接入协议报文所服务的终端的认证状态为完成认证，并且确定所述接入协议报文为除认证发起报文之外的认证报文时，丢弃所述接入协议报文。

10.根据权利要求6至8任意一项所述的装置,其特征在于,

所述接收单元还用于,接收所述控制面发送的指示;所述指示用于指示认证状态为未完成认证的已接入终端的数量高于预设数量;

所述处理单元还用于,限制向所述控制面发送所述认证发起报文的速率。

11.一种报文处理设备,其特征在于,所述设备包括:

控制面装置和转发面装置;

所述控制面装置用于,向所述转发面装置发送项目,所述项目包括已接入终端的标识,所述已接入终端是指已发起认证过程且还未完成认证的终端,或者是已完成认证且在线的终端;

所述转发面装置用于,接收来自所述控制面装置的项目和接收接入协议报文;当确定所述接入协议报文不是认证发起报文时,根据所述已接入终端的标识,确定所述接入协议报文所服务的终端是否为所述已接入终端,其中,所述认证发起报文为用于发起对所述认证发起报文所服务的终端的认证过程的认证报文;当所述接入协议报文不是认证发起报文,并且所述接入协议报文所服务的终端不是所述已接入终端时,丢弃所述接入协议报文。

12.根据权利要求11所述的设备,其特征在于,所述转发面装置还用于:

当确定所述接入协议报文是认证发起报文时,将所述接入协议报文放入新接入终端报文队列;

当确定所述接入协议报文不是认证发起报文且确定所述接入协议报文所服务的终端是所述已接入终端时,将所述接入协议报文放入已接入终端报文队列;

按照所述新接入终端报文队列和所述已接入终端报文队列各自的优先级,调度所述新接入终端报文队列和所述已接入终端报文队列,其中,所述新接入终端报文队列的优先级不同于所述已接入终端报文队列的优先级。

13.根据权利要求12所述的设备,其特征在于,所述项目还包括已接入终端的认证状态,所述认证状态为未完成认证或完成认证,所述已接入终端报文队列包括认证中报文队列和认证完成报文队列,所述认证中报文队列的优先级不同于所述认证完成报文队列的优先级;

所述转发面装置还用于:

当确定所述接入协议报文不是所述认证发起报文且确定所述接入协议报文所服务的终端是所述已接入终端时,确定所述接入协议报文所服务的终端的认证状态;

当所述接入协议报文所服务的终端的认证状态为未完成认证时,将所述接入协议报文放入所述认证中报文队列;

当所述接入协议报文所服务的终端的认证状态为完成认证时,将所述接入协议报文放入所述认证完成报文队列。

14.根据权利要求11至13任意一项所述的设备,其特征在于,所述项目还包括已接入终端的认证状态,所述认证状态为未完成认证或完成认证,所述转发面装置还用于:

当确定所述接入协议报文不是认证发起报文且确定所述接入协议报文所服务的终端是所述已接入终端时,确定所述接入协议报文所服务的终端的认证状态;

当所述接入协议报文所服务的终端的认证状态为未完成认证,并且确定所述接入协议报文为在线报文时,丢弃所述接入协议报文;

当所述接入协议报文所服务的终端的认证状态为完成认证，并且确定所述接入协议报文为除认证发起报文之外的认证报文时，丢弃所述接入协议报文。

15.根据权利要求11至13任意一项所述的设备，其特征在于，

所述控制面装置还用于：向所述转发面装置发送指示；所述指示用于指示认证状态为未完成认证的已接入终端的数量高于预设数量；

所述转发面装置还用于：接收所述控制面装置发送的指示，限制向所述控制面装置发送所述认证发起报文的速率。

一种报文处理方法、装置及设备

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种报文处理方法、装置及设备。

背景技术

[0002] 一般地，终端在访问网络前，有可能需要在认证设备处完成用户认证。在完成用户认证之后，终端方能访问网络(也称上线)。终端在在线过程中、以及退出其访问的网络(也称下线)时，也与认证设备通信。

[0003] 终端或者认证服务器通过接入协议与认证设备通信。常见的接入协议包括门户(英文:portal)协议、以太网上的点对点协议(英文:Point-to-Point Protocol over Ethernet，缩写:PPPoE)和基于局域网的可扩展认证协议(英文:Extensible Authentication Protocol over local area network，缩写:EAPOL)。其中，portal协议是采用网页(英文:web)认证开展局域网业务时的方案中的协议，包括密码认证协议(英文:Password Authentication Protocol，缩写:PAP)和询问握手认证协议(英文:Challenge Handshake Authentication Protocol，缩写:CHAP)。

[0004] 目前，为防止中央处理器(英文:central processing unit，缩写:CPU)被攻击，认证设备在接收接入协议报文的速率达到预设上限速率时，将限制接入协议报文的速率。具体的限制措施为，随机丢弃接入协议报文。

[0005] 随机丢弃报文后，将影响供应商的服务质量，用户的业务体验比较差。

发明内容

[0006] 为了解决由于随机丢弃报文所导致的用户的业务体验比较差的问题，本申请提供了一种报文处理方法、装置及设备。

[0007] 第一方面，提供了一种报文处理方法，所述方法包括：

[0008] 转发面接收来自所述转发面的控制面的项目；所述项目包括已接入终端的标识；

[0009] 所述转发面接收接入协议报文；

[0010] 当所述转发面确定所述接入协议报文不是认证发起报文时，所述转发面根据所述已接入终端的标识，确定所述接入协议报文所服务的终端是否为所述已接入终端，其中，所述认证发起报文为用于发起对所述认证发起报文所服务的终端的认证过程的认证报文；

[0011] 当所述接入协议报文不是认证发起报文，并且所述接入协议报文所服务的终端不是所述已接入终端时，所述转发面丢弃所述接入协议报文。

[0012] 通过接收来自控制面的项目，转发面可以获得已接入终端的标识。由于服务新接入终端的接入协议报文只能是认证发起报文，因此，当接入协议报文不是认证发起报文，而该接入协议报文所服务的终端又不是已接入终端时，转发面可以确定该接入协议报文为错误报文或攻击报文，丢弃该接入协议报文。相比于随机丢弃报文，既减轻了控制面的处理负担，又避免给用户带来不好的影响，能够提升用户业务体验。

[0013] 结合第一方面，在第一方面的第一实现中，所述方法还包括：

[0014] 当所述转发面确定所述接入协议报文是认证发起报文时，所述转发面将所述接入协议报文放入新接入终端报文队列；

[0015] 当所述转发面确定所述接入协议报文不是认证发起报文且所述转发面确定所述接入协议报文所服务的终端是所述已接入终端时，所述转发面将所述接入协议报文放入已接入终端报文队列；

[0016] 所述转发面按照所述新接入终端报文队列和所述已接入终端报文队列各自的优先级，调度所述新接入终端报文队列和所述已接入终端报文队列，其中，所述新接入终端报文队列的优先级不同于所述已接入终端报文队列的优先级。

[0017] 按照实际需要设置新接入终端报文队列和已接入终端报文队列的优先级，再按照队列的优先级调度各个队列，可以提升用户业务体验。比如，可以优先调度已接入终端报文队列，这样，可以保证已接入终端的业务能够及时处理。

[0018] 结合第一方面或第一方面的第一实现，在第一方面的第二实现中，所述项目还包括已接入终端的认证状态，所述认证状态为未完成认证或完成认证，所述已接入终端报文队列包括认证中报文队列和认证完成报文队列，所述认证中报文队列的优先级不同于所述认证完成报文队列的优先级；

[0019] 所述转发面将所述接入协议报文放入已接入终端报文队列，包括：

[0020] 所述转发面确定所述接入协议报文所服务的终端的认证状态；

[0021] 当所述接入协议报文所服务的终端的认证状态为未完成认证时，所述转发面将所述接入协议报文放入所述认证中报文队列；

[0022] 当所述接入协议报文所服务的终端的认证状态为完成认证时，所述转发面将所述接入协议报文放入所述认证完成报文队列。

[0023] 通过设置新接入终端报文队列、认证中报文队列和认证完成报文队列，并根据实施需要设置新接入终端报文队列、认证中报文队列和认证完成报文队列的优先级，在按照队列的优先级调度各个队列时，可以进一步提升用户业务体验。

[0024] 结合第一方面、第一方面的第一实现及第一方面的第二实现中的任意一个，在第一方面的第三实现中，所述项目还包括已接入终端的认证状态，所述认证状态为未完成认证或完成认证，所述方法还包括：

[0025] 当所述转发面确定所述接入协议报文不是认证发起报文且所述转发面确定所述接入协议报文所服务的终端是所述已接入终端时，所述转发面确定所述接入协议报文所服务的终端的认证状态；

[0026] 当所述接入协议报文所服务的终端的认证状态为未完成认证，并且所述转发面确定所述接入协议报文为在线报文时，丢弃所述接入协议报文；

[0027] 当所述接入协议报文所服务的终端的认证状态为完成认证，并且所述转发面确定所述接入协议报文为除认证发起报文之外的认证报文时，丢弃所述接入协议报文。

[0028] 由于服务认证状态为完成认证的已接入终端的接入协议报文只能是认证发起报文、在线报文或下线报文，而服务认证状态为未完成认证的已接入终端的接入协议报文只能是认证报文或下线报文，因此，为认证状态为完成认证的已接入终端服务的除认证发起报文之外的认证报文、以及为认证状态为未完成认证的已接入终端服务的在线报文，均为错误报文或攻击报文，丢弃错误报文或攻击报文后，将进一步提升用户体验，减轻控制面的

处理负担。

[0029] 结合第一方面、第一方面的第一实现、第一方面的第二实现及第一方面的第三实现中的任意一个，在第一方面的第四实现中，所述方法还包括：

[0030] 所述转发面接收所述控制面发送的指示，所述指示用于指示所述认证状态为未完成认证的已接入终端的数量高于预设数量；

[0031] 所述转发面限制向所述控制面发送所述认证发起报文的速率。

[0032] 当认证状态为未完成认证的已接入终端的数量高于预设数量时，表明控制面的处理负担大，这时转发面限制向控制面发送认证发起报文的速率，可以减轻控制面的处理负担。

[0033] 第二方面，提供了一种报文处理装置，所述装置包括若干单元，比如接收单元和处理单元，所述若干单元用于实现第一方面提供的方法。

[0034] 第三方面，提供了一种报文处理设备，所述设备包括控制面装置和转发面装置，

[0035] 所述控制面装置用于，向所述转发面装置发送项目，所述项目包括已接入终端的标识；

[0036] 转发面装置至少包括存储器、处理器和通信接口。存储器被配置为，存储指令；处理器被配置为，执行存储器存储的指令；通信接口被配置为，在处理器的控制下与控制面装置通信。其中，处理器通过执行存储器存储的指令，可以实现第一方面提供的方法。

[0037] 第四方面，提供了一种计算机可读存储介质，该计算机可读存储介质用于存储前述转发面装置在处理报文时所执行的程序代码。该程序代码包括用于实现第一方面提供的方法的指令。

附图说明

[0038] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0039] 图1是本发明实施例提供的认证系统的网络架构示意图；

[0040] 图2是本发明实施例提供的认证设备的结构示意图；

[0041] 图3是本发明实施例提供的一种报文处理方法的流程图；

[0042] 图4是本发明实施例提供的EAPOL报文的格式示意图。

具体实施方式

[0043] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0044] 为便于对本发明实施例提供的技术方案的理解，首先结合图1介绍一下认证系统的网络架构。如图1所示，该网络架构的网络设备至少包括终端、认证设备和认证服务器。认证设备为在终端和认证服务器之间进行接入协议报文处理的网络设备。比如，认证设备可以是路由器或网络交换机。接入协议报可以是portal协议报文、PPPoE协议报文和EAPOL报文中的任何一种。

[0045] 如果接入协议报为EAPOL报文，终端与认证设备采用EAPOL报文通信，认证设备与认证服务器采用远程用户拨号认证服务(英文:Remote Authentication Dial-In User Service，缩写:RADIUS)协议通信。

[0046] 如果接入协议报是portal协议报文，该网络架构的网络设备还包括门户服务器。门户服务器分别与认证设备和终端相连。比如，门户服务器可以是个人电脑，也可以是一个服务器网站(英文:web)应用服务器，该门户服务器中有强制门户(英文:captive portal)认证的软件。终端与门户服务器采用超文本传输协议(英文:Hypertext Transfer Protocol，缩写:HTTP)通信，认证设备与门户服务器采用portal协议通信。

[0047] 图2为图1示出的认证设备的一种可能的硬件结构示意图。如图2所示，认证设备包括控制面装置10和转发面装置20。控制面装置10可以是控制芯片。例如，控制面装置10可以由CPU实现，也可以由有控制面功能的网络处理器(英文:network processor，缩写:NP)实现。转发面装置20可以是交换芯片。例如，转发面装置20可以由专用集成电路(英文:application-specific integrated circuit，缩写:ASIC)，可编程逻辑器件(英文:programmable logic device，缩写:PLD)，NP，多核CPU中用于实现转发面的核心或其任意组合实现。上述PLD可以是复杂可编程逻辑器件(英文:complex programmable logic device，缩写:CPLD)，现场可编程逻辑门阵列(英文:field-programmable gate array，缩写:FPGA)，通用阵列逻辑(英文:generic array logic，缩写:GAL)或其任意组合。

[0048] 转发面装置20用于实现认证设备的转发面。认证设备接收的接入协议报文先由转发面装置20处理。转发面装置20确定是否将接入协议报文发送给控制面装置10。转发面装置20根据控制面装置10发送的项目维护终端状态表。终端状态表的表项中包括控制面装置10发送的项目中的已接入终端的标识。控制面装置10可以发送多个项目。控制面装置10发送的项目中也可以有多个已接入终端的标识。相应的，终端状态表的单个表项中可以存储多个已接入终端的标识，终端状态表也可以包括多个表项，每个表项各自存储一个已接入终端的标识。已接入终端是指已发起认证过程且还未完成认证的终端，或者是已完成认证且在线的终端。转发面装置20先确定接入协议报文是否为认证发起报文。认证发起报文是指用于发起对认证发起报文所服务的终端的认证过程的认证报文。接入协议报文所服务的终端是指该接入协议报文参与的认证过程所属的终端。例如，终端发送的为了认证该终端自身的接入协议报文为服务该终端的接入协议报文。又例如，服务器发送的指示终端的认证结果的接入协议报文为服务该终端的接入协议报文。如果接入协议报文是认证发起报文，转发面装置20将该接入协议报文发送至控制面装置10。可选地，转发面装置20将该接入协议报文放入报文队列，调度队列后将该接入协议报文发送至控制面装置10。报文队列用于存放转发面装置20向控制面装置10发送的报文。如果接入协议报文不是认证发起报文，则转发面装置20在终端状态表中查找匹配接入协议报文的表项。当转发面装置20没有找到与接入协议报文匹配的表项时，转发面装置20将接收的接入协议报文丢弃。当转发面装置20找到与接入协议报文匹配的表项时，转发面装置20将该接入协议报文发送至控制面装置10。可选地，转发面装置20将该接入协议报文放入报文队列，调度队列后将该接入协议报文发送至控制面装置10。控制面装置10收到转发面装置20发送的接入协议报文后，按照相应的接入协议处理接入协议报文。如果接入协议报文是认证发起报文，控制面装置10处理该接入协议报文后，该接入协议报文所服务的终端就成为了已接入终端。控制面装置10将包

括该已接入终端的标识的项目发送给转发面装置20。

[0049] 图2示出的认证设备中既有转发面装置也有控制面装置。在另一种可能的硬件结构中，控制面可以由独立的设备实现，例如在软件定义网络，控制面可以由控制器实现。控制器可以通过支持软件定义网络的协议(例如OpenFlow协议)控制转发面装置。这种情况下，也可以将独立实现转发面装置和控制面装置的设备的组合视为认证设备。

[0050] 在本发明实施例中，可以将接入协议报文区分为认证报文、在线报文或下线报文。认证报文为在认证过程中终端或服务器(比如门户服务器)向认证设备发送的报文。认证报文可以是认证发起报文，也可以是除认证发起报文之外的认证报文。在线报文和下线报文为认证完成后在在线过程中终端或服务器向认证设备发送的报文。在线报文和下线报文的不同之处在于，下线报文用于实现终端的下线，在线报文用于实现终端的在线业务(例如用于查询终端的流量)。

[0051] 图3是本发明实施例提供的一种报文处理方法的流程图。如图3所示，该方法包括如下步骤。

[0052] 步骤301、转发面接收来自控制面的项目。

[0053] 转发面可以由图2示出的认证设备的转发面装置实现。控制面可以由图2示出的认证设备的控制面装置实现。

[0054] 该项目包括已接入终端的标识。已接入终端的标识可以是已接入终端的媒体接入控制(英文:Media Access Control，缩写:MAC)地址和网际协议(英文:Internet Protocol，缩写:IP)地址。

[0055] 可选的，控制面发送的项目还包括已接入终端的认证状态，该认证状态为未完成认证或完成认证。

[0056] 转发面接收项目后，将项目包括的已接入终端的标识及认证状态存储到终端状态表中。具体地，终端状态表包括若干表项，表项中记录了已接入终端的标识和认证状态。

[0057] 控制面收到认证发起报文时，确定认证发起报文所服务的终端的认证状态为未完成认证。那么，控制面向转发面发送的项目中，该已接入终端的认证状态为未完成认证。如果该已接入终端后续完成了认证过程，则控制面更新该已接入终端的认证状态为完成认证，再向转发面发送更新认证状态后的项目，该项目中该已接入终端的认证状态为完成认证。进一步地，如果该接入终端后续又重新开始认证过程，则控制面更新该已接入中的认证状态为未完成认证，再向转发面发送更新认证状态后的项目，该项目中该已接入终端的认证状态为未完成认证。

[0058] 可选的，控制面还实时监控认证状态为未完成认证的已接入终端的数量。当认证状态为未完成认证的已接入终端的数量高于预设数量时，控制面向转发面发送指示，该指示用于指示认证状态为未完成认证的已接入终端的数量高于预设数量。基于此，步骤301还可以包括:转发面接收控制面发送的指示。

[0059] 在实现时，该预设数量可以根据控制面的性能参数估算出来。如果认证状态为未完成认证的已接入终端的数量高于预设数量，则控制面的负担达到或接近处理能力的上限。

[0060] 可选的，当认证状态为未完成认证的已接入终端的数量下降到预设范围时，控制面再向转发面发送另一指示，另一指示用于指示认证状态为未完成认证的已接入终端的数

量下降到预设范围。步骤301还包括:转发面接收控制面发送的另一指示。在实现时,预设范围的上限可以是前述的预设数量,也可以设置为比前述的预设数量小的值。

[0061] 步骤302、转发面接收接入协议报文。

[0062] 可选的,转发面在接收控制面发送的指示后,步骤302还包括:转发面限制向控制面发送认证发起报文的速率。

[0063] 在限制向控制面发送认证发起报文的速率时,可以限制单位时间内向控制面发送认证发起报文的数量或数据量。

[0064] 当认证状态为未完成认证的已接入终端的数量高于预设数量时,表明控制面的负担达到或接近处理能力的上限,这时转发面限制向控制面发送认证发起报文的速率,可以在控制控制面的处理负担的增量的同时,保证控制面对已接入终端的上线过程的处理。

[0065] 可选的,转发面在接收控制面发送的另一指示后,步骤302还包括:解除向控制面发送认证发起报文的速率的限制。

[0066] 步骤303、转发面确定接收的接入协议报文是否为认证发起报文。

[0067] 当接收的接入协议报文不为认证发起报文时,执行步骤304;当接收的接入协议报文为认证发起报文时,执行步骤306。

[0068] 可选的,接入协议报文包括用于指示接入协议报文的类型的字段。转发面可以根据该字段识别接入协议报文的类型,从而确定接入协议报文是否为认证发起报文。其中,接入协议报文的类型包括认证发起报文,除认证发起报文之外的认证报文、在线报文和下线报文。图4示出了EAPOL报文的格式。EAPOL报文中,如图4所示,端口访问实体(英文:Port Access Entity,缩写:PAE)以太网(英文:Ethernet)类型(英文:type)字段表示协议类型;协议版本(英文:protocol version)字段表示EAPOL报文的发送方所支持的协议版本号;数据帧体(英文:packet body)字段用于携带EAPOL报文的数据帧;类型(英文:type)字段表示数据帧的类型;长度(英文:length)字段表示数据长度,也就是数据帧体字段的长度。类型字段的取值与各个取值所表示的数据帧的类型不同。该类型字段可以用于指示接入协议报文的类型。例如,当EAPOL报文的类型字段的取值为1(或者表示为0x01)时,数据帧的类型为认证发起(英文:Start)帧,指示的EAPOL报文的类型为认证发起报文。

[0069] 步骤304、转发面根据已接入终端的标识,确定接入协议报文所服务的终端是否为已接入终端。

[0070] 当确定接入协议报文所服务的终端不是已接入终端时,即当该接入协议报文所服务的终端是新接入终端时,执行步骤305;当确定接接入协议报文所服务的终端是已接入终端时,执行步骤306。

[0071] 可选的,转发面根据接入协议报文所属的接入协议确定接入协议报文所服务的终端。例如,当接收的接入协议报文为EAPOL报文时,接入协议报文所服务的终端的标识为EAPOL报文的源MAC地址。当接收的接入协议报文为portal协议报文时,接入协议报文所服务的终端的标识为,portal协议报文中包括的所服务的终端的IP地址。

[0072] 可选的,转发面在终端状态表的表项中匹配接入协议报文所服务的终端标识。如果在表项中匹配到接入协议报文所服务的终端标识,则判定接入协议报文所服务的终端是已接入终端;如果在表项中未匹配到接入协议报文所服务的终端标识,则判定接入协议报文所服务的终端不是已接入终端。

[0073] 步骤305、转发面丢弃接入协议报文。

[0074] 一般地，终端或服务器向认证设备发送的接入协议报文是正常报文，比如新接入终端向认证设备发送的认证发起报文，又如已接入终端向认证设备发送的下线报文。如果终端或服务器出错，或者认证设备受到攻击，认证设备接收到的接入协议报文也可能是错误报文或攻击报文。比如错误报文或攻击报文可以是为新接入终端服务的在线报文或下线报文。在传统技术中，转发面不区分接入协议报文所服务的终端和接入协议报文的类型，将所有接收到的接入协议报文发送给控制面处理。如果错误报文或攻击报文足够多，可能占满控制面的处理能力。本发明实施例中，当接入协议报文不是认证发起报文而接入协议报文所服务的终端又是新接入终端时，转发面判定该接入协议报文为攻击报文或错误报文并丢弃该接入协议报文。这既可以提升用户体验，又可以减轻控制面的处理负担。

[0075] 步骤306、转发面向控制面发送接入协议报文。

[0076] 可选地，转发面可以按照接收接入协议报文的顺序，向控制面发送接入协议报文，即先接收的接入协议报文先发送，后接收的接入协议报文后发送。例如，转发面可以将该接入协议报文放入报文队列，该报文队列为先入先出(英文:first-in,first-out，缩写:FIFO)队列。转发面调度队列后将该接入协议报文发送至控制面。

[0077] 可选地，当转发面确定接入协议报文是认证发起报文时，转发面将接入协议报文放入新接入终端报文队列。当转发面确定接入协议报文不是认证发起报文且该接入协议报文所服务的终端是已接入终端时，转发面将接入协议报文放入已接入终端报文队列。转发面再按照新接入终端报文队列和已接入终端报文队列各自的优先级，调度新接入终端报文队列和已接入终端报文队列。新接入终端报文队列的优先级不同于已接入终端报文队列的优先级。

[0078] 可选的，新接入终端报文队列的优先级低于已接入终端报文队列的优先级。如果转发面向控制面待发送的接入协议报文少，新接入终端报文队列和已接入终端报文队列中的接入协议报文都可以顺利地发送至控制面。如果转发面向控制面待发送的接入协议报文多，转发面按照队列的优先级调度多个队列中的报文，已接入终端报文队列中的接入协议报文被优先发送至控制面。如果新接入终端报文队列被占满，新接入终端报文队列中的接入协议报文或将要放入新接入终端报文队列的接入协议报文可以被丢弃。

[0079] 在实现时，可以按照实际需要设置新接入终端报文队列和已接入终端报文队列的优先级，再按照队列的优先级调度各个队列，可以提升用户业务体验。比如，可以优先调度已接入终端报文队列，这样，可以保证已接入终端的业务能够及时处理。

[0080] 可选的，已接入终端报文队列包括认证中报文队列和认证完成报文队列。认证中报文队列的优先级不同于认证完成报文队列的优先级。

[0081] 转发面将接收的接入协议报文放入已接入终端报文队列具体可以包括:转发面确定接入协议报文所服务的终端的认证状态。当接入协议报文所服务的终端的认证状态为未完成认证时，转发面将接入协议报文放入认证中报文队列;当接入协议报文所服务的终端的认证状态为完成认证时，转发面将接入协议报文放入认证完成报文队列。

[0082] 一般地，终端未完成认证时，终端或服务器向认证设备发送的正常报文是除认证发起报文之外的认证报文或下线报文。终端完成认证后，终端或服务器向认证设备发送的正常报文是在线报文或下线报文。如果终端或服务器出错，或者认证设备受到攻击，认证设

备接收到的接入协议报文也可能是错误报文或攻击报文。比如错误报文或攻击报文可以是为未完成认证的终端服务的在线报文。错误报文或攻击报文也可以是为已完成认证的终端服务的除认证发起报文之外的认证报文。可选地，转发面可以丢弃这类报文。这进一步提升用户体验，减轻控制面的处理负担。

[0083] 例如，当接入协议报文所服务的终端的认证状态为未完成认证时，转发面判断接入协议协议报文是否为除认证发起报文之外的认证报文或下线报文。当接入协议报文为在线报文时，丢弃接入协议报文；当接入协议报文为除认证发起报文之外的认证报文或下线报文时，转发面将接入协议报文放入认证中报文队列。当接入协议报文所服务的终端的认证状态为完成认证时，转发面判断接入协议协议报文是否为在线报文或下线报文。当接入协议报文为除认证发起报文之外的认证报文时，丢弃接入协议报文；当接入协议报文为在线报文或下线报文时，转发面将接入协议报文放入认证完成报文队列。

[0084] 可选的，新接入终端报文队列、认证中报文队列和认证完成报文队列的优先级依次升高。具体地，当新接入终端报文队列、认证中报文队列和认证完成报文队列均有报文时，转发面优先将认证完成报文队列中的报文发送给控制面，直到认证完成报文队列中的报文发送完毕，转发面再将认证中报文队列中的报文发送给控制面。只有当认证完成报文队列和认证中报文队列中的报文发送完毕后，转发面才将新接入终端报文队列中的报文发送给控制面。如果转发面向控制面待发送的接入协议报文少，新接入终端报文队列、认证中报文队列和认证完成报文队列中的接入协议报文都可以顺利地发送至控制面。如果转发面向控制面待发送的接入协议报文多，认证完成报文队列中的接入协议报文被优先发送至控制面。如果认证中报文队列被占满，认证中报文队列中的接入协议报文或将要放入认证中报文队列的接入协议报文可以被丢弃。类似的，如果新接入终端报文队列被占满，新接入终端报文队列中的接入协议报文或将要放入新接入终端报文队列的接入协议报文可以被丢弃。

[0085] 通过设置新接入终端报文队列、认证中报文队列和认证完成报文队列，并根据实际需要设置新接入终端报文队列、认证中报文队列和认证完成报文队列的优先级，在按照队列的优先级调度各个队列时，可以进一步提升用户业务体验。

[0086] 本发明实施例中，转发面通过接收来自控制面的项目，可以获得已接入终端的标识；转发面接收接入协议报文；当转发面确定接入协议报文不是认证发起报文时，转发面根据已接入终端的标识，确定接收的接入协议报文所服务的终端是否为已接入终端；当接入协议报文所服务的终端不是已接入终端时，丢弃接入协议报文；由于服务新接入终端的接入协议报文只能是认证发起报文，因此，当接入协议报文不是认证发起报文，而该接入协议报文所服务的终端又不是已接入终端时，即该接入协议报文所服务的终端是新接入终端，那么，确定该接入协议报文为错误报文或攻击报文，丢弃该接入协议报文，相比于随机丢弃报文，既减轻了控制面的处理负担，又避免给用户带来不好的影响，能够提升用户业务体验。

[0087] 需要说明的是：上述实施例提供的报文处理装置在处理报文时，仅以上述各功能单元的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元完成，即将设备的内部结构划分成不同的功能单元，以完成以上描述的全部或者部分功能。另外，上述实施例提供的报文处理装置与报文处理方法实施例属于同一构思，其具体实

现过程详见方法实施例，这里不再赘述。

[0088] 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，所述的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。

[0089] 以上所述仅为本发明的较佳实施例，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

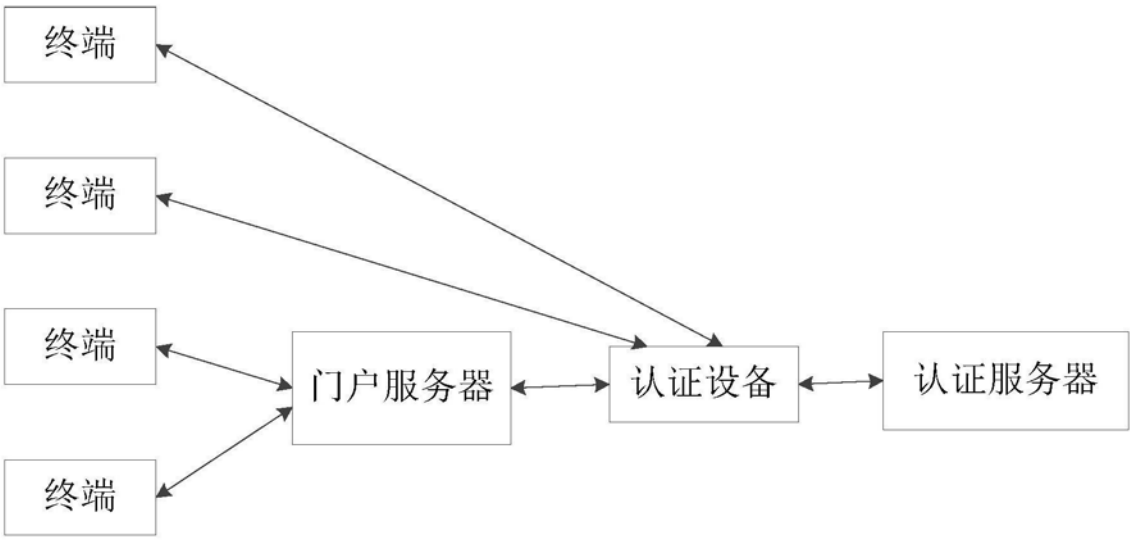


图1

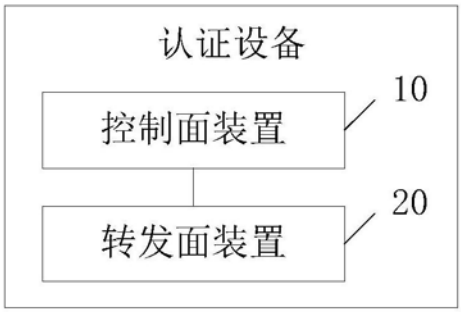


图2

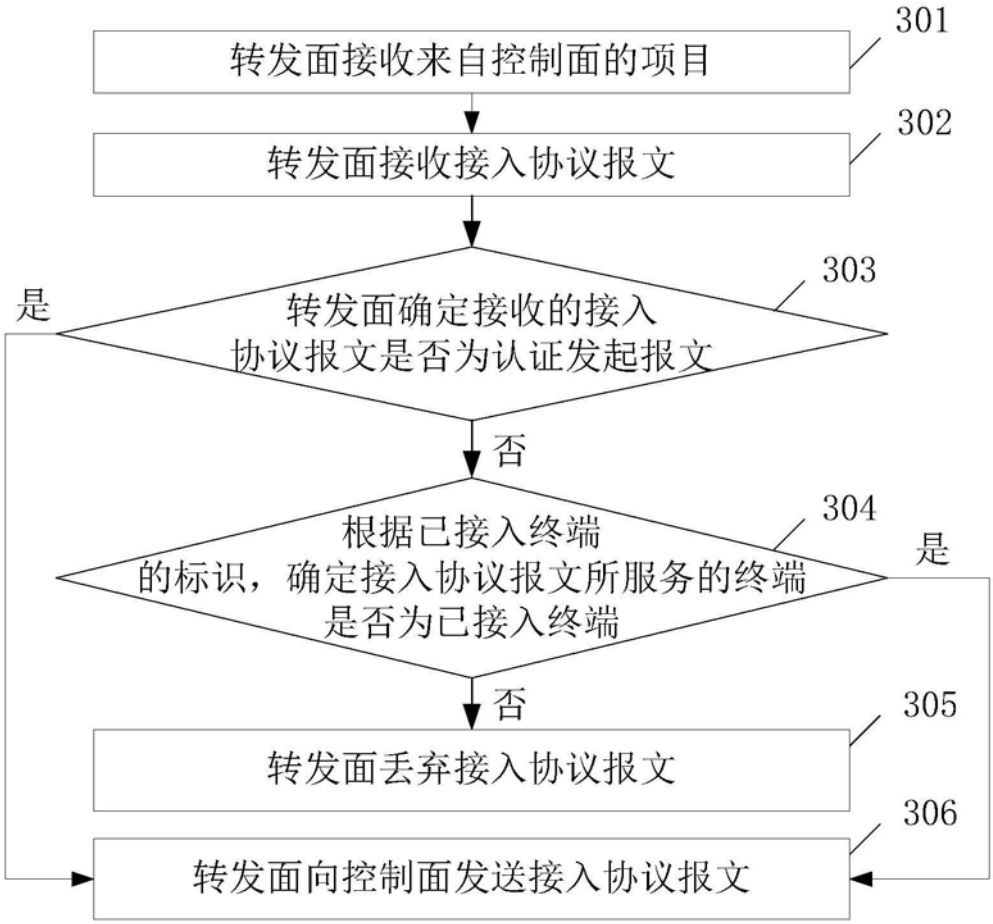


图3

EAPOL报文的格式

端口访问实体以太网类型	
协议版本	类型
长度	
数据帧体	

图4