(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102761534 B
(45)授权公告日 2016.05.11

(21)申请号 201110119721.0
(22)申请日 2011.04.29
(73)专利权人 北京瑞星信息技术股份有限公司
地址 100190 北京市海淀区中关村大街22号中科大厦1301
(72)发明人 冯景辉
(74)专利代理机构 北京永新同创知识产权代理有限公司 11376
代理人 钟胜光
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
(56)对比文件
US 7290050 B1,2007.10.30,
US 7249191 B1,2007.07.24,
CN 1765090 A,2006.04.26,
王钢．应用网关防火墙——网络的中间检查站．《计算机安全》.2004,
审查员 朱冬梅

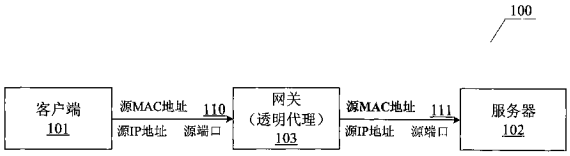
权利要求书2页 说明书7页 附图3页

(54)发明名称

实现媒体接入控制层透明代理的方法和装置

(57)摘要

公开了一种实现媒体接入控制(MAC)层透明代理的方法和装置。在网关中能够与源站进行通信的第一网卡所截取的从所述源站发往目的站的第一帧中包含的应用层数据被进行处理之后，要响应于所述第一帧而发给所述目的站的、包含经处理的所述应用层数据的第二帧的首部中的源MAC地址信息被修改为所述源站的MAC地址，并且，通过调用所述网关中能够与所述目的站进行通信的第二网卡的发送函数，所述第二帧被发送给所述目的站。



CN 102761534 B

1.一种实现媒体接入控制(MAC)层透明代理的方法,包括:

由网关中的应用层代理对由所述网关中能够与源站进行通信的第一物理网卡所截取的从所述源站发往目的站的第一帧中包含的应用层数据进行处理;

由所述网关中的虚拟网卡接收基于经所述虚拟网卡修改后的所述网关的路由策略而被路由到所述虚拟网卡的、要响应于所述第一帧而发给所述目的站的包含经处理的所述应用层数据的第二帧;

由所述虚拟网卡将所述第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址;以及

由所述虚拟网卡通过直接调用所述网关中能够与所述目的站进行通信的第二物理网卡的发送函数将所述第二帧发送给所述目的站,避免了通过网络协议栈来针对该第二物理网卡进行成帧的过程。

2.根据权利要求1所述的方法,还包括:

当所述第一帧被所述第一物理网卡截取时,记录所述第一帧的首部中的源MAC地址信息,作为所述源站的MAC地址。

3.根据权利要求2所述的方法,其中,

所述记录的步骤还包括:记录所述第一帧的首部中的目的MAC地址信息,作为所述目的站的MAC地址。

4.根据权利要求2所述的方法,其中,所述第一帧具有虚拟局域网(VLAN)标记,并且其中,

所述记录的步骤还包括:记录所述第一帧的VLAN标记中的VLAN标识符;并且

所述修改的步骤还包括:将所述第二帧的VLAN标记中的VLAN标识符修改为所记录的第一帧的VLAN标识符。

5.根据权利要求1所述的方法,还包括:

当要求在所述源站和所述目的站之间建立连接的请求帧被所述第一物理网卡截取时,记录所述请求帧的首部中的源MAC地址信息,作为所述源站的MAC地址,其中,所述第一帧是通过所要建立的连接来传输的。

6.根据权利要求5所述的方法,其中,

所述记录的步骤还包括:记录所述请求帧的首部中的目的MAC地址信息,作为所述目的站的MAC地址。

7.根据权利要求6所述的方法,还包括:

将响应于所述请求帧的应答帧的首部中的源MAC地址信息修改为所记录的所述目的站的MAC地址;以及

通过调用所述第一物理网卡的发送函数,将所述应答帧发送给所述源站。

8.根据权利要求5所述的方法,其中,所述请求帧具有虚拟局域网(VLAN)标记,并且其中,

所述记录的步骤还包括:记录所述请求帧的VLAN标记中的VLAN标识符;并且

所述修改的步骤还包括:将所述第二帧的VLAN标记中的VLAN标识符修改为所记录的请求帧的VLAN标识符。

9.根据权利要求2至8之任一所述的方法,其中,所记录的信息被存储在经扩展的连接

跟踪中。

10.一种实现媒体接入控制(MAC)层透明代理的装置,包括:

修改模块,用于在由网关中的应用层代理对由所述网关中能够与源站进行通信的第一物理网卡所截取的从所述源站发往目的站的第一帧中包含的应用层数据进行处理之后,由所述网关中的虚拟网卡将所接收的基于经所述虚拟网卡修改后的所述网关的路由策略而被路由到所述虚拟网卡的、要响应于所述第一帧而发给所述目的站的包含经处理的所述应用层数据的第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址;以及

发送模块,用于由所述虚拟网卡通过直接调用所述网关中能够与所述目的站进行通信的第二物理网卡的发送函数将所述第二帧发送给所述目的站,避免了通过网络协议栈来针对该第二物理网卡进行成帧的过程。

11.根据权利要求10所述的装置,还包括:

记录模块,用于当所述第一帧被所述第一物理网卡截取时,记录所述第一帧的首部中的源MAC地址信息,作为所述源站的MAC地址。

12.根据权利要求11所述的装置,其中,

所述记录模块还记录所述第一帧的首部中的目的MAC地址信息,作为所述目的站的MAC地址。

13.根据权利要求11所述的装置,其中,所述第一帧具有虚拟局域网(VLAN)标记,并且其中,

所述记录模块还记录所述第一帧的VLAN标记中的VLAN标识符;并且

所述修改模块还将所述第二帧的VLAN标记中的VLAN标识符修改为所记录的第一帧的VLAN标识符。

14.根据权利要求10所述的装置,还包括:

记录模块,用于当要求在所述源站和所述目的站之间建立连接的请求帧被所述第一物理网卡截取时,记录所述请求帧的首部中的源MAC地址信息,作为所述源站的MAC地址,其中,所述第一帧是通过所要建立的连接来传输的。

15.根据权利要求14所述的装置,其中,

所述记录模块还记录所述请求帧的首部中的目的MAC地址信息,作为所述目的站的MAC地址。

16.根据权利要求15所述的装置,还包括:

用于将响应于所述请求帧的应答帧的首部中的源MAC地址信息修改为所记录的所述目的站的MAC地址的模块;以及

用于通过调用所述第一物理网卡的发送函数,将所述应答帧发送给所述源站的模块。

17.根据权利要求14所述的装置,其中,所述请求帧具有虚拟局域网(VLAN)标记,并且其中,

所述记录模块还记录所述请求帧的VLAN标记中的VLAN标识符;并且

所述修改模块还将所述第二帧的VLAN标记中的VLAN标识符修改为所记录的请求帧的VLAN标识符。

18.根据权利要求11至17之任一项所述的装置,其中,所记录的信息被存储在经扩展的连接跟踪中。

实现媒体接入控制层透明代理的方法和装置

技术领域

[0001] 本发明总体上涉及信息处理领域，更具体地，涉及一种实现媒体接入控制(MAC)层透明代理的方法和装置。

背景技术

[0002] 基于网关的内容过滤设备(例如，防火墙)通常有两种实现方式：一种为过滤型，一种为代理型。所谓过滤型网关是指网络上传输的数据在经过网关设备时被该网关设备截获并分析其中的内容；而代理型网关则是由向服务器进行通信的客户端首先与网关代理进行通信，而网关代理再去与真实的服务器进行通信，在这个过程中，网关代理可以缓存数据内容。

[0003] 更具体地，作为一种实现透明传输的代理型网关，客户端和服务器之间的通信被代理到中间的网关设备身上；客户端以为是在与服务器直接进行通信，但实际上它是与网关设备进行通信，而网关设备再以客户端的身份与服务器进行通信。而且，该代理型网关可以模拟服务器的身份来改变与客户端通信的行为和细节；可以选择仅将与服务器通信的安全的数据返还给客户端。

[0004] 在这种透明传输模型中，如前所述，网关设备是以客户端的身份来与服务器进行通信。所谓客户端的身份，在通常的代理模型中是以客户端的网际协议(IP)地址来标识的。例如，网关设备使用客户端的IP地址来与服务器进行通信并传输数据，具体地，作为透明代理，网关设备保证发往服务器的分组的源IP地址信息与真实客户端的IP地址是一样的。在典型的网络七层协议体系结构中，IP处于网络层(即，第三层)，因此通常的代理模型实现了第三层透明。

发明内容

[0005] 根据本发明的一个实施例，公开了一种实现MAC层透明代理的方法。所述方法包括：在网关中能够与源站进行通信的第一网卡所截取的从所述源站发往目的站的第一帧中包含的应用层数据被进行处理之后，把要响应于所述第一帧而发给所述目的站的、包含经处理的所述应用层数据的第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址；以及，通过调用所述网关中能够与所述目的站进行通信的第二网卡的发送函数，将所述第二帧发送给所述目的站。

[0006] 根据本发明的另一个实施例，公开了一种实现MAC层透明代理的装置。所述装置包括：修改模块，用于在网关中能够与源站进行通信的第一网卡所截取的从所述源站发往目的站的第一帧中包含的应用层数据被进行处理之后，把要响应于所述第一帧而发给所述目的站的、包含经处理的所述应用层数据的第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址；以及发送模块，用于通过调用所述网关中能够与所述目的站进行通信的第二网卡的发送函数，将所述第二帧发送给所述目的站。

附图说明

[0007] 参照下列附图描述了本发明的示例性实施例。应该理解，这些附图仅是示例性的、而非限制性的，并且附图中相同或相似的参考标记指示对应的或类似的要素。

[0008] 图1示出了根据本发明的一个示例性实施例的系统的概览；

[0009] 图2更详细地示出了根据本发明的一个示例性实施例的系统；

[0010] 图3示出了根据本发明的一个示例性实施例的方法的流程图；以及

[0011] 图4示出了根据本发明的一个示例性实施例的装置的框图。

具体实施方式

[0012] 在下面的详细说明中，给出了大量的具体细节，以提供对本发明的实施例的透彻理解。然而，本领域技术人员应该理解，这些具体细节仅仅是示例性的而非限制性的，可以在没有这些具体细节的情况下实现本发明。在说明书中，并未详细描述一些公知的部件、结构和操作，以免不当地模糊本发明。

[0013] 说明书中提及的短语“一个实施例”或“实施例”等表示结合该实施例而描述的特定特征、结构或特性被包括在本发明的至少一个实施例中。因此，在本说明书中各处出现的短语“在一个实施例中”或“根据一个实施例”等并不一定指代同一个实施例。

[0014] 本领域技术人员可以理解，本文所述的实施例可以由硬件、软件、固件、中间件、微代码或其任意组合来实现。

[0015] 首先参考图1，其示出了根据本发明的一个示例性实施例的系统100的概览。

[0016] 在系统100的一种典型实现中，客户端101位于网络(例如，局域网，未示出)的一个区域中，服务器102位于同一网络的另一区域中，而网关103则位于这两个区域之间，起到桥接的作用。为了简便起见，对于该系统的各个组成部件，这里仅示出了单个的设备，然而本发明并不限于此。

[0017] 客户端101可以包括多种基于处理器的计算设备中的任意一种，其在网络内具有自己的唯一身份标识，例如，包括但不限于该客户端的物理地址(即，媒体接入控制(MAC)地址)、IP地址等等。所述客户端可以运行有各种操作系统中的一种或多种，例如，包括但不限于各种版本的Linux™、Unix™、Windows™，等等。

[0018] 类似地，服务器102和网关103也可以分别包括多种基于处理器的计算设备中的任意一种；同样，服务器102和网关103也可以分别运行有各种操作系统中的一种或多种。服务器102用于为包括客户端101在内的各种请求设备提供各种类型的服务。网关103处于桥接模式，用于实现客户端101和服务器102之间的通信。在本发明的实施例中，网关102还能够提供应用层代理服务，并且其代理功能对于网络七层协议体系结构中的第二层(数据链路层，更具体地说，其中的MAC子层)来说也是透明的。

[0019] 下面，以源站(例如，客户端101)向目的站(例如，服务器102)发送数据为例，说明在网关(或透明代理网关)103存在的情况下，客户端101与服务器102之间实际发生的一种通信过程。本领域技术人员可以理解，这里以客户端101作为源站、以服务器102作为目的站仅是一种示例情况，本发明并不限于此。

[0020] 客户端101发出的数据会首先被透明代理网关103所截取，而后者再去以客户端

101的身份向服务器102发送该数据。由此，通过居间的透明代理网关103，在客户端101和服务器102之间实现数据传输。从客户端101的角度来看，它是在直接与服务器102进行通信，但实际并非如此。

[0021] 更具体地，参照图1，在透明代理网关103接收(或截取)到客户端101向服务器102发出的帧110(如图中左侧的箭头所示)时，可以对该帧110的首部中所含的MAC层信息进行记录，例如，至少包括源MAC地址信息(即，客户端101自身的MAC地址)，等等。所记录的MAC层信息还可以包括帧110的目的MAC地址信息(即，服务器202的MAC地址)。此外，取决于实际需要，还可以记录其它信息，例如在使用802.1Q虚拟局域网(VLAN)的情况下(其中在以太网的帧格式中插入一个4字节的VLAN标记)，还可以记录VLAN标记中的VLAN标识符(ID)等等，本发明并不限于此。

[0022] 在上述记录操作完毕之后，在一个实施例中，可以开始对所接收到的帧110中包含的应用层数据进行应用层代理处理。所述应用层数据是指与应用进程的操作相关的数据，例如，包括但不限于电子邮件、HTTP报文等等，其是在分层协议信息结构的应用层中被进行处理的。在透明代理网关103中，应用层代理处理例如包括但不限于查杀病毒、内容过滤等等，如现有技术中所用到的那样。

[0023] 在应用层代理处理完毕之后，在适当的时机，透明代理网关103将以客户端101的身份来向服务器102发出帧111(如图中右侧的箭头所示)，该帧111中包含了之前处理完的应用层数据。需要注意的是，根据本发明，对于该帧111，可以使用之前所记录的帧110的源MAC地址信息来修改帧111的首部中的对应信息，然后再将修改后的帧111发给服务器102。通过这样的处理，可以理解，透明代理网关103发出的帧111的MAC层信息是同客户端101发出的原始帧110保持一致的，因此能够实现第二层透明。

[0024] 与之相比，在运行例如Linux系统的现有透明代理网关上，尽管可以通过调用系统API修改发起方的IP地址和端口(以使得从网关转发往目标服务器的分组看起来是从原始的客户端直接发出的，以此来实现第三层透明，如前所述)，但是却无法修改源MAC地址。在这种情况下，例如，作为网关设备和服务器之间的一些第二层过滤设备，可能完全看不到本来真实的客户端MAC地址，而导致相应的控制、准入策略等一系列的问题无法解决，造成这样的代理实现不是真正的透明，也就是说，其在对数据传输进行代理的过程中修改了客户端的一些身份标识信息。

[0025] 如前所述，利用本发明的设计，能够实现第二层透明，从而便利了用户网络部署，同时改进了用户体验。

[0026] 图2更详细地示出了根据本发明的一个示例性实施例的系统200。在下文中，省略了针对与图1中相同的单元(例如，客户端201、服务器202等等)的说明，而着重具体描述本发明的网关(或透明代理)203。

[0027] 如图所示，根据本发明的一个实施例，透明代理网关203可以包括记录逻辑204、应用层代理205、以及虚拟网卡(VIF)206。作为处于桥接模式的网关，其典型地具有多个接口(即，网卡)以用于与各自对应的目标站进行通信。为了描述的方便，在图2中针对透明代理网关203仅示出了两个接口，即能够与客户端201进行通信的网卡207、以及能够与服务器202进行通信的网卡208。

[0028] 如本领域技术人员所已知的，通常网关设备中维护有一个转发表(未示出)，其中

的条目(如果有的话)表明目标站(用其MAC地址来标识)与该网关的一个接口之间的对应关系,例如客户端201对应于网卡207、服务器202对应于网卡208等等。透明代理网关203(更具体地,例如,网卡207)在截取到从作为源站的客户端201发往作为目的站的服务器202的一个帧(例如,帧210)时,确定该网关能够与服务器202进行通信,例如,通过搜索转发表,发现存在与服务器202相对应的网卡208。

[0029] 在图2中,记录逻辑204用于记录网卡207所截取的从客户端201发往服务器202的帧210的有关信息。在本发明的一个示例性实施例中,所述信息至少包括帧210的源(即,客户端201)MAC地址,这可以从该帧的首部中获得。所述信息例如还可以包括但不限于:帧210的目的(即,服务器202)MAC地址,这也可以从该帧的首部中获得;与该目的MAC地址相对应的属于网关203的接口(即,网卡208),这可以从所述转发表中获得;等等。这些信息可以被相关联地存储,以便于使用。

[0030] 作为一个非限定性的例子,在基于Linux的透明代理网关中,可以使用连接跟踪来允许内核跟踪并记录所有的逻辑网络连接或会话。在本发明的一种示例实现中,可以扩展针对每个连接而维护的数据结构(例如,以IP地址和端口作为其标识)以便存储更多的信息。例如,记录逻辑204可以将所需的信息(例如,帧210的源和目的MAC地址等等)相关联地记录在扩展后的结构中,供后续过程使用。

[0031] 通过网络协议栈,之前接收到的帧210被逐层剥去首部并向更高层传递,最终其中包含的应用层数据被传递给应用层代理206以进行常规的应用层代理处理,例如,包括但不限于查杀病毒、内容过滤等等。本发明的主要改进不在于此,因此省略对其的进一步描述。

[0032] 继续参考图2,在本发明的一个示例性实施例中,对于透明代理网关203响应于接收到的帧210、而以客户端101的身份向服务器102发送的帧211,通过VIF 206能够实现该帧中源MAC地址的恢复。

[0033] 虚拟网卡VIF 206可以通过网卡驱动的形式来实现。在操作系统中加载该驱动从而对该网卡进行注册之后,VIF 206被操作系统识别成是一块普通的网卡。根据本发明的一个示例性实施例,VIF 206可以修改透明代理网关203的路由策略(例如,路由表),以使得对于经应用层代理205处理的、需要透明发送出去(例如,发给服务器202)的数据都被路由到VIF 206来进行发送。

[0034] VIF 206具有修改与帧210对应的帧211的源MAC地址的能力。按照本发明的一个实施例,例如,VIF 206可以参考之前由记录逻辑204记录(在扩展的连接跟踪中)的帧210的有关信息中的对应内容,作为客户端201的MAC地址;接着,将帧211的首部中的源MAC地址信息修改为所记录的源MAC地址(即,客户端201的MAC地址);然后,直接调用网卡208的发送函数将修改后的帧211发送给服务器202。

[0035] 由此,在透明代理网关203以客户端201的身份发送给服务器202的帧211中,能够确保源MAC地址信息也是与客户端201自身的MAC地址一样的,从而实现了第二层(MAC层)透明。

[0036] 在本发明的一个实施例中,例如可以利用之前记录的信息,参考该网关的转发表,来确定通过网卡208进行发送。

[0037] 这里,由VIF 206直接调用物理网卡(例如,网卡208)的发送函数,避免了通过网络协议栈来针对该物理网卡进行成帧的过程,从而确保了经该物理网卡发出的帧的源MAC地

址保持为经上述修改后的源MAC地址(即,客户端201的MAC地址)。

[0038] 本领域技术人员可以理解,上述各个部件的功能也可以相互组合,例如,记录逻辑204和VIF 205可以被在实现单个部件中。

[0039] 另外,考虑802.1Q VLAN的情况,根据本发明的一个实施例,记录逻辑204还可以附加地记录所接收到的帧(例如,帧210)的VLAN ID,例如,可以将其与该帧的MAC地址等信息相关联地记录在连接跟踪的扩展结构中;相应地,VIF 206还可以利用所记录的该VLAN ID来更改要发给服务器202的帧(例如,帧211)的VLAN ID,从而针对VLAN也能实现第二层透明代理。

[0040] 此外,利用本发明的设计思想,本领域技术人员可以理解,对于从服务器202发往客户端201的数据(这时,服务器202可以被看成是源站,而客户端201则可以被看成是目的站),透明代理网关203可以进行类似的处理,使得在客户端201看来,是真实的服务器202在与它进行直接通信,而事实上则是居间的透明代理网关203在以服务器202的身份与其进行通信。

[0041] 此外,考虑需要通过握手来建立连接(或会话)以进行数据传输的情况(例如,使用传输控制协议(TCP))。根据本发明的一个示例性实施例,在这种情况下,当客户端201初次向服务器202发出连接建立请求时,相应的请求帧会被透明代理网关203的网卡207所截取。网关203确认自己能够与服务器202进行通信,例如,这里是通过网卡208(否则的话,网关203可以选择将该请求帧直接通过该网关上除网卡207以外的其它网卡进行广播,如现有技术中的桥接设备所实现的那样)。然后,记录逻辑204可以记录该请求帧的有关信息,例如,该帧的首部中的源MAC地址作为客户端201的MAC地址,该帧的首部中的目的MAC地址作为服务器202的MAC地址,等等,本发明并不限于此。

[0042] 根据本发明的一个示例性实施例,在这样的信息被记录之后,按照握手协议,作为透明代理网关203响应于该请求帧而以服务器202的身份向客户端201发出的应答帧,VIF 206可以将该应答帧的首部中的源MAC地址信息修改为所记录的服务器202的MAC地址,并通过直接调用网卡207的发送函数来将修改后的该应答帧发给客户端201。本领域技术人员可以理解,客户端201然后会响应于接收到该应答帧而发出再次确认帧,正如现有技术所实现的那样。通过这样的握手过程,在客户端201与透明代理网关203之间建立了连接(当然,在客户端201看来,它是直接与服务器202建立了连接)。另外,在之后适当的时机,透明代理网关203以客户端201的身份(更具体地,该客户端的MAC地址)与服务器202之间建立连接的情况与上述类似,在此不再详述。

[0043] 客户端201与服务器202之间的数据传输(例如,帧210)正是通过这样建立的连接来进行的。利用之前所记录的信息,VIF 206可以把要发给服务器202的、与帧210相对应的帧211的首部中的源MAC地址信息修改为所记录的客户端201的MAC地址,以此来实现第二层透明,如前所述。

[0044] 下面参考图3,示出了根据本发明的一个示例性实施例的方法300的流程图。所述方法300可以在具有应用层代理功能的网关(例如,透明代理网关103、203)中实现。

[0045] 如图所示,该过程开始于步骤S301,在该步骤中,对网关中的第一网卡所截取的从源站发往目的站的第一帧中包含的应用层数据进行处理。参考结合图2给出的例子,对于透明代理网关203(更具体地,其中的能够与客户端201进行通信的网卡207)所截取的从客户

端201发往服务器202的帧210中包含的应用层数据，例如包括但不限于电子邮件、HTTP报文等等，作为具有应用层代理功能的网关203，其中的应用层代理205可以对该应用层数据进行处理，例如包括但不限于查杀病毒、内容过滤等等。

[0046] 网关为了实现代理功能，需要以源站的身份来将之前从源站截取的数据(其已经过了网关的处理)发往目的端。根据本发明的一个示例性实施例，在步骤S302，把要响应于所述第一帧而发给所述目的站的、包含经处理的应用层数据的第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址。继续参考图2，在应用层代理205对帧210中包含的应用层数据进行处理之后，VIF 206可以把所形成的包含经处理的该应用层数据的第二帧211的首部中的源MAC地址信息修改为客户端201自身的MAC地址。也就是说，这样修改后的帧211的首部中的MAC地址信息是与客户端201原始发出的帧210的首部中的MAC地址信息保持一致的。

[0047] 然后，该过程前进到步骤S303，在该步骤中，通过直接调用所述网关中的第二网卡的发送函数，将所述第二帧发送给所述目的站。继续参考图2，VIF 206可以在上述修改操作完成之后，直接调用透明代理网关203中真实的物理网卡208(其能够与服务器202进行通信)的发送函数，使得帧211被真正发给服务器202。由此，根据本发明的一个实施例的能够实现MAC层透明代理的方法300可以结束。

[0048] 此外，在本发明的一个实施例中，在步骤S301之前，还可以当所述第一帧(例如，帧210)被所述第一网卡(例如，网卡207)所截取时，记录帧210的首部中的源MAC地址信息，作为客户端201的MAC地址，以供后续的修改步骤使用。此外，在该记录步骤中，还可以记录帧210的首部中的目的MAC地址信息，作为服务器202的MAC地址。而且，在帧210具有VLAN标记的情况下，在该记录步骤中，还可以记录帧210的VLAN标识符；并且在所述修改步骤S302中，还可以将帧211的VLAN标识符修改为所记录的帧210的VLAN标识符。作为一种具体的实现方式，所记录的这些信息，例如包括但不限于源站的MAC地址、目的站的MAC地址以及VLAN标识符等等，可以被存储在经扩展的连接跟踪中，如前所述。

[0049] 此外，在本发明的一个实施例中，在步骤S301之前，还可以在要求在作为源站的客户端201和作为目的站的服务器202之间建立连接的请求帧被网卡207所截取时(例如，考虑需要通过握手来建立连接以继续数据传输的情况，其中，包含应用层数据的帧210是通过建立后的连接来进行传输的)，记录该请求帧的首部中的源MAC地址信息，作为客户端201的MAC地址，以供后续的修改步骤S302使用。类似地，还可以记录该请求帧的目的MAC地址信息以作为服务器202的MAC地址、以及VLAN标识符，等等。而且，响应于所截取的该请求帧，作为透明代理网关203以服务器202的身份与客户端201通过握手建立连接的一部分，还可以例如通过VIF 206，将响应于该请求帧的应答帧的首部中的源MAC地址信息修改为所记录的服务器202的MAC地址，然后调用网卡207的发送函数来将这样的应答帧发送给客户端201。

[0050] 以上参照图3描述了示例性的方法300，本领域技术人员可以理解，上述方法步骤仅仅是示例性的而非限制性的，取决于具体实现，所述方法还可以包含更多附加的/替代的步骤。在一个或多个方案中，这些方法步骤对应的功能可以在硬件、软件、固件或其任意组合中实现。

[0051] 图4示出了根据本发明的一个示例性实施例的装置400的框图。

[0052] 所述装置400至少包括如下部分：修改模块401，用于在网关中能够与源站进行通

信的第一网卡所截取的从所述源站发往目的站的第一帧中包含的应用层数据被进行处理之后，把要响应于所述第一帧而发送给所述目的站的、包含经处理的所述应用层数据的第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址；以及，发送模块402，用于通过调用所述网关中能够与所述目的站进行通信的第二网卡的发送函数，将所述第二帧发送给所述目的站。

[0053] 此外，所述装置400还可以包括附加的/替代的模块，用以实现更多对应的功能，例如，前面结合方法300所描述的。所述装置400例如可以对应于图1、图2所示的网关设备103、203，或者是其中的一个或多个组件。应当理解的是，装置400被描述为包括多个模块，其可以是表示由硬件、软件或其组合所实现的功能模块。

[0054] 尽管前面描述并示出了本发明的一些实施例，但是本领域技术人员很容易就能够想到，对于这些实施例的许多修改和变型也同样是可行的。因此，应该理解，所附权利要求旨在涵盖落入本发明的实质和范围之内的所有这样的修改和变型。

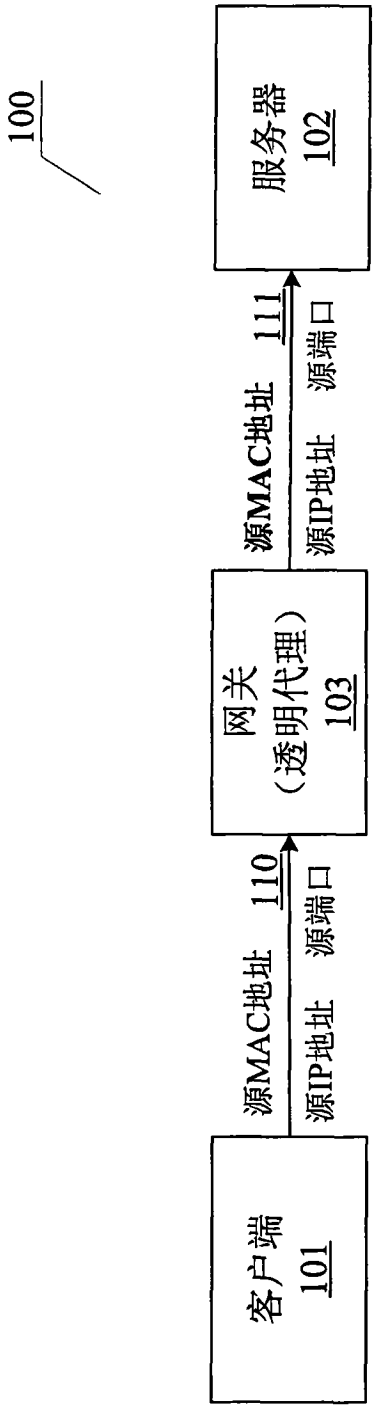

100
客户端
101
源MAC地址 110
源IP地址 源端口
网关
（透明代理）
103
源MAC地址 111
源IP地址 源端口
服务器
102

图1

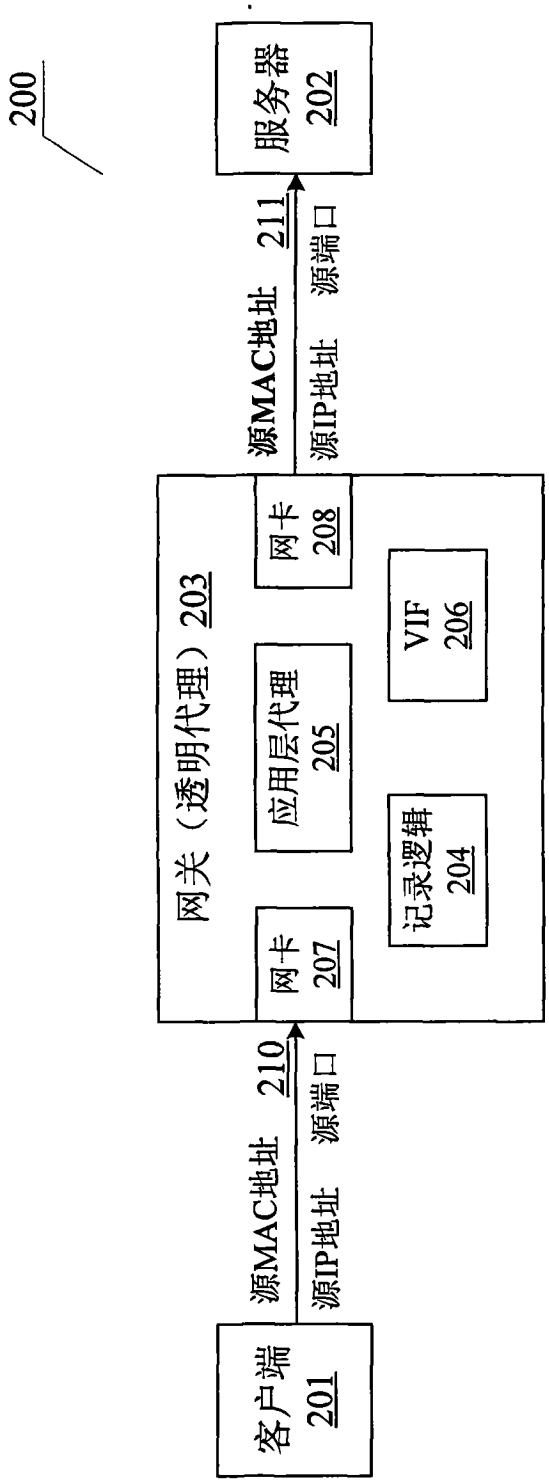

200
客户端
201
源MAC地址 210
源IP地址 源端口
网关（透明代理）203
网卡
207
应用层代理
205
网卡
208
记录逻辑
204
VIF
206
源MAC地址 211
源IP地址 源端口
服务器
202

图2

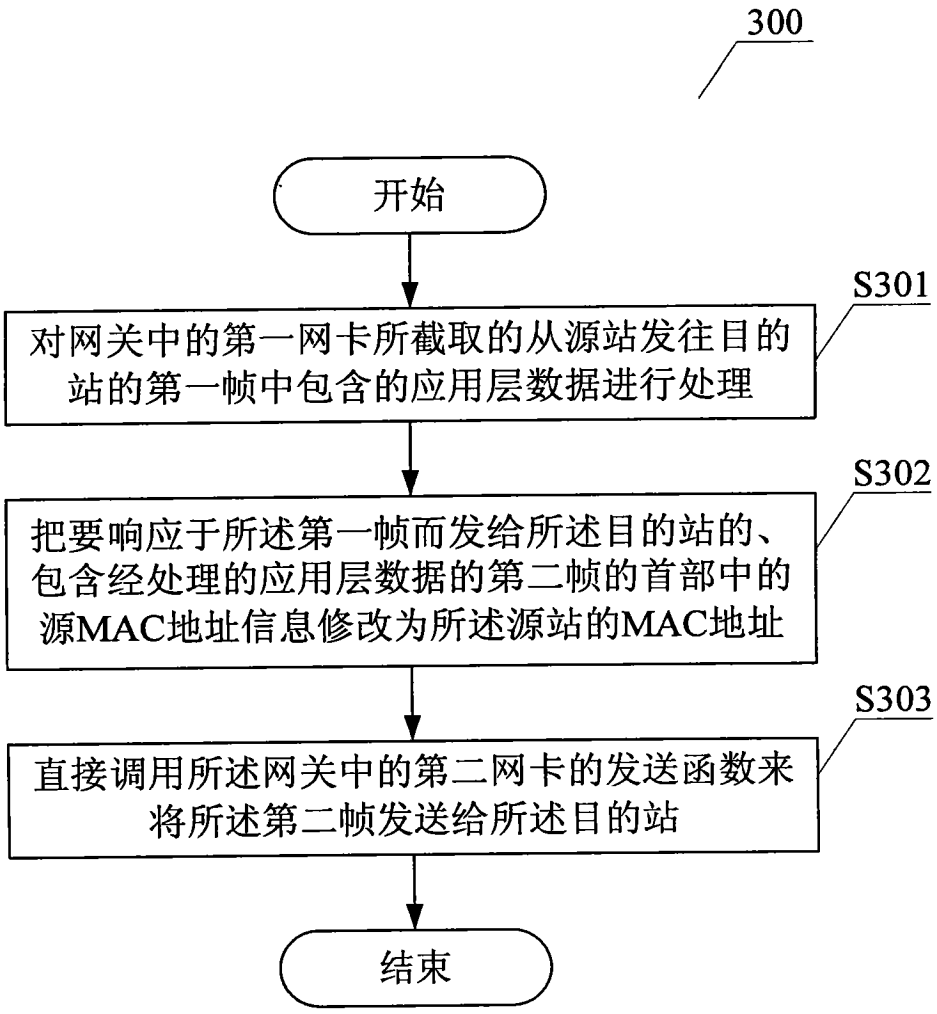

300
开始
S301
对网关中的第一网卡所截取的从源站发往目的站的第一帧中包含的应用层数据进行处理
S302
把要响应于所述第一帧而发给所述目的站的、包含经处理的应用层数据的第二帧的首部中的源MAC地址信息修改为所述源站的MAC地址
S303
直接调用所述网关中的第二网卡的发送函数来将所述第二帧发送给所述目的站
结束

图3

图4