



(12)发明专利

(10)授权公告号 CN 104601460 B

(45)授权公告日 2018.12.25

(21)申请号 201510085510.8

H04L 29/06(2006.01)

(22)申请日 2015.02.16

H04L 29/12(2006.01)

(65)同一申请的已公布的文献号

申请公布号 CN 104601460 A

(56)对比文件

CN 102377669 A, 2012.03.14,

(43)申请公布日 2015.05.06

CN 101610266 A, 2009.12.23,

(73)专利权人 新华三技术有限公司

CN 101257447 A, 2008.09.03,

地址 310052 浙江省杭州市滨江区长河路
466号

CN 1925493 A, 2007.03.07,

(72)发明人 张亚勇 王伟

CN 1536831 A, 2004.10.13,

(74)专利代理机构 北京博思佳知识产权代理有
限公司 11415

US 2014321265 A1, 2014.10.30,

代理人 林祥

审查员 胡智权

(51)Int.Cl.

H04L 12/703(2013.01)

权利要求书2页 说明书6页 附图4页

H04L 12/757(2013.01)

(54)发明名称

一种报文转发方法及装置

接收用户主机发送的ARP请求报文

201

(57)摘要

本发明提供一种报文转发方法及装置，所述方法应用于VRRP组网中的网络交换转发设备，所述方法包括：接收用户主机发送的ARP请求报文；当确认所述ARP请求报文目的IP与网关信息表项相匹配时，从所述网关信息表项中记录的接口发送所述ARP请求报文，其中，所述网关信息表项中包括所述VRRP组网中网关的虚IP地址。因此可以避免非法用户收到该ARP请求报文，提高用户主机在VRRP组网中的安全性。

当确认所述ARP请求报文目的IP与网关信息表项相匹配时，从所述网关信息表项中记录的接口发送所述ARP请求报文；其中，所述网关信息表项中包括所述VRRP组网中网关的虚IP地址

202

1. 一种报文转发方法，其特征在于，所述方法应用于虚拟路由冗余协议VRRP组网中的网络交换转发设备，所述方法包括：

接收用户主机发送的地址解析协议ARP请求报文；

当确认所述ARP请求报文目的IP与网关信息表项相匹配时，从所述网关信息表项中记录的网关接入接口发送所述ARP请求报文，其中，所述网关信息表项中包括所述VRRP组网中网关的虚IP地址和所述网关接入接口，所述网关接入接口为接收到VRRP控制报文的接口。

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：

监听所述VRRP组网中网关之间交互的控制报文；

获取所述控制报文的报文特征，所述控制报文的报文特征包括网关虚IP地址、网关优先级及网关接入接口；

根据所述控制报文的报文特征建立或更新所述网关信息表项。

3. 根据权利要求2所述的方法，其特征在于，所述根据所述控制报文的报文特征建立或更新所述网关信息表项，包括：

根据所述网关优先级判断所述网关的身份；

当所述网关为主网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，则更新所述网关信息表项的老化时间；

当所述网关为主网关，且不存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，则根据所述控制报文的网关虚IP地址及网关接入接口建立网关信息表项，并为该网关信息表项设置老化时间。

4. 根据权利要求3所述的方法，其特征在于，所述方法还包括：

当所述网关为备用网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，则删除该网关信息表项。

5. 根据权利要求1所述的方法，其特征在于，所述方法还包括：

当确认所述ARP请求报文目的IP与网关信息表项不匹配时，将所述ARP请求报文从所有接口广播。

6. 一种报文转发装置，其特征在于，所述装置应用于VRRP组网中的网络交换转发设备，所述装置包括：

请求接收单元，用于接收用户主机发送的ARP请求报文；

报文发送单元，用于在确认所述ARP请求报文目的IP与网关信息表项相匹配时，从所述网关信息表项中记录的网关接入接口发送所述ARP请求报文，其中，所述网关信息表项中包括所述VRRP组网中网关的虚IP地址和所述网关接入接口，所述网关接入接口为接收到VRRP控制报文的接口。

7. 根据权利要求6所述的装置，其特征在于，所述装置还包括：

报文监听单元，用于监听所述VRRP组网中网关之间交互的控制报文；

特征获取单元，用于获取所述控制报文中的报文特征，所述控制报文的报文特征包括网关虚IP地址、网关优先级及网关接入接口；

表项修改单元，用于根据所述控制报文的报文特征建立或更新所述网关信息表项。

8. 根据权利要求7所述的装置，其特征在于，所述表项修改单元，包括：

身份判断子单元，用于根据所述网关优先级判断所述网关的身份；

表项更新子单元，用于在所述网关为主网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，更新所述网关信息表项的老化时间；

表项建立子单元，用于在所述网关为主网关，且不存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，根据所述控制报文的网关虚IP地址及网关接入接口建立网关信息表项，并为该网关信息表项设置老化时间。

9. 根据权利要求8所述的装置，其特征在于，所述装置还包括：

表项删除单元，用于在所述网关为备用网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，删除该网关信息表项。

10. 根据权利要求6所述的装置，其特征在于，所述报文发送单元，还用于在确认所述ARP请求报文目的IP与网关信息表项不匹配时，将所述ARP请求报文从所有接口广播。

一种报文转发方法及装置

技术领域

[0001] 本发明涉及通信技术领域,尤其涉及一种报文转发方法及装置。

背景技术

[0002] 为了增加网关的可靠性,目前的组网中通常使用多台路由器作为网关,并使用VRRP(Virtual Router Redundancy Protocol,虚拟路由器冗余协议)进行管理。VRRP将能够承担网关功能的一组路由器加入到备份组中,形成一台虚拟路由器,并由VRRP的选举机制来决定哪台路由器负责转发任务。

[0003] 现有技术中,当连接上述虚拟路由器的网络交换转发设备收到用户主机发送的ARP(Address Resolution Protocol,地址解析协议)请求报文时,通常会在该设备所在的局域网内广播该ARP请求报文。由于该局域网内的非法主机亦可收到该ARP请求报文,并利用该ARP请求报文来冒充网关对用户主机实施ARP网关欺骗,因此会对用户主机的信息安全造成威胁。

发明内容

[0004] 有鉴于此,本发明提供一种报文转发方法及装置来解决VRRP组网中非法用户进行ARP网关欺骗的问题。

[0005] 具体地,本发明是通过如下技术方案实现的:

[0006] 一种报文转发方法,所述方法应用于VRRP组网中的网络交换转发设备,所述方法包括:

[0007] 接收用户主机发送的ARP请求报文;

[0008] 当确认所述ARP请求报文目的IP与网关信息表项相匹配时,从所述网关信息表项中记录的接口发送所述ARP请求报文,其中,所述网关信息表项中包括所述VRRP组网中网关的虚IP地址。

[0009] 进一步的,所述方法还包括:

[0010] 监听所述VRRP组网中网关之间交互的控制报文;

[0011] 获取所述控制报文的报文特征,所述控制报文的报文特征包括网关虚IP地址、网关优先级及网关接入接口;

[0012] 根据所述控制报文的报文特征建立或更新所述网关信息表项。

[0013] 进一步的,所述网关信息表项还包括网关接入接口,所述根据所述控制报文的报文特征建立或更新所述网关信息表项,包括:

[0014] 根据所述网关优先级判断所述网关的身份;

[0015] 当所述网关为主网关,且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,则更新所述网关信息表项的老化时间;

[0016] 当所述网关为主网关,且不存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,则根据所述控制报文的网关虚IP地址及网关接入接口建立网关

信息表项，并为该网关信息表项设置老化时间。

[0017] 进一步的，所述方法还包括：

[0018] 当所述网关为备用网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，则删除该网关信息表项。

[0019] 进一步的，所述方法还包括：

[0020] 当确认所述ARP请求报文目的IP与网关信息表项不匹配时，将所述ARP请求报文从所有接口广播。

[0021] 基于相同的构思，本发明还提供一种报文转发装置，所述装置应用于VRRP组网中的网络交换转发设备，所述装置包括：

[0022] 请求接收单元，用于接收用户主机发送的ARP请求报文；

[0023] 报文发送单元，用于在确认所述ARP请求报文目的IP与网关信息表项相匹配时，从所述网关信息表项中记录的接口发送所述ARP请求报文，其中，所述网关信息表项中包括所述VRRP组网中网关的虚IP地址。

[0024] 进一步的，所述装置还包括：

[0025] 报文监听单元，用于监听所述VRRP组网中网关之间交互的控制报文；

[0026] 特征获取单元，用于获取所述控制报文中的报文特征，所述控制报文的报文特征包括网关虚IP地址、网关优先级及网关接入接口；

[0027] 表项修改单元，用于根据所述控制报文的报文特征建立或更新所述网关信息表项。

[0028] 进一步的，所述网关信息表项还包括网关接入接口，所述表项修改单元，包括：

[0029] 身份判断子单元，用于根据所述网关优先级判断所述网关的身份；

[0030] 表项更新子单元，用于在所述网关为主网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，更新所述网关信息表项的老化时间；

[0031] 表项建立子单元，用于在所述网关为主网关，且不存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，根据所述控制报文的网关虚IP地址及网关接入接口建立网关信息表项，并为该网关信息表项设置老化时间。

[0032] 进一步的，所述装置还包括：

[0033] 表项删除单元，用于在所述网关为备用网关，且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时，删除该网关信息表项。

[0034] 进一步的，所述报文发送单元，还用于在确认所述ARP请求报文目的IP与网关信息表项不匹配时，将所述ARP请求报文从所有接口广播。由此可见，本发明的网络交换转发设备在收到用户主机发送的ARP请求后，当确认该ARP请求报文的目的IP与网关信息表项相匹配时，从该网关信息表项中记录的接口发送该ARP请求报文，从而可以避免非法用户收到该ARP请求报文，因此提高了用户主机在VRRP组网中的安全性。

附图说明

[0035] 图1是本发明一种示例性实施方式中的VRRP组网架构图；

[0036] 图2是本发明一种示例性实施方式中的一种报文转发方法的处理流程图；

[0037] 图3是本发明一种示例性实施方式中的报文转发方法的交互流程图；

- [0038] 图4是本发明一种示例性实施方式中的表项维护的处理流程图；
[0039] 图5是本发明一种示例性实施方式中报文转发装置所在的网络交换转发设备的硬件结构图；
[0040] 图6是本发明一种示例性实施方式中的一种报文转发装置的逻辑结构图。

具体实施方式

[0041] 请参见图1,是本发明一种示例性实施方式中的VRRP组网架构图,其中包括交换机、用户主机、非法主机、以及由多个具有网关功能的路由器组成虚拟路由器,根据VRRP的选举机制可以决定其中一台路由器承担该虚拟路由器的转发任务,即为主网关;其它路由器则为备用网关。

[0042] 通常交换机在收到用户主机发送的ARP请求报文时,会将该ARP请求报文进行广播。然而在上述VRRP组网中的非法主机也会收到该ARP请求报文,并通过伪造ARP应答来欺骗用户主机,从而给用户主机带来安全隐患。

[0043] 为了解决上述问题,本发明的网络交换转发设备在收到用户主机发送的ARP请求后,当确认该ARP请求报文的目的IP与网关信息表项相匹配时,从该网关信息表项中记录的接口发送该ARP请求报文,从而可以避免非法用户收到该ARP请求报文,因此提高了用户主机在VRRP组网中的安全性。

[0044] 请参考图2,是本发明一种示例性实施方式中的一种报文转发方法处理流程图,所述方法应用于VRRP组网中的网络交换转发设备,所述方法包括:

[0045] 步骤201、网络交换转发设备接收用户主机发送的ARP请求报文;

[0046] 其中,所述网络交换转发设备可以通过与用户主机之间已建立的连接接收用户主机发送的ARP请求报文。当该ARP请求报文是对网关的请求报文

[0047] CZ1411187时,该ARP请求报文中源IP地址为用户主机的IP地址,目的IP地址为目标网关的虚IP地址,此外,当该VRRP组网中存在多个虚拟局域网时,该ARP请求报文中还可包括该目标网关所属的VLAN ID。

[0048] 步骤202、当确认所述ARP请求报文目的IP与网关信息表项相匹配时,从所述网关信息表项中记录的接口发送所述ARP请求报文,其中,所述网关信息表项中包括所述VRRP组网中网关的虚IP地址;

[0049] 该网络交换转发设备中可预先设置包含该VRRP组网中网关虚IP地址的网关信息表项。该网络交换转发设备获取ARP请求报文中的目的IP地址后,可以判断该ARP请求报文的目的IP地址与该网关信息表项是否匹配。当确认该ARP请求报文目的IP与网关信息表项相匹配时,可根据该网关信息表项中记录的接口将所述ARP请求报文以单播的方式发送到该目标网关,以使目标网关对该ARP请求报文进行处理。

[0050] 相比于现有技术,本发明的网络交换转发设备在收到用户主机发送的ARP请求后,当确认该ARP请求报文的目的IP与网关信息表项相匹配时,从该网关信息表项中记录的接口发送该ARP请求报文,从而可以避免非法用户收到该ARP请求报文,因此提高了用户主机在VRRP组网中的安全性。

[0051] 在本发明可选的实施例中,网络交换转发设备可以实时对自身的网关信息表项进行维护,下面示例性的例举一种网关信息表项的维护方式。

[0052] 网络交换转发设备可以监听所述VRRP组网中网关之间交互的控制报文,如VRRP报文,并获取该控制报文中携带的报文特征,例如网关虚IP地址、网关接入接口及网关优先级等等,其中,网关优先级可以标识网关的身份,网关接入接口为接收到VRRP控制报文的接口。当网络交换转发设备的网关信息表项中可以包括网关虚IP地址及网关接入接口时,该网络交换转发设备可以先根据该控制报文的网关优先级确定发送该控制报文的网关身份,再根据控制报文中的网关虚IP地址及网关接入接口来判断维护网关信息表项。例如,当该网关为主网关,并且该网络交换转发设备存在与该控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,该网络交换转发设备更新该网关信息表项的老化时间。若网络交换转发设备中不存在与该控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,可根据所述控制报文的报文特征中记录的网关虚IP地址、网关接入接口创建网关信息表项,并为该网关信息表项设置老化时间。当该网关信息表项到达老化时间时,网络交换转发设备可以将该网关信息表项删除。因此网络交换转发设备可以通过监听控制报文来实时更新网关信息表项中的网关信息。

[0053] 当网络交换转发设备根据该控制报文的网关优先级确定发送该控制报文的网关为备用网关,并且该网络交换转发设备存在与该控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,由于在本发明的实施方案中备用网关不处理ARP请求报文,因此该网络交换转发设备可删除备用网关对应的网关信息表项。因此网络交换转发设备可通过监听控制报文来获知当前的主网关,从而将备用网关对应的网关信息表项删除,以减少存储空间占用,提高网络交换转发设备上的空间利用率及报文处理效率。

[0054] 若网络交换转发设备确认该ARP请求报文的目的IP地址与该网关信息表项不匹配时,则可将该ARP请求报文从自身所有接口广播出去,从而可保证该ARP请求报文能够被网关获取并进行处理。

[0055] 为使本发明的目的、技术方案及优点更加清楚明白,以下基于图1的网络架构,对本发明所述方案作进一步地详细说明。

[0056] 可知上述VRRP组网架构中包括交换机、用户主机、非法主机、以及一台主网关和一台备用网关。当用户主机发送ARP请求报文时,假设该ARP请求报文中的目的IP地址为IP1,则该交换机对该ARP请求报文的处理流程如图3所示,其中包括:

[0057] 步骤301、获取该ARP请求报文中的目的IP地址IP1;

[0058] 步骤302、判断该IP1是否与网关信息表项相匹配,若不匹配,则转步骤303;若匹配,则转步骤304;

[0059] 步骤303、将该ARP请求报文从所有接口广播,并结束;

[0060] 步骤304、从网关信息表项中记录的接口发送该ARP请求报文并结束。

[0061] 假设交换机上的网关信息表项与该ARP请求报文的目的IP地址相匹配,交换机可以按照该网关信息表项中记录的接口转发该ARP请求报文,从而可以避免该VRRP组网内的非法主机收到该ARP请求报文,因此可以提高用户主机的安全性。

[0062] 假设上述VRRP组网架构中主网关和备用网关的虚IP地址为IP1,接入接口分别为P1、P2,其中,主网关的接入接口为P1,那么交换机上的网关信息表项如表1所示:

[0063]

	虚IP地址	接入接口	老化时间
--	-------	------	------

1	IP1	P1	60秒
---	-----	----	-----

[0064] 表1

[0065] 其中该网关信息表项记录了主备网关的虚IP地址,接入接口以及表项的老化时间等信息。

[0066] 该交换机维护网关信息表项的处理流程如图4所示,其中包括:

[0067] 步骤401、监听网关之间发送的VRRP报文;

[0068] 步骤402、获取该VRRP报文中的源IP地址、接入接口及网关优先级;

[0069] 其中,VRRP报文中的源IP地址即为VRRP网关的虚IP地址。

[0070] 步骤403、判断网关优先级是否为零,若不为零,则转步骤404;若为零,则转步骤407;

[0071] 其中所述网关优先级为零代表备用网关,网关优先级不为零代表主网关。

[0072] 步骤404、判断是否存在与所述源IP地址及接入接口相匹配的网关信息表项,若不存在则转步骤405,若存在则转步骤406;

[0073] 步骤405、根据所述源IP地址及接入接口创建新的网关信息表项,并为该网关信息表项设置老化时间,并结束;

[0074] 假设该VRRP报文中的源IP地址为IP1,接入接口为P1,经查证与已存的网关信息表项不匹配,因此交换机可根据源IP地址及接入接口创建新的网关信息表项,并设置老化时间,如60秒,网关信息表项如表2所示:

[0075]

虚IP地址	接入接口	老化时间
IP1	P1	60秒

[0076] 表2

[0077] 步骤406、更新该网关信息表项的老化时间,并结束。

[0078] 假设该VRRP报文中的源IP地址为IP1,接入接口为P1,经查证已存的网关信息表项相匹配,如表1中的表项1所示,交换机进一步将表1中的表项1对应的老化时间重置。

[0079] 步骤407、若存在与所述源IP地址及接入接口匹配的网关信息表项,则删除该网关信息表项,并结束;

[0080] 如果交换机接收的VRRP报文的网关优先级为零,说明该VRRP报文来自备用网关,因此可以根据VRRP报文中的源IP地址及接入接口信息查找匹配的网关信息表项,然后将该网关信息表项删除。

[0081] 经过上述维护方式,可以保证交换机中网关信息表项根据网关的状态实时更新。

[0082] 基于相同的构思,本发明还提供一种报文转发装置,所述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,本发明的报文转发装置作为一个逻辑意义上的装置,是通过其所在网络转发设备的CPU将存储器中对应的计算机程序指令读取后运行而成。

[0083] 请参考图5及图6,是本发明一种示例性实施方式中的一种报文转发装置600,所述装置应用于VRRP组网中的网络交换转发设备,所述装置基本运行环境包括CPU,存储器以及其他硬件,从逻辑层面上来看,所述装置600包括:

[0084] 请求接收单元601,用于接收用户主机发送的ARP请求报文;

[0085] 报文发送单元602,用于在确认所述ARP请求报文目的IP与网关信息表项相匹配时,从所述网关信息表项中记录的接口发送所述ARP请求报文,其中,所述网关信息表项中包括所述VRRP组网中网关的虚IP地址。

[0086] 可选的,所述装置还可包括:

[0087] 报文监听单元603,用于监听所述VRRP组网中网关之间交互的控制报文;

[0088] 特征获取单元604,用于获取所述控制报文中的报文特征,所述控制报文的报文特征包括网关虚IP地址、网关优先级及网关接入接口;

[0089] 表项修改单元605,用于根据所述控制报文的报文特征建立或更新所述网关信息表项。

[0090] 可选的,所述网关信息表项还包括网关接入接口,所述表项修改单元605,可包括:

[0091] 身份判断子单元6051,用于根据所述网关优先级判断所述网关的身份;

[0092] 表项更新子单元6052,用于在所述网关为主网关,且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,更新所述网关信息表项的老化时间;

[0093] 表项建立子单元6053,用于在所述网关为主网关,且不存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,根据所述控制报文的网关虚IP地址及网关接入接口建立网关信息表项,并为该网关信息表项设置老化时间。

[0094] 可选的,所述装置还可包括:

[0095] 表项删除单元606,用于在所述网关为备用网关,且存在与所述控制报文的网关虚IP地址及网关接入接口相匹配的网关信息表项时,删除该网关信息表项。

[0096] 可选的,所述报文发送单元602,还用于在确认所述ARP请求报文目的IP与网关信息表项不匹配时,将所述ARP请求报文从所有接口广播。

[0097] 由此可见,本发明的网络交换转发设备在收到用户主机发送的ARP请求后,当确认该ARP请求报文的目的IP与网关信息表项相匹配时,从该网关信息表项中记录的接口发送该ARP请求报文,从而可以避免非法用户收到该ARP请求报文,因此提高了用户主机在VRRP组网中的安全性。

[0098] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明保护的范围之内。

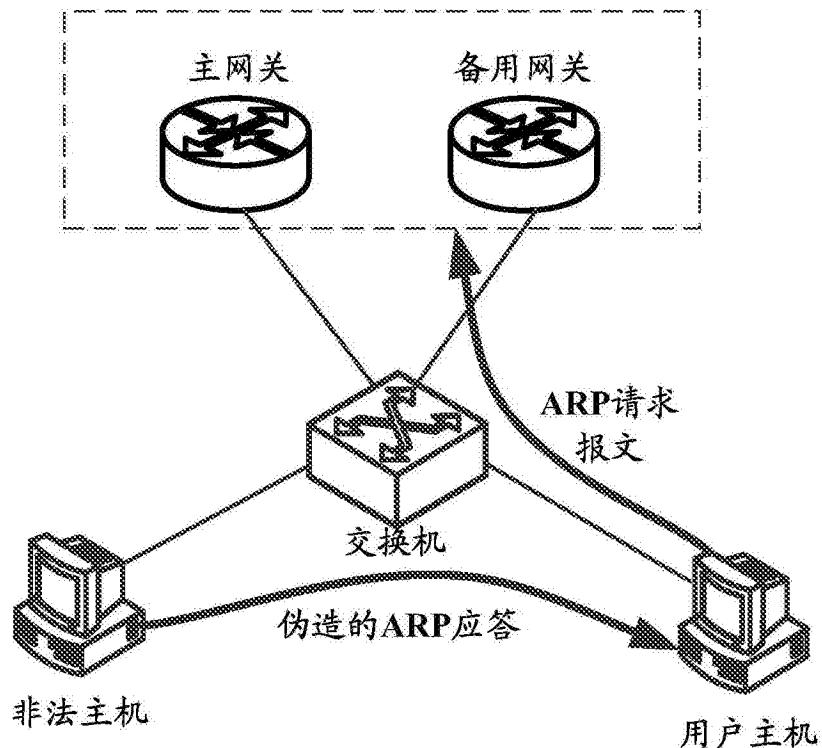


图1

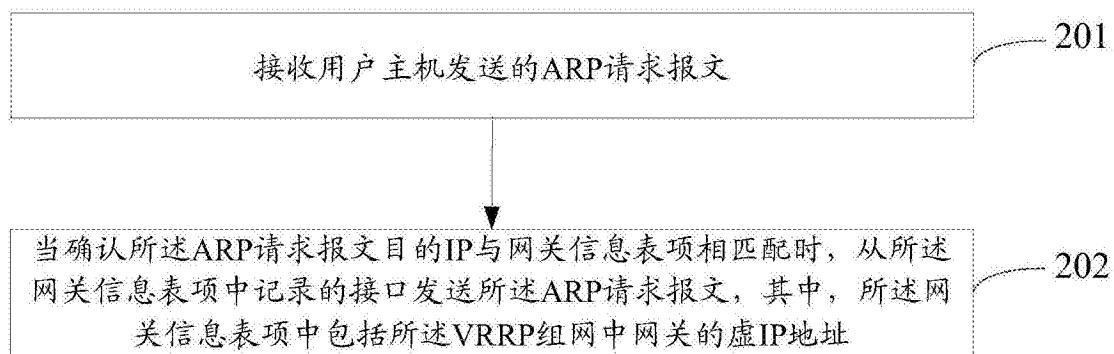
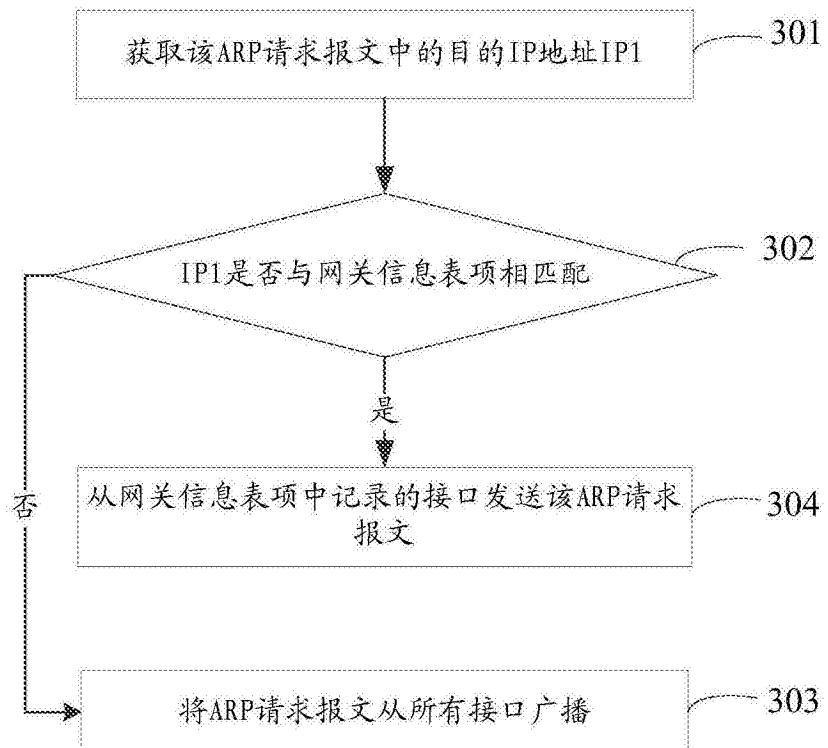


图2



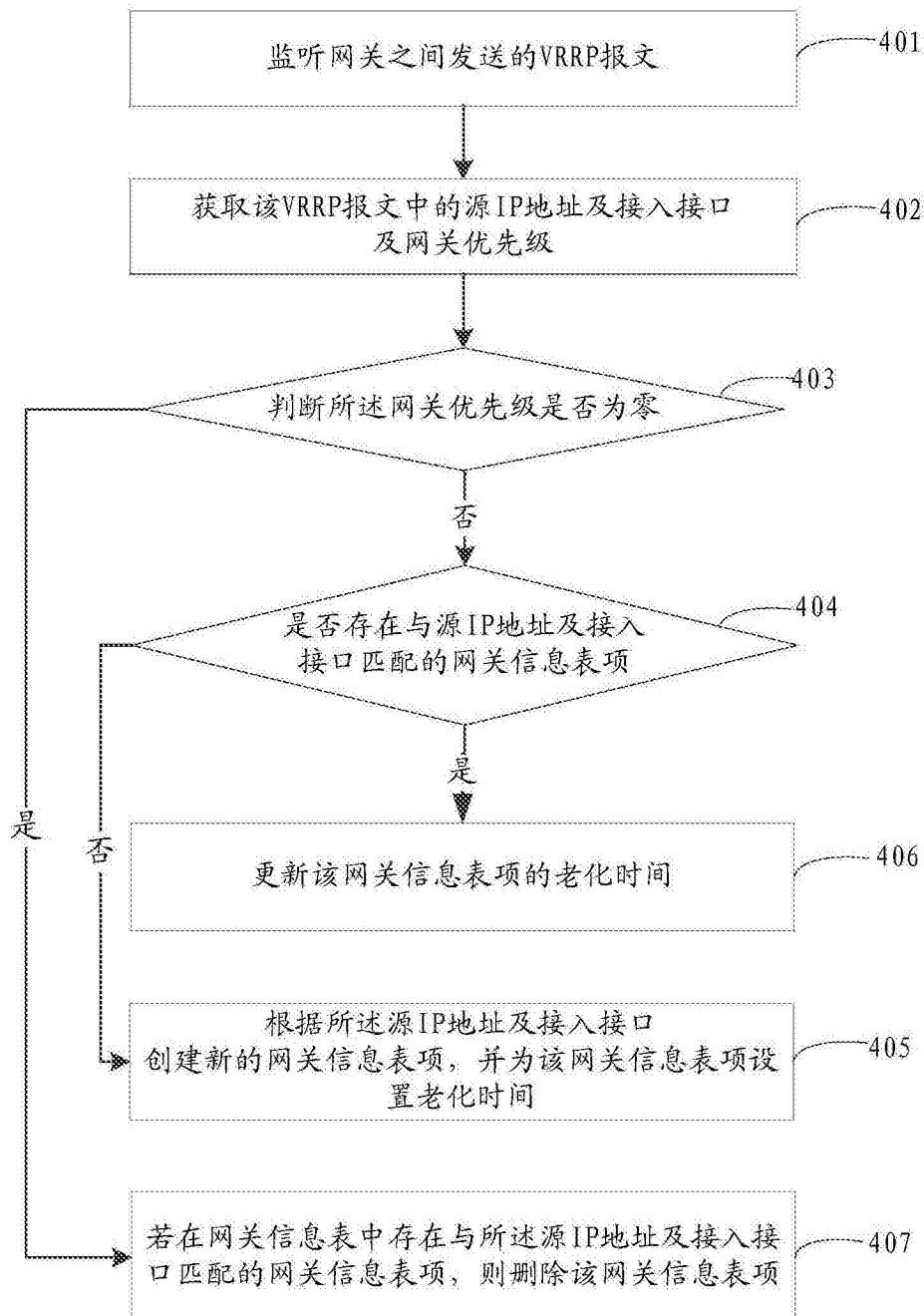


图4

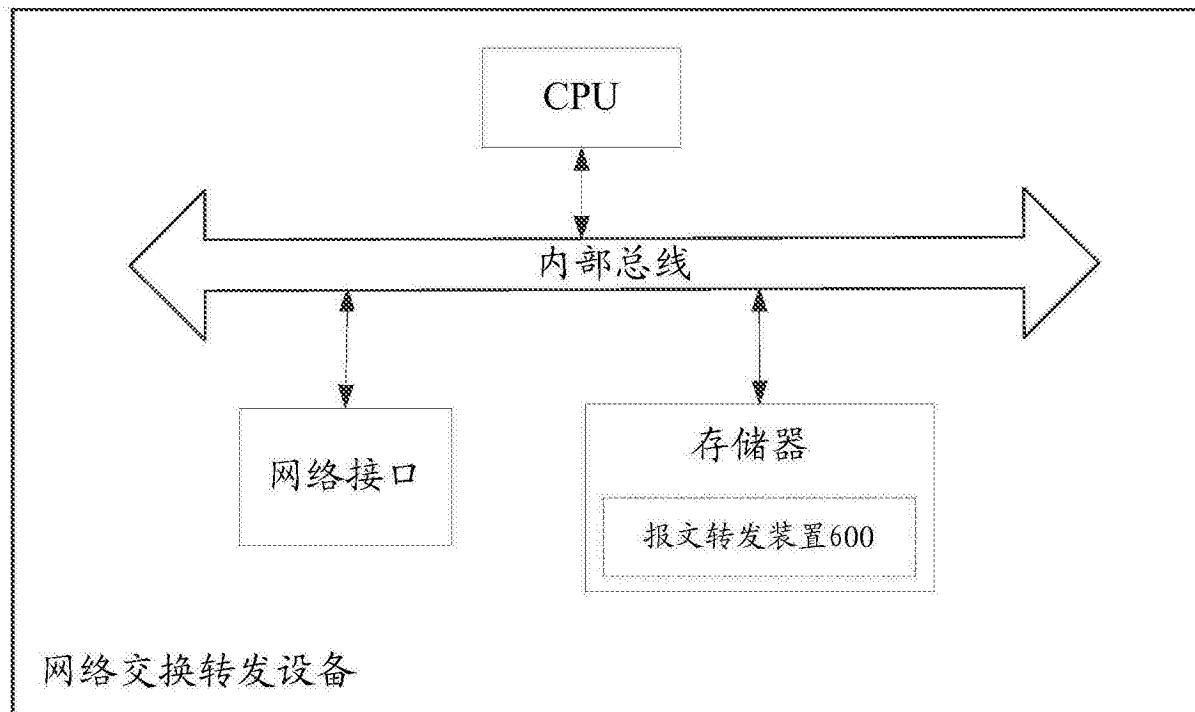


图5

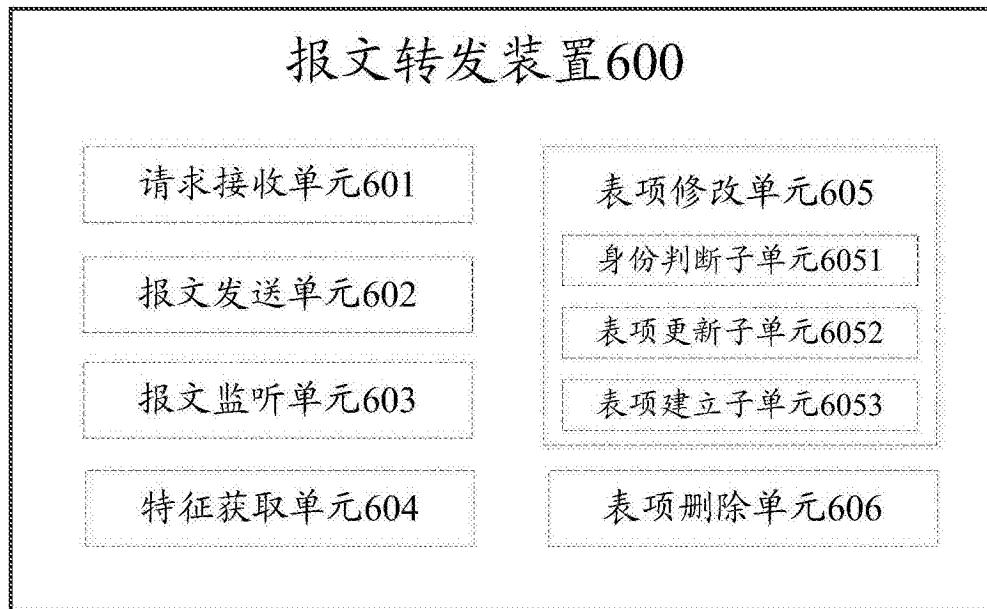


图6