



(12) 发明专利

(10) 授权公告号 CN 101321054 B

(45) 授权公告日 2011.02.09

(21) 申请号 200710110698.2

(22) 申请日 2007.06.08

(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 张群 柯波

(74) 专利代理机构 北京集佳知识产权代理有限
公司 11227

代理人 逯长明

(51) Int. Cl.

H04L 9/00 (2006.01)

H04L 12/56 (2006.01)

H04L 29/06 (2006.01)

(56) 对比文件

US 20050055570 A1, 2005.03.10, 全文.

CN 1855812 A, 2006.11.01, 全文.

JP 特开平 11122303 A, 1999.04.30, 全文.

US 6115376 A, 2000.09.05, 全文.

CN 1466341 A, 2004.01.07, 全文.

审查员 王歆玥

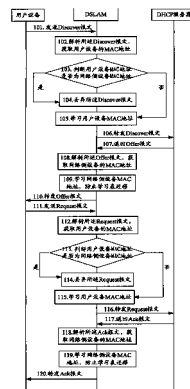
权利要求书 2 页 说明书 5 页 附图 3 页

(54) 发明名称

自动防止网络侧媒体接入控制地址被仿冒的方法及其装置

(57) 摘要

本发明提供一种自动防止网络侧媒体接入控制地址被仿冒的方法及其装置。所述自动防止网络侧媒体接入控制地址被仿冒的方法包括接入设备获取用户设备的媒体接入控制地址;判断接入设备所获取的用户设备的媒体接入控制地址是否为己获知的网络侧设备的媒体接入控制地址,如果否,则学习用户设备的媒体接入控制地址;接入设备学习网络侧设备的媒体接入控制地址,生成媒体接入控制地址学习表,并防止媒体接入控制地址学习表被迁移。通过本发明实施例所提供的技术方案,能够自动完成网络侧设备的媒体接入控制地址被仿冒,且便于管理和维护。



1. 一种自动防止网络侧媒体接入控制地址被仿冒的方法,其特征在于,所述方法包括:

接入设备获取用户设备的媒体接入控制地址;

判断接入设备所获取的用户设备的媒体接入控制地址是否为己获知的网络侧设备的媒体接入控制地址,如果否,则学习用户设备的媒体接入控制地址;如果是,则丢弃能够获取用户设备的媒体接入控制地址的报文;其中,所述能够获取用户设备的媒体接入控制地址的报文包括:请求网络侧为用户分配网际协议 IP 地址的报文、请求会话建立的报文、用户设备寻找网络侧设备的报文或请求会话建立服务的报文;

接入设备学习网络侧设备的媒体接入控制地址,生成媒体接入控制地址学习表,并防止媒体接入控制地址学习表被迁移。

2. 根据权利要求 1 所述的自动防止网络侧媒体接入控制地址被仿冒的方法,其特征在于,所述接入设备获取用户设备的媒体接入控制地址具体包括:

用户设备发送请求网络侧设备为用户分配 IP 地址的报文给接入设备;

接入设备解析所述请求网络侧设备为用户分配 IP 地址的报文,获取报文的源媒体接入控制地址,即用户设备的媒体接入控制地址。

3. 根据权利要求 2 所述的自动防止网络侧媒体接入控制地址被仿冒的方法,其特征在于,判断接入设备所获取的用户设备的媒体接入控制地址与己获知的网络侧设备的媒体接入控制地址是否相同,如果是,则丢弃请求网络侧设备为用户分配 IP 地址的报文。

4. 根据权利要求 2 所述的自动防止网络侧媒体接入控制地址被仿冒的方法,其特征在于,所述接入设备学习网络侧设备的媒体接入控制地址具体包括:

接入设备转发所述请求网络侧设备为用户分配 IP 地址给网络侧设备;

网络侧设备返回携带为用户分配 IP 地址的确认报文给接入设备;

接入设备解析所述携带为用户分配 IP 地址的确认报文,获取报文的源媒体接入控制地址,即网络侧设备的媒体接入控制地址。

5. 根据权利要求 2 所述的自动防止网络侧媒体接入控制地址被仿冒的方法,其特征在于,所述用户设备发送请求网络侧设备为用户分配 IP 地址的报文给接入设备之前还包括:

用户设备发送寻找网络侧设备或者请求会话建立服务的报文给接入设备;

接入设备解析所述报文,获取报文的源媒体接入控制地址,即用户设备的媒体接入控制地址;

判断接入设备所获取的用户设备的媒体接入控制地址与己获知的网络侧设备的媒体接入控制地址是否相同,如果否,则学习用户设备的媒体接入控制地址;如果是,则丢弃所述寻找网络侧设备或者请求会话建立服务的报文;

接入设备转发所述报文给网络侧设备;

网络侧设备返回携带网络侧设备信息的确认报文给接入设备;

接入设备解析所述携带网络侧设备信息的确认报文,获取报文的源媒体接入控制地址,即网络侧设备的媒体接入控制地址;

接入设备学习网络侧设备的媒体接入控制地址,并防止媒体接入控制地址学习表被迁移。

6. 根据权利要求 1 至 5 中任一权利要求所述的自动防止网络侧媒体接入控制地址被仿

冒的方法,其特征在于,所述网络侧设备包括宽带接入服务器或网关。

7. 根据权利要求1至5中任一权利要求所述的自动防止网络侧媒体接入控制地址被仿冒的方法,其特征在于,所述已获知的网络侧设备的媒体接入控制地址由接入设备通过路由协议或地址解释协议获知并存储在接入设备中。

8. 一种自动防止网络侧媒体接入控制地址被仿冒的装置,其特征在于,所述装置包括:

获取单元,用于获取并保存用户设备的媒体接入控制地址;

判断单元,用于判断获取单元所获取的用户设备的媒体接入控制地址是否为己获知的网络侧设备的媒体接入控制地址;

学习单元,用于当判断单元的判断结果为用户设备的媒体接入控制地址不是网络侧设备的媒体接入控制地址时,学习用户设备的媒体接入控制地址和网络侧设备的媒体接入控制地址,并生成媒体接入控制地址学习表;

设置单元,用于防止学习单元生成的媒体接入控制地址学习表迁移。

9. 根据权利要求8所述的自动防止网络侧媒体接入控制地址被仿冒的装置,其特征在于,所述装置还包括存储单元,用于存储已获知的网络侧设备的媒体接入控制地址。

自动防止网络侧媒体接入控制地址被仿冒的方法及其装置

技术领域

[0001] 本发明涉及互联网宽带接入技术和网络安全领域,特别涉及一种自动防止网络侧媒体接入控制地址被仿冒的方法及其装置。

背景技术

[0002] 随着互联网络技术的成熟和业务的不断推广,宽带接入业务已经如火如荼地开展起来。但是如何保证宽带用户使用宽带业务的安全性和网络运营商的安全性,是一个需要重点解决的问题。例如,接入用户假冒宽带接入服务器(BRAS, Broadband Remote Access Server)的媒体接入控制(MAC, MediaAccess Control)地址发起以太网点对点协议(PPPoE, Point-to-Point Protocolover)或动态主机配置协议(DHCP, Dynamic Host Configuration Protocol)申请导致接入设备上BRAS的MAC地址学习表从网络侧端口迁移到了用户侧端口,从而造成其他用户业务中断。

[0003] 接入设备的主要功能是提供各种接入手段将用户接入到网络获取网络服务,接入设备用来接入用户的端口通常称为用户侧端口,连接到局域网、城域网或核心网的端口通常称为网络侧端口。MAC地址表分为静态表和动态表,静态表一般手工在设备上配置,这种表的特点是该表一旦配置后一直保存在设备中,不会随着时间流逝而删除。动态表一般由设备自动学习生成,其特点是该表保存在设备一段时间后会自动删除。

[0004] 就目前宽带业务开展模式来说,用户接入网络使用宽带业务,一般使用两种PPPoE认证和DHCP认证两种方式。

[0005] PPPoE协议为使用桥接以太网接入的用户提供了一种宽带接入手段,同时还提供方便的接入控制和计费。

[0006] DHCP协议是在根协议(BOOTP, Bootstrap Protocol)基础上提出的,其作用是在网络中向主机提供配置信息。DHCP采用客户端/服务器模式,由客户端向服务器提出配置申请,包括分配的IP地址、子网掩码、缺省网关等参数,服务器根据策略返回相应配置信息。

[0007] 为了解决网络侧媒体接入控制地址被仿冒,而导致其他接入用户业务中断的问题,现有技术提供一种防止网络侧媒体接入控制地址被仿冒的方法,即在接入设备的用户侧端口上配置源MAC地址过滤功能:在接入设备的用户侧端口上手工配置的一个源MAC地址过滤列表,禁止接入用户使用过滤列表中的MAC地址作为源地址。如果接入用户使用了过滤列表中的地址,接入设备则丢弃该报文。

[0008] 从上述现有技术提供的方法可以看出:当更改BRAS或网络侧的主用BRAS发生切换时,用户侧端口的“源MAC地址过滤”需要重新配置,所述配置功能依赖于上层网络设备,网络管理维护工作量大;由于接入用户端口数量很多,逐个用户端口地配置“源MAC地址过滤”功能,网络管理员维护工作量大。因此,在进行本发明创造过程中,发明人发现现有技术中至少存在如下问题:现有技术提供的防止网络侧媒体接入控制地址被仿冒的方法,需要在接入设备的用户侧端口上手工配置一个源MAC地址过滤列表且网络管理维护工作量大。

[0009] 发明内容

[0010] 本发明实施例要解决的技术问题为提供一种自动防止网络侧媒体接入控制地址被仿冒的方法及其装置,能够自动防止网络侧媒体接入控制地址被仿冒的方法且便于管理和维护。

[0011] 为解决上述技术问题,本发明实施例的目的是通过以下技术方案实现的:

[0012] 本发明实施例提供一种自动防止网络侧媒体接入控制地址被仿冒的方法,包括:

[0013] 接入设备获取用户设备的媒体接入控制地址;

[0014] 判断接入设备所获取的用户设备的媒体接入控制地址是否为已获知的网络侧设备的媒体接入控制地址,如果否,则学习用户设备的媒体接入控制地址;如果是,则丢弃包含能够获取用户设备的媒体接入控制地址的报文;

[0015] 接入设备学习网络侧设备的媒体接入控制地址,生成媒体接入控制地址学习表,并防止媒体接入控制地址学习表被迁移。

[0016] 本发明实施例还提供一种自动防止网络侧媒体接入控制地址被仿冒的装置,包括:

[0017] 获取单元,用于获取并保存用户设备的媒体接入控制地址;

[0018] 判断单元,用于判断获取单元所获取的用户设备的媒体接入控制地址是否为已获知的网络侧设备的媒体接入控制地址;

[0019] 学习单元,用于当判断单元的判断结果为用户设备的媒体接入控制地址不是网络侧设备的媒体接入控制地址时,学习用户设备的媒体接入控制地址和网络侧设备的媒体接入控制地址,并生成媒体接入控制地址学习表;

[0020] 设置单元,用于防止学习单元生成的媒体接入控制地址学习表迁移。

[0021] 通过本发明实施例提供的自动防止网络侧媒体接入控制地址被仿冒的方法及其装置,当用户设备的媒体接入控制地址不是网络侧设备的媒体接入控制地址时,才允许接入设备学习用户设备和网络侧设备的媒体接入控制地址,并防止媒体接入控制地址学习表被迁移,从而可以自动防止用户仿冒网络侧设备接入网络,且可以防止其他端口学习网络侧设备的媒体接入控制地址,从而仿冒网络侧设备的媒体接入控制地址,且便于管理和维护。

附图说明

[0022] 图1为本发明自动防止网络侧媒体接入控制地址被仿冒的方法第一实施例的信令流程图;

[0023] 图2为本发明自动防止网络侧媒体接入控制地址被仿冒的方法第二实施例的信令流程图;

[0024] 图3为本发明自动防止网络侧媒体接入控制地址被仿冒的装置一个实施例的结构图。

具体实施方式

[0025] 本发明实施例提供一种防止接入用户仿冒其他媒体接入控制地址的方法及其装置。为使本发明的技术方案更加清楚明白,以下参照附图并列举实施例,对本发明进一步详

细说明。

[0026] 请参照图 1,为本发明自动防止网络侧媒体接入控制地址被仿冒的方法第一实施例的信令流程图。本实施例的应用场景为用户采用 DHCP 技术向网络侧设备申请分配 IP 地址,且用户为第一次接入网络侧设备。所述防止接入用户仿冒其他媒体接入控制地址的方法具体过程包括:

[0027] 步骤 101:用户发送 Discover 报文给接入设备,用于寻找 DHCP 服务器;

[0028] 本实施例中,接入设备为数字用户线接入复用设备(DSLAM, Subscriber Line Access Multiplexer)。。

[0029] 步骤 102:接入设备对接收的 Discover 报文进行解析,获取报文的源 MAC 地址,即用户设备的 MAC 地址;

[0030] 步骤 103:判断接入设备所获取的用户设备的 MAC 地址是否为己获知的网络侧设备的 MAC 地址,如果是,则进行步骤 104,如果否,则进行步骤 105;

[0031] 接入设备可以通过路由协议或地址解释协议(ARP, Address Resolution Protocol)获知网络中的网络侧设备的 MAC 地址,并将己获知的网络侧设备的 MAC 地址存储在接入设备中。本实施例中,网络侧设备为 DHCP 服务器。

[0032] 步骤 104:丢弃所述 Discover 报文。

[0033] 可以防止用户仿冒网络侧设备的 MAC 地址,例如仿冒 BRAS 的 MAC 地址。

[0034] 步骤 105:接入设备学习己获取的用户设备的 MAC 地址;

[0035] 步骤 106:接入设备向网络侧设备转发所述 Discover 报文;

[0036] 步骤 107:网络侧设备返回 Offer 报文给接入设备,并携带网络侧设备的信息;

[0037] 网络侧设备的信息包括网络侧设备的 IP 地址、MAC 地址等。

[0038] 步骤 108:接入设备对接收的 Offer 报文进行解析,获取 Offer 报文的源 MAC 地址,即网络侧设备的 MAC 地址;

[0039] 步骤 109:接入设备学习网络侧设备的 MAC 地址,生成媒体接入控制地址学习表,并且防止 MAC 地址学习表迁移,以防其它端口学习 MAC 地址网络侧设备的地址;

[0040] 防止媒体接入控制地址学习表被迁移的具体方式为设置所述媒体接入控制地址学习表为静态媒体接入控制地址表或者通过逻辑芯片对其他用户侧端口使用网络侧的媒体介入控制地址表进行过滤。

[0041] 步骤 110:接入设备将 Offer 报文转发给用户,并携带网络侧设备的信息。

[0042] 步骤 111:用户发送 Request 报文给接入设备,用于请求网络侧设备为用户分配 IP 地址;

[0043] 步骤 112:接入设备对接收的 Request 报文进行解析,获取报文的源 MAC 地址,即用户设备的 MAC 地址;

[0044] 步骤 113:判断接入设备所获取的用户设备的 MAC 地址是否为己获知的网络侧设备的 MAC 地址,如果是,则进行步骤 114,如果否,则进行步骤 115;

[0045] 步骤 114:丢弃所述 Request 报文,防止用户仿冒网络侧设备的 MAC 地址。

[0046] 步骤 115:接入设备学习己获取的用户设备的 MAC 地址;

[0047] 步骤 116:接入设备向网络侧设备转发所述 Request 报文;

[0048] 步骤 117:网络侧设备为用户分配 IP 地址,返回携带为用户分配的 IP 地址的 ACK

报文给接入设备；

[0049] 步骤 118 :接入设备对接收的 ACK 报文进行解析,获取 ACK 报文的源 MAC 地址,即网络侧设备的 MAC 地址；

[0050] 步骤 119 :接入设备学习网络侧设备的 MAC 地址,生成媒体接入控制地址学习表,并且防止 MAC 地址学习表迁移,以防其它端口学习 MAC 地址网络侧设备的地址；

[0051] 防止媒体接入控制地址学习表被迁移的具体方式为设置所述媒体接入控制地址学习表为静态媒体接入控制地址表或者通过逻辑芯片对其他用户侧端口使用网络侧的媒体介入控制地址表进行过滤。

[0052] 步骤 120 :接入设备将 ACK 报文转发给用户,并携带网络侧设备为用户分配的 IP 地址。

[0053] 如果用户之前已经通过网络侧设备的接入认证,那么步骤 101 到步骤 110 可以省略。

[0054] 请参照图 2,为本发明自动防止网络侧媒体接入控制地址被仿冒的方法第二实施例的信令流程图。本实施例的应用场景为用户采用 PPPoE 技术请求建立会话。所述防止接入用户仿冒其他媒体接入控制地址的方法具体过程包括：

[0055] 步骤 201 :用户发送 PADI 报文给接入设备,用于请求会话建立服务；

[0056] 本实施例中,接入设备为数字用户线接入复用设备 (DSLAM, DigitalSubscriber Line Access Multiplexer)。

[0057] 步骤 202 :接入设备对接收的 PADI 报文进行解析,获取报文的源 MAC 地址,即用户设备的 MAC 地址；

[0058] 步骤 203 :判断接入设备所获取的用户设备的 MAC 地址是否为己获知的 网络侧设备的 MAC 地址,如果是,则进行步骤 204,如果否,则进行步骤 205；

[0059] 接入设备可以通过路由协议或其他方法学习到网络侧设备的 MAC 地址。本实施例中,网络侧设备为 BRAS。

[0060] 步骤 204 :丢弃所述 PADI 报文。

[0061] 可以防止用户仿冒网络侧设备的 MAC 地址,例如仿冒 BRAS 的 MAC 地址。

[0062] 步骤 205 :接入设备学习已获取的用户设备的 MAC 地址；

[0063] 步骤 206 :接入设备向网络侧设备转发所述 PADI 报文；

[0064] 步骤 207 :网络侧设备返回 PADO 报文给接入设备,并携带网络侧设备的信息；

[0065] 网络侧设备的信息包括网络侧设备 MAC 地址等。

[0066] 步骤 208 :接入设备对接收的 PADO 报文进行解析,获取 PADO 报文的源 MAC 地址,即网络侧设备的 MAC 地址；

[0067] 步骤 209 :接入设备学习网络侧设备的 MAC 地址,生成媒体接入控制地址学习表,并且防止 MAC 地址学习表迁移,以防其它端口学习 MAC 地址网络侧设备的地址；

[0068] 例如,可以将 MAC 地址学习表设置为静态 MAC 地址表。

[0069] 步骤 210 :接入设备将 PADO 报文转发给用户,并携带网络侧设备的信息。

[0070] 步骤 211 :用户发送 PADR 报文给接入设备,用于请求会话建立服务；

[0071] 步骤 212 :接入设备对接收的 PADR 报文进行解析,获取报文的源 MAC 地址,即用户设备的 MAC 地址；

[0072] 步骤 213 :判断接入设备所获取的用户设备的 MAC 地址是否为己获知的网络侧设备的 MAC 地址,如果是,则进行步骤 214, 如果否,则进行步骤 215 ;步骤 214 :丢弃所述 PADR 报文,防止用户仿冒网络侧设备的 MAC 地址。

[0073] 步骤 215 :接入设备学习已获取的用户设备的 MAC 地址 ;

[0074] 步骤 216 :接入设备向网络侧设备转发所述 PADR 报文 ;

[0075] 步骤 217 :网络侧设备为用户提供会话服务建立连接,返回 PADS 报文给接入设备 ;

[0076] 步骤 218 :接入设备对接收的 PADS 报文进行解析,获取 PADS 报文的源 MAC 地址,即网络侧设备的 MAC 地址 ;

[0077] 步骤 219 :接入设备学习网络侧设备的 MAC 地址,生成媒体接入控制地址学习表,并且防止 MAC 地址学习表迁移,以防其它端口学习 MAC 地址网络侧设备的地址 ;

[0078] 例如,可以将 MAC 地址学习表设置为静态 MAC 地址表。

[0079] 步骤 220 :接入设备将 PADS 报文转发给用户。

[0080] 通过本发明实施例提供的防止接入用户仿冒其他媒体接入控制地址的方法,。

[0081] 请参照图 3,为本发明自动防止网络侧媒体接入控制地址被仿冒的装置一个实施例的结构图。所述自动防止网络侧媒体接入控制地址被仿冒的装置包括获取单元 31、判断单元 32、学习单元 33、设置单元 34 以及存储单元 35。

[0082] 所述获取单元 31 用于获取并保存用户设备的媒体接入控制地址 ;所述存储单元 35 用于存储已获知的网络侧设备的媒体接入控制地址 ;所述判断单元 32 用于判断获取单元 31 所获取的用户设备的媒体接入控制地址是否为存储单元 35 中存储的网络侧设备的媒体接入控制地址 ;所述学习单元 33 用于当判断单元 32 的判断结果为用户设备的媒体接入控制地址不是网络侧设备的媒体接入控制地址时,学习用户设备的媒体接入控制地址和网络侧设备的媒体接入控制地址,并生成媒体接入控制地址学习表 ;所述设置单元 34 用于防止学习单元 33 生成的媒体接入控制地址学习表迁移。

[0083] 通过上述本发明实施例提供的自动防止网络侧媒体接入控制地址被仿冒的方法及其装置,当用户设备的媒体接入控制地址不是网络侧设备的媒体接入控制地址时,才允许接入设备学习用户设备和网络侧设备的媒体接入控制地址,并防止媒体接入控制地址学习表被迁移,从而可以防止用户仿冒网络侧设备接入网络,且可以防止其他端口学习网络侧设备的媒体接入控制地址,从而仿冒网络侧设备的媒体接入控制地址,且便于管理和维护。

[0084] 以上对本发明所提供的一种自动防止网络侧媒体接入控制地址被仿冒的方法及其装置行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明所揭示的技术方案 ;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

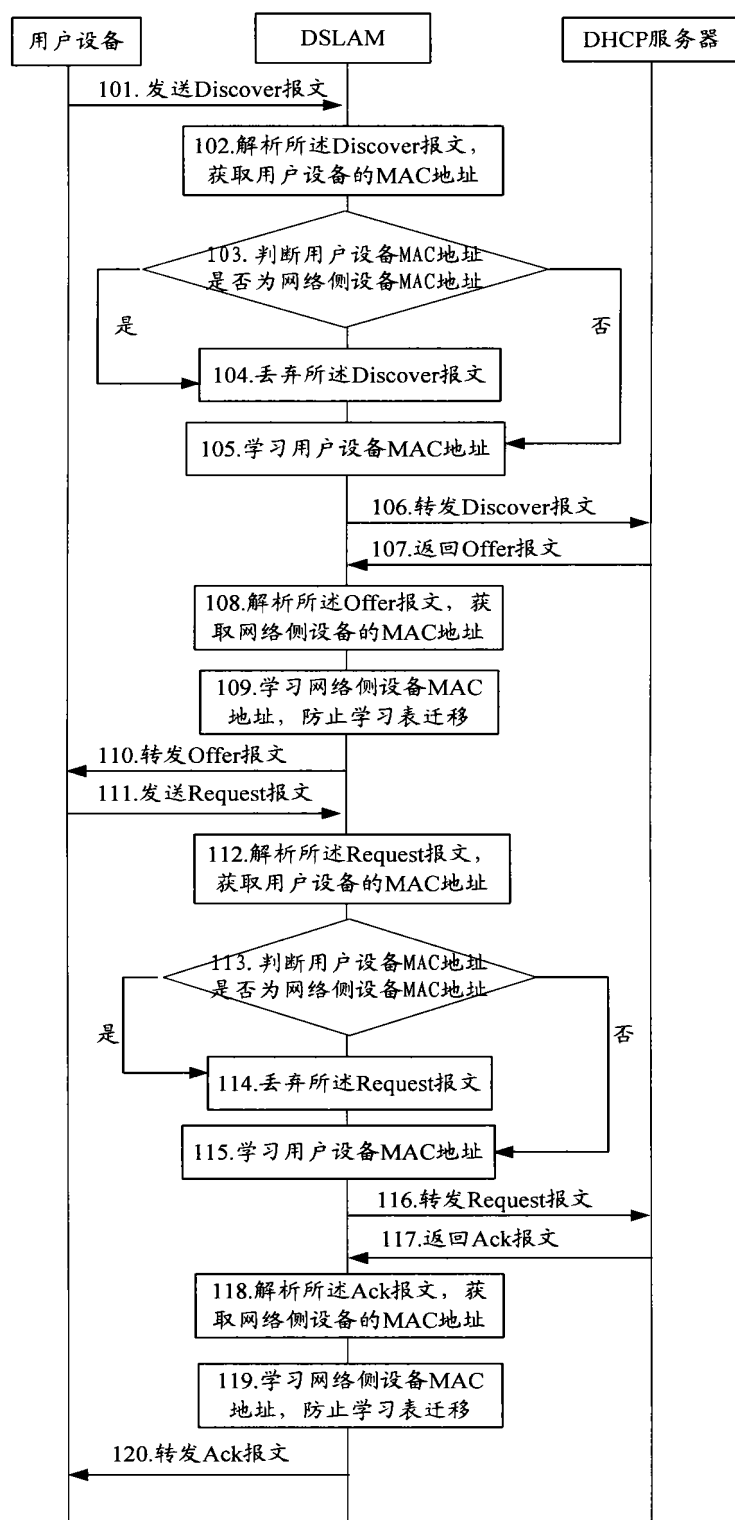


图 1

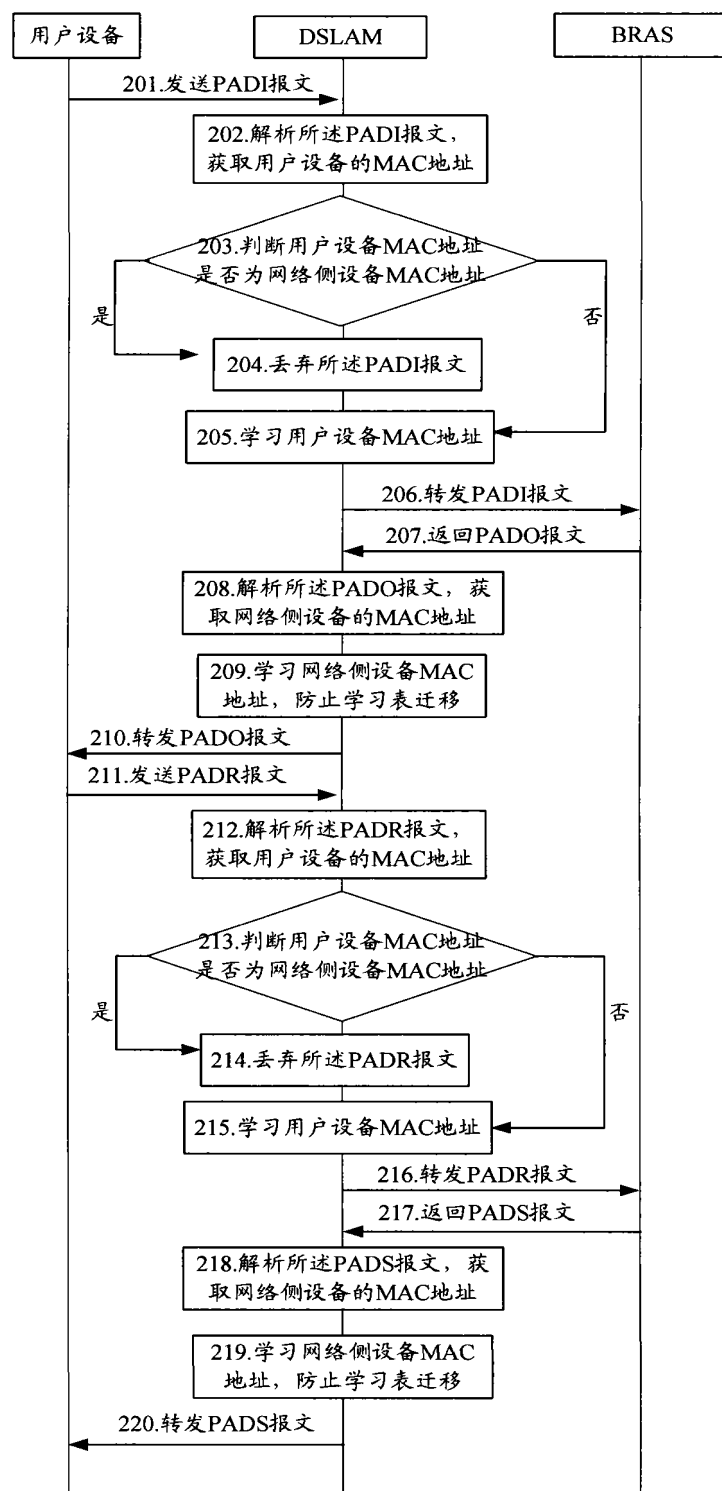


图 2

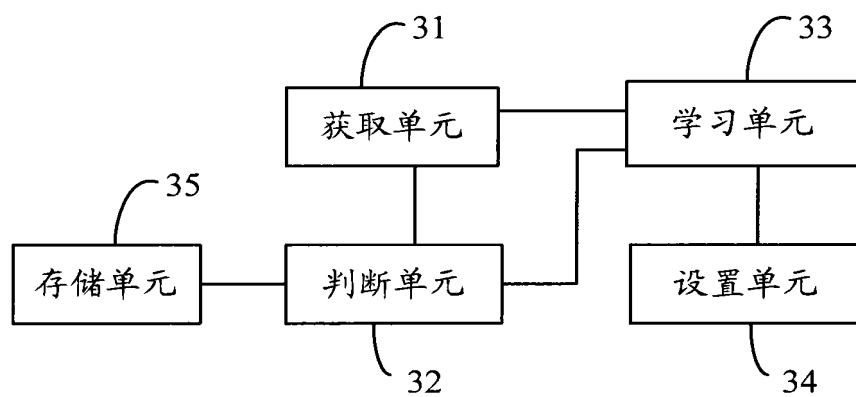


图3