



(12) 发明专利

(10) 授权公告号 CN 111327523 B

(45) 授权公告日 2022.03.22

(21) 申请号 202010130487.0

H04L 45/02 (2022.01)

(22) 申请日 2020.02.28

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 1764193 A, 2006.04.26

申请公布号 CN 111327523 A

US 2017063672 A1, 2017.03.02

CN 102347905 A, 2012.02.08

(43) 申请公布日 2020.06.23

US 9369372 B1, 2016.06.14

(73) 专利权人 深信服科技股份有限公司

CN 108989085 A, 2018.12.11

地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋

审查员 朱星杰

(72) 发明人 乔鹏

(74) 专利代理机构 北京派特恩知识产权代理有限公司 11270

代理人 贾伟 张颖玲

(51) Int. Cl.

H04L 45/24 (2022.01)

H04L 45/28 (2022.01)

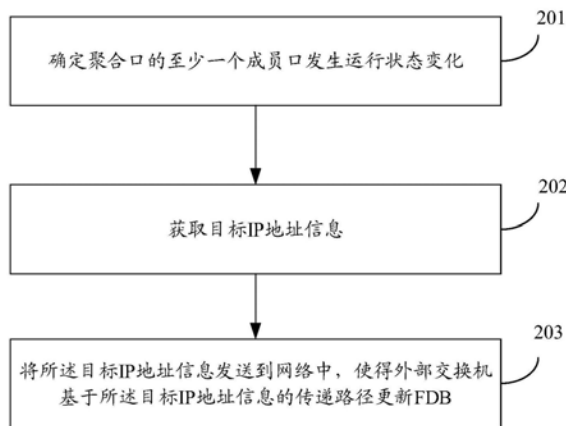
权利要求书2页 说明书8页 附图4页

(54) 发明名称

基于聚合口的网络保护方法、装置、网络设备及存储介质

(57) 摘要

本发明公开了一种基于聚合口的网络保护方法、装置、网络设备及存储介质。其中,该方法包括:确定聚合口的至少一个成员口发生运行状态变化;获取目标IP地址信息;将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新FDB。本发明实施例中,外部交换机基于目标IP地址信息的传递路径更新FDB,能够在聚合口的成员口发生运行状态变化后,及时得到正确的FDB,保证网络的畅通。



1. 一种基于聚合口的网络保护方法,其特征在于,包括:
 - 确定聚合口的至少一个成员口发生运行状态变化;
 - 获取目标互联网协议IP地址信息,所述目标IP地址信息为与聚合口相连的虚拟环境中虚拟终端设备的IP地址信息;
 - 将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新转发表FDB;
 - 所述将所述目标IP地址信息发送到网络中,包括:
 - 控制所述目标IP地址信息对应的终端设备生成并发送免费地址解析协议ARP报文。
2. 根据权利要求1所述的方法,其特征在于,所述确定聚合口的至少一个成员口发生运行状态变化,包括:
 - 确定聚合口的至少一个成员口由工作UP状态切换为故障DOWN状态或者由DOWN状态恢复为UP状态。
3. 根据权利要求1所述的方法,其特征在于,所述获取目标IP地址信息,包括:
 - 根据与所述聚合口相连的分布式虚拟交换机DVS确定目标终端设备,获取所述目标终端设备的IP地址信息,将所述目标终端设备的IP地址信息作为所述目标IP地址信息;其中,所述目标终端设备为连接至所述DVS上的一个或者多个终端设备。
4. 根据权利要求1所述的方法,其特征在于,所述获取目标IP地址信息,包括:
 - 获取与所述聚合口相连的分布式虚拟交换机DVS的FDB中的目标媒体接入控制MAC地址,基于所述目标MAC地址确定所述目标IP地址信息;其中,所述目标MAC地址为所述DVS的FDB中除与所述聚合口相连的端口之外的其他端口对应的MAC地址。
5. 根据权利要求1所述的方法,其特征在于,所述聚合口包括:主成员口和备用成员口,其中,所述主成员口连接外部的第一交换机,所述备用成员口连接外部的第二交换机,所述第一交换机与所述第二交换机级联连接;所述确定聚合口的至少一个成员口发生运行状态变化,包括:
 - 确定所述主成员口由UP状态切换为DOWN状态或者由DOWN状态恢复为UP状态。
6. 一种基于聚合口的网络保护装置,其特征在于,包括:
 - 确定模块,用于确定聚合口的至少一个成员口发生运行状态变化;
 - 获取模块,用于获取目标IP地址信息,所述目标IP地址信息为与聚合口相连的虚拟环境中虚拟终端设备的IP地址信息;
 - 报文发送模块,用于将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新FDB;
 - 所述将所述目标IP地址信息发送到网络中,包括:
 - 控制所述目标IP地址信息对应的终端设备生成并发送免费地址解析协议ARP报文。
7. 一种网络设备,其特征在于,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,其中,
 - 所述处理器,用于运行计算机程序时,执行权利要求1至5任一项所述方法的步骤。
8. 一种网络系统,其特征在于,包括外部交换机和权利要求7所述的网络设备,所述外部交换机包括级联连接的至少两个交换机,所述至少两个交换机分别连接至所述网络设备的聚合口上的成员口。

9. 一种存储介质,所述存储介质上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时,实现权利要求1至5任一项所述方法的步骤。

基于聚合口的网络保护方法、装置、网络设备及存储介质

技术领域

[0001] 本发明涉及通信网络技术领域,尤其涉及一种基于聚合口的网络保护方法、装置、网络设备及存储介质。

背景技术

[0002] 链路聚合(Link Aggregation)是一种将多个物理端口捆绑成一个逻辑端口(即聚合口)的技术,可以将多个物理连接当作一个单一的逻辑连接来处理,即将多种网卡虚拟成一张网卡。聚合口的多个成员口可以支持多种模式,比如,负载均衡模式、主备切换模式。

[0003] 相关技术中,当聚合口的成员口发生变化时,往往导致网络出现断网的现象。

发明内容

[0004] 有鉴于此,本发明实施例提供了一种基于聚合口的网络保护方法、装置、网络设备及存储介质,旨在聚合口的成员口发生变化时,保障网络的畅通。

[0005] 本发明实施例的技术方案是这样实现的:

[0006] 本发明实施例提供了一种基于聚合口的网络保护方法,包括:

[0007] 确定聚合口的至少一个成员口发生运行状态变化;

[0008] 获取目标互联网协议(IP)地址信息;

[0009] 将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新转发表(Forwarding DataBase,FDB)。

[0010] 本发明实施例还提供了一种基于聚合口的网络保护装置,包括:

[0011] 确定模块,用于确定聚合口的至少一个成员口发生运行状态变化;

[0012] 获取模块,用于获取目标IP地址信息;

[0013] 报文发送模块,用于将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新FDB。

[0014] 本发明实施例又提供了一种网络设备,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,其中,所述处理器,用于运行计算机程序时,执行本发明任一实施例所述方法的步骤。

[0015] 本发明实施例还提供了一种网络系统,包括外部交换机和前述实施例所述的网络设备,所述外部交换机包括级联连接的至少两个交换机,所述至少两个交换机分别连接至所述网络设备的聚合口上的成员口。

[0016] 本发明实施例又提供了一种存储介质,所述存储介质上存储有计算机程序,所述计算机程序被处理器执行时,实现本发明任一实施例所述方法的步骤。

[0017] 本发明实施例提供的技术方案,确定聚合口的至少一个成员口发生运行状态变化,获取目标IP地址信息,将所述目标IP地址信息发送到网络中,使得外部交换机基于目标IP地址信息的传递路径更新FDB,能够在聚合口的成员口发生运行状态变化后,及时得到正确的FDB,保证网络的畅通。

附图说明

- [0018] 图1为相关技术中基于聚合口的网络拓扑结构示意图；
 [0019] 图2为本发明实施例基于聚合口的网络保护方法的流程示意图；
 [0020] 图3为本发明应用实施例基于聚合口的网络保护方法的流程示意图；
 [0021] 图4为本发明实施例基于聚合口的网络保护装置的结构示意图；
 [0022] 图5为本发明实施例网络设备的结构示意图；
 [0023] 图6为本发明实施例网络系统的结构示意图。

具体实施方式

- [0024] 下面结合附图及实施例对本发明再作进一步详细的描述。
 [0025] 除非另有定义，本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文中在本发明的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本发明。
 [0026] 相关技术中，当聚合口的成员口发生变化时，往往导致网络出现断网的现象。比如，实际应用中，如图1所示，客户端(PC) 101通过外部交换机102连接网络设备，其中，外部交换机102包括用于支持主备模式的两个交换机sw1、sw2，sw1与sw2级联连接，这里，级联连接是指sw1与sw2在逻辑上是各自独立的，不同于堆叠模式的交换机。网络设备包括聚合口103、DVS(Distributed Virtual Switch, 分布式虚拟交换机) 104及连接DVS 104的虚拟终端设备，比如，虚拟机vm1、vm2、虚拟路由器vr1等。这里，分布式虚拟交换机是管理多台主机上的虚拟交换机(基于软件的虚拟交换机或智能网卡虚拟交换机)的虚拟网络管理方式，包括对主机的物理端口和虚拟机虚拟端口的管理。分布式虚拟机交换机可以保证虚拟机在主机之间迁移时网络配置的一致性。
 [0027] 如图1所示，外部环境的PC持续访问虚拟环境中的虚拟机vm1。
 [0028] 流量走向以及交换机建表顺序如下：
 [0029] PC访问vm1，首先要知道vm1的MAC(Media Access Control, 媒体接入控制)地址。通过ARP(Address Resolution Protocol, 地址解析协议)学习vm1的MAC地址。
 [0030] PC-->sw2时，报文发生flood(泛洪)。sw2学习到一条新的FDB表项。

sw2 FDB

[0031] MAC port

AA-BB-CC-DD-EE-FF sw2-1

[0032] 由sw2-->sw1时，报文继续flood。Sw1学习到一条新的FDB表项。

sw1 FDB

[0033] MAC port

AA-BB-CC-DD-EE-FF sw1-1

[0034] 假定聚合口103中eth0为主口，eth1为备用口，则由sw2-->eth1的链路不通。

[0035] 报文由sw1-->eth0，通过聚合口103，到达DVS 104。DVS 104学习到一条新的FDB表

项。

DVS FDB

[0036] MAC port

AA-BB-CC-DD-EE-FF dvs-1

[0037] DVS 104继续flood,报文到达vm1。vm1回报文。DVS 104会学习到一条新的FDB表项。

DVS FDB

[0038] MAC port

AA-BB-CC-DD-EE-FF dvs-1

AA-BB-CC-DD-EE-11 dvs-2

[0039] 回包的报文,由DVS 104经过聚合口103,走到外部环境的交换机sw1上。sw1会学习到一条新的FDB表项。

sw1 FDB

[0040] MAC port

AA-BB-CC-DD-EE-FF sw1-1

AA-BB-CC-DD-EE-11 sw1-2

[0041] 回包的报文,由sw1-->sw2,sw2学习到一条新的FDB表项。

sw2 FDB

[0042] MAC port

AA-BB-CC-DD-EE-FF sw2-1

AA-BB-CC-DD-EE-11 sw2-3

[0043] 由sw2-->PC,经由sw2-1到达。这样,后续报文就畅通了。

[0044] 但是当物理口eth0发生故障,由UP-->DOWN,那么聚合口104根据切换原则,会切换到备口eth1上。但是这时,外部交换机sw2中的FDB表项没有更新。

sw2 FDB

[0045] MAC port

AA-BB-CC-DD-EE-FF sw2-1

AA-BB-CC-DD-EE-11 sw2-3(无效)

[0046] 所以,由PC去往vm1的流量会继续将流量送给交换机sw1,但是sw1去往eth0的通路已经断了,需要在交换机sw1上flood来找一条新路,但是由于交换机flood的原则,除了sw1通往sw2的口,向其它口flood都不能到达vm1。所以这时会发生断网的现象。

[0047] 因此,当聚合口103的成员口发生变化时,如果没有将这种变化通知外部网络,外部网络残留的无效FDB表项,导致网络不通。

[0048] 基于此,在本发明的各种实施例中,当聚合口的至少一个成员口发生运行状态变化时,及时将变化通知至外部环境,使得外部环境中的外部交换机能够及时更新FDB,保证网络的畅通。这里,外部环境是相对于与聚合口相连的内部虚拟环境而言。

[0049] 本发明实施例提供了一种基于聚合口的网络保护方法,如图2所示,该方法包括:

[0050] 步骤201,确定聚合口的至少一个成员口发生运行状态变化;

[0051] 步骤202,获取目标IP地址信息;

[0052] 步骤203,将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新FDB。

[0053] 这里,所述确定聚合口的至少一个成员口发生运行状态变化,包括:确定聚合口的至少一个成员口由工作(UP)状态切换为故障(DOWN)状态或者由DOWN状态恢复为UP状态。目标IP地址信息是指与聚合口相连的内部虚拟环境中虚拟终端设备的IP地址信息。外部交换机可以基于所述目标IP地址信息的传递路径更新本地的FDB,从而能够在聚合口的成员口发生运行状态变化后,及时更新外部网络中残留的无效FDB表项,得到正确的FDB,保证网络的畅通。

[0054] 在一实施例中,所述获取目标IP地址信息,包括:

[0055] 根据与所述聚合口相连的DVS确定目标终端设备,获取所述目标终端设备的IP地址信息,将所述目标终端设备的IP地址信息作为所述目标IP地址信息;其中,所述目标终端设备为连接至所述DVS上的一个或者多个终端设备。

[0056] 在一应用示例中,如图1所示,可以将连接DVS 104的vm1、vm2及vr1均为作为目标终端设备,获取vm1、vm2及vr1的IP地址信息作为目标IP地址信息。从而可以对连接DVS的各终端设备更新FDB,确保网络的畅通。

[0057] 在另一实施例中,所述获取目标IP地址信息,包括:

[0058] 获取与所述聚合口相连的DVS的FDB中的目标MAC地址,基于所述目标MAC地址确定所述目标IP地址信息;其中,所述目标MAC地址为所述DVS的FDB中除与所述聚合口相连的端口之外的其他端口对应的MAC地址。

[0059] 在一应用示例中,可以根据DVS的FDB中存在的MAC地址,选取除dvs-1以外的其他端口对应的MAC地址作为目标MAC地址,基于该目标MAC地址确定目标IP地址信息。如确定vm1的IP地址:4.3.2.2作为目标IP地址信息,这样可以准确地选择IP地址信息,减少报文传递。

[0060] 在一实施例中,所述将所述目标IP地址信息发送到网络中,包括:

[0061] 控制所述目标IP地址对应的终端设备生成并发送免费ARP报文。

[0062] 这里,免费ARP报文是指,报文发送端IP地址和目的IP地址都是本机IP地址,报文源MAC地址是本机MAC地址,报文的目的地MAC地址是广播地址。这样,外部交换机接收到相应终端设备的免费ARP报文,就可以在本地的FDB中更新相应终端设备对应的FDB表项,即MAC地址和端口的对应关系。

[0063] 在一实施例中,所述聚合口包括:主成员口和备用成员口,其中,所述主成员口连接外部的第一交换机,所述备用成员口连接外部的第二交换机,所述第一交换机与所述第

二交换机级联连接;所述确定聚合口的至少一个成员口发生运行状态变化,包括:确定所述主成员口由UP状态切换为DOWN状态或者由DOWN状态恢复为UP状态。

[0064] 实际应用中,若聚合口的主成员口由UP切换为DOWN,则通过获取目标IP地址信息,并控制目标IP地址对应的终端设备生成并发送免费ARP报文,使得外部交换机能够及时更新FDB,保证网络畅通。若聚合口的主成员口由DOWN切换为UP,同理,可以通过获取目标IP地址信息,并控制目标IP地址对应的终端设备生成并发送免费ARP报文,及时恢复聚合口的抢占模式。

[0065] 下面结合应用实施例对本发明再作进一步详细的描述。

[0066] 本应用实施例的网络拓扑结构如图1所示,当聚合口的成员口eth0由UP切换为DOWN后,需要将内部虚拟环境中的部分IP地址信息,同步到外部环境中,具体如图3所示,包括:

[0067] 步骤301,确定聚合口的成员口发生运行状态变化;

[0068] 当聚合口的成员口eth0由UP切换为DOWN时,控制器(controller)可以检测到此事件,从而确定聚合口的成员口发生运行状态变化。这里,控制器在内部虚拟环境中,能够获取内部虚拟环境中的配置。

[0069] 步骤302,通过控制器检测需要告知外部环境的IP地址信息;

[0070] 这里,控制器获取与聚合口直接相连的分布式虚拟交换机,将分布式虚拟交换机中存在的FDB表项的目标MAC地址进行IP地址查询,得到相应的IP地址信息作为目标IP地址信息。这里,目标MAC地址为分布式虚拟交换机的FDB中除与所述聚合口相连的端口之外的其他端口对应的MAC地址。比如,可以基于dvs-2的MAC地址:AA-BB-CC-DD-EE-11,得到目标IP地址:4.3.2.2。

[0071] 步骤303,控制器将需要知会的IP地址信息发送免费ARP报文;

[0072] 控制器基于目标IP地址:4.3.2.2,确定vm1需要发送免费ARP报文,控制vm1发送免费ARP报文。

[0073] 步骤304,外部环境中的交换机,收到免费ARP报文,更新FDB。

[0074] 实际应用中,vm1发送免费ARP报文的传递路径为:vm1-->DVS-->eth1-->sw2。sw2学习到正确的FDB表项,如下:

sw2 FDB

	MAC	port
[0075]	AA-BB-CC-DD-EE-FF	sw2-1
	AA-BB-CC-DD-EE-11	sw2-3
	AA-BB-CC-DD-EE-11	sw2-2

[0076] 这样,PC后续访问虚拟机vm1的路径为:PC-->sw2-->eth1-->DVS-->vm1,保证了网络畅通。

[0077] 为了实现本发明实施例的方法,本发明实施例还提供一种基于聚合口的网络保护装置,该基于聚合口的网络保护装置与上述基于聚合口的网络保护方法对应,上述基于聚合口的网络保护方法实施例中的各步骤也完全适用于本基于聚合口的网络保护装置实施

例。

[0078] 如图4所示,该基于聚合口的网络保护装置包括:确定模块401、获取模块402、报文发送模块403,其中,确定模块401用于确定聚合口的至少一个成员口发生运行状态变化;获取模块402用于获取目标IP地址信息;报文发送模块403用于将所述目标IP地址信息发送到网络中,使得外部交换机基于所述目标IP地址信息的传递路径更新FDB。

[0079] 在一实施例中,确定模块401具体用于:确定聚合口的至少一个成员口由UP状态切换为DOWN状态或者由DOWN状态恢复为UP状态。

[0080] 在一实施例中,获取模块402具体用于:根据与所述聚合口相连的DVS确定目标终端设备,获取所述目标终端设备的IP地址信息,将所述目标终端设备的IP地址信息作为所述目标IP地址信息;其中,所述目标终端设备为连接至所述DVS上的一个或者多个终端设备。

[0081] 在一实施例中,获取模块402具体用于:获取与所述聚合口相连的DVS的FDB中的目标MAC地址,基于所述目标MAC地址确定所述目标IP地址信息;其中,所述目标MAC地址为所述DVS的FDB中除与所述聚合口相连的端口之外的其他端口对应的MAC地址。

[0082] 在一实施例中,报文发送模块403具体用于:控制所述目标IP地址对应的终端设备生成并发送免费ARP报文。

[0083] 在一实施例中,所述聚合口包括:主成员口和备用成员口,其中,所述主成员口连接外部的第一交换机,所述备用成员口连接外部的第二交换机,所述第一交换机与所述第二交换机级联连接。确定模块401具体用于:确定所述主成员口由UP状态切换为DOWN状态或者由DOWN状态恢复为UP状态。

[0084] 实际应用时,确定模块401、获取模块402及报文发送模块403,可以由基于聚合口的网络保护装置中的处理器来实现。当然,处理器需要运行存储器中的计算机程序来实现它的功能。

[0085] 需要说明的是:上述实施例提供的基于聚合口的网络保护装置在进行基于聚合口的网络保护时,仅以上述各程序模块的划分进行举例说明,实际应用中,可以根据需要而将上述处理分配由不同的程序模块完成,即将装置的内部结构划分成不同的程序模块,以完成以上描述的全部或者部分处理。另外,上述实施例提供的基于聚合口的网络保护装置与基于聚合口的网络保护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。

[0086] 基于上述程序模块的硬件实现,且为了实现本发明实施例的方法,本发明实施例还提供一种网络设备。图5仅仅示出了该网络设备的示例性结构而非全部结构,根据需要可以实施图5示出的部分结构或全部结构。

[0087] 如图5所示,本发明实施例提供的网络设备500包括:至少一个处理器501、存储器502、用户接口503和至少一个网络接口504。网络设备500中的各个组件通过总线系统505耦合在一起。可以理解,总线系统505用于实现这些组件之间的连接通信。总线系统505除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图5中将各种总线都标为总线系统505。

[0088] 其中,用户接口503可以包括显示器、键盘、鼠标、轨迹球、点击轮、按键、按钮、触感板或者触摸屏等。网络接口504包括聚合口,网络设备通过聚合口与外部环境中的通信设备

连接。

[0089] 本发明实施例中的存储器502用于存储各种类型的数据以支持网络设备的操作。这些数据的示例包括：用于在网络设备上操作的任何计算机程序。

[0090] 本发明实施例揭示的基于聚合口的网络保护方法可以应用于处理器501中，或者由处理器501实现。处理器501可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，基于聚合口的网络保护方法的各步骤可以通过处理器501中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器501可以是通用处理器、数字信号处理器(DSP, Digital Signal Processor)，或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器501可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本发明实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器502，处理器501读取存储器502中的信息，结合其硬件完成本发明实施例提供的基于聚合口的网络保护方法的步骤。

[0091] 在示例性实施例中，网络设备可以被一个或多个应用专用集成电路(ASIC, Application Specific Integrated Circuit)、DSP、可编程逻辑器件(PLD, Programmable Logic Device)、复杂可编程逻辑器件(CPLD, Complex Programmable Logic Device)、FPGA、通用处理器、控制器、微控制器(MCU, Micro Controller Unit)、微处理器(Microprocessor)、或者其他电子元件实现，用于执行前述方法。

[0092] 可以理解，存储器502可以是易失性存储器或非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(ROM, Read Only Memory)、可编程只读存储器(PROM, Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM, Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM, Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM, ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM, Compact Disc Read-Only Memory)；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM, Random Access Memory)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(SRAM, Static Random Access Memory)、同步静态随机存取存储器(SSRAM, Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM, Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM, Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM, Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM, Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM, SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM, Direct Rambus Random Access Memory)。本发明实施例描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

[0093] 本发明实施例还提供一种网络系统，如图6所示，包括外部交换机600和前述实施例所述的网络设备500，所述外部交换机600包括级联连接的至少两个交换机，所述至少两

个交换机分别连接至所述网络设备500的聚合口上的成员口。比如,外部交换机600包括交换机sw1、sw2,聚合口包括成员口eth0、eth1,其中,sw1连接eth0,sw2连接eth1,sw1与sw2级联连接。

[0094] 在示例性实施例中,本发明实施例还提供了一种存储介质,即计算机存储介质,具体可以是计算机可读存储介质,例如包括存储计算机程序的存储器502,上述计算机程序可由网络设备的处理器501执行,以完成本发明实施例方法所述的步骤。计算机可读存储介质可以是ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或CD-ROM等存储器。

[0095] 需要说明的是:“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。

[0096] 另外,本发明实施例所记载的技术方案之间,在不冲突的情况下,可以任意组合。

[0097] 以上所述,仅为本发明的具体实施方式,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以权利要求的保护范围为准。

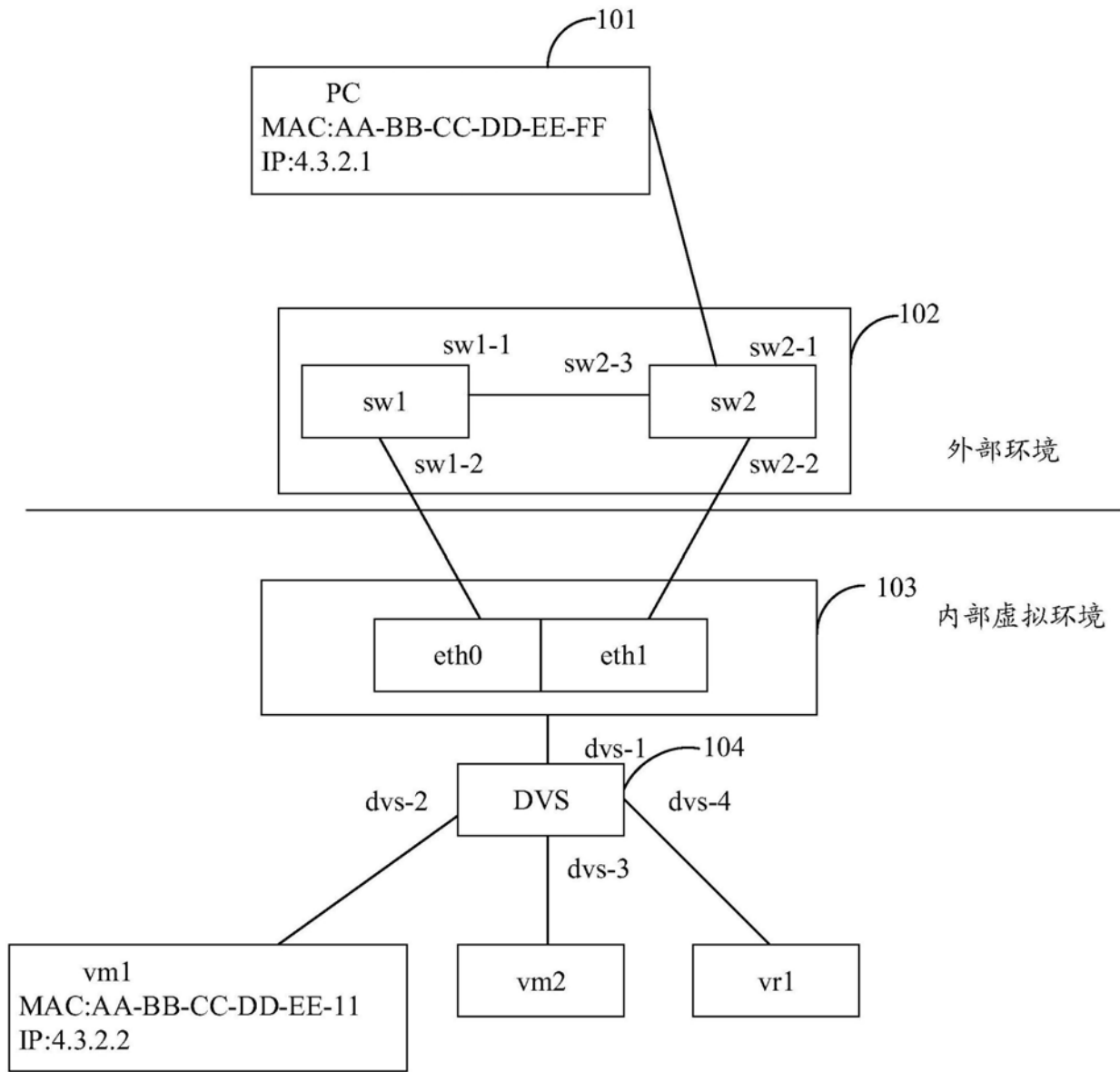


图1

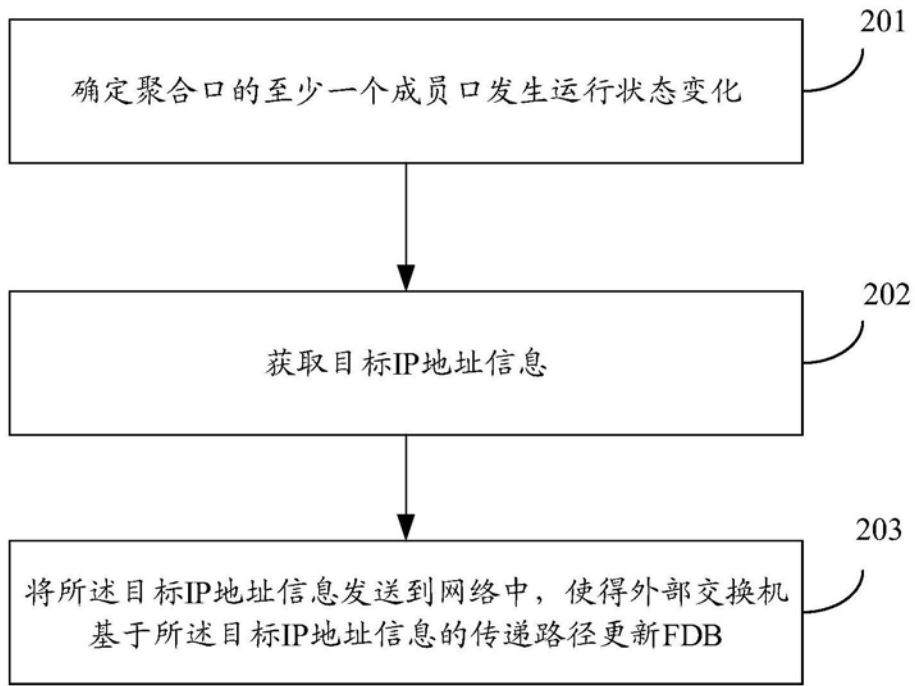


图2

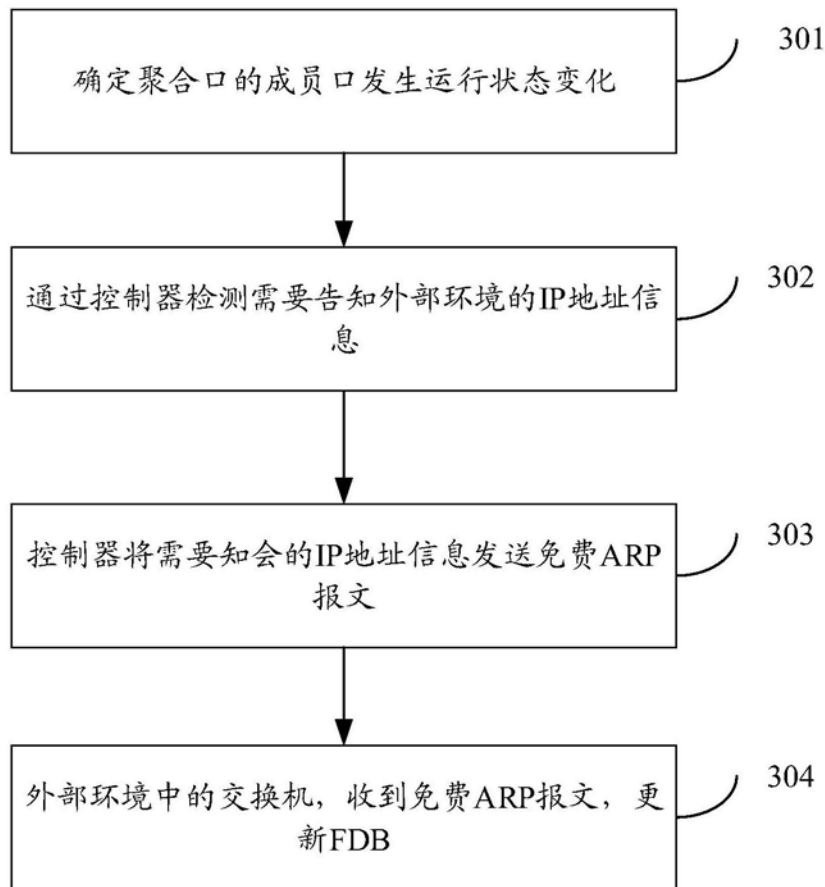


图3



图4

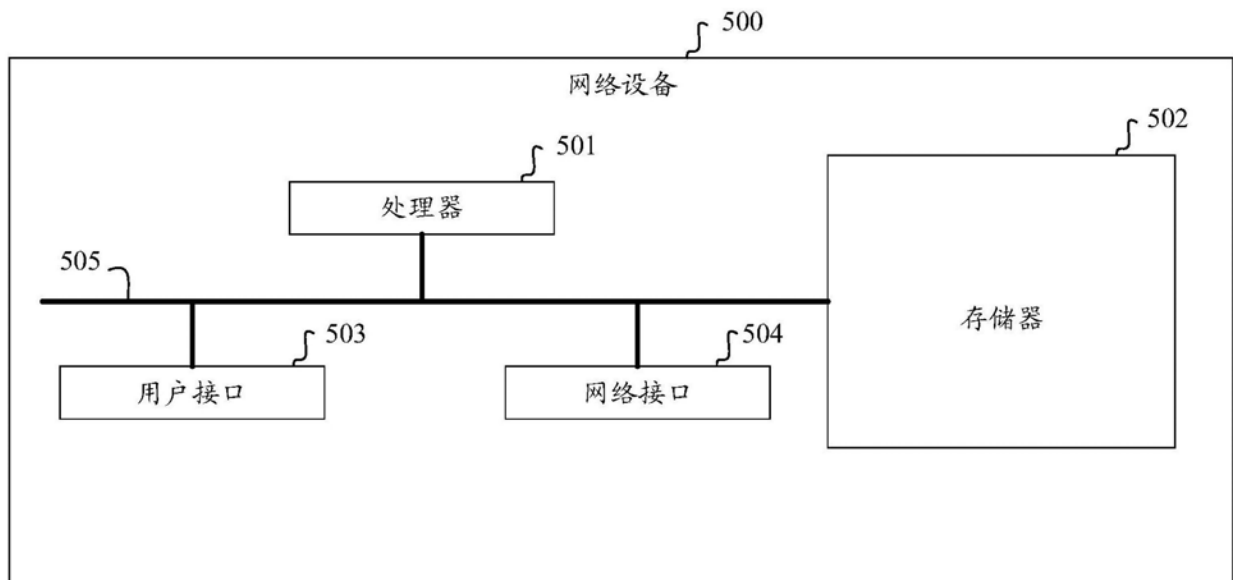


图5

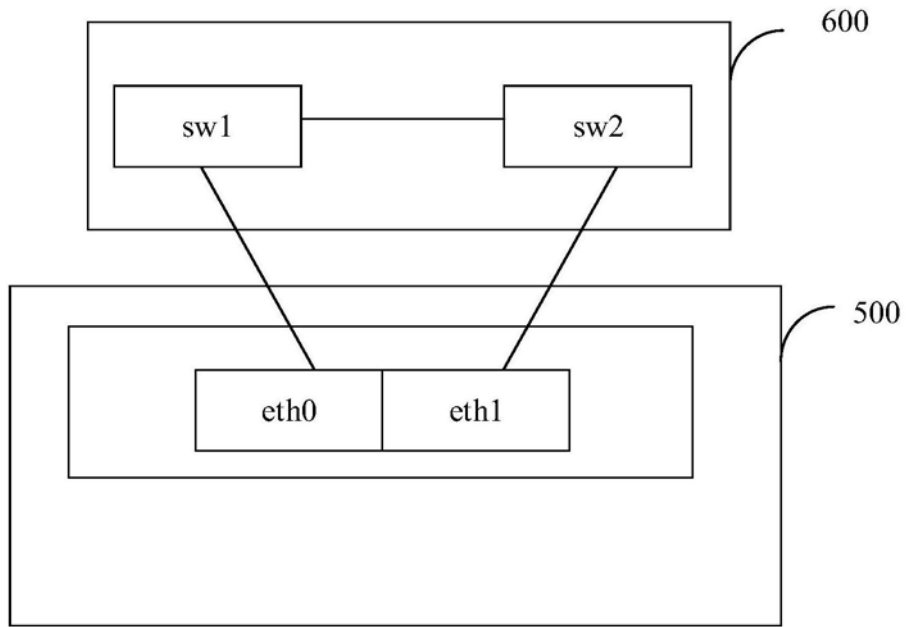


图6