



(12) 发明专利申请

(10) 申请公布号 CN 106506439 A

(43) 申请公布日 2017. 03. 15

(21) 申请号 201510860530. 8

(22) 申请日 2015. 11. 30

(71) 申请人 杭州华三通信技术有限公司  
地址 310052 浙江省杭州市滨江区长河路  
466 号

(72) 发明人 徐燕成 王伟

(51) Int. Cl.  
H04L 29/06(2006. 01)  
H04L 12/28(2006. 01)

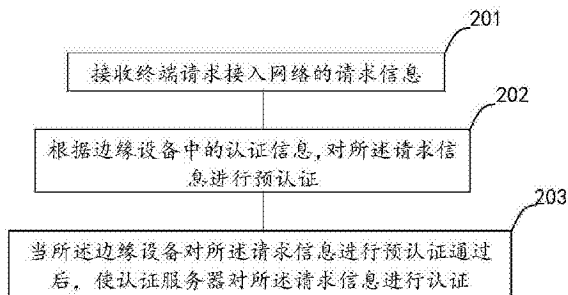
权利要求书2页 说明书11页 附图2页

(54) 发明名称

一种认证终端接入网络的方法和装置

(57) 摘要

本发明提供了一种认证终端接入网络的方法及装置,所述方法应用于边缘设备,所述方法包括,接收终端请求接入网络的请求信息,根据边缘设备中的认证信息,对所述请求信息进行预认证,当对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证,实现了在认证服务器对终端发送的请求信息进行认证前,先对请求信息进行一次预认证,从而避免了认证服务器因对包含了错误的用户名信息和 / 或密码信息的请求信息进行认证而浪费一次认证资源。



1. 一种认证终端接入网络的方法,应用于边缘设备,其特征在于,所述方法包括:  
接收终端请求接入网络的请求信息;  
根据边缘设备中的认证信息,对所述请求信息进行预认证;  
对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。
2. 如权利要求1所述的方法,其特征在于,所述请求信息携带的信息包括终端发送的请求接入网络的第一用户名信息,和/或第一密码信息,和/或第一线路信息;  
对所述请求信息进行预认证,包括:  
将所述请求信息携带的信息,与所述认证信息中相应的信息进行匹配;  
若匹配一致,则对所述请求信息预认证通过。
3. 如权利要求1所述的方法,其特征在于,所述边缘设备中的认证信息为:  
在所述边缘设备中预置的认证信息;或者,  
所述边缘设备根据从认证服务器接收的携带认证信息的报文获取的认证信息。
4. 如权利要求3所述的方法,其特征在于,所述边缘设备根据从认证服务器接收的携带认证信息的报文获取的认证信息,包括:  
所述边缘设备向认证服务器发送用于认证信息获取的报文,并接收所述认证服务器发出的携带有认证信息的反馈报文,并从所述反馈报文中获取的认证信息。
5. 一种认证终端接入网络的方法,应用于认证服务器,其特征在于,所述方法包括:  
向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息;  
以及接收经所述边缘设备预认证通过后的请求信息,并对所述请求信息进行认证,并将认证结果发送至所述边缘设备。
6. 如权利要求5所述的方法,其特征在于,所述向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息,包括:  
所述认证服务器接收所述边缘设备发送的用于认证信息获取的报文;  
所述认证服务器收集自身记录的与认证信息获取报文中携带的信息相应的认证信息,并将所述认证信息携带在反馈报文中发送至所述边缘设备,以使所述边缘设备对终端发送的请求信息进行预认证。
7. 一种认证终端接入网络的装置,其特征在于,所述装置应用于边缘设备,所述装置包括:  
接收模块,用于接收终端请求接入网络的请求信息;  
处理模块,用于根据边缘设备中的认证信息,对所述请求信息进行预认证,并当对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。
8. 如权利要求7所述的装置,其特征在于,所述装置还包括:发送模块,所述发送模块用于向所述认证服务器发送认证信息获取报文。
9. 如权利要求7或8所述的装置,其特征在于,所述装置还包括:获取模块,所述获取模块用于获取认证信息,具体包括:  
所述获取模块用于获取预置的认证信息,或者,  
所述获取模块用于接收所述认证服务器发送的反馈报文,并获取所述反馈报文中的所述认证信息。
10. 如权利要求7所述的装置,其特征在于,所述处理模块包括:

匹配子模块,用于将所述请求信息,与所述认证信息中相应的信息进行匹配,若匹配一致,则对所述请求信息预认证通过,具体的,所述请求信息携带终端发送的请求接入网络的第一用户名信息,和/或第一密码信息,和/或第一线路信息;

对所述请求信息进行预认证,包括:

将所述请求信息中携带的信息,与所述认证信息中相应的信息进行匹配;

若匹配一致,则对所述请求信息预认证通过。

11.一种认证终端接入网络的装置,其特征在于,所述装置应用于认证服务器,所述装置包括:

发送模块,用于向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息,以及用于向边缘设备发送认证结果;

接收模块,用于接收所述终端发送的请求信息;

处理模块,用于对所述请求信息进行认证。

12.如权利要求11所述的装置,其特征在于,所述接收模块,还用于接收边缘设备发送的认证信息获取的报文;

所述处理模块,还用于收集自身记录的与所述认证信息获取报文中携带的信息相应的认证信息;

所述发送模块,还用于将所述认证信息携带在反馈报文中发送至所述边缘设备,以使所述边缘设备对终端发送的请求信息进行预认证。

## 一种认证终端接入网络的方法和装置

### 技术领域

[0001] 本发明涉及通信技术领域,特别涉及一种认证终端接入网络方法和装置。

### 背景技术

[0002] 目前用户在使用终端接入网络时,均是在终端所呈现的认证界面中输入用户名和密码并经认证后方可接入网络,而现有的认证方式均是在认证服务器中完成,当大量终端同时发起认证时,认证服务器的负荷加剧,使得用户等待认证的时间加长,并且,当终端所发起的认证信息中包含了错误的认证信息时,认证服务器依然要对错误的认证信息进行认证,从而浪费了认证资源。

### 发明内容

[0003] 有鉴于此,本发明提出一种认证终端接入网络的方法,应用于边缘设备,所述方法包括:

[0004] 接收终端请求接入网络的请求信息;

[0005] 根据边缘设备中的认证信息,对所述请求信息进行预认证;

[0006] 对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。

[0007] 本发明提供一种认证终端接入网络的方法,应用于认证服务器,所述方法包括:

[0008] 向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息;

[0009] 以及接收经所述边缘设备预认证通过后的请求信息,并对所述请求信息进行认证,并将认证结果发送至所述边缘设备。

[0010] 本发明还提供一种认证终端接入网络的装置,所述装置应用于边缘设备,所述装置包括:

[0011] 接收模块,用于接收终端请求接入网络的请求信息;

[0012] 处理模块,用于根据边缘设备中的认证信息,对所述请求信息进行预认证,并对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。

[0013] 本发明还提供一种认证终端接入网络的装置,所述装置应用于认证服务器,所述装置包括:

[0014] 发送模块,用于向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息,以及用于向边缘设备发送认证结果;

[0015] 接收模块,用于接收所述终端发送的请求信息;

[0016] 处理模块,用于对所述请求信息进行认证。

[0017] 由于采用上述技术方案,在本发明实施例中,当边缘设备接收到终端发送的接入网络的请求信息时,可先根据认证信息,对该请求信息进行一次预认证,当预认证通过后,认证服务器再对终端发送的请求信息进行认证,相当于在认证服务器进行认证前做了一次筛选,从而避免了认证服务器因对包含了错误的请求信息进行认证而浪费一次认证资源,同时由于当用户输入了包含了错误的请求信息时,边缘设备可较快的反馈给用户认证失败

的消息,无需等待认证服务器进行认证,因此用户可以很快的进入再次输入用户名和密码的认证界面。

### 附图说明

- [0018] 图1为本发明实施例中一种实现认证终端接入网络的方法的组网示意图;
- [0019] 图2为本发明实施例所提供的一种认证终端接入网络的方法流程示意图;
- [0020] 图3为本发明实施例所提供的一种认证终端接入网络的方法流程示意图;
- [0021] 图4为本发明实施例所提供的一种认证终端接入网络的方法流程示意图;
- [0022] 图5为本发明实施例所提供的一种认证终端接入网络的方法流程示意图。

### 具体实施方式

[0023] 为使本发明的目的、技术方案及优点更加清楚明白,以下参照附图并举实施例,对本发明所述方案作进一步地详细说明,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

[0024] 在本发明的实施例中,为了区分方便,将终端发送的请求信息中的用户名信息、密码信息和线路信息称为第一用户名信息、第一密码信息和第一线路信息,将认证信息中的用户名信息、密码信息和线路信息称为第二用户名信息、第二密码信息和第二线路信息。

[0025] 如图1所示,一种实现认证终端接入网络的方法为,用户通过终端发送请求接入网络的请求信息,所述请求信息分别经过数字用户线路接入复用器DSLAM(Digital Subscriber Line Access Multiplexer),以及宽带远程接入服务器BRAS(Broadband Remote Access Server)发送至认证服务器中,所述认证服务器对所述请求信息进行认证,当认证通过时,认证服务器向BRAS发送允许所述终端接入网络的通知,BRAS接收到所述通知后允许所述终端接入网络,当认证不通过时,认证服务器向BRAS发送认证失败消息,BRAS接收到所述认证失败消息后,向所述终端发送认证失败通知,所述终端接收到所述认证失败通知后,用户方可再次通过认证界面输入用户名信息和密码信息。

[0026] 如图2所示,本发明实施例提供了一种认证终端接入网络的方法,所述方法应用于边缘设备中,该方法包括:

[0027] 步骤201,接收终端请求接入网络的请求信息。

[0028] 步骤202,根据边缘设备中的认证信息,对所述请求信息进行预认证。

[0029] 步骤203,当所述边缘设备对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。

[0030] 在本发明的实施例中,用户通过终端发起请求接入网络的请求信息,发起该请求信息的方式有多种,如802.1X、PORTAL、PPPOE网络认证方式,例如,当用户通过PPPOE的认证方式通过终端发送出请求信息时,该请求信息中包括了用户在认证界面中所输入的第一用户名信息和/或第一密码信息,具体的,第一用户名信息和第一密码信息为计算机能够识别的多种字符的排列组合。

[0031] 在本发明的实施例中,边缘设备自身置有第二线路信息,所述第二线路信息包括边缘设备从下层设备获取的第二线路信息,或者为边缘设备预配的第二线路信息,进一步

的,所述第二线路信息包括链路信息和端口信息,例如,包括链路类型、链路传输模式、链路号、端口号等信息,进一步的,作为一种优选的实施方式,边缘设备可以根据上述第二线路信息向认证服务器获取与第二线路信息相对应的认证信息。

[0032] 在步骤202中所述的边缘设备中的认证信息,为:在所述边缘设备中预配置的认证信息,或者边缘设备根据从认证服务器接收的携带认证信息的报文中获取的认证信息,其中,边缘设备根据从认证服务器接收的携带认证信息的报文包括,认证服务器主动发送的携带认证信息的报文,或者认证服务器根据边缘设备的请求发送的携带认证信息的报文,在本实施例中,以认证服务器根据边缘设备的请求发送的携带认证信息的报文为例进行说明,具体包括,所述边缘设备向认证服务器发送认证信息获取的报文,并接收认证服务器发送的携带了与认证信息获取报文中信息相应的认证信息的反馈报文,并获取记录该反馈报文中的认证信息。其中,所述的与认证信息获取报文中信息相应的认证信息,可以解释为与认证信息获取报文中所携带的第二线路信息相应的认证信息。其中,所述认证信息包括:第二线路信息、或第二用户名信息、或第二密码信息,进一步的,所述第二用户名信息和第二密码信息可具体包括第二用户名长度、第二用户名内容、第二用户名类型、第二密码长度、第二密码内容、第二密码类型中的任意项。在本发明的实施例中,当边缘设备获取了认证信息后,边缘设备根据该认证信息对终端发送的请求信息进行预认证,包括:边缘设备将请求信息中所携带的信息,与所述认证信息中相应的第二用户名信息、第二密码信息、第二线路信息进行匹配,若匹配一致,则对请求信息预认证通过,边缘设备将请求信息发送至认证服务器中进行认证(在其他实现方式中,当预认证通过后,可由终端直接将请求信息发送至认证服务器中进行认证),进而当认证服务器接收到边缘设备发送的请求信息后,对该请求信息进行认证,并将认证结果发送至边缘设备,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息,具体如下:

[0033] 当认证信息包括:第二线路信息时,边缘设备将请求信息中包括的第一线路信息,与认证信息中包括的第二线路信息进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二线路信息包括链路信息和端口信息,当边缘设备接收到请求信息中的第一线路信息后,将第一线路信息中的链路信息和/或端口信息与认证信息中的第二线路信息进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0034] 或者,当认证信息包括:第二用户名信息时,具体的包括第二用户名长度时,边缘设备将请求信息中包括的第一用户名信息的长度,与认证信息中包括的第二用户名长度进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二用户名长度可以理解为边缘设备中预置的用户名内容的字符个数,或者从认证服务器中获取的用户名中每个用户名内容的字符个数,并进行统计记录,当边缘设备接收到请求信息中的第一用户名信息后,分析出该用户名信息的字符个数,边缘设备将分析出的第一用户名信息的字符个数与认证信息中的第二用户名长度(即认证信息中第二用户名内容的字符个数)进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。其中,边缘设备可以选择直接从认证服务器中获取不同用户

名的字符个数,或者边缘设备先从认证服务器中获取认证信息,之后再对所获取的认证信息中的用户名进行分析,分析出用户名所对应的字符个数。

[0035] 或者,当认证信息包括:第二用户名信息时,具体的包括第二用户名类型时,边缘设备将请求信息中包括的第一用户名信息,与认证信息中包括的第二用户名类型进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二用户名类型可以理解为边缘设备中预置的用户名的类型,或者边缘设备从认证服务器中获取的用户名类型,所述的用户名类型可以包括:字母、大写字母、小写字母、符号、数字五者之一或者五者的任意组合,当边缘设备接收到请求信息中的第一用户名信息后,分析出该用户名信息的类型,边缘设备将分析出的第一用户名信息的类型与认证信息中的第二用户名类型进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0036] 或者,当认证信息包括:第二用户名信息时,具体的包括第二用户名内容时,边缘设备将请求信息中包括的第一用户名信息,与认证信息中包括的第二用户名内容进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二用户名内容可以理解为边缘设备中预置的用户名的每个用户名的字符排列组合,或者边缘设备从认证服务器中获取的用户名中每个用户名的字符排列组合,并进行统计记录,当边缘设备接收到的请求信息中的第一用户名信息后,分析出该第一用户名信息中各字符的排列组合,边缘设备将分析出的第一用户名信息中各字符的排列组合与认证信息中的第二用户名内容进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0037] 或者,当认证信息包括:第二密码信息时,具体的包括第二密码长度时,边缘设备将请求信息中包括的第一密码信息的长度,与认证信息中包括的第二密码长度进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二密码长度可以理解为边缘设备中预置的密码内容的字符个数,或者边缘设备从认证服务器中获取的密码中每个密码内容的字符个数,并进行统计记录,当边缘设备接收到请求信息中的第一密码信息后,分析出该第一密码信息的字符个数,边缘设备将分析出的第一密码信息的字符个数与认证信息中的第二密码长度(即认证信息中第二密码内容的字符个数)进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。其中,边缘设备可以选者直接从认证服务器中获取不同密码的字符个数,或者边缘设备先从认证服务器中获取密码内容,之后再对所获取的密码内容进行分析,分析出密码内容所对应的字符个数。

[0038] 或者,当认证信息包括:第二密码信息时,具体的包括第二密码类型时,边缘设备将请求信息中包括的第一密码信息,与认证信息中包括的第二密码类型进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二密码类型可以理解为边缘设备中预置的密码的类型,或者边缘设备从认证服务器中获取的密码的类型,所述的密码类型可以包括:字母、大写字母、小写字母、符号、数字五者之一或者五者的任意组合,当边

缘设备接收到请求信息中的第一密码信息后,分析出该密码信息的类型,边缘设备将分析出的第一密码信息的类型与认证信息中的第二密码类型进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0039] 或者,当认证信息包括:第二密码信息时,具体的包括第二密码内容时,边缘设备将请求信息中包括的第一密码信息,与认证信息中包括的第二密码内容进行匹配,若匹配一致,则对请求信息预认证通过,具体的,认证信息所包括的第二密码内容可以理解为边缘设备中预置的密码的每个密码的字符排列组合,或者边缘设备从认证服务器中获取的密码中每个密码的字符排列组合,并进行统计记录,当边缘设备接收到的请求信息中的第一密码信息后,分析出该第一密码信息中各字符的排列组合,边缘设备将分析出的第一密码信息中各字符的排列组合与认证信息中的第二密码内容进行匹配,若匹配一致,则对所述请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0040] 或者,当认证信息包括:第二用户名信息和第二密码信息时,具体的包括第二用户名长度和第二密码长度时,边缘设备将请求信息中包括的第一用户名信息的长度和第一密码信息的长度,与认证信息中包括的第二用户名长度和第二密码长度进行匹配,若均匹配一致,则对请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若第一用户名信息的长度和第一密码信息的长度与第二用户名长度和/或第二密码长度匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0041] 或者,当认证信息包括:第二用户名信息和第二密码信息时,具体的包括第二用户名内容和第二密码内容时,边缘设备将请求信息中包括的第一用户名信息和第一密码信息,与认证信息中包括的第二用户名内容和第二密码内容进行匹配,若均匹配一致,则对请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若第一用户名信息和第一密码信息与第二用户名内容和/或第二密码内容匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0042] 或者,当认证信息包括:第二用户名信息和第二密码信息时,具体包括第二用户名长度和第二密码内容时,边缘设备将请求信息中包括的第一用户名信息的长度和第一密码信息,与认证信息中包括的第二用户名长度和第二密码内容进行匹配,若均匹配一致,则对请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若第一用户名信息的长度和第一密码信息与第二用户名长度和/或第二密码内容匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0043] 或者,当认证信息包括:第二用户名信息和第二密码信息时,具体包括第二用户名内容和第二密码长度时,边缘设备将请求信息中包括的第一用户名信息和第一密码信息的长度,与认证信息中包括的第二用户名内容和第二密码长度进行匹配,若均匹配一致,则对请求信息预认证通过,边缘设备将请求信息发送至认证服务器进行认证,若第一用户名信息和第一密码信息的长度与第二用户名内容和/或第二密码长度匹配不一致,则对请求信息进行预认证不通过,边缘设备丢弃该请求信息,并向终端发送认证失败信息。

[0044] 当终端接收到该认证失败信息后,可允许用户再次输入用户名信息和密码信息。



上述各例仅为本发明实施例所列举的几种实例,由于认证信息包括第二线路信息、第二用户名信息、第二密码信息,其中,第二用户名信息和第二密码信息又可包括:第二用户名长度、第二密码长度、第二用户名内容、第二密码内容、第二用户名类型及第二密码类型等匹配条件,因此可将认证信息中所包括的上述匹配条件进行任意组合成新的匹配条件,并用新的匹配条件对请求信息中的内容进行匹配。

[0045] 由于在网络认证中,用户名内容和密码内容是认证一个终端是否可以接入网络的重要认证条件之一,因此在本发明的实施例中,当边缘设备中记录的认证信息至少包括第二用户名内容和第二密码内容时,将终端发送的请求信息中包括的第一用户名信息和第一密码信息均与认证信息进行匹配一致后,该边缘设备可先允许发送该请求信息的终端接入网络,再将该终端所发送的请求信息发送至认证服务器中进行认证,缩短了用户等待认证的时间。

[0046] 显然,采用上述技术方案,当边缘设备接收到终端发送的接入网络的请求信息时,可先根据认证信息,对该请求信息进行一次预认证,当预认证通过后,再将终端发送的请求信息发送至认证服务器中进行认证,相当于在认证服务器进行认证前做了一次筛选,从而避免了认证服务器因对包含了错误的请求信息进行认证而浪费一次认证资源,同时由于当用户输入了包含了错误的请求信息时,边缘设备可较快的反馈给用户认证失败的消息,无需等待认证服务器进行认证并反馈认证失败的信息,因此用户可以很快的进入再次输入用户名和密码的认证界面。

[0047] 如图3所示,本发明实施例提供了一种认证终端接入网络的方法,该方法应用于认证服务器,该方法包括:

[0048] 步骤301,向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息。

[0049] 具体包括,认证服务器主动向边缘设备发送认证信息,或者,当认证服务器接收到边缘设备发送的认证信息获取报文后,认证服务器收集自身记录的与认证信息获取报文中携带信息相应的认证信息,并将所述认证信息携带在反馈报文中发送至所述边缘设备,以使所述边缘设备对终端发送的请求信息进行预认证。

[0050] 步骤302,接收所述终端发送的请求信息,并对所述请求信息进行认证,并将认证结果发送至所述边缘设备。

[0051] 其中,步骤302中所接收的请求信息为经过边缘设备预认证通过后的请求信息。

[0052] 在本发明的实施例中引入了边缘设备,该边缘设备包括安装在骨干网边缘网络上的交换机、路由器、路由交换机、综合接入IAD(Internet addiction disorder)等设备,为了更好的说明本发明的技术方案,本发明实施例分别提供了当边缘设备为数字用户线路接入复用器DSLAM或宽带远程接入服务器BRAS时的实施例,应当可以理解,因为边缘设备包括了安装在骨干网边缘网络上的交换机、路由器等设备,因此边缘设备自然可包括DSLAM以及BRAS,并且属于安装于骨干网边缘网络上的交换机、路由器、路由交换机、IAD等设备均适用于本发明的技术方案,在本发明的实施例中,所述的认证服务器可以为远程用户拨号认证服务器RADIUS(Remote Authentication Dial In User Service)。

[0053] 如图4所示,本发明实施例提供了一种认证终端接入网络的方法,当边缘设备为数字用户线路接入复用器DSLAM时,该方法包括:

[0054] 步骤401,DSLAM接收终端请求接入网络的请求信息;

[0055] 步骤402,DSLAM根据认证信息,对所述请求信息进行预认证;

[0056] 步骤403,当DSLAM对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。

[0057] 在本发明的实施例中,DSLAM可与至少一个终端连接,其作用包括,用于接收多个终端发送的请求接入网络的请求信息,并根据认证信息(所述认证信息为在DSLAM中预置的认证信息,或者所述认证信息为DSLAM接收认证服务器发出的携带认证信息的反馈报文,并获取记录该反馈报文中的认证信息)对所述请求信息进行预认证,并将通过预认证的请求信息发送至认证服务器(在其他实现方式中,当预认证通过后,可由终端直接将请求信息发送至认证服务器中进行认证),以使认证服务器对请求信息进行认证,或者丢弃未通过预认证的请求信息,并向终端发送认证失败信息。

[0058] 以及在DSLAM与认证服务器间还包括BRAS,BRAS用于从认证服务器中获取认证信息,并将认证信息发送至DSLAM中,以及用于将终端发送的请求信息发送至认证服务器中进行认证。其中,BRAS位于骨干网的边缘层,可以完成用户的IP/ATM网的数据数据接入,实现商业楼宇及小区住户的宽带上网。

[0059] 针对步骤402中DSLAM根据认证信息,对请求信息进行预认证的过程,本发明实施例提供一种优选的实施方法,具体方法包括:

[0060] DSLAM与BRAS通过节点控制协议ANCP(Access Node Control Protocol)建立ANCP连接,进而在DSLAM与BRAS间建立ANCP通道,用于完成DSLAM与BRAS间的报文交互,同时BRAS自身增加DSLAM enable的使能命令,用于当检测到DSLAM上线后向认证服务器获取认证信息,或者用于当检测到DSLAM上线后将从认证服务器获取的认证信息主动发送至DSLAM中。

[0061] 当DSLAM与BRAS建立ANCP连接后,BRAS通过ANCP协议获得DSLAM的线路信息(该技术已为现有技术,因此不再赘述),该线路信息为第二线路信息,BRAS根据从DSLAM获得的第二线路信息向认证服务器发送携带该第二线路信息的认证信息获取报文。

[0062] 当认证服务器接收到认证信息获取报文后,根据报文中所携带的第二线路信息,将认证服务器自身中所记录的与该第二线路信息对应的认证信息携带在反馈报文中,并将该反馈报文发送至BRAS。

[0063] 当BRAS接收到认证服务器发送的反馈报文后,提取反馈报文中的认证信息,并将认证信息通过ANCP通道发送至DSLAM。

[0064] DSLAM根据接收到的认证信息,对终端发送的请求信息进行预认证,当对请求信息进行预认证通过后,将预认证通过的请求信息经ANCP通道发送至BRAS,BRAS在接收到该请求信息后,将该请求信息发送至认证服务器,以使认证服务器对该请求信息进行认证,认证服务器对该信息认证通过后,反馈给BRAS认证通过的通知,BRAS在接收到该通知后,允许发送上述请求信息的终端接入网络。

[0065] 在本发明的实施例中,当DSLAM根据认证信息,对终端所发送的请求信息进行预认证不通过时,DSLAM丢弃该请求信息,并向发送该请求信息的终端发送认证失败信息,进一步的,当终端接收到该认证失败信息后,可允许用户再次输入用户名信息和密码信息。

[0066] 其中,DSLAM根据认证信息,对请求信息进行预认证的过程已在边缘设备预认证的实施例中说明,因此不再赘述。

[0067] 在本发明的实施例中,进一步还包括,当DSLAM从认证服务器中获取的认证信息至

少包括第二用户名内容和第二密码内容时,DSLAM将终端发送的请求信息中包括的第一用户名信息和第一密码信息与认证信息中的第二用户名内容和第二密码内容进行匹配,当匹配一致后,DSLAM通过ANCP通道向BRAS发送该请求信息以及预认证通过的通知,BRAS接收到该通知后,BRAS可先允许发送该请求信息的终端接入网络,并将接收到的请求信息发送至认证服务器中进行认证。

[0068] 在本发明的实施例中,由于存在用户因个人需求会在终端接入网络后,对认证服务器中记录的对应该终端的第二用户名信息、第二密码信息进行修改的情况,为了避免DSLAM对终端发送的请求信息因用户修改的原因做出错误的预认证结果,因此需要对DSLAM中所记录的认证信息进行更新,该更新的方法包括对DSLAM中预置的认证信息进行更新,或者BRAS定期获取DSLAM的线路信息(即第二线路信息),并根据第二线路信息定期向认证服务器发送对第二线路信息中所有终端的认证信息进行更新的请求更新报文,认证服务器接收到该请求更新报文后,认证服务器将自身记录的与该请求更新报文中第二线路信息一致的认证信息发送给BRAS,BRAS接收到认证服务器所发送的认证信息后通过ANCP协议将新的认证信息发送给DSLAM进行更新存储,或者当用户对认证服务器中所存储的认证信息进行修改时,认证服务器判断被修改的认证信息是否属于之前认证服务器发送给BRAS的认证信息,如果是,则向BRAS发送更新后的认证信息,BRAS接收到该更新后的认证信息,并将该更新后的认证信息发送给DSLAM进行记录。

[0069] 显然,采用上述技术方案,当DSLAM接收到终端发送的接入网络的请求信息时,可先根据认证信息,对该请求信息进行一次预认证,当预认证通过后,将该请求信息经BRAS发送至认证服务器中进行认证,相当于在认证服务器进行认证前做了一次筛选,从而避免了认证服务器因对包含了错误的请求信息进行认证而浪费一次认证资源,同时由于当用户输入了包含了错误的请求信息时,DSLAM在进行预认证后便反馈给终端认证失败的消息,因此用户无需等待认证服务器进行认证,并将认证结果反馈给BRAS的过程,用户可以很快的进入再次输入用户名和密码的认证界面。

[0070] 如图5所示,本发明实施例提供了一种认证终端接入网络的方法,当边缘设备为宽带接入服务器BRAS时,该方法包括:

[0071] 步骤501,BRAS接收终端请求接入网络的请求信息;

[0072] 步骤502,BRAS根据认证信息,对所述请求信息进行预认证;

[0073] 步骤503,当BRAS对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。

[0074] 在本发明的实施例中,BRAS自身预置认证信息,或者BRAS从认证服务器中获取认证信息,本实施例提供一种优选方案,具体为BRAS根据从下层网络设备获取的第二线路信息或者BRAS自身配置的第二线路信息向认证服务器发送携带第二线路信息的认证信息获取报文。

[0075] 当认证服务器接收到认证信息获取报文后,根据报文中所携带的第二线路信息,将认证服务器自身中所记录的与第二线路信息对应的认证信息携带在反馈报文中,并将该反馈报文发送至BRAS。

[0076] BRAS接收认证服务器服务器发送的反馈报文,提取反馈报文中的认证信息并进行记录,进一步的,BRAS根据所记录的认证信息对BRAS下层网络的交换机所挂载的终端发送

的请求接入网络的请求信息进行预认证,当BRAS对请求信息进行预认证通过后,将预认证通过后的请求信息发送至认证服务器中,以使认证服务器对该请求信息进行认证,认证服务器对该信息认证通过后,反馈给BRAS认证通过的通知,BRAS在接收到该通知后,允许发送上述请求信息的终端接入网络。

[0077] 在本发明的实施例中,当BRAS根据认证信息,对终端所发送的请求信息进行预认证不通过时,BRAS丢弃该请求信息,并向发送该请求信息的终端发送认证失败信息,进一步的,当终端接收到该认证失败信息后,可允许用户再次输入用户名信息和密码信息。

[0078] 其中,BRAS根据从认证服务器中获取的认证信息,对请求信息进行预认证的过程已在边缘设备预认证的实施例中说明,因此不再赘述。

[0079] 在本发明的实施例中,进一步还包括,当BRAS从认证服务器中获取的认证信息至少包括第二用户名内容和第二密码内容时,BRAS将终端发送的请求信息中包括的第一用户名信息和第一密码信息与认证信息中的第二用户名内容和第二密码内容进行匹配,当匹配一致后,BRAS可先允许发送该请求信息的终端接入网络,并将接收到的请求信息发送至认证服务器中进行认证。

[0080] 在本发明的实施例中,由于存在用户因个人需求会在终端接入网络后,对认证服务器中记录的对应终端的第二用户名信息、第二密码信息进行修改的情况,为了避免BRAS对终端发送的请求信息因用户修改的原因做出错误的预认证结果,因此需要对BRAS中所记录的认证信息进行更新,该更新的方法包括BRAS定期向认证服务器发送对第二线路信息所对应的终端的认证信息进行更新的请求更新报文,认证服务器接收到该请求更新报文后,认证服务器将自身记录的与该请求更新报文中第二线路信息一致的认证信息发送给BRAS,BRAS接收到认证服务器所发送的认证信息后进行更新记录,或者当用户对认证服务器中所存储的认证信息进行修改时,认证服务器判断被修改的认证信息是否属于之前认证服务器发送给BRAS的认证信息,如果是,则向BRAS发送更新后的认证信息,BRAS接收到该更新后的认证信息后进行更新记录。

[0081] 显然,采用上述技术方案,当BRAS接收到终端发送的接入网络的请求信息时,可先根据认证信息,对该请求信息进行一次预认证,当预认证通过后,将该请求信息发送至认证服务器中进行认证,相当于在认证服务器进行认证前做了一次筛选,从而避免了认证服务器因对包含了错误的请求信息进行认证而浪费一次认证资源,同时由于当用户输入了包含了错误的请求信息时,BRAS在进行预认证后便反馈给终端认证失败的消息,因此用户无需等待认证服务器进行认证,并将认证结果反馈给BRAS的过程,用户可以很快的进入再次输入用户名和密码的认证界面。

[0082] 基于与上述方法同样的发明构思,本发明实施例中还提供了一种认证终端接入网络的装置,该装置应用在边缘设备上,例如在本发明实施例中,该装置具体应用在DSLAM或BRAS上,其中,该装置可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为一个逻辑意义上的装置,是通过其所在的DSLAM或BRAS中的处理器,将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言,本发明提出的认证终端接入网络的装置所在的DSLAM或BRAS为硬件结构,除了包括了处理器、网络接口、内存以及非易失性存储器外,DSLAM或BRAS还可以包括其他硬件,如负责处理报文的转发芯片等;从硬件结构上来讲,该DSLAM或BRAS还可能是分布式设备,可能包括多个

接口卡,以便在硬件层面进行报文处理的扩展。

[0083] 本发明的实施例提供了一种认证终端接入网络的装置,该装置应用于边缘设备,该装置包括:

[0084] 接收模块,用于接收终端请求接入网络的请求信息。

[0085] 处理模块,用于根据边缘设备中的认证信息,对所述请求信息进行预认证,并对所述请求信息进行预认证通过后,使认证服务器对所述请求信息进行认证。

[0086] 在本发明的实施例中,所述装置还包括发送模块,用于向认证服务器发送携带第二线路信息的认证信息获取报文,以及用于当对所述请求信息进行预认证通过时,将所述请求信息发送至认证服务器进行认证,以及还用于当第一处理模块预认证不通过时,向所述终端发送认证失败信息。

[0087] 在本发明的实施例中,所述装置还包括获取模块,用于获取在边缘设备中预置的认证信息,以及从认证服务器发送的携带有认证信息的反馈报文中获取认证信息,具体包括:获取模块接收所述认证服务器发出的与所述认证信息获取报文中第二线路信息对应的认证信息的反馈报文,并获取所述反馈报文中的所述认证信息。

[0088] 在本发明的实施例中,所述处理模块还用于当对所述请求信息进行预认证不通过时,丢弃所述请求信息,进一步的,处理模块具体包括:匹配子模块,该匹配子模块用于将所述请求信息(所述请求信息包括:第一用户名信息,和/或第一密码信息,和/或第一线路信息),与所述认证信息中相应的信息进行匹配,若匹配一致,则对所述请求信息预认证通过,若不匹配,则所述边缘设备丢弃所述终端发送的请求信息。

[0089] 本发明实施例还提供了一种认证终端接入网络的装置,该装置应用于认证服务器中,该装置包括:

[0090] 发送模块,用于向边缘设备发送用于对终端发送的请求信息进行预认证的认证信息,以及用于向边缘设备发送认证结果。

[0091] 接收模块,用于接收所述边缘设备发送的请求信息。

[0092] 处理模块,用于对所述请求信息进行认证。

[0093] 在本发明的实施例中,处理模块,还用于收集自身记录的与所述认证信息获取报文中携带的信息相应的认证信息,例如作为一种优选的实施方式,处理模块,还用于收集自身记录的与所述认证信息获取报文中携带的第二线路信息相应的认证信息。

[0094] 在本发明的实施例中,发送模块,还用于将所述认证信息携带在反馈报文中发送至所述边缘设备,以使所述边缘设备根据从认证服务器中获取的认证信息,对终端发送的请求信息进行预认证。

[0095] 在上述实施例中,所述的边缘设备适用于DSLAM、BRAS等属于安装于骨干网边缘网络上的交换机、路由器、路由交换机、IAD以及各种MAN/WAN设备,所述的认证服务器可以为远程用户拨号认证服务器RADIUS(Remote Authentication Dial In User Service)。

[0096] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的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)执行本发

明各个实施例所述的方法。本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

[0097] 本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块，也可进一步拆分成多个子模块。上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0098] 以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

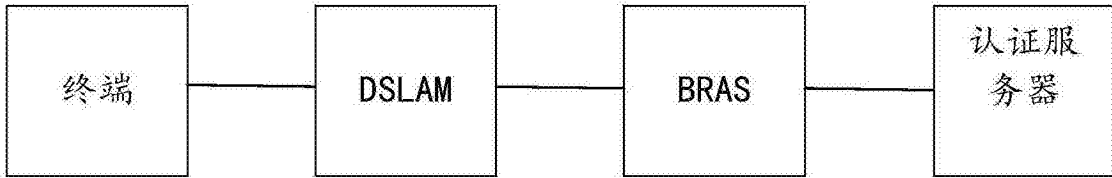


图1

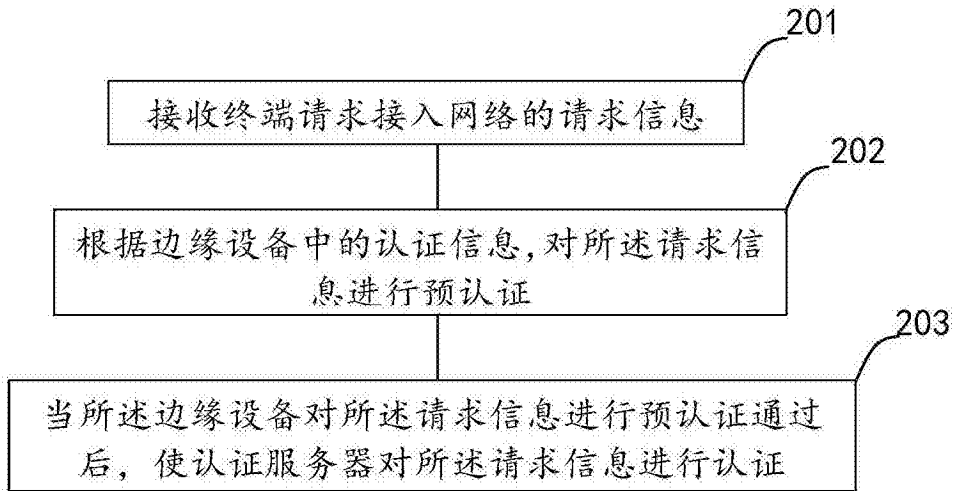


图2

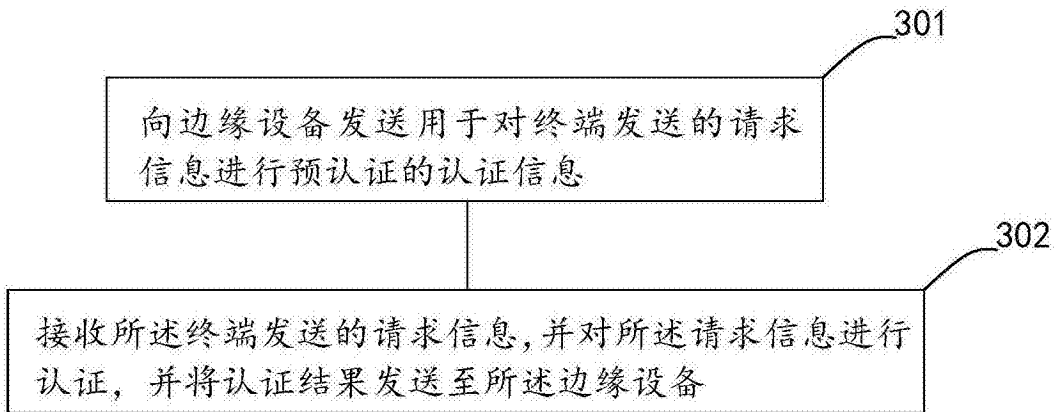


图3

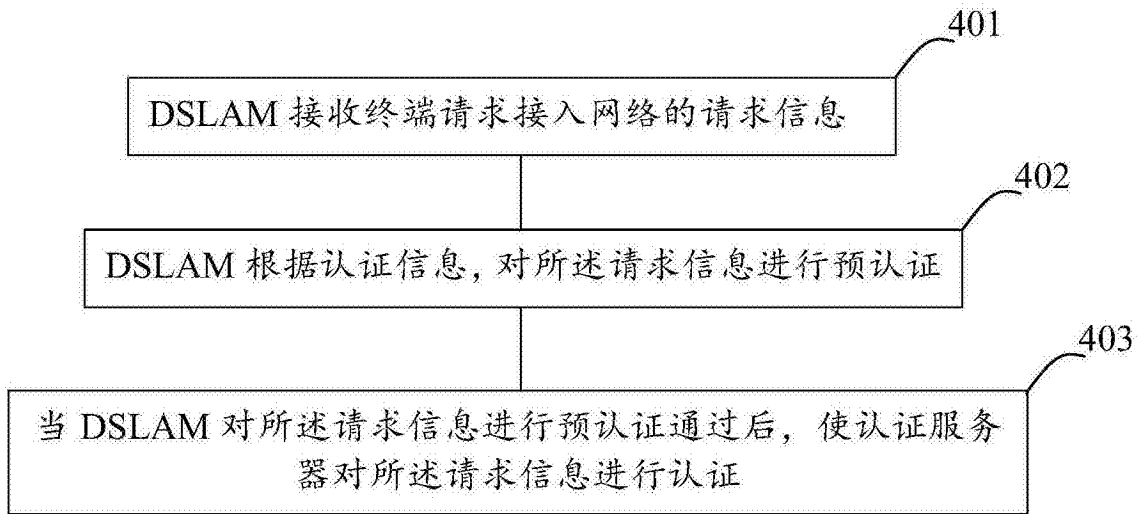


图4

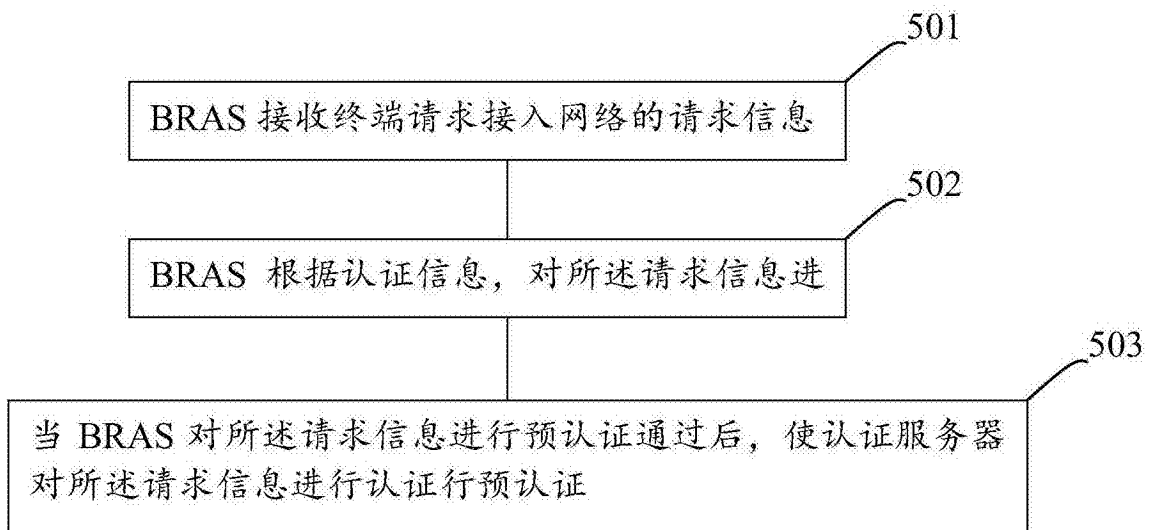


图5