(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103595711 A
(43)申请公布日 2014.02.19

(21)申请号 201310546098.6

(22)申请日 2013.11.06

(71)申请人 神州数码网络(北京)有限公司
地址 100085 北京市海淀区上地九街 9 号数码科技广场一段三层 A 区
申请人 上海神州数码有限公司

(72)发明人 梁小冰 向阳朝 陈翔

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 胡彬

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/947(2013.01)

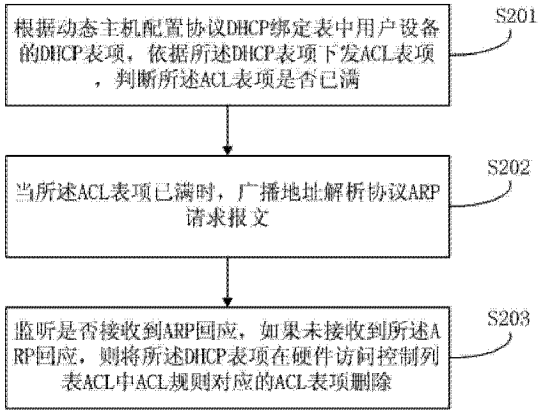
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种调整安全接入的方法及交换机

(57)摘要

本发明公开了一种调整安全接入的方法及交换机，所述方法包括：根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据 DHCP 表项下发 ACL 表项，判断 ACL 表项是否已满；当 ACL 表项已满时，广播地址解析协议 ARP 请求报文；监听是否接收到 ARP 回应，如果未接收到 ARP 回应，则将 DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。通过本发明公开的一种调整安全接入的方法及交换机，可以更多 DHCP 用户设备的接入要求，提高了交换机访问控制列表的利用率。



CN 103595711 A

1. 一种调整安全接入的方法，其特征在于，包括：

根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满；

当所述 ACL 表项已满时，广播地址解析协议 ARP 请求报文，其中，所述 ARP 请求报文的发送端的 IP 地址和目标端的 IP 地址为所述 DHCP 表项中所述用户设备的 IP 地址，所述 ARP 请求报文的发送端的媒体访问控制 MAC 地址为所述 DHCP 表项中所述用户设备的 MAC 地址，所述 ARP 请求报文的目标端的 MAC 地址为广播地址；

监听是否接收到 ARP 回应，如果未接收到所述 ARP 回应，则将所述 DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。

2. 根据权利要求 1 所述的调整安全接入的方法，其特征在于，在所述根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满之前，还包括：

接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文，其中，所述 DHCP 请求报文包括 DHCP 探听过程的 MAC 地址、接入端口号和虚拟局域网 VLAN 号，所述 DHCP 服务器的回应报文包括 DHCP 探听过程的 IP 地址、租期、网关和域名系统 DNS 号；

根据所述用户设备的 DHCP 请求报文和所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项；

根据所述 DHCP 表项，生成 ACL 表项。

3. 根据权利要求 2 所述的调整安全接入的方法，其特征在于，在所述接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文之前，还包括：

使能交换机的 DHCP 探听的监听功能；

下发一条 DHCP 报文重定向至交换机 CPU 的 ACL 规则，同时下发一条默认不转发所有报文的 ACL 规则。

4. 根据权利要求 2 所述的调整安全接入的方法，其特征在于，所述根据所述用户设备的 DHCP 请求报文和所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项，包括：

将所述 DHCP 请求报文中的 MAC 地址、接入端口和 VLAN 号信息保存到所述用户设备的绑定表的 DHCP 表项中；

在收到所述 DHCP 服务器的回应报文之后，提取所述回应报文中的 IP 地址和租期，并将所述 IP 地址和租期添加到所述用户设备的绑定表的 DHCP 表项中。

5. 根据权利要求 1 所述的调整安全接入的方法，其特征在于，所述 ACL 表项包括：所述用户设备的 IP 地址、MAC 地址、接入端口和 VLAN 号。

6. 一种交换机，其特征在于，包括：

判断表项模块，用于根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满；

报文请求模块，用于当所述 ACL 表项已满时，广播地址解析协议 ARP 请求报文，其中，所述 ARP 请求报文的发送端的 IP 地址和目标端的 IP 地址为所述 DHCP 表项中所述用户设备的 IP 地址，所述 ARP 请求报文的发送端的媒体访问控制 MAC 地址为所述 DHCP 表项中所述用户设备的 MAC 地址，所述 ARP 请求报文的目标端的 MAC 地址为广播地址；

监听回复模块，用于监听是否接收到 ARP 回应，如果未接收到所述 ARP 回应，则将所述

DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。

7. 根据权利要求 6 所述的交换机，其特征在于，还包括：

接收报文模块，用于在所述根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满之前，接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文，其中，所述 DHCP 请求报文包括 DHCP 探听过程的 MAC 地址、接入端口号和虚拟局域网 VLAN 号，所述 DHCP 服务器的回应报文包括 DHCP 探听过程的 IP 地址、租期、网关和域名系统 DNS 号；

创建表项模块，用于根据所述用户设备的 DHCP 请求报文和所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项；

生成表项模块，用于根据所述 DHCP 表项，生成 ACL 表项。

8. 根据权利要求 7 所述的交换机，其特征在于，还包括：

配置模块，用于在接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文之前，使能交换机的 DHCP 探听的监听功能，下发一条 DHCP 报文重定向至交换机 CPU 的 ACL 规则，同时下发一条默认不转发所有报文的 ACL 规则。

9. 根据权利要求 7 所述的交换机，其特征在于，所述创建表项模块具体用于：

将所述 DHCP 请求报文中的 MAC 地址、接入端口和 VLAN 号信息保存到所述用户设备的绑定表的 DHCP 表项中；

在收到所述 DHCP 服务器的回应报文之后，提取所述回应报文中的 IP 地址和租期，并将所述 IP 地址和租期添加到所述用户设备的绑定表的 DHCP 表项中。

10. 根据权利要求 6 所述的交换机，其特征在于，所述监听回复模块中的 ACL 表项包括：所述用户设备的 IP 地址、MAC 地址、接入端口和 VLAN 号。

一种调整安全接入的方法及交换机

技术领域

[0001] 本发明涉及计算机网络数据通信技术领域，尤其涉及一种调整安全接入的方法及交换机。

背景技术

[0002] DHCP(Dynamic Host Configuration Protocol，动态地址解析协议）是一种自动为用户分配 IP（Internet Protocol，网络之间互连的协议)地址以及其他选项(如网关、域名系统）的协议，广泛应用于局域网中，DHCP 简化了网络的部署、也易于网络的维护。DHCP SNOOPING 是一种监听 DHCP 请求过程的私有协议，它在交换装置中使用，将每一个成功获取 IP 的用户生成一个 DHCP 绑定信息。

[0003] 免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 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 MAC 地址是广播地址。设备通过对外发送免费 ARP 报文来确定其它设备的 IP 地址是否与本机的 IP 地址冲突。当其它设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。

[0004] ACL（Access Control List，访问控制列表）是一或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。网络设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

[0005] 为了防止用户私自接入网络，便于网络的维护和管理，可结合DHCP SNOOPING来实施接入控制策略，通过 DHCP 方式获取 IP 的主机可以访问网络，而私设 IP 的主机将不允许访问网络。这种接入策略需要结合交换机硬件 ACL 来实现，每一个 DHCP 用户需要下发一条允许访问网络的 ACL 规则。由于交换设备 ACL 表项容量有限，因此，当 DHCP 绑定表项数目大于设备的 ACL 表项数目时，一些 DHCP 绑定表项对应的 ACL 无法下发，则这些 DHCP 用户无法访问网络。

[0006] 在现有技术中，交换设备的ACL表项容量有限，因此，当DHCP绑定表项数目大于设备的 ACL 表项的容量的数目时，一些 DHCP 绑定表项对应的 ACL 表项将无法下发，这些 DHCP 用户设备就无法访问网络，访问控制列表的利用率较低。

发明内容

[0007] 有鉴于此，本发明实施例提供了一种调整安全接入的方法及交换机，以解决以上背景技术部分提到的交换机访问控制列表的利用率的技术问题。

[0008] 一方面，本发明实施例提供了一种调整安全接入的方法，包括：

[0009] 根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满；

[0010] 当所述 ACL 表项已满时，广播地址解析协议 ARP 请求报文，其中，所述 ARP 请求报

文的发送端的 IP 地址和目标端的 IP 地址为所述 DHCP 表项中所述用户设备的 IP 地址，所述 ARP 请求报文的发送端的媒体访问控制 MAC 地址为所述 DHCP 表项中所述用户设备的 MAC 地址，所述 ARP 请求报文的目标端的 MAC 地址为广播地址；

[0011] 监听是否接收到 ARP 回应，如果未接收到所述 ARP 回应，则将所述 DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。

[0012] 优选地，在所述根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满之前，还包括：

[0013] 接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文，其中，所述 DHCP 请求报文包括 DHCP 探听过程的 MAC 地址、接入端口号和虚拟局域网 VLAN 号，所述 DHCP 服务器的回应报文包括 DHCP 探听过程的 IP 地址、租期、网关和域名系统 DNS 号；

[0014] 根据所述用户设备的 DHCP 请求报文和所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项；

[0015] 根据所述 DHCP 表项，生成 ACL 表项。

[0016] 优选地，在所述接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文之前，还包括：

[0017] 使能交换机的 DHCP 探听的监听功能；

[0018] 下发一条 DHCP 报文重定向至交换机 CPU 的 ACL 规则，同时下发一条默认不转发所有报文的 ACL 规则。

[0019] 优选地，所述根据所述用户设备的 DHCP 请求报文和所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项，包括：

[0020] 将所述 DHCP 请求报文中的 MAC 地址、接入端口和 VLAN 号信息保存到所述用户设备的绑定表的 DHCP 表项中；

[0021] 在收到所述 DHCP 服务器的回应报文之后，提取所述回应报文中的 IP 地址和租期，并将所述 IP 地址和租期添加到所述用户设备的绑定表的 DHCP 表项中。

[0022] 优选地，所述 ACL 表项包括：所述用户设备的 IP 地址、MAC 地址、接入端口和 VLAN 号。

[0023] 与之相对应，本发明实施例提供了一种交换机，包括：

[0024] 判断表项模块，用于根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满；

[0025] 报文请求模块，用于当所述 ACL 表项已满时，广播地址解析协议 ARP 请求报文，其中，所述 ARP 请求报文的发送端的 IP 地址和目标端的 IP 地址为所述 DHCP 表项中所述用户设备的 IP 地址，所述 ARP 请求报文的发送端的媒体访问控制 MAC 地址为所述 DHCP 表项中所述用户设备的 MAC 地址，所述 ARP 请求报文的目标端的 MAC 地址为广播地址；

[0026] 监听回复模块，用于监听是否接收到 ARP 回应，如果未接收到所述 ARP 回应，则将所述 DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。

[0027] 优选地，所述交换机还包括：

[0028] 接收报文模块，用于在所述根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满之前，接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文，其中，所述 DHCP 请求报文包括 DHCP 探听过

程的 MAC 地址、接入端口号和虚拟局域网 VLAN 号，所述 DHCP 服务器的回应报文包括 DHCP 探听过程的 IP 地址、租期、网关和域名系统 DNS 号；

[0029] 创建表项模块，用于根据所述用户设备的 DHCP 请求报文和所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项；

[0030] 生成表项模块，用于根据所述 DHCP 表项，生成 ACL 表项。

[0031] 优选地，所述交换机还包括：

[0032] 配置模块，用于在接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文之前，使能交换机的 DHCP 探听的监听功能，下发一条 DHCP 报文重定向至交换机 CPU 的 ACL 规则，同时下发一条默认不转发所有报文的 ACL 规则。

[0033] 优选地，所述创建表项模块具体用于：

[0034] 将所述 DHCP 请求报文中的 MAC 地址、接入端口和 VLAN 号信息保存到所述用户设备的绑定表的 DHCP 表项中；

[0035] 在收到所述 DHCP 服务器的回应报文之后，提取所述回应报文中的 IP 地址和租期，并将所述 IP 地址和租期添加到所述用户设备的绑定表的 DHCP 表项中。

[0036] 优选地，所述监听回复模块中的 ACL 表项包括：所述用户设备的 IP 地址、MAC 地址、接入端口和 VLAN 号。

[0037] 本发明实施例提供的一种调整安全接入的方法及交换机，具有如下特点：可以更多 DHCP 用户设备的接入要求，提高了交换机访问控制列表的利用率。

附图说明

[0038] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0039] 图 1 是本发明实施例所适用的网络应用图；

[0040] 图 2 是本发明第一实施例提供调整安全接入的方法的实现流程图；

[0041] 图 3 是本发明第二实施例提供的调整安全接入的方法的实现流程图；

[0042] 图 4 是本发明第三实施例提供的交换机的装置的结构示意图。

具体实施方式

[0043] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例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他实施例，都属于本发明保护的范围。

[0044] 本发明实施例所适用的网络环境如图 1 所示。网络中设置有交换机，其分别与 DHCP 服务器和多个用户设备相连。

[0045] 实施例一

[0046] 图 1 是本发明第一实施例提供的调整安全接入的方法的实现流程图。本发明实施例提供的方法可以在图 1 所示的网络环境中由本发明实施例提供的交换机来执行。如图 2

所示，本发明实施例一提供的一种调整安全接入的方法包括：

[0047] 步骤S201，根据动态主机配置协议DHCP绑定表中用户设备的DHCP表项，依据所述DHCP表项下发ACL表项，判断所述ACL表项是否已满。

[0048] 步骤202，当所述ACL表项已满时，广播地址解析协议ARP请求报文。

[0049] 在步骤202中，所述ARP请求报文可以为免费ARP请求报文，其发送端的IP地址和目标端的IP地址为所述DHCP表项中所述用户设备的IP地址，所述ARP请求报文的发送端的MAC地址为所述DHCP表项中所述用户设备的MAC地址，所述ARP请求报文的目标端的MAC地址为广播地址。由此，可以让与交换机相连的各用户设备均接收到此报文，并根据已有协议进行回应。由于ARP请求报文是基于每个表项的地址发送的，所以若用户设备在线，则必然会接收到与自身地址一致的ARP请求报文，并按照协议需进行ARP回应。

[0050] 步骤S203，监听是否接收到ARP回应，如果未接收到所述ARP回应，则将所述DHCP表项在硬件访问控制列表ACL中ACL规则对应的ACL表项删除。

[0051] 需要进行说明的是，交换机监听是否接收到ARP回应，如果在所述第二定时器设定时长截止前未接收到ARP回应，则确定所述DHCP表项的用户设备处于离线状态。

[0052] 在步骤S203中，所述ACL规则是访问控制列表中用于识别报文流的匹配条件的判断语句，所述ACL表项可包括：所述用户设备的IP地址、MAC地址、接入端口和VLAN号。

[0053] 本实施例一提供的调整安全接入的方法，通过监控是否接收到ARP回应，来判断DHCP表项的对应用户设备是否处于离线状态，并删除离线状态下的DHCP表项的用户设备对应的ACL表项，能够为用户设备提供ACL表项空间，提高了交换机访问控制列表的利用率。在上述方案中，可以及时对ACL表项进行清理维护。利用了免费ARP请求报文及其ARP回应，有效利用了已有的报文机制，无需扩展额外的设备和软件，因此技术的推广便捷、成本低。

[0054] 实施例二

[0055] 图3是本发明第二实施例提供一种调整安全接入的方法的实现流程图。本实施例以实施例一为基础，软硬件环境与实施例一相同。如图3所示，本发明实施例提供的方法包括：

[0056] 步骤301，接收用户设备的DHCP请求报文和DHCP服务器的回应报文。

[0057] 在本发明实施例中，所述DHCP请求报文包括DHCP SNOOPING过程的MAC地址、接入端口号和VLAN号，所述DHCP服务器的回应报文包括DHCP SNOOPING过程的IP地址、租期、网关和域名系统DNS号。

[0058] 步骤302，根据所述用户设备的DHCP请求报文和所述DHCP服务器的回应报文，在DHCP绑定表中创建DHCP表项。

[0059] 在本发明实施例中，所述DHCP表项包括：MAC地址、接入端口、VLAN号、IP地址和租期。所述DHCP表项的创建过程：将所述DHCP请求报文中的MAC地址、接入端口和VLAN号信息保存到所述用户设备的绑定表的DHCP表项中；在收到所述DHCP服务器的回应报文之后，提取所述回应报文中的IP地址和租期，并将所述IP地址和租期添加到所述用户设备的绑定表的DHCP表项中。

[0060] 步骤303，根据所述DHCP表项，生成ACL表项。

[0061] 其中，所述DHCP表项包括：IP地址、MAC地址、接入端口、VLAN号和租期。提取所

述 DHCP 表项中的 IP 地址、MAC 地址、接入端口和 VLAN 号，生成对应的 ACL 表项。交换机收到的报文后，只有报文中的表项与交换机中的所述 ACL 表项中的一条子项相匹配时，才能够转发所述报文。

[0062] 步骤 304，判断所述 ACL 表项是否已满，当所述 ACL 表项已满时，广播地址解析协议 ARP 请求报文；

[0063] 步骤 S305 监听是否接收到 ARP 回应，如果未接收到所述 ARP 回应，则将所述 DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。

[0064] 本实施例提供的调整安全接入的方法，是在实施例一的基础上提出的优选实施例，达到相同的功能，能够为用户设备提供 ACL 表项空间，提高了交换机访问控制列表的利用率。

[0065] 进一步的，在所述接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文之前，优选还包括：使能交换机的 DHCP 探听的监听功能；下发一条 DHCP 报文重定向至交换机 CPU 的 ACL 规则，同时下发一条默认不转发所有报文的 ACL 规则，其中，所述 ACL 规则是访问控制列表中用于识别报文流的匹配条件的判断语句。该方案的有益之处在于启动 DHCP SNOOPING 过程的安全功能，并预先配置 ACL 规则，使交换机根据 ACL 规则有针对性的转发报文信息，保证交换机转发报文的安全性。

[0066] 实施例三

[0067] 图 4 是本发明第三实施例提供的交换机包括的装置的结构示意图。如图 4 所示，本发明实施例提供的装置包括：判断表项模块 405、报文请求模块 406 和监听回复模块 407。

[0068] 判断表项模块 405，用于根据动态主机配置协议 DHCP 绑定表中用户设备的 DHCP 表项，依据所述 DHCP 表项下发 ACL 表项，判断所述 ACL 表项是否已满；报文请求模块 406，用于当所述 ACL 表项已满时，广播地址解析协议 ARP 请求报文，其中，所述 ARP 请求报文的发送端的 IP 地址和目标端的 IP 地址为所述 DHCP 表项中所述用户设备的 IP 地址，所述 ARP 请求报文的发送端的媒体访问控制 MAC 地址为所述 DHCP 表项中所述用户设备的 MAC 地址，所述 ARP 请求报文的目标端的 MAC 地址为广播地址；监听回复模块 407，用于监听是否接收到 ARP 回应，如果未接收到所述 ARP 回应，则将所述 DHCP 表项在硬件访问控制列表 ACL 中 ACL 规则对应的 ACL 表项删除。

[0069] 在上述方案中，通过判断表项模块 405 来广播 ARP 请求报文，并判断接收到 ARP 回应，进而判断 DHCP 表项的对应用户设备是否处于离线状态，通过监听回复模块 407 删除离线状态下的 DHCP 表项的用户设备对应的 ACL 表项，能够对离线的用户设备的 ACL 表项进行及时清理维护，提高了交换机访问控制列表的利用率。有效利用了已有的报文机制，无需扩展额外的设备和软件，因此技术的推广便捷、成本低。

[0070] 在上述方案中，优选是，还包括：接收报文模块 402、创建表项模块 403 和生成表项模块 404。

[0071] 其中，所述接收报文模块 402，用于在按照第一定时器定时周期，根据 DHCP 绑定表中用户设备的 DHCP 表项，广播 ARP 请求报文之前，接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文，其中，所述 DHCP 请求报文包括 DHCPSNOOPING 过程的 MAC 地址、接入端口号和 VLAN 号，所述 DHCP 服务器的回应报文包括 DHCP SNOOPING 过程的 IP 地址、租期、网关和域名系统 DNS 号。所述创建表项模块 403，用于根据所述用户设备的 DHCP 请求报文和

所述 DHCP 服务器的回应报文，在 DHCP 绑定表中创建 DHCP 表项。所述生成表项模块 404，用于根据所述 DHCP 表项，生成 ACL 表项。

[0072] 在上述方案中，优选是，还包括：配置模块 401，用于在接收用户设备的 DHCP 请求报文和 DHCP 服务器的回应报文之前，使能交换机的 DHCP SNOOPING 的监听功能，下发一条 DHCP 报文重定向至交换机 CPU 的 ACL 规则，同时下发一条默认不转发所有报文的 ACL 规则。

[0073] 进一步的，所述创建表项模块 403 具体用于：将所述 DHCP 请求报文中的 MAC 地址、接入端口和 VLAN 号信息保存到所述用户设备的绑定表的 DHCP 表项中；在收到所述 DHCP 服务器的回应报文之后，提取所述回应报文中的 IP 地址和租期，并将所述 IP 地址和租期添加到所述用户设备的绑定表的 DHCP 表项中。

[0074] 在本发明实施例中，所述监听回复模块 407 中的 ACL 表项可以包括：所述用户设备的 IP 地址、MAC 地址、接入端口和 VLAN 号。

[0075] 本实施例提供的交换机用于执行本发明任意实施例提供的调整安全接入的方法，具备相应的功能模块，达到相同的技术效果。

[0076] 显然，本领域技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个计算装置上，或者分布在多个计算装置所组成的网络上，可选地，他们可以用计算机装置可执行的程序代码来实现，从而可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件的结合。

[0077] 以上仅为本发明的优选实施例，并不用于限制本发明，对于本领域技术人员而言，本发明可以有各种改动和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

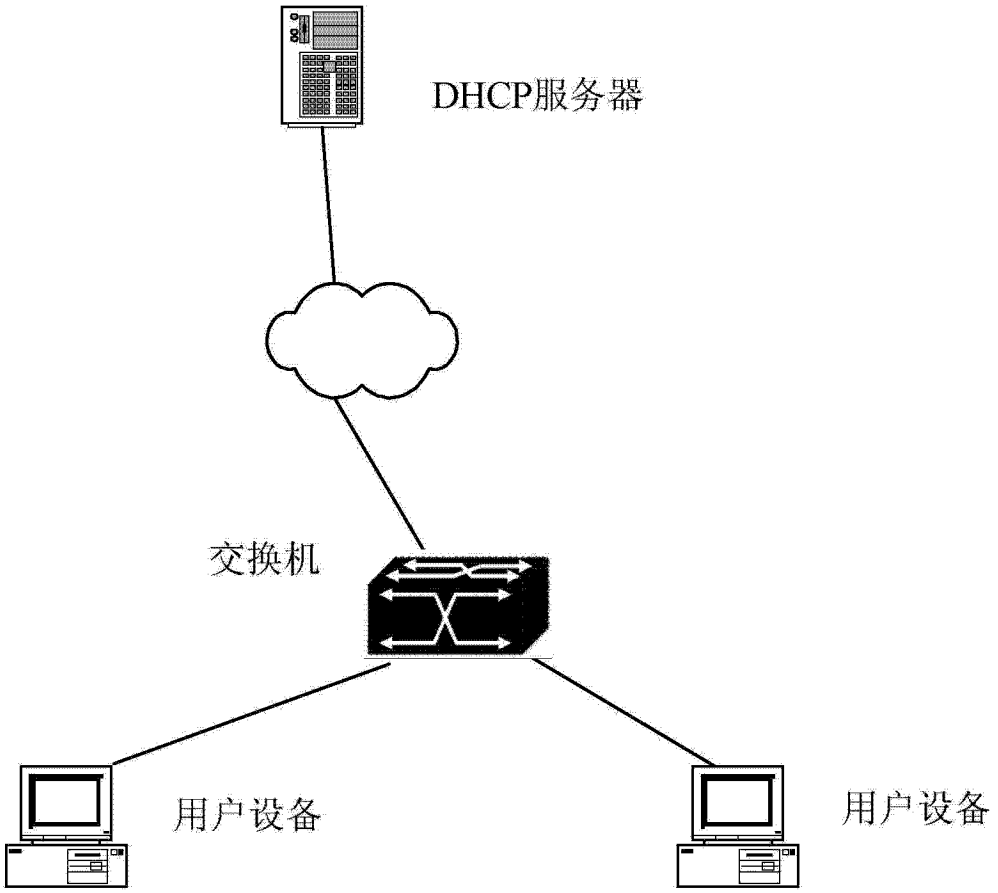

DHCP服务器
交换机
用户设备
用户设备

图 1

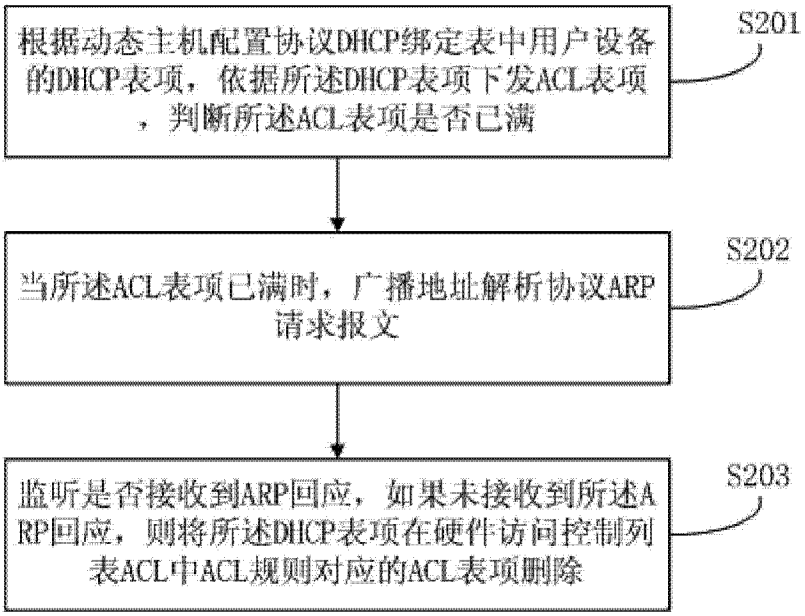

根据动态主机配置协议DHCP绑定表中用户设备的DHCP表项，依据所述DHCP表项下发ACL表项，判断所述ACL表项是否已满
S201
当所述ACL表项已满时，广播地址解析协议ARP请求报文
S202
监听是否接收到ARP回应，如果未接收到所述ARP回应，则将所述DHCP表项在硬件访问控制列表ACL中ACL规则对应的ACL表项删除
S203

图 2

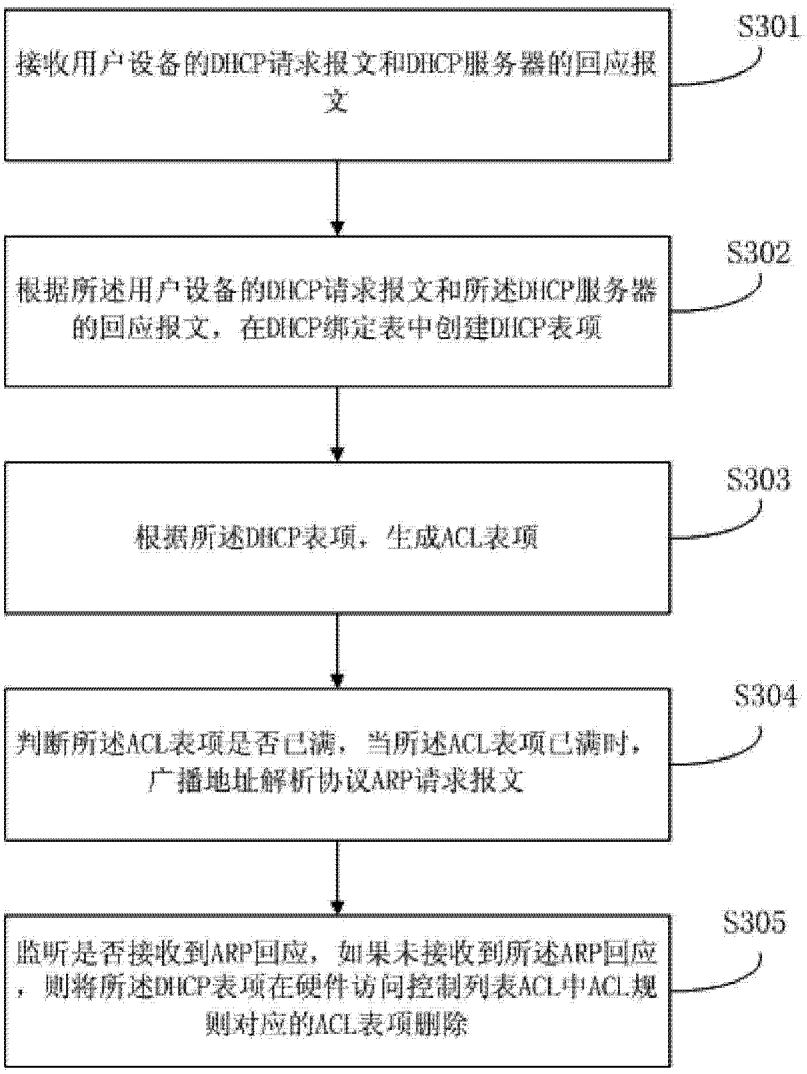

S301
接收用户设备的DHCP请求报文和DHCP服务器的回应报文
S302
根据所述用户设备的DHCP请求报文和所述DHCP服务器的回应报文，在DHCP绑定表中创建DHCP表项
S303
根据所述DHCP表项，生成ACL表项
S304
判断所述ACL表项是否已满，当所述ACL表项已满时，广播地址解析协议ARP请求报文
S305
监听是否接收到ARP回应，如果未接收到所述ARP回应，则将所述DHCP表项在硬件访问控制列表ACL中ACL规则对应的ACL表项删除

图 3

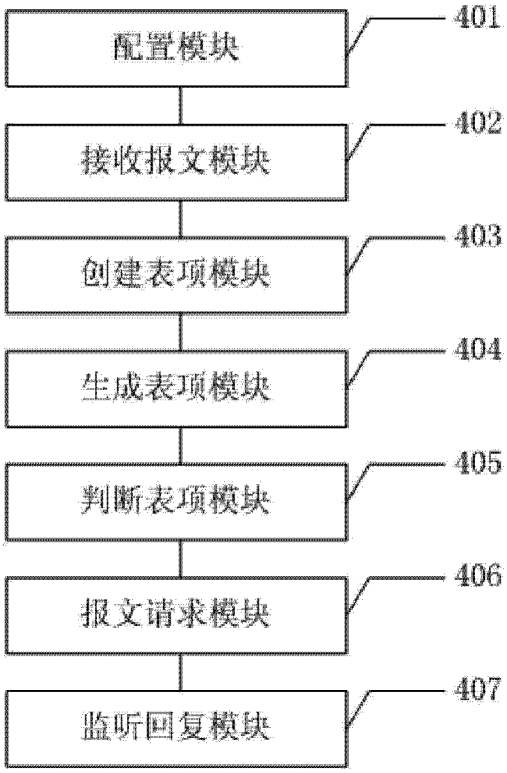

配置模块
401
接收报文模块
402
创建表项模块
403
生成表项模块
404
判断表项模块
405
报文请求模块
406
监听回复模块
407

图 4