



(12) 发明专利申请

(10) 申请公布号 CN 102325197 A

(43) 申请公布日 2012. 01. 18

(21) 申请号 201110134271. 2

(22) 申请日 2011. 05. 23

(71) 申请人 杭州华三通信技术有限公司

地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号华为杭州生产基地

(72) 发明人 王军 周迪

(74) 专利代理机构 北京德琦知识产权代理有限公司 11018

代理人 谢安昆 宋志强

(51) Int. Cl.

H04L 29/12(2006. 01)

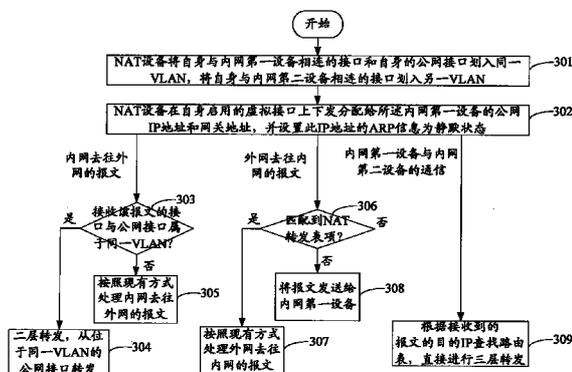
权利要求书 2 页 说明书 7 页 附图 2 页

(54) 发明名称

一种内网设备与外网设备通信的方法和网络地址转换设备

(57) 摘要

本发明公开了一种内网设备与外网设备通信的方法和 NAT 设备: NAT 设备将自身与内网第一设备相连的接口和自身的公网接口划入同一 VLAN, 将自身与内网第二设备相连的接口划入另一 VLAN, 在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址, 并设置此 IP 地址的 ARP 信息为静默状态; 将接收到的内网第一设备发送到外网的报文从与该报文的入接口位于同一 VLAN 的公网接口转发; 将进行了网络地址端口转换处理后的内网第二设备发送到外网的报文从公网接口转发; 根据是否匹配到 NAT 转发表转发外网设备发送的报文。应用本发明所述的方法和 NAT 设备, 使得局域网中的一台设备利用公网 IP 地址快捷地实现同公网的交互、其它设备通过 NAT 转换实现同公网的交互。



1. 一种内网设备与外网设备通信的方法,其特征在于,该方法包括:

网络地址转换 NAT 设备将自身与内网第一设备相连的接口和自身的公网接口划入同一虚拟局域网 VLAN,将自身与内网第二设备相连的接口划入另一 VLAN,在自身启用的虚拟接口上下发分配给所述内网第一设备的公网因特网协议 IP 地址和网关地址,并设置此 IP 地址的地址解析协议 ARP 信息为静默状态;

所述内网第一设备和外网设备进行通信时,NAT 设备接收所述内网第一设备发送到外网的报文,该报文的媒体接入控制 MAC 地址为网关的 MAC 地址,NAT 设备将该报文进行二层转发,从与该报文的入接口位于同一 VLAN 的公网接口转发出去;

所述内网第二设备与外网设备进行通信时,NAT 设备接收所述内网第二设备发送到外网的报文,对该报文进行网络地址端口转换处理,转化后的源 IP 地址为所述分配给内网第一设备的公网 IP 地址,在本地记录 NAT 转发表,将进行了网络地址端口转换处理后的报文从公网接口转发出去;

当外网设备发送的报文到达 NAT 设备时,NAT 设备以目的 IP 地址和端口号来匹配所述 NAT 转发表,如果能匹配其中的表项,则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备;如果未能匹配其中的表项则直接将报文转发给所述第一设备。

2. 根据权利要求 1 所述的方法,其特征在于,在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址包括:

当所述内网第一设备通过动态主机配置协议 DHCP 方式获取公网 IP 地址时,NAT 设备侦听所述内网第一设备和 DHCP 服务器交互的 DHCP 报文,将帧听到的 DHCP ACK 类型报文中客户端 IP 地址和网关地址下发到虚接口上;

当所述内网第一设备通过以太网上的点到点协议 PPPoE 方式获取工位 IP 地址时,NAT 设备侦听 PPPoE 过程的交互报文,将 PPPoE 服务器分配给所述第一设备的 IP 地址下发到虚接口上;

当所述内网第一设备静态配置公网 IP 地址网关地址时,NAT 设备在自身的虚接口上静态配置该公网 IP 地址和网关地址。

3. 根据权利要求 1 所述的方法,其特征在于,该方法进一步包括:

所述内网第一设备和内网第二设备通信时,NAT 设备根据接收到的报文的的目的 IP 进行三层转发。

4. 一种网络地址转换 NAT 设备,其特征在于,该 NAT 设备包括:划分单元、下发单元和处理单元,其中,

所述划分单元,用于将与内网第一设备相连的接口和公网接口划入同一虚拟局域网 VLAN,将与内网第二设备相连的接口划入另一 VLAN;

所述下发单元,用于在启用的虚拟接口上下发分配给所述内网第一设备的公网因特网协议 IP 地址和网关地址,并设置此 IP 地址的地址解析协议 ARP 信息为静默状态;

所述处理单元,用于,当所述内网第一设备和外网设备进行通信时,接收所述内网第一设备发送到外网的报文,该报文的媒体接入控制 MAC 地址为网关的 MAC 地址,NAT 设备将该报文进行二层转发,从与该报文的入接口位于同一 VLAN 的公网接口转发出去;

当所述内网第二设备与外网设备进行通信时,接收所述内网第二设备发送到外网的报

文,对该报文进行网络地址端口转换处理,转化后的源 IP 地址为所述分配给内网第一设备的公网 IP 地址,在本地记录网络地址转换 NAT 转发表,将进行了网络地址端口转换处理后的报文从公网接口转发出去;

当外网设备发送的报文到达 NAT 设备时,以目的 IP 地址和端口号来匹配所述 NAT 转发表,如果能匹配其中的表项,则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备;如果未能匹配其中的表项则直接将报文转发给所述第一设备。

5. 根据权利要求 4 所述的 NAT 设备,其特征在于,所述下发单元,还用于,当所述内网第一设备通过动态主机配置协议 DHCP 方式获取公网 IP 地址时,侦听所述内网第一设备和 DHCP 服务器交互的 DHCP 报文,将帧听到的 DHCP ACK 类型报文中客户端 IP 地址和网关地址下发到虚接口上;

当所述内网第一设备通过以太网上的点到点协议 PPPOE 方式获取工位 IP 地址时,帧听 PPPOE 过程的交互报文,将 PPPOE 服务器分配给所述第一设备的 IP 地址下发到虚接口上;

当所述内网第一设备静态配置公网 IP 地址网关地址时,在虚接口上静态配置该公网 IP 地址和网关地址。

6. 根据权利要求 4 所述的 NAT 设备,其特征在于,所述处理单元还用于,当所述内网第一设备和内网第二设备通信时,根据接收到的报文的的目的 IP 进行三层转发。

一种内网设备与外网设备通信的方法和网络地址转换设备

技术领域

[0001] 本发明涉及网络地址转换 (NAT) 应用技术领域,特别涉及一种内网设备与外网设备通信的方法和 NAT 设备。

背景技术

[0002] 随着互联网技术的迅猛发展,因特网协议 (IP) 地址越来越匮乏,为了解决这一问题,NAT 技术应运而生。NAT 本质上是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址,从而实现使用少量的公网 IP 地址代表较多的私网 IP 地址,减缓可用 IP 地址空间的枯竭。

[0003] 图 1 为现有 NAT 处理方式的过程示意图。如图 1 所示,要实现私网主机 (Host) 与公网中的文件传输协议服务器 (FTP server) 的互访,需要在 NAT 中配置私网地址 192.168.0.10 到公网地址 50.10.10.10 的映射,具体处理过程包括以下步骤:

[0004] 步骤 101:私网 Host 和公网 FTP server 之间通过传输控制协议 (TCP) 三次握手成功建立控制连接。

[0005] 步骤 102:Host 向 FTP server 发送端口 (Port) 报文,Port 报文载荷中携带私网 Host 指定的数据连接的目的地址和端口,用于通知 FTP server 使用该地址和端口同自己进行数据连接。

[0006] 步骤 103:Port 报文在经过 NAT 设备时,报文载荷中的私网地址和端口会被转换成对应的公网地址和端口,即,NAT 设备将接收到的 Port 报文载荷中的私网地址 192.168.0.10 转换成公网地址 50.10.10.10,端口 1024 转换成 5000。

[0007] 需要说明的是,在本步骤中,只有当 NAT 设备具备应用层网关 (ALG) 功能时,NAT 设备才能够将接收到的 Port 报文载荷中的地址和端口进行转换,以完成私网同公网的交互。

[0008] 步骤 104:公网的 FTP server 收到 Port 报文后,解析其内容,并向 Host 发起数据连接,该数据连接的目的地址为 50.10.10.10,端口为 5000。

[0009] 步骤 105:Port 报文在经过 NAT 设备时,报文载荷中的公网地址和端口会被转换成对应的私网地址和端口,即,NAT 设备将接收到的 Port 报文载荷中的公网地址 50.10.10.10 转换成私网地址 192.168.0.10,端口 5000 转换成 1024。

[0010] 同步骤 103 一样,在本步骤中,也是只有当 NAT 设备具备应用层网关 (ALG) 功能时,NAT 设备才能够将接收到的 Port 报文载荷中的地址和端口进行转换,以完成私网同公网的交互。

[0011] 步骤 106:在完成了地址和端口转换后,FTP server 向 Host 发起数据连接。

[0012] 至此,即完成了现有 NAT 处理方式的整个工作过程。在建立完数据连接后,Host 和 FTP server 即可在已经建立的数据连接上进行数据传输。

[0013] 图 2 为现有一种家庭组网拓扑示意图,如图 2 所示,局域网中的网络摄像机 (IPC)、个人计算机 -A (PC-A) 或者 PC-B 利用同一个公网的 IP 地址同公网中的服务器进行交互时,通常是通过虚拟服务器 (又称端口映射) 或隔离区 (DMZ) 方式来实现的,下面分别对这两种方式进行介绍。

[0014] 虚拟服务器方式:本质上是将公网 IP 地址、端口号(外部端口)和局域网内服务器 IP 地址、端口号(内部端口)建立映射关系,所有对该公网口某服务端口的访问将会被重定向到对应的局域网内服务器的相应内部端口。

[0015] DMZ 方式:DMZ 主机实际上就是一个缺省的虚拟服务器,当 DMZ 主机接收到一个来自外部网络的连接请求时,首先查找虚拟服务列表,如果有匹配的表项,就把请求消息发送到对应的虚拟服务器上去。如果没有查到匹配的表项,就直接把该报文的目的 IP 修改为事先设置好的 DMZ 主机的 IP 地址,然后转发到 DMZ 主机上去。

[0016] 通过上述分析可以看出,现有家庭组网中所采用的虚拟服务器方式或者 DMZ 方式本质上都采用了 NAT 转换,即都需要将一个 IP 地址转换为另一个 IP 地址,而采用 NAT 方式时需要 NAT 设备具有 ALG 功能,对于某些私有协议、或者目前还没有支持 ALG 功能的协议,是无法穿透 NAT 设备的,也就无法实现局域网中的设备同公网中的服务器的交互。进一步地,对于局域网中的某个设备来说,可能需要频繁地与公网中的服务器进行交互,而现有的处理方式需要进行地址转换过程,也就延缓了交互过程。

发明内容

[0017] 有鉴于此,本发明提供了一种内网设备与外网设备通信的方法,能够使得局域网中的一台设备利用公网 IP 地址快捷地实现同公网的交互、其它设备通过 NAT 转换实现同公网的交互,而且实现方式灵活。

[0018] 本发明还提供了一种 NAT 设备,能够使得局域网中的一台设备利用公网 IP 地址快捷地实现同公网的交互、其它设备通过 NAT 转换实现同公网的交互,而且实现方式灵活。

[0019] 为了达到上述目的,本发明提出的技术方案为:

[0020] 一种内网设备与外网设备通信的方法,该方法包括:

[0021] 网络地址转换 NAT 设备将自身与内网第一设备相连的接口和自身的公网接口划入同一虚拟局域网 VLAN,将自身与内网第二设备相连的接口划入另一 VLAN,在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址,并设置此因特网协议 IP 地址的地址解析协议 ARP 信息为静默状态;

[0022] 所述内网第一设备和外网设备进行通信时,NAT 设备接收所述内网第一设备发送到外网的报文,该报文的目的媒体接入控制 MAC 地址为网关的 MAC 地址,NAT 设备将该报文进行二层转发,从与该报文的入接口位于同一 VLAN 的公网接口转发出去;

[0023] 所述内网第二设备与外网设备进行通信时,NAT 设备接收所述内网第二设备发送到外网的报文,对该报文进行网络地址端口转换处理,转化后的源 IP 地址为所述分配给内网第一设备的公网 IP 地址,在本地记录 NAT 转发表,将进行了网络地址端口转换处理后的报文从公网接口转发出去;

[0024] 当外网设备发送的报文到达 NAT 设备时,NAT 设备以目的 IP 地址和端口号来匹配所述 NAT 转发表,如果能匹配其中的表项,则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备;如果未能匹配其中的表项则直接将报文转发给所述第一设备。

[0025] 在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址包括:

[0026] 当所述内网第一设备通过动态主机配置协议 DHCP 方式获取公网 IP 地址时, NAT 设备侦听所述内网第一设备和 DHCP 服务器交互的 DHCP 报文, 将帧听到的 DHCP ACK 类型报文中客户端 IP 地址和网关地址下发到虚接口上;

[0027] 当所述内网第一设备通过以太网上的点到点协议 PPPOE 方式获取工位 IP 地址时, NAT 设备侦听 PPPOE 过程的交互报文, 将 PPPOE 服务器分配给所述第一设备的 IP 地址下发到虚接口上;

[0028] 当所述内网第一设备静态配置公网 IP 地址网关地址时, NAT 设备在自身的虚接口上静态配置该公网 IP 地址和网关地址。

[0029] 该方法进一步包括:

[0030] 所述内网第一设备和内网第二设备通信时, NAT 设备根据接收到的报文的 IP 进行三层转发。

[0031] 一种网络地址转换 NAT 设备, 该 NAT 设备包括: 划分单元、下发单元和处理单元, 其中,

[0032] 所述划分单元, 用于将与内网第一设备相连的接口和公网接口划入同一虚拟局域网 VLAN, 将与内网第二设备相连的接口划入另一 VLAN;

[0033] 所述下发单元, 用于在启用的虚拟接口上下发分配给所述内网第一设备的公网因特网协议 IP 地址和网关地址, 并设置此 IP 地址的地址解析协议 ARP 信息为静默状态;

[0034] 所述处理单元, 用于, 当所述内网第一设备和外网设备进行通信时, 接收所述内网第一设备发送到外网的报文, 该报文的媒体接入控制 MAC 地址为网关的 MAC 地址, NAT 设备将该报文进行二层转发, 从与该报文的入接口位于同一 VLAN 的公网接口转发出去;

[0035] 当所述内网第二设备与外网设备进行通信时, 接收所述内网第二设备发送到外网的报文, 对该报文进行网络地址端口转换处理, 转化后的源 IP 地址为所述分配给内网第一设备的公网 IP 地址, 在本地记录网络地址转换 NAT 转发表, 将进行了网络地址端口转换处理后的报文从公网接口转发出去;

[0036] 当外网设备发送的报文到达 NAT 设备时, 以目的 IP 地址和端口号来匹配所述 NAT 转发表, 如果能匹配其中的表项, 则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备; 如果未能匹配其中的表项则直接将报文转发给所述第一设备。

[0037] 所述下发单元, 还用于, 当所述内网第一设备通过动态主机配置协议 DHCP 方式获取公网 IP 地址时, 侦听所述内网第一设备和 DHCP 服务器交互的 DHCP 报文, 将帧听到的 DHCP ACK 类型报文中客户端 IP 地址和网关地址下发到虚接口上;

[0038] 当所述内网第一设备通过以太网上的点到点协议 PPPOE 方式获取工位 IP 地址时, 侦听 PPPOE 过程的交互报文, 将 PPPOE 服务器分配给所述第一设备的 IP 地址下发到虚接口上;

[0039] 当所述内网第一设备静态配置公网 IP 地址网关地址时, 在虚接口上静态配置该公网 IP 地址和网关地址。

[0040] 所述处理单元还用于, 当所述内网第一设备和内网第二设备通信时, 根据接收到的报文的 IP 进行三层转发。

[0041] 综上所述, 本发明所采用的内网设备与外网设备通信的方法和 NAT 设备, 是通过

将自身与内网第一设备相连的接口和自身的公网接口划入同一 VLAN,将自身与内网第二设备相连的接口划入另一 VLAN,在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址,从而使得内网第一设备与外网进行通信时,无需通过 NAT 转换,而是直接将报文从与该报文的入接口位于同一 VLAN 的公网接口转发出去;而内网第二设备与外网设备进行通信时,需要通过 NAT 转换来进行;当外网设备发送的报文到达 NAT 设备时,NAT 设备能够根据是否匹配到 NAT 转发表来确实将报文转发给内网第一设备还是内网第二设备。因此,本发明所采用的内网设备与外网设备通信的方法能够使得与内网第一设备直接通过公网 IP 地址无需进行 NAT 转换直接与公网进行交互,而内网第二设备需要经过 NAT 转换完成同公网的交互,并且内网第一设备和内网第二设备对外网显示的公网 IP 地址是同一个公网 IP 地址。

附图说明

[0042] 图 1 为现有 NAT 处理方式的过程示意图

[0043] 图 2 为现有一种家庭组网拓扑示意图;

[0044] 图 3 为本发明内网设备与外网设备通信方法的工作流程图;

[0045] 图 4 为本发明所采用的 NAT 设备的结构示意图。

具体实施方式

[0046] 为了解决现有技术中存在的问题,本发明提出了一种新的内网设备与外网设备通信的方法,其具体实现包括:

[0047] NAT 设备将自身与内网第一设备相连的接口和自身的公网接口划入同一 VLAN,将自身与内网第二设备相连的接口划入另一 VLAN,在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址,并设置此 IP 地址的 ARP 信息为静默状态;

[0048] 所述内网第一设备和外网设备进行通信时,NAT 设备接收所述内网第一设备发送到外网的报文,该报文的目的 MAC 地址为网关的 MAC 地址,NAT 设备将该报文进行二层转发,从与该报文的入接口位于同一 VLAN 的公网接口转发出去;

[0049] 所述内网第二设备与外网设备进行通信时,NAT 设备接收所述内网第二设备发送到外网的报文,对该报文进行网络地址端口转换处理,转化后的源 IP 地址为所述分配给内网第一设备的公网 IP 地址,在本地记录 NAT 转发表,将进行了网络地址端口转换处理后的报文从公网接口转发出去;

[0050] 当外网设备发送的报文到达 NAT 设备时,NAT 设备以目的 IP 地址和端口号来匹配所述 NAT 转发表,如果能匹配其中的表项,则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备;如果未能匹配其中的表项则直接将报文转发给所述第一设备。

[0051] 为使本发明的目的、技术方案和优点更加清楚,下面将结合附图及具体实施例对本发明作进一步地详细描述。

[0052] 图 3 为本发明内网设备与外网设备通信方法的工作流程图。如图 3 所示,该流程包括预先设置和对报文进行处理两个过程,其中,预先设置可参见步骤 301-302,对报文进行处理可参见步骤 303-308,以下分别对这两个过程进行详细介绍:

[0053] 步骤 301 :NAT 设备将自身与内网第一设备相连的接口和自身的公网接口划入同一 VLAN,将自身与内网第二设备相连的接口划入另一 VLAN。

[0054] 需要说明的是,在本步骤中,由于内网第一设备需要利用公网 IP 地址直接与外网设备进行通信,所以内网第一设备直接先将报文发送给自己的网关,封装的报文的 MAC 地址为网关的 MAC 地址,然后,由 NAT 设备对该报文进行二层转发,从公网接口发送出去。因此,需要将 NAT 设备与内网第一设备相连的接口和 NAT 设备自身的接口划入同一 VLAN。

[0055] 步骤 302 :NAT 设备在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址,并设置此 IP 地址的 ARP 信息为静默状态。

[0056] 需要说明的是,在本步骤中,内网第一设备获取公网 IP 地址可采用如下三种方式:

[0057] 1、以太网上的点到点协议 (PPPOE) 方式,与公网进行快捷交互的设备获取公网 IP 地址,NAT 设备监听与公网进行快捷交互的设备 PPPOE 过程的交互报文,在交互到 IP 控制协议 (IPCP) 阶段时,监听 PPPOE 服务器给 PPPOE 客户端回应的地址确认消息,记录下服务器分给 PPPOE 客户端的 IP 地址,该 IP 地址即为公网 IP 地址;

[0058] 2、动态主机配置协议 (DHCP) 获取方式,NAT 设备监听 DHCP 报文的 DHCP 确认信息 (ACK) 类型报文,在记录下 DHCP ACK 报文里的客户端 IP 地址 (Client IP Address) 和网关信息,该 IP 地址即为公网 IP 地址;

[0059] 3、手动静态配置的方式,这种方式需要在 NAT 设备上手工静态配置公网 IP 地址和网关等信息。

[0060] 在实际中,还可采用其他方式来获取公网 IP 地址和公网网关信息,以不影响本发明实施例的实现为准。

[0061] 还需说明的是,在侦听到公网 IP 地址和网关地址后,NAT 设备需要启用一个虚拟接口,并在该虚拟接口上下发侦听到的公网 IP 地址和网关地址,以便与内网第一设备能够根据公网 IP 地址与公网进行交互,内网设备去往外网时能够利用这个虚拟接口上的地址建立 NAT 转发表项。同时,NAT 设备需设定侦听到的公网 IP 地址的地址解析协议 (ARP) 信息为静默状态,即既不发送免费 ARP 也不回应该 ARP 的请求,以避免发生地址冲突。

[0062] 在本步骤中,内网第一设备需要与外网设备利用公网 IP 地址进行通信,因此,设置 NAT 设备既不发送针对公网 IP 地址的免费 ARP 报文,也不回应针对该公网 IP 地址的 ARP 请求报文,以避免 NAT 设备和内网第一设备之间检测到 IP 地址冲突。

[0063] 在完成了上述设置之后,即可进行内网设备与外网设备之间的通信,在本实施例中,主要以内网去往外网的报文、外网去往外网的报文、内网第一设备与内网第二设备通信的报文这三种报文为例来介绍具体的处理过程:

[0064] 对于内网去往外网的报文,

[0065] 步骤 303 :NAT 设备判断接收到的内网去往外网的报文的接口与公网接口是否属于同一 VLAN,如果是,执行步骤 304 ;否则,执行步骤 305。

[0066] 步骤 304 :NAT 设备将该报文进行二层转发,从与该报文的入接口位于同一 VLAN 的公网接口转发。

[0067] 步骤 305 :NAT 设备按照现有的方式对接收到的内网去往外网的报文进行处理,结束处理过程。

[0068] 当 NAT 设备判断出接收到的内网去往外网的报文的接口与公网接口不属于同一 VLAN 时,说明发出该报文的设备不是与公网进行快捷交互的设备,也即内网第二设备,则按照现有的 NAT 转发表项进行处理即可,也即按照现有流程对该报文进行处理,具体如何采用现有流程处理报文可参见图 1,这里不再赘述。

[0069] 需要说明的是,现有的 NAT 转发表项可参见如下表 1。

[0070] 表 1

[0071]

Protocol	GlobalAddr	GlobalPort	InsideAddr	Port	DestAddr	Port
TCP	200.0.0.28	12288	192.168.0.10	512	162.105.26.246	512

[0072] 至此,即完成了对内网去往外网的报文的处理过程。

[0073] 对于外网去往外网的报文,

[0074] 步骤 306 :NAT 设备将接收到的外网去往外网的报文与 NAT 转发表项进行匹配,如果匹配到对应的 NAT 转发表项,则执行步骤 307 ;否则,执行步骤 308。

[0075] 步骤 307 :NAT 设备按照现有的方式对接收到的外网去往外网的报文进行处理,结束处理过程。

[0076] 步骤 308 :NAT 设备将该报文从与该报文的入接口位于同一 VLAN 的接口发送,即直接发送给内网第一设备。

[0077] 需要说明的是,当外网设备发送的报文到达 NAT 设备时,NAT 设备以目的 IP 地址和端口号来匹配所述 NAT 转发表,如果能匹配其中的表项,则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备 ;如果未能匹配其中的表项则直接将报文转发给所述内网第一设备。

[0078] 至此,即完成了对外网去往外网的报文的处理过程。

[0079] 对于内网第一设备与内网第二设备通信的报文,

[0080] 步骤 309 :NAT 设备根据接收到的报文的的目的 IP 查找路由表,直接进行三层转发。

[0081] 当与公网进行快捷交互的设备与内网中与其不在同一网段的其它设备进行通信时,当报文达到 NAT 设备时,NAT 设备检测到这两个设备不在同一网段,需要进行三层转发,即查找路由表,发现其下一跳即直连网段,再查 ARP 表,封装对应的 MAC 地址,从该 MAC 地址对应的出接口转发出去。

[0082] 至此,即完成了对内网第一设备与内网第二设备通信的报文的处理过程。

[0083] 在完成了对上述三种报文的处理后,即完成了本发明内网设备与外网设备通信的方法的整个工作流程。

[0084] 基于上述方法,图 4 为本发明所采用的 NAT 设备的结构示意图,如图 4 所示,该 NAT 设备包括 :划分单元 41、下发单元 42 和处理单元 43,其中,

[0085] 所述划分单元 41,用于将与内网第一设备相连的接口和公网接口划入同一 VLAN,将与内网第二设备相连的接口划入另一 VLAN。

[0086] 由于内网第一设备需要利用公网 IP 地址直接与外网设备进行通信,所以内网第一设备直接先将报文发送给自己的网关,封装的报文的的目的 MAC 地址为网关的 MAC 地址,然后,对该报文需要进行二层转发,从公网接口发送出去。因此,需要将内网第一设备相连的

接口和公网接口划入同一 VLAN。

[0087] 所述下发单元 42,用于在启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址,并设置此 IP 地址的 ARP 信息为静默状态。

[0088] 进一步地,所述下发单元 42,还用于当所述内网第一设备通过 DHCP 方式获取公网 IP 地址时,侦听所述内网第一设备和 DHCP 服务器交互的 DHCP 报文,将帧听到的 DHCP ACK 类型报文中客户端 IP 地址和网关地址下发到虚接口上;

[0089] 当所述内网第一设备通过 PPPoE 方式获取工位 IP 地址时,帧听 PPPoE 过程的交互报文,将 PPPoE 服务器分配给所述第一设备的 IP 地址下发到虚接口上;

[0090] 当所述内网第一设备静态配置公网 IP 地址网关地址时,在虚接口上静态配置该公网 IP 地址和网关地址。

[0091] 所述处理单元 43,用于所述内网第一设备和外网设备进行通信时,接收所述内网第一设备发送到外网的报文,该报文的源 MAC 地址为网关的 MAC 地址,NAT 设备将该报文进行二层转发,从与该报文的入接口位于同一 VLAN 的公网接口转发出去;

[0092] 所述内网第二设备与外网设备进行通信时,接收所述内网第二设备发送到外网的报文,对该报文进行网络地址端口转换处理,转化后的源 IP 地址为所述分配给内网第一设备的公网 IP 地址,在本地记录 NAT 转发表,将进行了网络地址端口转换处理后的报文从公网接口转发出去;

[0093] 当外网设备发送的报文到达 NAT 设备时,以目的 IP 地址和端口号来匹配所述 NAT 转发表,如果能匹配其中的表项,则按照表项记录的内容进行网络地址端口转换处理并将转换后的报文发送内网第二设备;如果未能匹配其中的表项则直接将报文转发给所述第一设备。

[0094] 进一步地,所述处理单元 41 还用于,所述内网第一设备和内网第二设备通信时,根据接收到的报文的源 IP 进行三层转发。

[0095] 至此,即得到了本发明所采用的 NAT 设备。

[0096] 图 4 所采用的 NAT 的具体工作流程请参照图 3 所示方法实施例中的相应说明,此处不再赘述。

[0097] 总之,本发明所采用的内网设备与外网设备通信的方法和 NAT 设备,是通过将自身与内网第一设备相连的接口和自身的公网接口划入同一 VLAN,将自身与内网第二设备相连的接口划入另一 VLAN,在自身启用的虚拟接口上下发分配给所述内网第一设备的公网 IP 地址和网关地址,从而使得内网第一设备与外网进行通信时,无需通过 NAT 转换,而是直接将报文从与该报文的入接口位于同一 VLAN 的公网接口转发出去;而内网第二设备与外网设备进行通信时,需要通过 NAT 转换来进行;当外网设备发送的报文到达 NAT 设备时,NAT 设备能够根据是否匹配到 NAT 转发表来确实将报文转发给内网第一设备还是内网第二设备。因此,本发明所采用的内网设备与外网设备通信的方法能够使得与内网第一设备直接通过公网 IP 地址无需进行 NAT 转换直接与公网进行交互,而内网第二设备需要经过 NAT 转换完成同公网的交互,并且内网第一设备和内网第二设备对外网显示的公网 IP 地址是同一个公网 IP 地址。

[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。

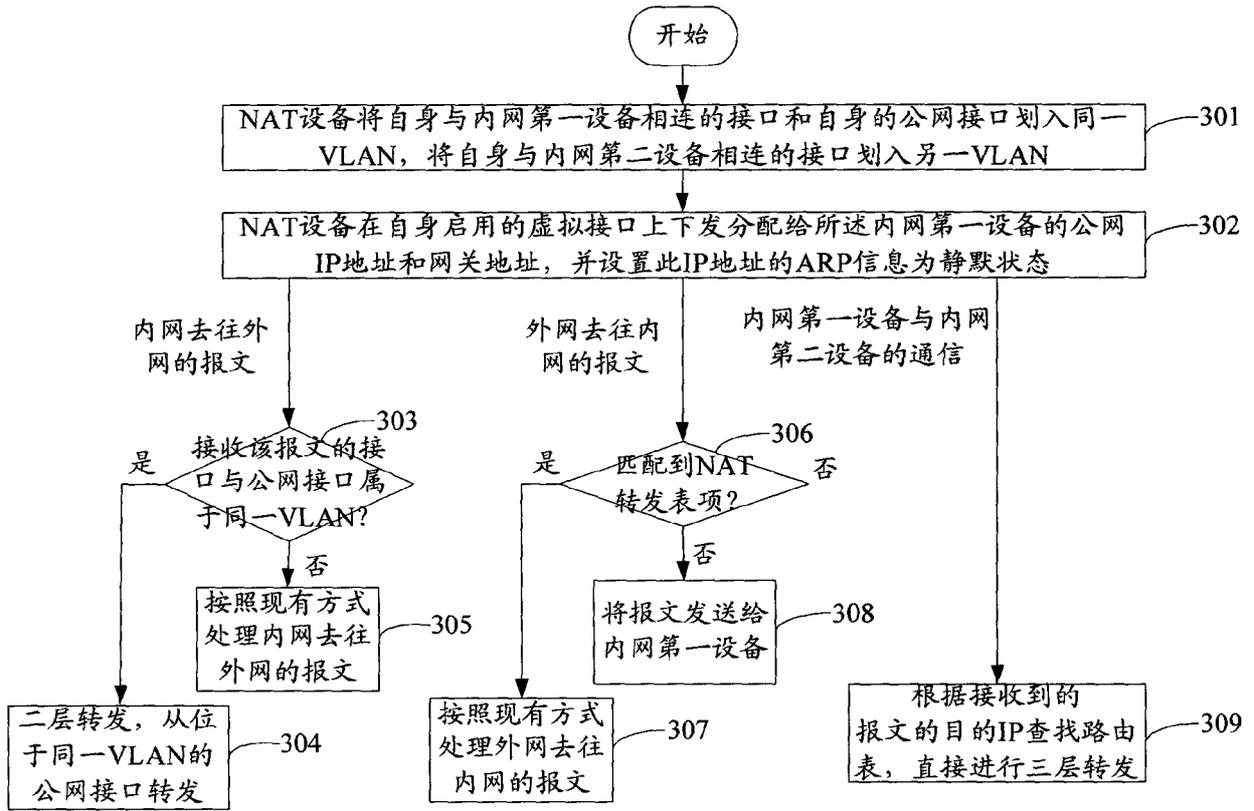


图 3

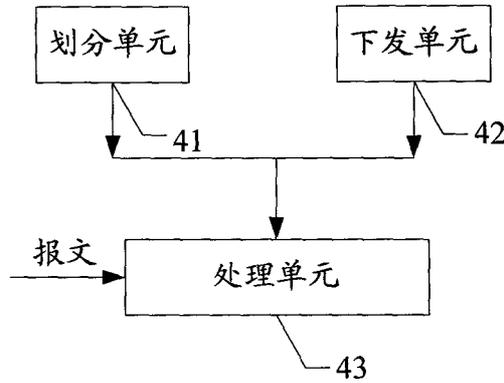


图 4