(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 107547562 B
(45)授权公告日 2020.04.28

(21)申请号 201710875442.4

(22)申请日 2017.09.25

(65)同一申请的已公布的文献号
申请公布号 CN 107547562 A

(43)申请公布日 2018.01.05

(73)专利权人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 王阳 廖以顺

(74)专利代理机构 北京市隆安律师事务所 11323
代理人 权鲜枝 何立春

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
US 8514828 B1,2013.08.20,
CN 105959188 A,2016.09.21,
CN 102075904 A,2011.05.25,
US 8769626 B2,2014.07.01,
Steffen Gebert等.Demonstrating a personalized secure-by-default bring your own device solution based on software defined networking.《2016 28th International Teletraffic Congress (ITC 28) 1》.2016,197-200.

审查员 胡鑫

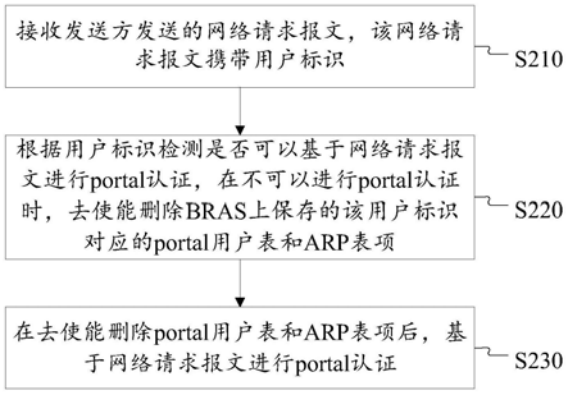
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种portal认证方法和装置

(57)摘要

本申请公开了一种portal认证方法和装置。该方法包括:接收发送方发送的网络请求报文,该网络请求报文携带用户标识;根据所述用户标识检测是否可以基于所述网络请求报文进行portal认证,在不可以进行portal认证时,去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项;删除所述portal用户表和ARP表项后,基于所述网络请求报文进行portal认证。本申请能够保证支持跨VLAN漫游,保证用户及时触发漫游上线,无需等待portal用户表老化后才能上线。



CN 107547562 B

1.一种portal认证方法,其特征在于,应用于宽带远程接入服务器BRAS,该方法包括:

接收发送方发送的网络请求报文,该网络请求报文携带用户标识;

根据所述用户标识检测是否可以基于所述网络请求报文进行portal认证,在可以进行portal认证时,去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项;

在去使能所述portal用户表和ARP表项后,基于所述网络请求报文进行portal认证。

2.根据权利要求1所述的portal认证方法,其特征在于,所述根据所述用户标识检测是否可以基于所述网络请求报文进行portal认证包括:

检测所述用户标识是否存在对应的portal用户表,若不存在所述portal用户表,则判断可以进行portal认证,此时基于所述网络请求报文进行portal认证;

若存在所述portal用户表,则检测所述发送方是否在线,若所述发送方不在线,则判断可以进行portal认证,此时去使能所述portal用户表和相应的ARP表项,并基于所述网络请求报文进行portal认证。

3.根据权利要求2所述的portal认证方法,其特征在于,在检测所述发送方在线时,所述方法还包括:

判断不可以进行portal认证,此时提取所述portal用户表中的IP地址字段、物理地址字段、认证接口字段、虚拟局域网字段、固定时间字段中的一种或多种生成禁止用户漫游表项,所述禁止用户漫游表项通过所述用户标识唯一标识,所述禁止用户漫游表项用于禁止携带其用户标识的网络请求报文进行portal认证。

4.根据权利要求3所述的portal认证方法,其特征在于,在检测所述用户标识是否存在对应的portal用户表之前,所述方法还包括:

检测所述用户标识是否存在对应的禁止用户漫游表项,若存在所述禁止用户漫游表项,则禁止所述发送方进行portal认证;

若不存在所述禁止用户漫游表项,则检测所述用户标识是否存在对应的portal用户表。

5.根据权利要求3所述的portal认证方法,其特征在于,在生成禁止用户漫游表项时,所述方法还包括:

配置所述禁止用户漫游表项的老化时间;

或者,配置所述禁止用户漫游表项与所述portal用户表相关联,在删除portal用户表时联动删除所述禁止用户漫游表项。

6.一种portal认证装置,其特征在于,应用于宽带远程接入服务器BRAS,该装置包括:

接收单元,用于接收发送方发送的网络请求报文,该网络请求报文携带用户标识;

检测单元,用于根据所述用户标识检测是否可以基于所述网络请求报文进行portal认证;

认证处理单元,用于在可以进行portal认证时,去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项,去使能所述portal用户表和ARP表项后,基于所述网络请求报文进行portal认证。

7.根据权利要求6所述的portal认证装置,其特征在于,

所述检测单元,用于检测所述用户标识是否存在对应的portal用户表,以及在所述用户标识存在所述portal用户表时,检测所述发送方是否在线;

所述认证处理单元，用于在所述检测单元检测所述用户标识不存在所述portal用户表时，判断可以进行portal认证，基于所述网络请求报文进行portal认证；以及在所述检测单元检测所述发送方不在线时，判断可以进行portal认证，去使能所述portal用户表和相应的ARP表项，并基于所述网络请求报文进行portal认证。

8.根据权利要求7所述的portal认证装置，其特征在于，所述认证处理单元，还用于在所述检测单元检测所述发送方在线时，判断不可以进行portal认证，提取所述portal用户表中的IP地址字段、物理地址字段、认证接口字段、虚拟局域网字段、固定时间字段中的一种或多种生成禁止用户漫游表项，所述禁止用户漫游表项通过所述用户标识唯一标识，所述禁止用户漫游表项用于禁止携带其用户标识的网络请求报文进行portal认证。

9.根据权利要求8所述的portal认证装置，其特征在于，

所述检测模块，还用于在检测所述用户标识是否存在对应的portal用户表之前，检测所述用户标识是否存在对应的禁止用户漫游表项；

所述认证处理单元，用于在所述检测单元检测所述用户标识存在对应的禁止用户漫游表项时，禁止所述发送方进行portal认证，在所述检测单元检测所述用户标识不存在所述禁止用户漫游表项，驱动所述检测单元检测所述用户标识是否存在对应的portal用户表。

10.根据权利要求8所述的portal认证装置，其特征在于，所述认证处理单元，还用于配置所述禁止用户漫游表项的老化时间，或者，配置所述禁止用户漫游表项与所述portal用户表相关联，使在删除portal用户表时联动删除所述禁止用户漫游表项。

11.一种报文处理装置，包括处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令，所述处理器被所述机器可执行指令促使：执行如权利要求1～5任一所述的portal认证方法。

12.一种机器可读存储介质，存储有机器可执行指令，在被处理器调用和执行时，所述机器可执行指令促使所述处理器：执行如权利要求1～5任一所述的portal认证方法。

一种portal认证方法和装置

技术领域

[0001] 本申请涉及网络通信技术领域,特别涉及一种portal认证方法和装置。

背景技术

[0002] portal认证(入口认证)通常也称为Web认证,即通过Web页面接受用户输入的用户名和密码,对用户进行身份认证,以达到对用户访问进行控制的目的。portal网络中主要包括:portal客户端、接入设备和portal服务器,其中,接入设备可以是BRAS(Broadband Remote Access Server,宽带接入服务器)。

[0003] 在portal网络中,连接外网,如连接互联网的接入设备与portal客户端、portal服务器相连,接入设备的主要作用是对portal客户端发起的访问外网的流量进行控制;portal服务器的作用是接收portal客户端的认证请求,并向portal客户端提供Web认证页面以便用户在该Web认证页面中输入用户名、密码等认证信息,对portal客户端的认证信息进行认证。

发明内容

[0004] 本申请提供一种portal认证方法和装置,以解决目前portal认证不支持跨VALN的漫游的问题。

[0005] 为达到上述目的,本申请的技术方案是这样实现的:

[0006] 一方面,本申请提供了一种portal认证方法,应用于BRAS,该方法包括:

[0007] 接收发送方发送的网络请求报文,该网络请求报文携带用户标识;

[0008] 根据所述用户标识检测是否可以基于所述网络请求报文进行portal认证,在不可以进行portal认证时,去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项;

[0009] 在去使能所述portal用户表和ARP表项后,基于所述网络请求报文进行portal认证。

[0010] 另一方面,本申请还提供了一种portal认证装置,应用于BRAS,该装置包括:

[0011] 接收单元,用于接收发送方发送的网络请求报文,该网络请求报文携带用户标识;

[0012] 检测单元,用于根据用户标识检测是否可以基于网络请求报文进行portal认证;

[0013] 认证处理单元,用于在不可以进行portal认证时,去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项;在去使能所述portal用户表和ARP表项后,基于所述网络请求报文进行portal认证。

[0014] 另一方面,本申请提供了一种portal认证装置,包括处理器和机器可读存储介质,该机器可读存储介质存储有能够被处理器执行的机器可执行指令,该处理器被机器可执行指令促使:执行上述的portal认证方法。

[0015] 另一方面,本申请提供了一种机器可读存储介质,存储有机器可执行指令,在被处理器调用和执行时,该机器可执行指令促使处理器:执行上述的portal认证方法。

[0016] 本申请的有益效果是:基于在BRAS上保存有该用户标识对应的portal用户表和

ARP表项时，该ARP表项无法实现BRAS与发送方之间的数据转发的前提，通过网络请求报文的用户标识检测是否可以进行portal认证，在不可以进行portal认证时，删除BRAS上保存的该用户标识对应的portal用户表和ARP表项，使得可以基于网络请求报文进行portal认证，保证用户及时触发漫游上线，而无需等待portal用户表老化。

附图说明

[0017] 图1为本申请实施例示出的漫游场景下的portal组网示意图；

[0018] 图2为本申请实施例提供的一种portal认证方法流程图；

[0019] 图3为本申请实施例提供的portal认证流程示意图；

[0020] 图4为本申请实施例提供的一种portal认证装置结构框图；

[0021] 图5为本申请实施例示出的一种portal认证装置的硬件结构示意图。

具体实施方式

[0022] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0023] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0024] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0025] 目前的portal认证方式，当用户从注册区域接入到BRAS后，漫游到漫游区域并从漫游区域的VLAN(Virtual Local Area Network，虚拟局域网)接入BRAS，这时候如果用户在注册区域接入BRAS，且BRAS上生成的portal用户表没有老化，若在漫游区域再次发起portal认证，会导致认证界面无法推出，无法进行portal认证。

[0026] 图1示例性示出了漫游场景下的portal组网示意图，用户user从区域A的vlan a接入BRAS后，漫游到区域B后从区域B的vlan b接入BRAS，这时候如果用户user在区域A接入BRAS，BRAS上生成的portal用户表没有老化，用户user在到达区域B后再次发起portal认证，会导致认证界面都无法推出，产生该问题的原因在于用户user在区域A接入的时候生成的portal用户表后会下发相应的ARP表项如下述表1中标号Index为1的ARP表项，用户user从区域B再次发起网络访问的时候会生成如下述表1中标号Index为2的ARP表项。

[0027] 表1

[0028]

Index	IP	MAC	VLAN	PORT	Type
1	User-ip	User-mac	a	Port1	R

2	User-ip	User-mac	b	Port2	D

[0029] 图上述表1所示，用户user在区域B上线后，BRAS生成的ARP表项的类型Type为R，若对应于区域A的portal用户表项不老化，相应的标号Index为1的ARP表项也不会老化，由于ARP表项1早于ARP表项2生成，所有后续BRAS上命中该用户的流量都会优先命中并依照ARP表项1进行流量发送。

[0030] 因此用户user从区域B发起网络访问时，BRAS推送WEB服务器的认证界面，此时，由于用户user流量到服务器没有问题，而由服务器回到用户的流量在BRAS上做三层转发的时候会优先命中ARP表项1，导致流量下发到了区域A，区域B的用户自然无法获取到portal认证界面，最终导致用户漫游失败。

[0031] 本申请实施例针对上述情况，提供了一种portal认证方法，实现跨VLAN或者跨端口漫游。

[0032] 图2为本申请实施例提供的一种portal认证方法流程图，本实施例的方法应用于BRAS，如图2所示，该方法包括：

[0033] S210，接收发送方发送的网络请求报文，该网络请求报文携带用户标识。

[0034] 用户在发起网络访问时，用户终端会向BRAS发送网络请求报文，如HTTP(Hyper Text Transfer Protocol，超文本传输协议)报文，本实施例示例性地，用户标识为该网络请求报文的源IP地址，当然，实际应用中，也可以将MAC地址作为用户标识，对此本实施例不做具体限定，只要在整个portal网络中该用户标识能够唯一标识portal用户表、ARP表项和禁止用户漫游表项。

[0035] S220，根据用户标识检测是否可以基于网络请求报文进行portal认证，在不可以进行portal认证时，去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项。

[0036] 本申请实施例可以通过删除、置无效的方式实现去使能用户标识对应的portal用户表和ARP表项。为节省BRAS的存储空间，以及便于BRAS管理portal用户表和ARP表项，本申请实施例，在不可以进行portal认证时，删除用户标识对应的portal用户表和ARP表项。

[0037] 本申请实施例可以检测BRAS上是否有该用户标识对应的portal用户表，若检测到该用户标识没有对应的portal用户表，判断可以进行portal认证；若检测到用户标识有对应的portal用户表，且该portal用户表对应的用户在线，判断当前接收到的网络请求报文为非法报文，此时不可以进行portal认证；相应的，若检测到用户标识有对应的portal用户表，且该portal用户表对应的用户未在线，判断发送方处于漫游状态，此时可以进行portal认证。

[0038] S130，在去使能portal用户表和ARP表项后，基于网络请求报文进行portal认证。

[0039] 示例性地，若认证通过，则生成相应的portal用户表，若认证未通过，提示发送方认证失败。

[0040] 本实施例基于在BRAS上保存有该用户标识对应的portal用户表和ARP表项时，在ARP表项无法实现BRAS与发送方之间的数据转发的前提下，通过网络请求报文的用户标识检测是否可以进行portal认证，在不可以进行portal认证时，去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项，使得可以基于网络请求报文进行portal认证，保证用户及时触发漫游上线，而无需等待portal用户表老化后才能上线。

[0041] 在本实施例的一个实现方案中，根据下述方式检测是否可以基于接收到的网络请

求报文进行portal认证：

[0042] 检测用户标识是否存在对应的portal用户表，若不存在portal用户表则基于网络请求报文进行portal认证，认证通过，生成相应的portal用户表，认证未通过，提示发送方认证失败；

[0043] 若存在portal用户表，则检测发送方是否在线，若发送方不在线，则去使能portal用户表和相应的ARP表项，并基于网络请求报文进行portal认证，portal认证通过，生成相应的portal用户表，portal认证未通过，提示发送方认证失败。

[0044] 本实施例在检测发送方不在线时，还可以基于用户标识生成禁止用户漫游表项，禁止用户漫游表项通过用户标识唯一标识，本实施例的禁止用户漫游表项用于禁止携带其用户标识的网络请求报文进行portal认证。

[0045] 在其中一种实现方式中，若发送方在线，标记网络请求报文为非法报文，禁止发送方进行portal认证；实际应用中，在检测到网络请求报文为非法报文时，可以丢弃或删除该非法包文。

[0046] 实际应用中，可以对网络请求报文的源IP地址进行探测，示例性的，参考图2，BRAS通过VLAN a向用户user发送ICMP(Internet Control Message Protocol，Internet控制报文协议)探测包，若在探测时间内接收到响应，则认为用户user在线，否则认为用户user不在线。

[0047] 为防止BRAS受到网络攻击，及时、有效地对非法的网络请求报文进行处理，本实施例在基于网络请求报文进行portal认证前，首先检测该用户标识是否存在对应的禁止用户漫游表项。

[0048] 若该用户标识存在禁止用户漫游表项，禁止发送方进行portal认证；本实施例在检测该用户标识存在对应的禁止用户漫游表项时，可以丢弃该网络请求报文，不进行后续的portal认证处理。

[0049] 若该用户标识不存在禁止用户漫游表项，则检测该用户标识是否存在对应的portal用户表，按照上述方案进行portal认证处理。

[0050] 在本实施例的另一个实现方案中，可以通过下述方案生成禁止用户漫游表项：

[0051] 提取该用户标识对应的portal用户表中的IP字段、MAC字段、认证接口PORT字段、VLAN字段、固定时间TIME字段中的一种或多种生成禁止用户漫游表项。

[0052] 示例性地，参考下述表2，本实施例生成的禁止用户漫游表项包括IP字段、MAC字段、PORT字段、VLAN字段和TIME字段，其中，IP字段为用户IP地址，MAC字段为用户MAC地址，PORT字段为用户接入认证的接口，VLAN字段为用户接入认证的VLAN，TIME字段为禁止用户漫游时间，该TIME字段的数值可以为秒级、分钟级等，可以根据应用需求进行配置。

[0053] 表2

[0054]

IP	MAC	PORT	VLAN	TIME
ip1	mac1	port1	vlan1	T1

[0055]

ip2	mac2	port2	vlan2	T2

[0056] 对于禁止用户漫游表项的老化时间，可以根据TIME字段数值配置该禁止用户漫游

表项的老化时间，或者，配置禁止用户漫游表项与portal用户表相关联，在删除portal用户表时联动删除禁止用户漫游表项。

[0057] 本申请通过下述实施例详细说明本实施例提供的portal认证过程。

[0058] 图3为本申请实施例提供的portal认证流程示意图，如图3所示，portal认证过程如下：

[0059] S310，基于访问请求报文判断是否命中禁止用户漫游表，若命中则执行步骤S370，若未命中则执行步骤S320。

[0060] 用户在发起网络访问时，会将访问请求报文上送BRAS平台，BRAS平台获取访问请求报文中的源IP，基于该源IP查看禁止用户漫游表项，如果存在该源IP对应的禁止用户漫游表项中则执行步骤S370，否则执行步骤S320。

[0061] S320，基于源IP判断是否命中portal用户表，若命中执行步骤S330，若未命中执行步骤S340。

[0062] 检测BRAS平台上是否存在该源IP对应的portal用户表，如果存在则执行步骤S330，如果不存在则执行步骤S340。

[0063] S330，对该源IP进行探测，探测成功执行步骤S350，探测失败则删除portal用户表和相应的ARP表项，并执行步骤S340。

[0064] 示例性地，BRAS通过该portal用户表中的VLAN向用户发送ICMP探测包，若在探测时间内接收到响应，则认为用户在线，此时探测成功，否则认为用户不在线，此时探测失败。

[0065] S340，基于访问请求报文进行portal认证，认证通过执行步骤S360，认证未通过执行步骤S370。

[0066] S350，生成禁止用户漫游表项。

[0067] 本实施在步骤S350判断，源IP对应的portal用户表的用户是在线的，那么步骤S310的访问请求报文为非法报文，此时禁止用户进行portal认证。

[0068] 由于非法报文的攻击时间一般为秒级以下，如在微秒级进行攻击，由此，本申请实施例将禁止用户漫游表项的老化时间设置为秒级或分钟级，以避免非法报文的攻击。

[0069] 且将禁止用户漫游表项的老化时间设置为秒级或分钟级，还能够避免在禁止用户漫游表项的老化时间内，用户漫游无法及时上线。因为实际应用中，用户发生漫游的时间通常为小时级以上，即用户发生漫游时间通常大于禁止用户漫游表项的老化时间，因此，本申请设置的禁止用户漫游表项的老化时间能够保证合法用户在漫游时能够及时上线。

[0070] S360，生成portal用户表。

[0071] 此时可以根据portal用户表生成相应的ARP表项，基于该ARP表项向用户终端发送认证界面等相关数据，使用户进行portal认证。

[0072] S370，禁止用户进行portal认证。

[0073] 与上述portal认证方法相对应的，本申请该提供了portal认证装置。

[0074] 图4为本申请实施例提供的一种portal认证装置结构框图，本实施例的portal认证装置应用于BRAS，如图4所示，该装置40包括：接收单元41、检测单元42和认证处理单元43；

[0075] 接收单元41，用于接收发送方发送的网络请求报文，该网络请求报文携带用户标识，用户标识为网络请求报文的源IP地址；

[0076] 检测单元42，用于根据用户标识检测是否可以基于网络请求报文进行portal认证；

[0077] 认证处理单元43，用于在不可以进行portal认证时，去使能BRAS上保存的该用户标识对应的portal用户表和ARP表项，去使能所述portal用户表和ARP表项后，基于所述网络请求报文进行portal认证。

[0078] 在本实施例的一个实现方案中，检测单元42，还用于检测用户标识是否存在对应的portal用户表，以及在用户标识存在所述portal用户表时，检测发送方是否在线；认证处理单元43，用于在检测单元42检测用户标识不存在portal用户表时，基于网络请求报文进行portal认证；以及在检测单元42检测发送方不在线时，去使能portal用户表和相应的ARP表项，并基于网络请求报文进行portal认证。

[0079] 在本实现方案中，认证处理单元43，还用于在检测单元42检测发送方在线时，标记网络请求报文为非法报文，禁止发送方进行portal认证；实际应用中，认证处理单元43在检测单元检测到网络请求报文为非法报文时，丢弃或删除该非法包文。

[0080] 本实现方案的认证处理单元43，进一步用于在检测单元42检测发送方在线时，提取portal用户表中的IP地址字段、物理地址字段、认证接口字段、虚拟局域网字段、固定时间字段中的一种或多种生成禁止用户漫游表项；禁止用户漫游表项通过用户标识唯一标识，禁止用户漫游表项用于禁止携带其用户标识的网络请求报文进行portal认证。

[0081] 实际应用中，认证处理单元43，还用于配置所述禁止用户漫游表项的老化时间，或者，配置禁止用户漫游表项与portal用户表相关联，使在删除portal用户表时联动删除禁止用户漫游表项。

[0082] 在本实施例的另一个实现方案中，检测模块42，还用于在检测用户标识是否存在对应的portal用户表之前，检测用户标识是否存在对应的禁止用户漫游表项。认证处理单元43，在检测单元42检测用户标识存在对应的禁止用户漫游表项时，禁止发送方进行portal认证，在检测单元42检测用户标识不存在禁止用户漫游表项，驱动检测单元42检测用户标识是否存在对应的portal用户表。

[0083] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的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模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0084] 本申请提供的portal认证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，参照图5所示，本申请提供的portal认证装置40可包括处理器501、存储有机器可执行指令的机器可读存储介质502。处理器501与机器可读存储介质502可经由系统总线503通信。并且，通过读取并执行机器可读存储介质502中与portal认证逻辑对应的机器可执行指令，处理器501可执行上文描述的portal认证方法。

[0085] 本申请中提到的机器可读存储介质502可以是任何电子、磁性、光学或其它物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，机器可读存储介质可以是：RAM(Radom Access Memory，随机存取存储器)、易失存储器、非易失性存储器、闪存、存储驱

动器(如硬盘驱动器)、固态硬盘、任何类型的存储盘(如光盘、DVD等),或者类似的存储介质,或者它们的组合。

[0086] 根据本申请公开的示例,本申请还提供了一种包括机器可执行指令的机器可读存储介质,例如图5中的机器可读存储介质502,所述机器可执行指令可由portal认证装置40中的处理器501执行以实现以上描述的portal认证方法。

[0087] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0088] 以上所述仅为本申请的较佳实施例而已,并非用于限定本申请的保护范围。凡在本申请的精神和原则之内所作的任何修改、等同替换、改进等,均包含在本申请的保护范围内。

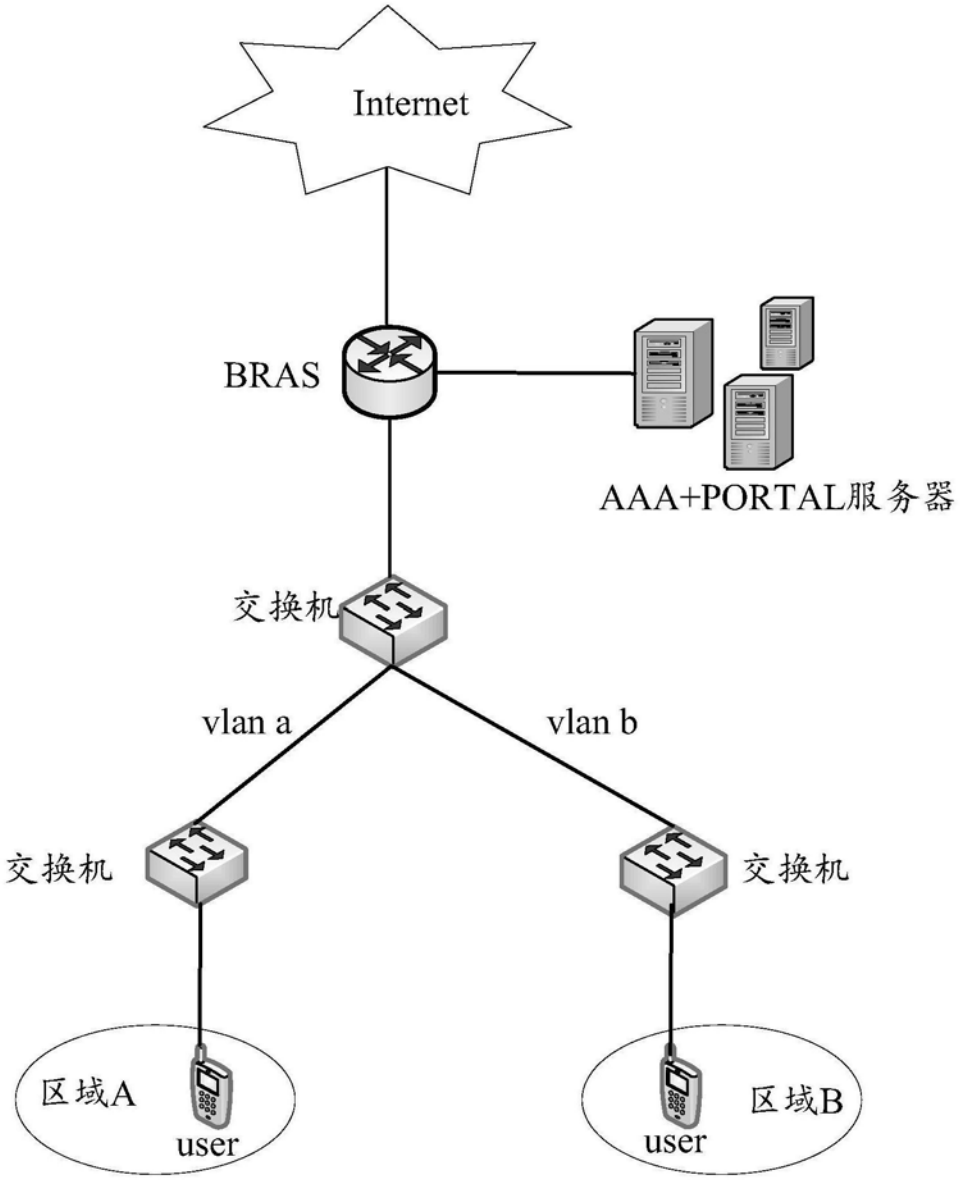

Internet
BRAS
AAA+PORTAL服务器
交换机
vlan a
vlan b
交换机
交换机
区域A
user
区域B
user

图1

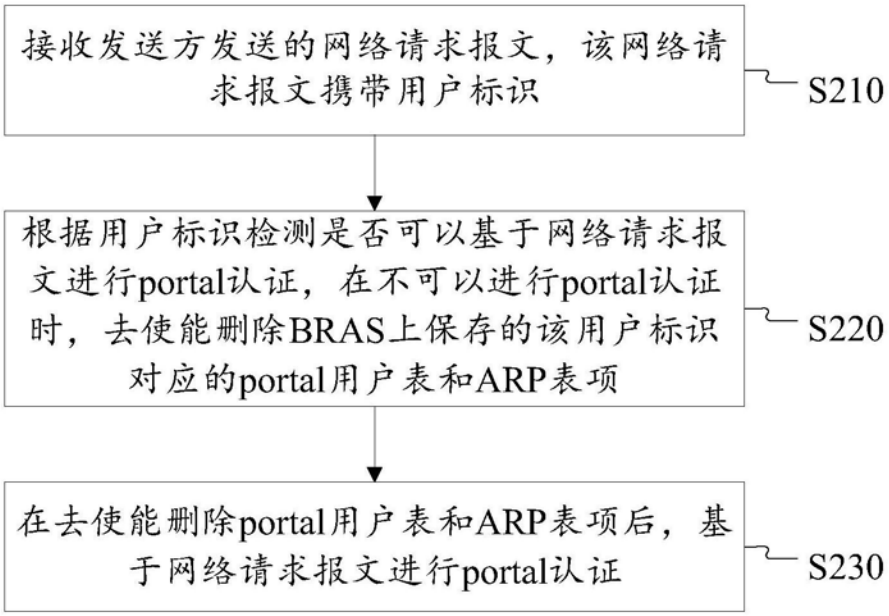

接收发送方发送的网络请求报文，该网络请求报文携带用户标识
S210
根据用户标识检测是否可以基于网络请求报文进行portal认证，在不可以进行portal认证时，去使能删除BRAS上保存的该用户标识对应的portal用户表和ARP表项
S220
在去使能删除portal用户表和ARP表项后，基于网络请求报文进行portal认证
S230

图2

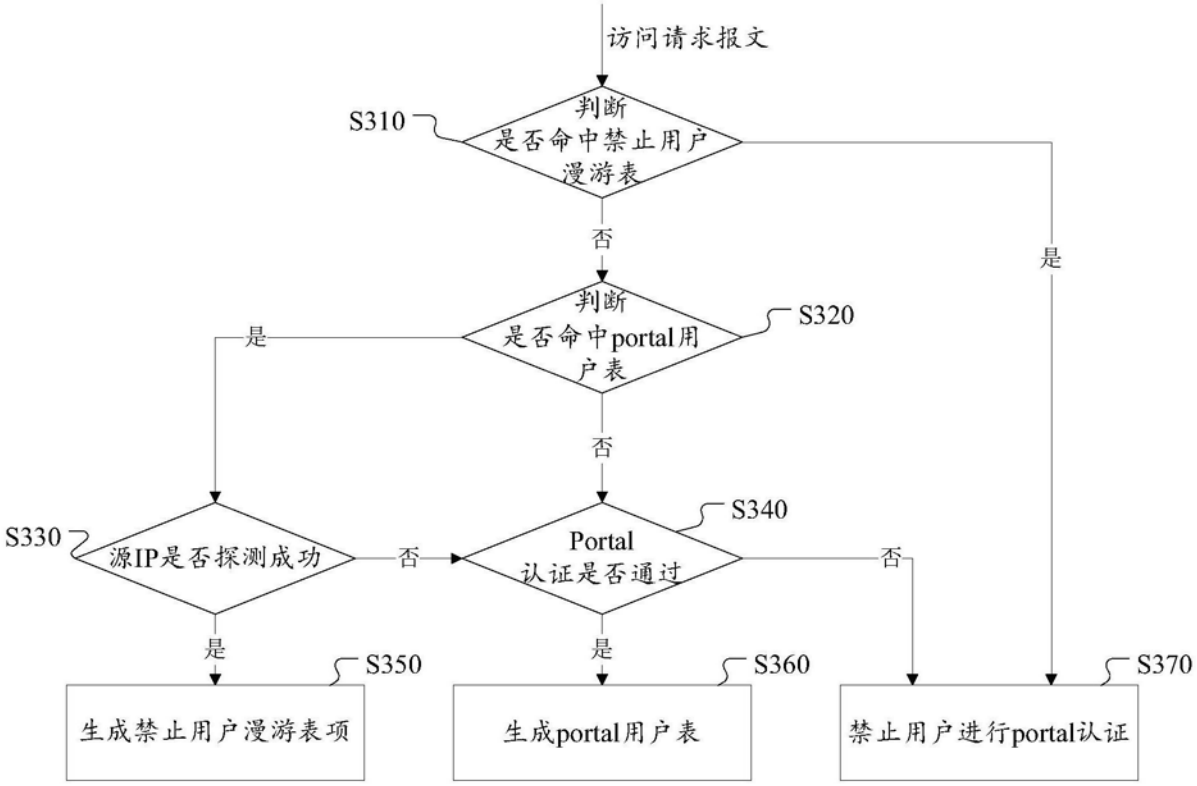

访问请求报文
S310
判断是否命中禁止用户漫游表
否
是
判断是否命中portal用户表
S320
是
否
S330
源IP是否探测成功
否
S340
Portal认证是否通过
否
是
是
S350
生成禁止用户漫游表项
S360
生成portal用户表
S370
禁止用户进行portal认证

图3

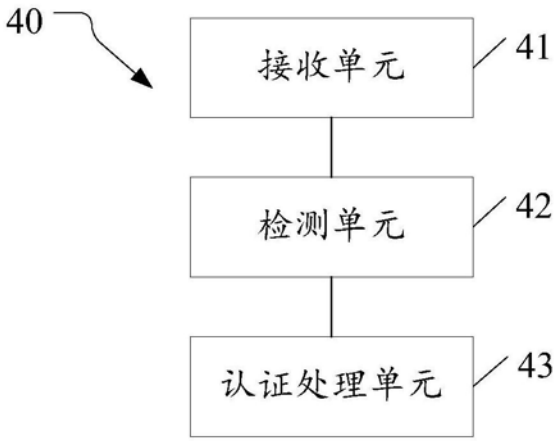

40
接收单元
41
检测单元
42
认证处理单元
43

图4

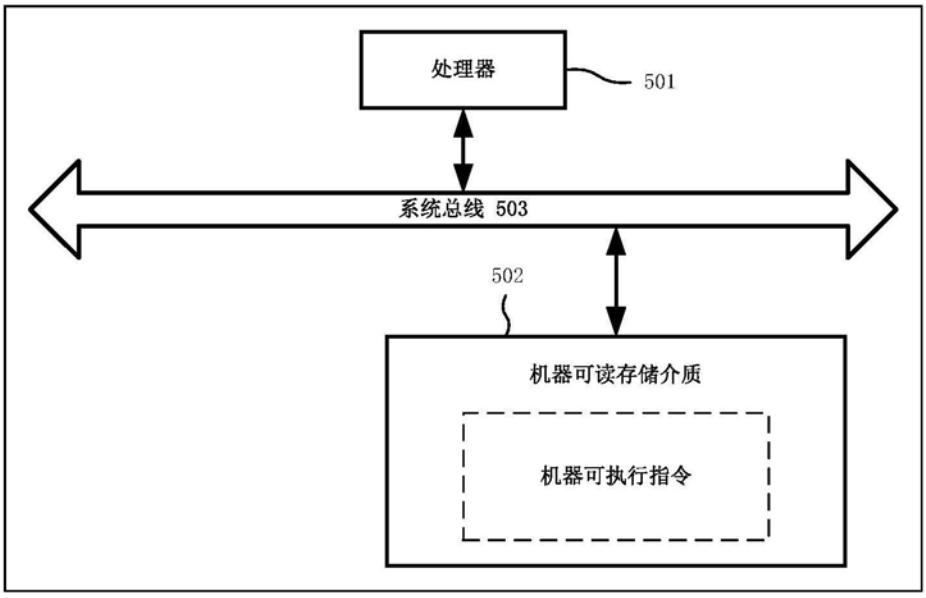

处理器
501
系统总线 503
502
机器可读存储介质
机器可执行指令

图5