

(12) 发明专利

(10) 授权公告号 CN 101179566 B

(45) 授权公告日 2012. 08. 15

(21) 申请号 200710077419. 7

(22) 申请日 2007. 11. 24

(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 李冠峰

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 12/56 (2006. 01)

(56) 对比文件

CN 1674563 A, 2005. 09. 28, 全文 .

US 2006/0268863 A1, 2006. 11. 30, 全文 .

审查员 冯楠

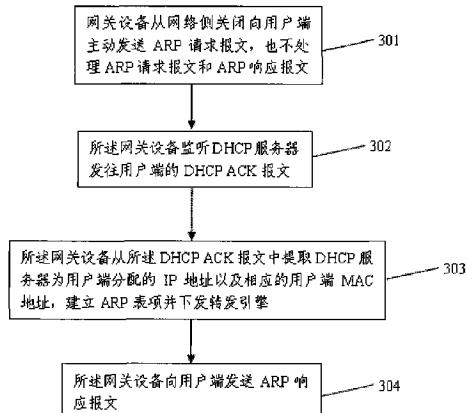
权利要求书 1 页 说明书 5 页 附图 2 页

(54) 发明名称

一种防御 ARP 报文攻击的方法和装置

(57) 摘要

本发明涉及通信领域，公开了一种防御 ARP 报文攻击的方法，解决了现有技术无法避免来自地址合法用户的 ARP 报文攻击问题。该方法中网关设备不主动向用户端发送 ARP 请求报文，不处理 ARP 请求报文和 ARP 响应报文；网关设备通过监听 DHCP ACK 报文，建立 ARP 表项；网关设备向用户端发送 ARP 响应报文，以刷新用户端的 ARP 缓存表。本方法从根本上阻断了 ARP 报文攻击问题，避免了用户端 ARP 缓存表的非正常老化。本发明还公开了一种防御 ARP 报文攻击的装置。



1. 一种防御 ARP 报文攻击的方法,其特征在于:

网关设备丢弃接收到的 ARP 请求报文和 ARP 响应报文;

所述网关设备通过监听发送给用户端的动态主机配置协议应答报文,建立 ARP 表项;其中,所述 ARP 表项中包含 DHCP 服务器为用户端分配的互联网协议 IP 地址以及用户端的物理 MAC 地址

所述网关设备根据所述 ARP 表项向所述用户端发送 ARP 响应报文,刷新所述用户端的 ARP 缓存表。

2. 根据权利要求 1 所述的方法,其特征在于:

所述动态主机配置协议应答报文中包含 Option82 选项。

3. 根据权利要求 1 所述的方法,其特征在于:

所述网关设备根据所述用户的地址信息向所述用户端发送 ARP 响应报文,具体为:所述网关设备根据所述用户的地址信息,以一定的时间周期向所述用户端发送 ARP 响应报文。

4. 一种防御 ARP 报文攻击的装置,其特征在于,包括控制单元、接收单元、处理单元、存储单元和发送单元:

控制单元:用于控制所述接收单元,使得所述接收单元不将接收到的 ARP 请求报文和 ARP 响应报文发送给所述处理单元;用于控制所述发送单元,使得所述发送单元不主动向用户端发送 ARP 请求报文;

接收单元:用于接收报文,并将接收到的动态主机配置协议应答报文发送给所述处理单元;

处理单元:用于处理所述接收单元发送的动态主机配置协议应答报文,提取所述动态主机配置协议应答报文中的动态主机配置协议服务器为所述用户端分配的 IP 地址和所述用户端 MAC 地址,建立 ARP 表项发送至所述存储单元;

存储单元:用于存储所述处理单元发送的 ARP 表项信息;

发送单元:用于根据所述 ARP 表项向用户端发送 ARP 响应报文。

5. 根据权利要求 4 所述的装置,其特征在于:

所述接收单元不将接收到的 ARP 请求报文和 ARP 响应报文发送给所述处理单元,将所述 ARP 请求报文和 ARP 响应报文直接丢弃。

6. 根据权利要求 4 或 5 所述的装置,其特征在于:

所述动态主机配置协议应答报文中包含 Option82 选项。

一种防御 ARP 报文攻击的方法和装置

技术领域

[0001] 本发明涉及通信领域,特别涉及一种防御 ARP(AddressResolution Protocol, 地址解析协议)报文攻击的方法和装置。

背景技术

[0002] ARP 是一种将 IP 地址映射到 MAC 地址(物理地址)的二层协议。其基本功能就是通过目标设备的 IP 地址,查询目标设备的 MAC 地址,以保证通信的顺利进行。如图 1 所示,以主机 A(IP 地址为 192.168.1.1) 向主机 B(IP 地址为 192.168.1.2) 发送数据为例。当发送数据时,主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果在 ARP 缓存表中没有找到相对应的 IP 地址,主机 A 就会在网络上广播一个 ARP 请求报文,请求 IP 地址为 192.168.1.2 的主机做出响应,尽管网络上所有的主机都收到了主机 A 的 ARP 请求报文,但是只有主机 B 才会做出回应,返回的 ARP 响应报文中包含了主机 B 的 MAC 地址: bb-bb-bb-bb-bb-bb。这样,主机 A 就知道了主机 B 的 MAC 地址。同时它还更新了自己的 ARP 缓存表,下次再向主机 B 发送信息时,直接从 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制,在一段时间内如果表中的某一行没有使用,就会被删除。

[0003] 这样的设计高效且易于维护,但是在安全方面却存在着缺陷。首先,主机 A 收到主机 B 的 ARP 响应报文后,在自己的 ARP 缓存表中建立主机 B 的 IP 地址与 MAC 地址的对应关系,但是主机 A 并不维护这种对应关系的真实性、有效性和一致性。其次,主机 A 默认任何接收到的 ARP 响应报文都是合法的,甚至在主机 A 没有发送 ARP 请求报文的情况下,也会根据接收到的 ARP 响应报文改写其 ARP 缓存表;同样,主机 A 也会在没有 ARP 请求报文的情况下,向别的主机发送 ARP 响应报文。

[0004] ARP 报文攻击正是利用了 ARP 协议本身固有的缺陷。常见的 ARP 报文攻击手段有两种:ARP 报文欺骗和拒绝服务。

[0005] ARP 报文欺骗。由于网络中 ARP 报文的真实性无法保证,同时没有请求的 ARP 响应报文也能被接受并因此而改写 ARP 缓存表,实施 ARP 报文欺骗的主机构造一个 ARP 响应报文,发送给想要欺骗的主机,报文中 IP 地址和 MAC 地址的对应关系是错误的,或者报文中的 IP 地址和 MAC 地址是虚假的。例如,图 1 中主机 C(IP 地址为 192.168.1.3) 向主机 D(IP 地址为 192.168.1.4) 发送 ARP 响应报文,告诉主机 D,IP 地址 192.168.1.2(主机 B 的 IP 地址)对应的 MAC 地址为 cc-cc-cc-cc-cc-cc(主机 C 的 MAC 地址)。主机 D 对报文的信息毫不怀疑,并以此在自己的 ARP 缓存表中建立了这样的对应关系。于是,在此后的通信中,主机 D 上发送给主机 B 的报文会全都发送到主机 C 上。或者,主机 C 告诉主机 D,IP 地址 192.168.1.2(主机 B 的 IP 地址)对应的 MAC 地址为 ee-ee-ee-ee-ee-ee(不存在的 MAC 地址),这样,主机 D 与主机 B 之间将无法正常通信。

[0006] 拒绝服务。实施 ARP 报文攻击的主机通过构造大量的虚假 ARP 请求报文发送给被攻击的主机,由于 ARP 请求报文中的信息错误,被攻击的主机无法正常处理,导致系统资源耗尽,无法响应正常的请求。若网关设备受到 ARP 报文攻击,将导致整个局域网无法与外界

正常通信。

[0007] 为了防御 ARP 报文攻击,现有技术中利用 DHCP(Dynamic Host Configuration Protocol,动态主机配置协议)来建立 IP 地址与 MAC 地址的动态绑定表。DHCP 是一个对网络上的主机动态提供配置参数的协议。DHCP 服务器向用户端发送的 DHCP 报文中携带有为用户端分配的 IP 地址、子网掩码、网关以及租期等信息。同时为了保证安全性,交换机等接入设备(DHCP 中称为中继代理,Relay Agent)在用户发送给 DHCP 服务器的 DHCP 报文中加入了中继代理的信息域,即所谓的 Option82,使得 DHCP 服务器通过该 Option82 选项能够了解到远端用户的信息以及中继代理的相关信息。DHCP 服务器只为带有合法 Option82 选项的用户端分配 IP 地址。需要说明的是,当用户端发送的 DHCP 报文通过多个接入设备时,第一个接入设备在所述 DHCP 报文中插入了 Option82 选项,当后续接入设备接收到所述 DHCP 报文时,检测到该报文中已经插入了 Option82 选项,则所述后续接入设备可以将自己的信息插入 Option82 选项,以替换之前的接入设备的 Option82 选项;也可以不对报文做任何修改,直接将报文转发出去。

[0008] 在防御来自用户端对网关设备的 ARP 报文攻击时,通常是在接入设备监听携带 Option82 选项的 DHCP ACK(应答)报文,建立 DHCP Snooping 绑定表,绑定表项包含 DHCP 服务器为用户端分配的 IP 地址、用户的 MAC 地址以及 VLAN ID 等相关信息。当接入设备接收到来自用户端的 ARP 请求报文时,首先利用 DHCP Snooping 绑定表对报文的合法性进行检查,不合法的报文就直接丢弃;而对于合法的报文,则在出端口限制其流出的速率,可以降低网关设备受到 ARP 报文攻击的危害。

[0009] 但是,在实现本发明的过程中,发明人发现现有技术中至少存在以下问题:一方面对于网关设备来说,即使接入设备限制了报文的流出速率,可以通过合法性检查的 ARP 请求数量仍然很大;而对报文合法性的检查也无法避免地址合法的用户通过 ARP 请求对网关设备进行攻击。另一方面对于用户来说,由于限制了报文的转发速率,有可能造成合法用户的合法 ARP 请求报文的丢失,造成用户端 ARP 缓存表非正常老化,使得个别用户的 ARP 报文攻击的影响扩散,影响其他用户的正常业务。

发明内容

[0010] 有鉴于此,本发明实施例提供一种防御 ARP 报文攻击的方法和装置,以解决现有技术中网关设备无法避免来自地址合法用户端的 ARP 报文攻击问题。

[0011] 一种防御 ARP 报文攻击的方法,包括:

[0012] 网关设备丢弃接收到的 ARP 请求报文和 ARP 响应报文;

[0013] 所述网关设备通过监听发送给用户端的动态主机配置协议应答报文,建立 ARP 表项;所述网关设备根据所述 ARP 表项向所述用户端发送 ARP 响应报文,刷新所述用户端的 ARP 缓存表。

[0014] 一种防御 ARP 报文攻击的装置,包括控制单元、接收单元、处理单元、存储单元和发送单元:

[0015] 控制单元:用于控制所述接收单元,使得所述接收单元不将接收到的 ARP 请求报文和 ARP 响应报文发送给所述处理单元;用于控制所述发送单元,使得所述发送单元不主动向用户端发送 ARP 请求报文;

[0016] 接收单元：用于接收报文，并将接收到的动态主机配置协议应答报文发送给所述处理单元；

[0017] 处理单元：用于处理所述接收单元发送的动态主机配置协议应答报文，提取所述动态主机配置协议应答报文中的动态主机配置协议服务器为所述用户端分配的 IP 地址和所述用户端 MAC 地址，建立 ARP 表项发送至所述存储单元；

[0018] 存储单元：用于存储所述处理单元发送的 ARP 表项信息；

[0019] 发送单元：用于向用户端发送 ARP 响应报文。

[0020] 相较于现有技术，采用本发明实施例提供的一种防御 ARP 报文攻击的方法和装置，能够从根本上阻断来自地址合法用户的 ARP 报文攻击，避免合法用户的 ARP 缓存表非正常老化。

[0021] 图 1 为 ARP 的基本原理示意图；

[0022] 附图说明

[0023] 图 2 为本发明一个较佳实施例示意图；

[0024] 图 3 为本发明较佳实施例提供的一种防御 ARP 报文攻击的方法流程图；

[0025] 图 4 为本发明较佳实施例提供的一种防御 ARP 报文攻击的装置结构示意图。

具体实施方式

[0026] 为使本发明的目的、技术方案及优点更加清楚明白，以下参照附图并举实施例，对本发明作进一步地详细说明。

[0027] 本发明的核心思想是，网关设备从网络侧关闭向用户端主动发送 ARP 请求报文，也不处理接收到的 ARP 请求报文和 ARP 响应报文，通过对 DHCP ACK 报文的监听，建立 ARP 表项，表项中包含 DHCP 服务器为用户端分配的 IP 地址以及用户端的 MAC 地址。利用 ARP 表项中的信息，网关设备主动向用户端发送 ARP 响应报文，将自己的 MAC 地址通报给用户端。

[0028] 下面以图 2 所示的应用场景对本发明的一个较佳实施例进行具体说明。如图 2 所示，用户主机在本地子网中广播一个 DHCP Discover（发现）报文，请求 DHCP 服务器为其分配 IP 地址等相关配置，由于用户主机和 DHCP 服务器不在一个子网中，该 DHCP Discover 报文需要经过中继代理传递到 DHCP 服务器。

[0029] 当交换机 1 接收到该 DHCP Discover 报文时，插入 Option82 选项，本实施例中，插入的信息包括：用户主机的 VLAN ID，以及交换机 1 中接收到该 DHCP Discover 报文的端口号。当交换机 n（n 为大于 1 的自然数）接收到该 DHCP Discover 报文时，检测到报文中已经存在 Option82 选项，本实施例中，交换机 n 对报文不做任何修改，直接转发出去。该 DHCP Discover 通过中继代理后，通过单播方式发送到 DHCP 服务器 1 和 DHCP 服务器 2。

[0030] DHCP 服务器 1 和 DHCP 服务器 2 接收到该 DHCP Discover 报文后，向用户主机回应一个 DHCP Offer（提供）报文，报文中包含自己能够为用户主机分配的 IP 地址等相关配置。当这些 DHCP Offer 报文通过交换机 n 时，交换机 n 对报文不做任何处理，直接转发出去；当这些 DHCP Offer 报文通过交换机 1 时，交换机 1 将插入的 Option82 选项删除，然后将这些 DHCP Offer 报文发送给用户主机。本实施例中，用户主机选择了第一个收到的 DHCP Offer 报文（来自 DHCP 服务器 1）。

[0031] 用户主机在本地子网广播一个 DHCP Request（请求）报文，报文中包含 DHCP 服务

器 1 的标识,表明用户主机已经选择了 DHCP 服务器 1 为自己分配的 IP 地址等相关配置。

[0032] 被选择的 DHCP 服务器 1 接收到用户主机的 DHCP Request 报文后,向用户主机发送一个 DHCP ACK(应答)报文,表明自己已经认可了用户主机的选择,该 DHCP ACK 报文中包含分配给用户主机的 IP 地址等相关配置信息。

[0033] 本实施例中,DHCP 服务器接收到用户主机发送的 DHCP Discover 或者 DHCP Request 报文后,会对报文中携带的 Option82 选项进行合法性检查,DHCP 服务器只为带有合法 Option82 选项的用户主机分配 IP 地址。并且,交换机 1 ~ 交换机 n 对 DHCP Request 报文的处理,与上述交换机 1 ~ 交换机 n 对 DHCP Discover 报文的处理相同;交换机 1 ~ 交换机 n 对 DHCP ACK 报文的处理,与上述交换机 1 ~ 交换机 n 对 DHCP Offer 报文的处理相同,故不再重复介绍。

[0034] 因此交换机设备等接入设备通过对 DHCP ACK 报文的监听,就能够获取用户主机的 MAC 地址、IP 地址以及 VLAN ID 等相关信息,并建立 DHCP Snooping 绑定表。

[0035] 当恶意用户主机利用 ARP 报文(ARP 请求报文或者 ARP 响应报文)对网关设备实施攻击和欺骗的时候,首先交换机等接入设备会通过 DHCP Snooping 绑定表来检查所述 ARP 报文的合法性,对于不合法的报文,接入设备直接将其丢弃;而对于某些地址合法的 ARP 报文,则顺利通过了合法性的检查。这些貌似合法的 ARP 报文转发到了网关设备。

[0036] 本实施例中,网关设备对接收到的 ARP 请求报文和 ARP 响应报文并不进行任何处理,将其直接丢弃,同时也不主动向用户主机发送 ARP 请求报文,这样不仅从源头上阻断了大量 ARP 报文对网关设备的拒绝服务攻击,也能从根本上避免伪造的 ARP 报文对网关设备的欺骗。

[0037] 但是子网内的合法用户主机需要与外界进行联系,必须知道网关设备的 MAC 地址。为了让合法用户主机知道网关设备的 MAC 地址,本实施例中,网关设备会主动向用户主机发送 ARP 响应报文,将自己的 MAC 地址通报给用户主机,防止合法用户主机 ARP 缓存表的非正常老化。由于用户主机的 ARP 缓存表存在一定的老化周期,因此网关设备会以一定的时间周期、在用户主机的 ARP 缓存表老化前向用户主机发送 ARP 响应报文。

[0038] 而网关设备向用户主机发送 ARP 响应报文前需要知道用户主机正确的 IP 地址和 MAC 地址。本实施例中,网关设备对通过其的 DHCP ACK 报文进行监听,从而保证了用户主机 IP 地址和 MAC 地址信息的正确性。网关设备从 DHCP ACK 报文中提取用户主机的 IP 地址和 MAC 地址,建立 ARP 表项,利用所述 ARP 表项信息构造 ARP 响应报文发送给用户主机,向用户通报自身的 MAC 地址。

[0039] 图 3 为本发明较佳实施例提供的一种防御 ARP 报文攻击的方法流程图。如图 3 所示,包括以下步骤:

[0040] 步骤 301:网关设备从网络侧关闭向用户端主动发送 ARP 请求报文,也不处理接收到的 ARP 请求报文和 ARP 响应报文。

[0041] 步骤 302:所述网关设备监听 DHCP 服务器发往用户端的 DHCP ACK 报文。

[0042] 步骤 303:所述网关设备从所述 DHCP ACK 报文中提取 DHCP 服务器为用户端分配的 IP 地址以及相应的用户端 MAC 地址,建立 ARP 表项并下发转发引擎。

[0043] 步骤 304:所述网关设备向用户端发送 ARP 响应报文,所述 ARP 响应报文中包含有所述网关设备的 MAC 地址。

[0044] 图 4 为本发明较佳实施例提供的一种防御 ARP 报文攻击的装置结构示意图。如图 4 所示，该装置包括控制单元 401、接收单元 402、处理单元 403、存储单元 404 和发送单元 405。

[0045] 控制单元 401：用于控制所述接收单元 402，使得所述接收单元 402 不处理接收到的 ARP 请求报文和 ARP 响应报文；用于控制所述发送单元 405，使得所述发送单元 405 不主动向用户端发送 ARP 请求报文。

[0046] 接收单元 402：用于接收报文，并将报文发送给所述处理单元 403。本实施例中，接收单元 402 将接收到的 DHCP ACK 报文发送给所述处理单元 403；将接收到的 ARP 请求报文和 ARP 响应报文直接丢弃。

[0047] 处理单元 403：用于处理所述接收单元 402 发送的 DHCP ACK 报文，提取报文中 DHCP 服务器为用户端分配的 IP 地址以及用户端的 MAC 地址，并将所述 IP 地址和 MAC 地址建立 ARP 表项发送至所述存储单元 404。

[0048] 存储单元 404：用于存储所述处理单元 403 发送的 ARP 表项信息。

[0049] 发送单元 405：用于利用所述存储单元 404 中的 ARP 表项信息构造一个 ARP 响应报文，发送给用户端，以刷新用户端的 ARP 缓存表项。本实施例中，控制单元 401 对发送单元 405 的控制通过软件来实现。由于用户端的 ARP 缓存表存在一定的老化周期，因此在本实施例中，发送单元 405 以一定的时间周期向用户端发送 ARP 响应报文。

[0050] 采用本发明较佳实施例提供的方法和装置，关闭了网关设备向用户端的 ARP 请求报文，也拒绝处理来自用户端的 ARP 请求报文以及 ARP 响应报文，从根本上解决了来自用户端的 ARP 报文攻击问题，避免了由于 ARP 报文攻击而导致的系统资源消耗。同时，网关设备定时主动向用户端发送 ARP 响应报文，以刷新用户端的 ARP 缓存表，避免了用户端 ARP 缓存表的非正常老化。

[0051] 以上仅为本发明的较佳实施例，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，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。

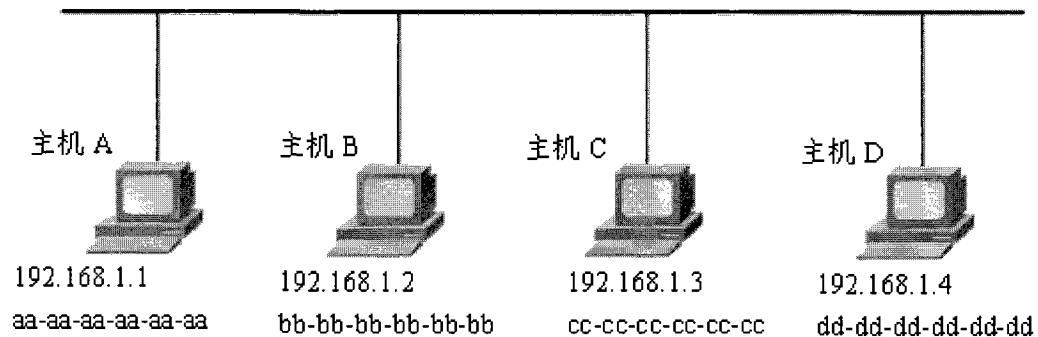


图 1

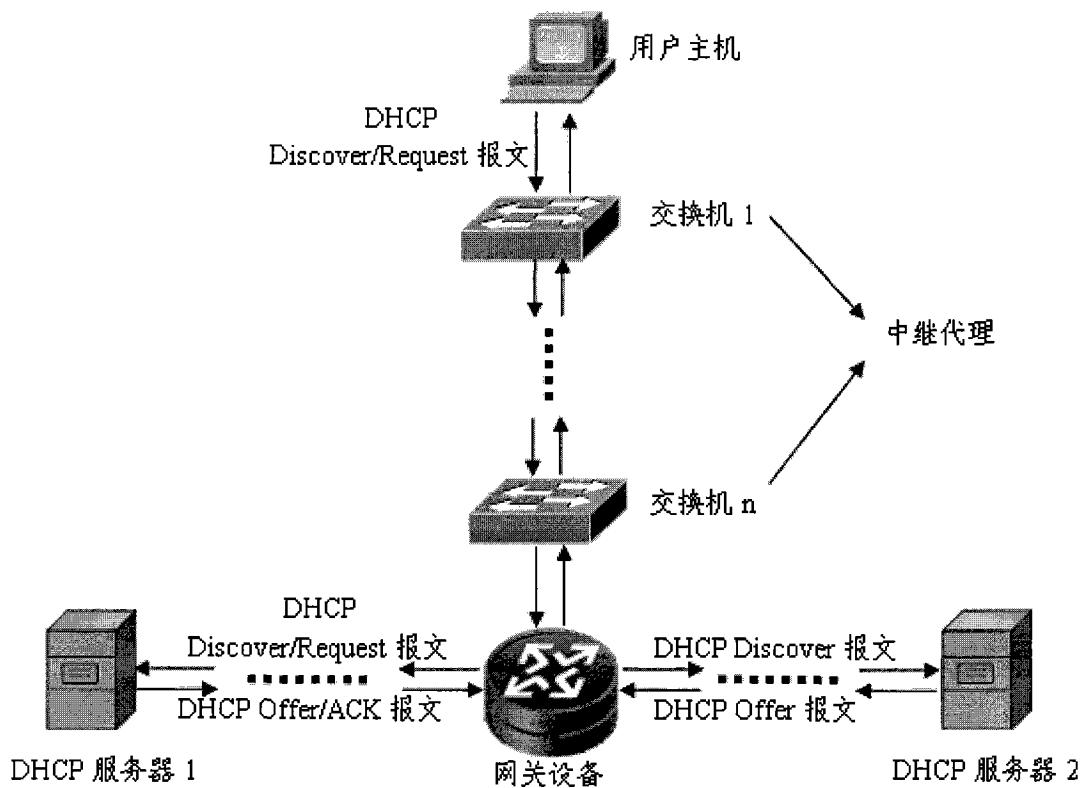


图 2

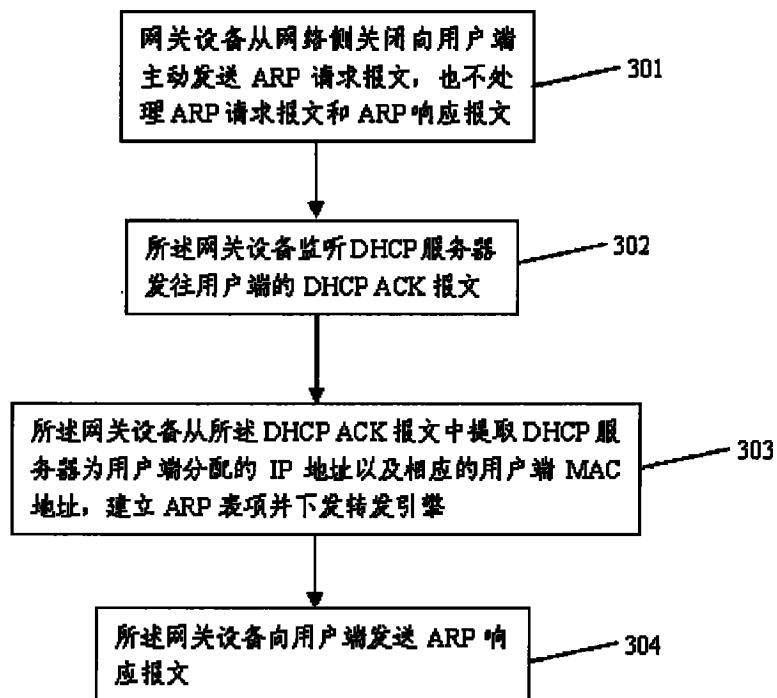


图 3

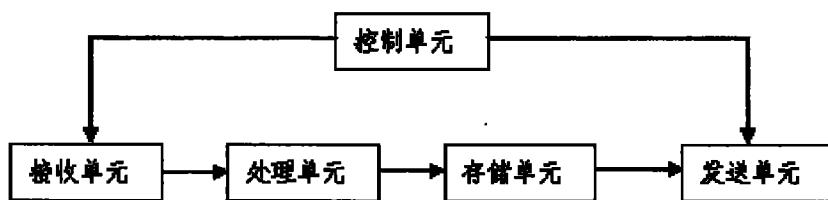


图 4