

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 17/00

H04L 29/06



[12] 发明专利申请公开说明书

[21] 申请号 01823364.3

[43] 公开日 2004 年 7 月 28 日

[11] 公开号 CN 1516841A

[22] 申请日 2001.6.15 [21] 申请号 01823364.3

[86] 国际申请 PCT/SG2001/000121 2001.6.15

[87] 国际公布 WO2002/103547 英 2002.12.27

[85] 进入国家阶段日期 2003.12.15

[71] 申请人 先进网络科技私人有限公司

地址 新加坡邮区一七八八八四首都大厦二楼六号史丹福路十一号

[72] 发明人 张伟达 仁迪·星

[74] 专利代理机构 北京邦信阳专利商标代理有限公司

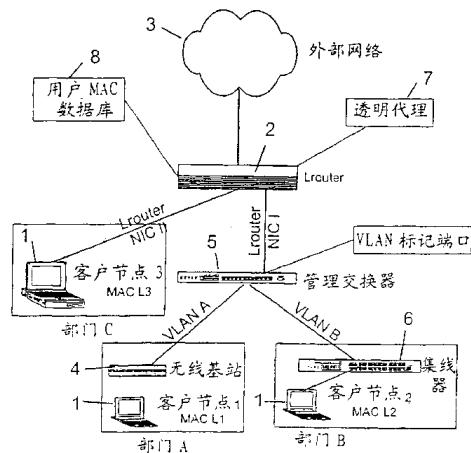
代理人 黄泽雄 张耀丽

权利要求书 3 页 说明书 16 页 附图 10 页

[54] 发明名称 计算机网络

[57] 摘要

本发明描述了一个计算机网络，其中客户节点网卡的数据链路层地址，如 MAC 地址，在为应用层服务提供网络时被用来唯一地识别节点。一个链路警报路由器可以从一个客户节点所发送的数据包中确定该客户节点的 MAC 地址，并基于与用户属性有关的客户节点 MAC 地址的一个数据库来确定为该用户提供的服务，如该数据包的一个代理重新定向。通过确定 MAC 地址，该路由器也能识别一个未注册的 MAC 地址，并能将一个未注册用户的 HTTP 请求转发至一个远端配置网页，以注册该用户或将请求转发到一个安全警告网页。该路由器也可支持使用该 MAC 地址的网络地址转换和域名系统服务，将一个全资格域名、主机名或类似物分配到该 MAC 地址。



I S S N 1 0 0 8 - 4 2 7 4

1. 一个计算机网络系统，包括多个客户节点，每一客户节点具有一个唯一的数据层链路地址，其中所述系统包括至少一个网络设备，该网络设备能够访问一个所述客户节点的数据链路层地址，并且其中所述网络设备利用所述被访问的数据链路层地址来唯一地识别所述客户节点并基于所述数据链路层地址为该节点提供网络层或上层服务。
2. 如权利要求 1 的系统，其中所述系统包括至少一个路由器，该路由器能够确定一个已发送一个数据包的客户节点的链路层地址，并且所述系统还包括一个链路层地址和用户信息的数据库。
3. 如权利要求 2 的系统，其中所述路由器基于所述链路层地址和数据库信息执行一个或多个对所述客户节点的政策。
4. 如权利要求 2 或 3 的系统，其中所述路由器确定一个客户节点的链路层地址是否包括在所述数据库中，并且当所述地址没有包括在所述数据库中时，启动一个配置程序。
5. 如权利要求 2、3 或 4 的系统，其中所述路由器确定一个终端用户的链路层地址是否包括在所述数据库中，并且当所述地址没有包括在所述数据库中时，启动一个安全程序。
6. 如前述权利要求之一的系统，其中所述系统确定一个所述客户节点的位置信息并且将该信息记录在所述数据库中。
7. 如前述权利要求之一的系统，包括一个 DNS 服务器，其中所述 DNS 服务器通过将一个客户节点的链路层地址与一个唯一的名字进行映射，从而将该唯一的名称分配给该客户节点。
8. 如权利要求 7 的系统，其中 DNS 服务器包括关于全资格域名的链路层地址的一个数据库。
9. 如权利要求 7 的系统，其中 DNS 服务器包括一个关于主机名的链路层地址的数据库。
10. 如权利要求 7、8 或 9 的系统，其中当业务由一个客户节点产生时，该路由器从该客户节点的链路层地址中为该客户节点确定所述唯一

- 名字，并且在一个 DDNS 表中为所述名字更新 IP 地址。
11. 如前述权利要求之一的系统，其中所述系统包括一个网络地址转换器，用于将一个客户节点 IP 地址映射到一个被分配的 IP 地址。
 12. 如权利要求 11 的系统，其中所述网络地址转换器在将所述终端节点的一个 IP 地址映射到一个被分配的节点中利用了一个客户节点的链路层地址。
 13. 如权利要求 11 或 12 的系统，其中所述网络地址转换器在客户节点的一个 IP 地址的映射中利用了该客户节点的物理位置信息。
 14. 如权利要求 11、12 或 13 的系统，其中所述网络地址转换器提供一个反向 NAT 操作，其中一个被分配的 IP 地址被映射到一个客户节点 IP 地址和数据链路层地址。
 15. 如权利要求 11 至 14 之一的系统，其中所述网络地址转换器提供一个两次 NAT 操作，其中提供一个客户节点 IP 地址到一个被分配的 IP 地址的映射，还提供一个被分配的 IP 地址到一个客户节点 IP 地址与它的数据链路层地址的映射。
 16. 一个计算机网络系统，包括多个终端系统，一个 NAT 路由器和一个 DNS 服务器，其中所述路由器能够确定该终端系统的链路层地址，并且其中 NAT 和 DNS 程序是基于所述链路层地址的，每一所述链路层地址与一个唯一的名字关联。
 17. 一个计算机网络系统，包括多个终端系统和一个 NAT 路由器，其中所述 NAT 路由器创建实际源终端系统 IP 地址和表观源终端系统 IP 地址的绑定，并且其中所述 NAT 路由器将所述源终端系统的链路层地址记录为所述绑定的一部分。
 18. 一个计算机网络系统，包括多个终端系统和一个 DNS 服务器，其中所述 DNS 服务器将所述终端系统链路层地址与唯一的名字映射。
 19. 一个计算机网络系统，包括多个终端系统和一个或多个中间系统，并且其中数据通过利用网络和链路层协议的中间系统在终端系统间进行传输，其中通过为每一终端系统的链路层地址分配一个唯一的名字，从而在系统中对终端系统唯一地进行识别，所述唯一的名字用于将数据经由中间系统路由至终端系统。
 20. 一个计算机网络系统，包括多个客户节点和一个代理服务器，其中

该代理服务器被配置用于恢复由所述节点发送的数据包中的数据链路层地址信息，并基于所述数据链路层地址信息，用于按照网络层或上层的政策规定为所述客户节点提供服务。

21. 一个计算机网络系统，包括多个具有数据链路层地址的网络节点和一个用于往返于所述节点间的路由业务的路由器，其中所述系统包括关于节点属性的所述数据链路层地址的数据库，所述路由器被配置用于确定所述节点的数据链路层地址，并用于执行所述数据库的查找，以便为所述节点提供服务。

22. 一种为计算机网络上的节点提供服务的方法，该计算机网络包括多个此类节点以及一个用于往返于所述节点间的路由业务的路由器，包括以下步骤：

 为所述节点获得数据链路层地址；

 构造一个与所述节点用户的属性有关的所述地址的数据库；

 从一个节点接收到业务时，在所述数据库中执行一个该节点的所述地址的查找；及

 基于从所述查找中获得的属性信息，为所述节点提供服务。

23. 计算机系统的一种 NAT 的方法，该系统包括多个具有数据链路层地址的节点和一个用于往返于所述节点间的路由业务的路由器，包括以下步骤：

 确定一个所述节点的链路层地址；及

 创建由路由器分配的一个 IP 地址和该节点的 IP 地址及它的链路层地址之间的绑定。

24. 一种在计算机网络中识别一个节点的方法，该计算机网络包括多个具有数据链路层地址的节点和一个用于往返于所述节点间的路由业务的路由器，包括步骤：

 为所述网络提供一个 DNS 服务器，该服务器将一个唯一的名字映射到一个所述节点的数据链路层地址。

计算机网络

发明领域

本发明涉及计算机网络，该计算机网络使用 IP 协议并包含数据链路层地址，如结合了以太网和无线局域网 WaveLan 技术以及令牌环 (token ring) 和光纤分布式数据接口 (FDDI) 技术的网络。

背景技术

因特网上的所有节点通过 IP 地址来识别。不幸的是，由于可获得的公共 IP 地址池(IP address pool)有限以及由于管理和维护的要求，常常不可能给一个用户分配一个静态 IP 地址。反之，对于每一因特网访问会话 (access session)，用户例如可以例如接收一个不同的 IP 地址。

这可能会在识别一个内部网或因特网上的终端用户时造成问题。

针对这一问题，已经提出了各种各样的解决方案，如使用了主机名到 IP 地址的动态映射的 DDNS(动态域名系统)，将用户信息嵌入其中的 X503 客户认证，以及甚至简单的用户注册验证。

然而，这些方案有着其自身的局限性，如需要额外的客户软件支持并且依赖于终端客户来启动通讯。

本发明的一个目的是提供一个便于识别终端用户的网络系统。尽管本发明可能提供了一个以上所述方案的替换方案，但并不一定与这些方案互相排斥。

本发明还特别地、但不限于对例如于 2000 年 8 月 17 日申请的、名为“可重构的计算机网络”的国际专利申请 PCT/SG00/00170 中所描述的计算机系统有用，在此声明该申请的内容结合进本申请，以供参考。

发明内容

根据第一个方面，本发明提供了一个计算机网络系统，其包括多个客户节点，每一节点有一个唯一的数据层链路地址，其中，该系统包括至少

一个可以访问一个客户节点的数据链路层地址的网络设备，而且，该网络设备利用该被访问的数据链路层地址来唯一地识别客户节点，并基于所述数据链路层地址为该节点提供网络层或上层（如应用层）服务。

根据本发明，一个路由器（作为网络设备）例如可以监视数据链路层信息，该信息例如包含在一个由客户节点所传输的数据包中，从而扩展标准的网络和应用服务的功能性，并且能够利用一个客户节点的数据链路层地址来唯一地识别一个主机和与之相关联的终端用户。

本发明与传统的、利用一个 IP 地址来提供此类服务并映射到一个客户节点的方法形成对照。

该数据链路层地址通常可包含一个媒体访问控制（MAC）地址。网络的每一客户节点包括至少一个附加的网络接口卡 NIC（或者称作网卡或网络适配器卡）以便将该客户节点物理地连接到该网络。每个 NIC 卡有一个与之相关联的唯一的 MAC 地址。这些 MAC 地址包括一个 6 字节的域。前三个字节（OUI—组织唯一标识符）确定卡的厂商并由 IEEE 在全球进行分配。后三个字节由厂商按保证每一卡片有一个唯一地址的方式分配。

本发明所基于的原理是硬件，即网卡，与其他由软件控制的网络配置相比，它们默认的硬编码的 MAC 地址更不易变化，因此与仅依靠 IP 地址来识别网络和应用层中的节点不同，网卡利用的是 MAC 地址。

在一个优选实施方案中，该系统包括一个能够确定一个已发送一个数据包的客户节点的链路层地址的链路警报路由器，并包括一个链路层地址和用户信息的数据库，该数据库可由路由器托管。该信息可以是例如与客户节点的用户所注册的部门有关，并和其权限及安全许可证等级有关。

因此，当从一个客户节点接收到一个请求，如一个 HTTP 请求，路由器能够从该客户节点的 MAC 地址识别出该客户节点，并且能够执行一个或多个由网络管理员可能为该客户节点限定的适当的网络和应用政策。

例如，在 HTTP 请求的情况下，路由器可以提供一个透明代理功能，从而在两个客户节点请求同一个 URL 时，为该两个节点提供一个不同的网页。这可以依如客户节点所注册的部门而定。或者，对某一功能、如电子邮件、万维网网页、FTP 或类似功能的使用可以被拒绝和/或被限制，以包括或排除某些域。

在一个优选的形式中，例如当系统为一个如 PCT/SG00/00170 所公开的可重构的计算机网络，路由器可以确定一个终端用户的链路层地址是否包括在数据库中，并且当所述地址没有包括在所述数据库中时，例如通过将来自客户节点的一个 HTTP 请求重新定向至一个配置页，从而启动一个配置程序。

更优选的是，该路由器确定一个客户节点的链路层地址是否包括在数据库中，并且当所述地址没有包括在所述数据库中时，例如通过将一个 HTTP 请求重新定向至一个警告有一个未被授权的访问尝试的网页来启动一个安全程序。

该系统还可确定一个客户节点的位置信息并将该信息记录在数据库中。该信息可为例如接收到来自客户节点的数据包的路由器的网卡 NIC 的号码（如，用 eth0 表示以太网卡号 0）。它还可包括关于一个客户节点分配至一个虚拟 LAN 的信息，如一个 VLAN ID。因此，和由 MAC 地址确定的服务一样，可为客户节点提供位置特定服务，如位置特定网页内容。

在一个特别优选的实施方案中，该系统包括一个被托管在链路警报路由器上的透明 DNS 服务器。当使用一个 DNS 服务器时，DNS 服务器优选通过映射一个客户节点的链路层地址和一个唯一的名字，从而将该唯一名字分配给该客户节点。该名字可以为例如一个全资格域名（FQDN）或一个主机名。还可能将其他属性分配给该链路层地址，该链路层地址可能事先已经与一个 IP 地址相关联。这可以包括网络资源，如一个打印机和动态防火墙规则（如非静态的 IP）。

通过直接将一个 MAC 地址映射到一个 DNS A 型资源记录，可能将一个 FQDN 或主机名分配给一个终端用户计算机而无需来自客户的额外支持，并且一个节点通过它的 FQDN 或主机名在链路警报 DNS 网络内能够总是到达一个同级对应节点，而与该同级节点的当前 IP 地址无关。

更优选的是，该系统包括一个网络地址转换器（NAT），用于将一个客户节点 IP 地址映射到一个被分配的 IP 地址。这样便允许跨地址区域的透明路由，其中例如一个 LAN 的专用 IP 地址被映射到一个或多个公共地址，并且当使用一个网络地址端口转换器（NAPT）时，可能被映射到一个或多个 IP 地址和端口的结合。为方便起见，在此的描述中，术语 NAT 应视作包括了 NAPT。

优选地，网络地址转换器利用了一个客户节点链路层地址，将所述终端节点的一个 IP 地址映射到一个被分配的节点。这样便允许具有相同 IP 地址的客户节点由 NAT 提供服务。

当提供一个例如 PCT/SG00/00170 中所公开的可配置的路由器时，对一个客户节点，网络地址转换器可以利用物理位置信息来映射该客户节点的 IP 地址。这可包括路由器 NIC 号，来自客户节点的数据包和 VLAN ID 在此被接收到。

优选地，该网络地址转换器提供一个相反的 NAT 操作，其中一个被分配的 IP 地址被映射到一个客户节点 IP 地址和数据链路层地址。

更优选地，网络地址转换器提供两次 NAT (twice NAT) 功能，其中均提供一个客户节点 IP 地址到一个被分配的 IP 地址的映射，和一个被分配的 IP 地址到一个客户节点 IP 地址和它的数据链路层地址的映射。

从另一方面看，本发明提供了一个包括多个终端系统、一个 NAT 路由器和一个 DNS 服务器的计算机网络系统，其中所述路由器能够确定终端系统的链路层地址，并且其中 NAT 和 DNS 程序是基于所述链路层地址的，每一所述链路层地址与一个唯一的名字关联。

另一方面，本发明提供了一个包括多个终端系统和一个 NAT 路由器的计算机网络系统，其中所述 NAT 路由器创建实际的源终端系统 IP 地址和表观源终端系统 IP 地址的绑定 (binding)，并且其中所述 NAT 路由器将所述源终端系统的链路层地址记录为所述绑定的一部分。

从另一方面看，本发明提供了一个包括多个终端系统和一个 DNS 服务器的计算机网络系统，其中所述 DNS 服务器将所述终端系统的链路层地址与唯一的名字映射。

从另一方面看，本发明提供了一个包括多个终端系统和一个或多个中间系统的计算机网络系统，其中，数据通过使用网络和链路层协议的中间系统在终端系统间传输，其中在系统中通过分配一个唯一名字到每一终端系统的链路层地址来唯一地识别终端系统，在将数据通过中间系统路由到终端系统中使用了所述唯一名字。

从另一方面看，本发明提供了一个包括多个客户节点和一个代理服务器的计算机网络系统，其中代理服务器被配置用来从所述节点发送的数据包中恢复数据链路层地址信息，并基于所述数据链路层地址信息、按照网

络层或上层（如应用层）政策说明来为所述客户节点提供服务。

从另一方面看，本发明提供了一个计算机网络系统，其包括多个具有数据链路层地址的网络节点和一个用于与节点间路由业务（traffic）的路由器，其中，该系统包括一个关于节点属性的数据链路层地址的数据库，该路由器被配置用来确定节点的数据链路层地址，并执行对数据库的查找，从而为节点提供服务。

本发明还延伸到按以上特征管理和维护计算机系统的方法，以及延伸到执行该方法的软件和硬件。

附图说明

现在参考附图，仅以示例形式描述本发明的不同实施方案。应当理解，附图的细节并不代替本发明前述的一般性。

图 1 为根据本发明一个实施方案的一种可能的网络拓扑示意图；

图 2 和图 3 为示意图表，描述了根据本发明的一个实施方案的、往返于计算机网络的一个客户节点、并往返于一个具有一个或多个中间系统的链路警报路由器的输出和输入业务；

图 4 为根据本发明的一个实施方案的、托管（hosting）一个链路警报 DNS 服务器的链路警报路由器示意图；

图 5 至图 7 为示意图，描述了图 5 中所示路由器可以用于一个内部网的两个节点间的业务路由；

图 8 至图 11 为示意图，描述根据本发明的一个实施方案的一个跨路由区域界线地连接节点的路由器；

图 12 至图 14 为示意图，描述一个跨路由区域界线地连接节点的路由器，其中在一个接收节点和该接收节点内部网的另一节点之间发生了地址冲突；

图 15 至图 17 为示意图，描述了在一个内部网内具有同样 IP 地址的两个节点间的通讯。

发明内容

图 1 描述了根据本发明一个实施方案的计算机网络系统的一个可能的网络拓扑图，该计算机网络系统包括一个链路警报路由器，当然许多其

它的拓扑图也是可能的。

图 1 中，多个客户节点 1 连接到一个路由器 2，该路由器 2 又连接到一个外部网络 3。该外部网络可以有许多不同形式，并且可以例如包括因特网。

本例中，客户节点 Node 1，通过无线基站 4 和具有 VLAN 标记端口的管理交换器（managed switch）5 连接到路由器 2 的第一网卡 NIC I 上，而第二客户节点 Node 2 通过集线器 6 和管理交换器 5 连接到同样的路由器网卡 NIC I 上。这些节点 Node 1 和 Node 2 位于不同的虚拟 LAN，即分别位于与例如运行该网络的组织内的部门相对应的 VLAN A 和 VLAN B 内，并且为此在它们的输出数据包中含有相应标识。

另一客户节点 Node 3 直接连接到路由器 2 的第二网卡 NIC II。

路由器 2 可以例如通过使用不同的透明代理 7 为包括客户节点 1 在内的专用网络提供代理服务，而且可以将所有用户请求从专用网络集中到外部网络 3，并将应答散发向合适的用户。它还可以提供其他的标准代理服务，如万维网网页和文件传输协议缓存，以及应用防火墙保护。

路由器可采取如名称为“可重构的计算机网络”的国际专利申请 PCT/SG00/00107 中所描述的可重构的路由器形式。这种情况下，可在任何时候、在同样的或可供选择的逻辑和物理网络位置将客户节点 1 从网络中删除以及添加至网络，而路由器 2 适当地在每一连接/非连接状态时更新其记录，以允许网络用户无缝地使用客户节点 1。因此，可以从到来的数据包链路信息（如嵌入在数据包数据中的 VLAN ID）和接收客户节点发送的数据包的路由器网卡（如 NIC I 或 II）来确定每一客户节点的位置。

每一客户节点 Node 1、Node 2 和 Node 3 具有一个唯一的 MAC 地址，即 L1、L2 和 L3。

该 MAC 地址为一个物理地址（即它是特定硬件），并且是该客户节点网络适配器卡的唯一系列号，当制造该网络适配器时便烙上了该系列号。MAC 地址包括一个六字节的域，其中前三个字节（OUI—组织唯一识别符）确定卡的厂商并且由 IEEE 分配，而后三个字节由厂商分配。

通常，这些地址用于网络的数据链接层，例如用在以太网或令牌环（Token Ring）的 MAC 层。

然而，根据本发明，这些 MAC 地址还用来唯一地识别网络直至网络

应用层的客户节点，并且配置路由器 2，从而知道每一个节点 1 的 MAC 地址。

因此，路由器 2 包括一个有关用户信息的 MAC 地址的数据库 8。该信息可以采取任何合适的形式，并且可以与拥有该客户节点的用户的详细情况有关，包括他们的名字、部门、访问特权以及客户节点当前的和允许的位置信息。

通过提供这样的数据库，以及通过使得路由器 2 能够获得客户节点 1 的 MAC 地址，路由器 2 基于从用户数据库的 MAC 地址所得到的选择性用户的用户配置文件，并且如需要，也可基于他们的逻辑和/或物理网络位置（如通过 VLAN ID 和输入的路由器 NIC 号），便能通过产生可供利用的有关特定网络和应用的服务为选择性的用户提供智能服务传输。

因此，基于从 MAC 地址所得到的用户属性（如用户名字、部门或类似属性）和从输入的路由器 NIC 号和/或 VLAN ID 所得到的网络位置，能够执行网络和应用政策。这可以添加到现有网络应用（如使用 IP 地址）中已经得到支持的任何其他规格标准中。

作为示例，一个公司可以维护一个内部网站，并且所有员工可被分配一个客户节点，如一个个人计算机，并有一个专用的具有一个 MAC 地址的网卡。然后为所有的 MAC 地址和终端用户建立一个数据库，使得这些地址和信息与这些终端用户有关。当来自两个不同部门的员工从他们分配到的计算机访问同样的 URL 时，可以向他们显示不同的、与他们部门需要有关的网页。甚至当他们拥有同样的 IP 地址或连接到同样的网络点时，这也是可能的，因为使用了他们唯一的 MAC 地址来识别他们。

此外，对于不同的物理网络位置，当网页内容取决于位置时，对于同一 URL，由其 MAC 地址来识别的同一员工可能获得不同网页的服务。

本示例可利用一个透明 HTTP 代理服务器和路由器 2 来执行。因此，每一个 HTTP 请求可被路由器 2 的一个防火墙截取（如通过在一个数据包的 TCP 头部确定目的端口号 80,8080 或 3128，或通过截取所有的输出 TCP 数据包并分析用于 HTTP 请求的有效载荷，如“GET http://*.*.*HTTP/1.0”），并且将被重新定向至 HTTP 代理服务器（如，通过目的 IP 地址 NAT，而不是传统的源 IP 地址 NAT）。该代理服务器然后恢复该请求的源 MAC 地址以及（如适用）VLAN ID 和输入的路由器

NIC 信息，并且基于 MAC 地址及（如适用）VLAN ID 和输入的路由器 NIC 信息来执行相关信息查找。然后，基于该信息，将原请求映射至一个必需的不同的 URL，并向新的 URL 发布一个代理请求。

上述中，防火墙可以执行一个目的 IP 地址 NAPT，如 www. antlabs. com, 80 的一个目的地址和端口可以 NAPT(转换)为代理服务器所驻的本地主机的目的 IP 地址和目的 TCP 端口 3128。然后可在客户与透明代理之间建立一个 TCP 插座 (socket) 连接，而不是与网服务器 www. antlabs. com连接。每一 TCP 插座将存储增大的、包含客户 MAC 地址和输入的 NIC 逻辑索引号(由于一个 NIC 所监视的每一 VLAN ID 被分配一个新的逻辑号，因此可能从逻辑号中截取 NIC 和 VLAN ID) 在内的终端节点会话信息。对于代理服务器读取的每一个截取的 TCP 数据包，可以使一个插座选择呼叫包含客户 MAC 地址和所选择插座的 NIC 逻辑号。

在另一示例中，路由器具有如 PCT/SG00/00170 所描述的零配置能力，可利用两种技术的结合、通过一个基于万维网的 GUI 远程配置一个新的网络设备。

因此，路由器 2 能够检测来自一个不同的、未列入数据库中的 MAC 地址的 HTTP 请求，并且例如该 HTTP 请求源自一个被分配用于远程配置的路由器 NIC，而且路由器 2 能够将终端用户重新定向至一个默认的启动配置页。

因此，对于每一个被检测出的新用户，使用一个启动页来注册该用户的信息，如名字，部门，优先选择（如未来启动页），偏好的打印机等。这一特征也可用来配置一个新的网络设备如一个万维网服务器（一个基于万维网的被管理的“黑匣子”，而不是一个传统的计算机服务器），对于该设备来说，提供一个初始的 IP 地址会有问题。对于本发明而言，不需要设立一个初始的 IP 地址，相反，可以简单地将万维网服务器接通并启动其万维网浏览器。然后会出现启动配置页，基于万维网的管理（人员）能在此设置一个 IP 以便用于 WAN 连接、其他设备的配置等。

此外，使用相似的方法，可将路由器 2 用作一个安全访问控制设备。因此，与通常的、以数据包为基础的并基于 IP 地址的防火墙控制（该防火墙控制易受 IP 欺骗的影响）不同，任何来自一个未注册的客户节点网

络适配器卡（即来自一个未将 MAC 地址在数据库注册的网卡）的 HTTP 请求能够被重新定向至一个网页警报，该警报告知终端用户：他们正试图进行未经授权的访问。

按这一方法，并且不同于现有的应用防火墙，对于每一个单独的应用可以提供从物理插座连接到用户（由他们的 MAC 地址识别）的全程安全控制。

如同提供服务传输一样，MAC 地址的使用允许路由器 2 能通过直接利用该 MAC 地址，以作出合适的返回数据包转发决定。

图 2 和图 3 描述了往返于客户节点 1 的输出和输入业务在例如图 1 的系统中怎样配置，尽管这些图示出了在客户节点 1 和链路警报路由器 2 之间也可能提供其他的路由器。

通常，两个通讯节点间的客户节点 1 中的至少 1 个（本例中，一个节点具有 MAC 地址 L1 和 IP 地址 N1）应为链路警报路由器 2 的一个路由器跳跃 (router hop)。然而，在客户节点 1 和链路警报路由器 2 之间也可有多个介入层 2 转换器 (VLAN 或其他)。在客户节点 1 和链路警报路由器 2 之间还可有协同路由器 9 (如透明路由器或根据 PCT/SG00/00170 的一个路由器)，可例如为链路警报路由器 2 提供必需的信息，使之能通知协同边缘路由器 10，以产生正确的输出数据包层 2 链路报头，并将其发送回客户节点。

中间路由器 9 将数据包路由到链路警报路由器 2，以便使之能确定政策决定。如需要，它们能为输出业务做出路由决定，例如，基于目的 IP 地址，业务可能被发送至一个不同的链路警报路由器。它们还可使路由能从一个 VLAN 到另一个 VLAN。

由图 1 和 2 可知，客户节点 MAC，L1 可被嵌入到一个链路报头（包括源和目的物理地址）和一个网络报头（包括源和目的 IP 地址）之间的一个数据包中。或者，在一个基于交换的执行中，源 MAC 地址不变，客户 MAC 可形成链路报头的一部分。这仅是两个示例，而其他的为链路警报路由器 2 和边缘路由器 10 提供客户 MAC 地址的方法也是可能的，如带外消息 (out-of-band message)。

链路警报路由器 2 和下一个跳跃路由器 (hop router) 11 (例如在该路由器 2 的因特网一侧) 间的路由作业将按本领域所熟知的、例如路由器 11

和相似的设备来进行，它确定在网络报头中的、来自 IP 地址目的地的数据包的目的地，并且对该数据包按照 IP 地址的路由表进行路由。

链路警报路由器 2 也可提供如本领域所熟知的 NAT（网络地址转换）或 NAPT（网络地址和端口转换），以便例如将专用 IP 地址映射到公共 IP 地址，以及防止地址冲突问题。NAPT 还允许映射该端口号，并且为了实现本发明的目的，对 NAT 的引用应当认为同样包括对 NAPT 和 NAT 的其他变体（例如端口转发所用的两次 NAPT 和透明代理所用的目的 NAT）的引用。

本发明中，一个链路警报路由器，如图 1 中的路由器 2，可提供 NAT，在映射中也结合了客户节点的 MAC 地址。

因此，NAT 功能可按与标准 NAT 功能（包括任何变体，如目的 NAT 和例如“IP 网络地址转换器（NAT）术语和考虑”（RFC2663, P. Srisuresh, M. Holdrege, 1999 年 8 月）所指出的 NAT）同样的方式运行，但以下除外：

1) 对每一个为 NAT 的新输入的会话，除了其他通常要求的 NAT 信息外，客户 MAC 地址、输入的路由器 NIC 号（如适用）和任何其他的可选择的位置特定信息（如 VLAN ID），也被存储在初始的和特定的 IP 地址的绑定中。

2) 对于任何将客户 IP 地址（此外和 NAPT 的传输端口号）映射回来的匹配的反向会话业务，用于业务转发的路由器利用先前存储的链路信息产生数据包并将该数据包传输给客户，绕过了一般的路由程序。

对于上述步骤 2，如果客户是移动的并且支持移动检测（如 PCT/SG00/00170 中所述），输出业务所发往的路由器 NIC 号可与步骤 1 中事先记录的不同，并且这一信息应通过存在检测程序（presence detection process）更新。然而，MAC 地址将不会改变。

链路警报 NAT 程序允许具有相同 IP 地址的两个客户使用 NAT，即使他们位于相同的链路广播域中，因为通过他们的 MAC 地址能够将他们相互区别开，并且由于返回路由不需例如发布一个 ARP 请求。

为了在具有同样 IP 地址的两个节点间通讯，须有一个单独的唯一的端到端形式的识别，如一个完全资格域名（FQDN）。

以下讨论链路警报 NAT 程序和 FQDN 规定的示例，该等示例涉及本发明的进一步特征，即链路警报动态域名服务器。

如所讨论的，附加到一个客户节点 1 的网络接口卡片的 MAC 地址能被用来唯一地识别客户节点 1 和它的关联终端用户（而不是如现有技术那样利用一个 IP 地址来映射到一个客户节点）。

将这一概念延伸到 DNS 系统，可能在由一个链路警报动态 KNS 系统提供服务的网络内将一个全资格域名(FQDN)如 john.antlabs.com 或一个主机名如 john 分配到一个终端用户计算机，而不需客户提供额外的支持。

通过直接将一个 MAC 地址映射到一个 DNS A 型的源记录，一个节点通过它的 FQDN 或主机名在一个链路警报 DNS 网络内通常能够总是到达一个同级对应节点，而与该同级节点的当前 IP 地址无关，并且不需客户节点注册其 IP 地址。

在一个链路警报 DNS 系统中，每一节点通过其 MAC 地址被识别，并且通过如 PCT/SG00/00170 所描述的那样监视网络业务和执行移动检测，一个链路警报路由器能确定每一用户节点和他们关联的 MAC 和 IP 地址的位置。

如图 4 所示，一个链路警报 DNS 系统可由一个链路警报路由器 2 和一个链路警报 DNS 服务器组成，其链路警报 DNS 服务器可被托管(hosted)在链路警报路由器 2 上，并且该 DNS 系统包括一个事先配置的、对应 FQDN 表 2 的 MAC 地址。

对于一个没有地址冲突的内部 LAN，对链路警报路由器而言，最简单的机制是动态地建立起基于主机的路由，并利用它所发现的每一个单独客户的实际 IP 地址来更新 DNS。

当一个客户解析了一个 FQDN 或主机名，该主机的实际当前 IP 地址被返回。任何指定发往对应主机的业务将通过建立起的、动态的、基于主机的路由（如果客户节点移动，该路由可改变）被转发。

图 5 描述了这样一个内部 LAN。当业务由一个客户节点 1 产生，链路警报路由器 2 上的一个路由表 13 和一个 DDNS 表 14 被更新。例如，具有一个 MAC 地址 A 和一个源 IP 地址 1.1.1.1 的数据包在路由器 NIC1 上被接收，便在路由表 13 中设立一个基于主机的路由。该路由器然后在链路警报 DNS 表 12 中对 MAC 地址 A 进行查找，并返回 FQDN “albert.a.com”。DDNS 表 14 然后被更新，将 FQDN “albert.a.com” 表现为 IP 地址 1.1.1.1。

如图 6 所示, 当一个客户节点 1 执行一个如对 albert.a.com 的 DNS 询问, 该询问被链路警报路由器 2 的透明链路警报 DNS 服务器截取。如果在 DDNS 表 14 中发现了该 FQDN, 那么 FDQN 的当前 IP 地址, 如 1.1.1.1, 在 DNS 的应答中被返回。如果没有发现, 那么按照标准的已知的 DNS 操作, 使用回归的 DNS 解决方案。

如图 7 所示, 一旦 FQDN 被解析, 业务能通过路由器 2 在发送和接收节点 1 之间路由, 这是由于图 5 所示的路由表 13 中事先建立了基于主机的路由的缘故。

在存在地址冲突或出现了跨两个或更多的路由区域通讯的情况下, 一种形式的 NAT 可与链路警报 DNS 服务器一起应用。

例如, 在没有网络冲突的跨路由区域通讯的情况下, 可用一个永久的 FDQN 或主机名来发现一个客户节点的 IP 地址, 并向该 IP 地址发送业务。当客户对应节点从一个发送节点接收一个数据报(datagram), 该节点无需对发送端的 FDQN 或主机名进行相似的名称查找, 因为对应节点从接收到的数据报中已经知晓目的 IP 地址(即发送端的 IP 地址)。因此, 这种情况下, 只需要在一个方向上进行名字查找。

如果启动名字查找的节点的 IP 地址是唯一的(即没有地址冲突), 那么链路警报路由器仅需要支持域名服务器应用层网关(DNS_ALG), 并且如果在专用网络中没有地址冲突, 那么具有 DNS_ALG 的 NAT 就足够了。链路警报 DNS 服务器仍需要在发现客户时更新 DDNS 表中的对应节点 IP 地址。

图 8 示出了一个没有冲突的、跨一个路由区域的通讯的示例, 该路由区域位于一个公共网络 3(如因特网)的节点 15 和一个专用网络的客户节点 1 之间, 该专用网络具有一个经注册的域名“a.com”和一个链路警报路由器 2, 该路由器 2 能够提供 NAT, 支持 DNS_ALG 并为域名“a.com”的权威域名服务器。

如图 8 所示, 链路警报路由器 2 已经发现了客户节点 MAC 地址 A 并且已经为“albert.a.com”更新了路由表 13(用于路由器 2 输入的 NIC, 在此处接收到来自客户节点 1 的数据包)和 DNNS 表 14。

如图 9 所示, 当具有 IP 地址 10.0.0.3 的公共网络节点 15 尝试解析“albert.a.com”时, DNS 询问被发送到链路警报路由器 2, 因为它是域名

“a.com”的权威域名服务器。因此，DNS_ALG 询问专用网络链路警报 DNS 服务器，即 DDNS 表 14，该表返回结果 1.1.1.1。DNS_ALG 然后设立一个地址绑定 16，来将客户节点的 IP 地址 1.1.1.1 映射到一个为 NAT 之目的而属于链路警报路由器 2 的公共 IP 地址(这时 IP 地址为 11.0.0.1)，并将 11.0.0.1 的 DNS 应答传输至请求节点 15。

一旦完成 DNS 解析，节点 15 和 1 之间的通讯按照“DNS 至网络地址转换器 (DNS_ALG) 的延伸”(RFC2694, P. Srisuresh, G. Tsirtsis, P. Akkiraju 和 A. Heffernan, 1999 年 9 月) 所确定的标准进行。

图 10 示出了作为结果的、对从具有 IP 地址 10.0.0.3 的节点 15 到具有 IP 地址 1.1.1.1 的对应节点 1 的业务的 NAT 操作，而图 11 示出了从对应节点 1 到公共节点 15 的应答业务的 NAT 操作。

现在看地址冲突的可能性，一种冲突是对应客户节点(由外部节点查找的名字目标)和另一个位于相同专用网络的客户节点间的地址冲突。这可通过使链路警报路由器支持反向链路警报 NAT 来解决。这需要利用客户节点链路层信息。

在这种情况下，由于通过专用网络外部的一个公共节点而不是通过存在冲突问题的专用节点 1 中之一来建立通讯，因此在 DNS_ALG 创建绑定信息时可建立反向链路警报 NAT 链路层信息。

对于跨路由区域的通讯，如从因特网 3 到一个专用网络的通讯，需要将一个公共 IP 地址分配到专用网络的对应节点 1。

对于所有的方案，必须使用一个与任何其他可能的对应节点都不冲突的、唯一的 IP 地址(不必是公共的)。

图 12 示出了用于专用网络 a.com 的链路警报 DNS 表 12 和 DDNS 表 14，该网络 a.com 有两个具有相同 IP 地址 1.1.1.1 的客户节点 1。

如图 13 所示，在图 8 至 11 的无冲突的实施方案中，当一个公共节点 15 对“alber.a.com”传输一个 DNS 请求时，DNS_ALG 询问 DDNS 服务器，从而获得具有域名“albert.a.com”的对应节点的 IP 地址 1.1.1.1，然后设立一个公共 IP 地址 11.0.0.1 与专用客户节点地址 1.1.1.1 的 DNS_ALG 绑定 16。

此外，为了启动反向链路警报 NAT，DNS_ALG 将分配给对应节点的 FQDN 的公共 IP 地址 11.0.0.1 告知链路警报 DNS 服务器。利用该信息，

链路警报 DNS 服务器然后能建立一个反向链路警报 NAT 表 17, 该表将分配的 IP 地址 11.0.0.1 映射到适当的以其 MAC 地址 A 为特征的客户节点。该表能够建立是因为 MAC 地址对 FQDN/主机名的映射（图 12 的链路警报 DNS 表 12 的映射）是唯一的（一对一），因此从 FQDN/主机名中进行反向查找以恢复对应节点的 MAC 地址是可能的。

路由器 2 为每一客户节点 1 监视链路层和输入的 NIC 信息，从而更新链路警报 DNS 系统，该链路警报路由器 2 能够建立对应节点 1 的 IP 地址和网络位置。具有了对应节点的实际的和动态分配（通过 DNS_ALG）的 IP 地址，其 MAC 地址和输入的 NIC 接口信息（如有，和 VLAN ID 一起）执行反向链路警报 NAT。

图 14 描述了利用反向链路警报 NAT 对从节点 IP 地址 10.0.0.3 到对应节点地址 1.1.1.1 的业务的 NAT 操作。从对应节点 1.1.1.1, MAC A 到节点 IP 地址 10.0.0.3 的应答业务可按照标准方法使用 NAT 来执行。

图 15 至 17 示出了一个实施方案，其中，在一个由链路警报 DNS 提供服务的专用网络中、在节点 1 和 1' 之间存在一个 IP 冲突，并且没有跨路由区域的通讯（所有通讯节点为一个来自链路警报路由器 2 的跳跃）。

当在通讯节点存在此类 IP 冲突时，链路警报两次 NAT 可以使用，即为源和目的 IP 地址均执行链路警报 NAT。

按照这一方法，一个唯一的 IP 地址（对于该地址不存在地址冲突），本例中的 11.0.0.2 与执行名字查找的发送端节点 1' 共置（co-located）。链路警报 NAT 记录该共置的 IP 地址 11.0.0.2 并使它与发送端节点地址 1.1.1.1 和 MAC 地址 B、以及输入的 NIC 信息和 VLAN ID（如有）匹配。该信息被存储在链路警报 NAT 表 18 中。

在对发送节点 1' 的 DNS 应答中，DNS_ALG 就将与对应节点 1 共置的另一唯一 IP 地址 11.0.0.2 返回。该 IP 地址 11.0.0.1，和客户节点的 IP 地址 1.1.1.1 及 MAC 地址、以及 NIC 接口信息和 VLAN ID（如有）一起由链路警报 NAT 存储。可按如图 12 至 14 的实施方案所示的同样方法得到这些信息，并将其存储在一个反向链路警报 NAT 表 17 中。

这两个被共置的 IP 地址 11.0.0.1 和 11.0.0.2 在另一名字查找前、在两个节点 1 和 1' 间的任何现有的通讯期间是有效的。

两个节点 1 和 1' 间的任何通讯为两次 NAT。与传统的两次 NAT 不同

的是，可用的链路层和 NIC 信息使得不再需要任何路由表查找（当存在一个地址冲突时该查找就会中断）或 ARP 请求（当存在多个地址冲突时该请求便会产生多个应答）以便构造一个数据包并向节点 1 和 1' 中的任何一个传输该数据包。

当与 MAC 地址 B 对应的节点发布一个 DNS 询问时，DNS_ALG 绑定 16、链路警报 NAT 表 18 和链路警报反向 NAT 表 17 便被设置。

图 16 描述了利用链路警报两次 NAT 对从具有 MAC 地址 B 的客户节点 1' 到具有 MAC 地址 A 的对应客户节点 1 的业务的 NAT 操作，而图 17 描述了利用链路警报两次 NAT 对从具有 MAC 地址 A 的对应节点 1 到具有 MAC 地址 B 的客户节点 1' 的 NAT 操作。

在跨路由区域通讯（从一个专用网络开始至因特网或反之）和在专用节点和公共节点存在地址冲突的情况下，位于专用网络内的一个唯一的 IP 地址必须与该公共的对应节点共置，属于链路警报路由器的一个唯一公共 IP 地址必须与该专用节点共置，并且该具有 DNS_ALG 的两次 NATA 被用来使得能够进行如“DNS 至网络地址转换器的延伸（DNS_ALG）”（RFC2694 第 6 节）所证明的通讯。如果在专用网络内仍发生地址冲突，应对从公共节点到专用节点的、而不是从专用节点到公共节点的业务 NAT 使用链路警报两次 NAT。

总之，本发明的特征，尤其当与 PCT/SG00/00170 可重构的网络系统一起使用时提供了许多的优点。

该技术足以按要求为终端用户提供网络访问而无需管理员的接入，并且必要时可重构。需要单独地重构终端用户系统的可以由管理员配置和使用以实时地用于整个网络，并且配置改变甚至可应用至单个用户的范围。例如，一个网络管理员可以从一个基于万维网的服务器管理页远程地切换至一个新的 SMTP、改变内部网服务器机器或 URL、安装新的网络资源并使所有用户均能访问（如一个打印机）、将一个新的全资格域名或内部主机名分配给一个终端用户的计算机、或将一个可公开访问的 IP 地址分配给一个终端用户的计算机。

此外，该技术不仅能够将客户节点连接至网络，并且可以作为智力服务传输的发射台。服务器能够有网络中的每一个客户系统的一个完全数据库，包括它们的用户信息到它们的当前位置；并且一个管理员可以配置对

选定用户有效的特定服务，并且能够基于物理位置和用户信息指定对此类服务的访问。

人们可以理解的不变的虚拟 FQDN 或主机名可以被用来识别客户节点，而不是依赖于不友好的 IP 地址来识别，并且一个终端用户可以通过它的所被分配的名字到达一个同级的对应节点，即使该同级节点改变了 IP 地址或漂移到了一个新的位置。

例如，一个有着彩色激光打印机（销售）定额的销售员工可以无线地连接到一个 LAN，并将一个紧急的彩色册子（打印任务）指定传输到离一个同事最近的一台彩色激光打印机（受限制的访问），该同事位于一个建筑物中未知部分。同样，一个销售演示可以数字地传输到第一个未被占用的会议室（没有检测到客户节点），当指定显示器被连接到网络时，信息可以通过一个自动的备忘录反馈到该显示器。

安全控制可在从一个物理的插座连接到一个实际用户的单独应用访问和监视的全过程中进行。从一个具有网络可配置的点到点安全的集中服务器中执行防火墙规则、访问控制和网络政策，并且，在链路层，规则可施加在单独用户的链路层 MAC 地址和网络的起始点。在网络和传输层，服务器可像一个基于主机的防火墙那样运行，并基于客户的物理位置和用户分类等实施动态防火墙规则、插入和删除。一个基于万维网的认证页能对一个用户所实时连接的具体端口进一步授予其访问指定服务的权限。当客户断开与网络的连接时，动态防火墙可自动地删除特权访问。

在应用层，一般的应用请求如 DNS，电子邮件（SMTP）和万维网（HTTP）可基于物理连接、链路框架或网络地址基础/标准被监视并使得其行为受控。

应当理解，在不脱离本发明范围的情况下，可以对前面所述部分做出不同的变化、增加和/或修改，并且，按照本发明所公开的内容，可以用不同的软件和/或硬件方式执行各种不同的网络部分和功能。

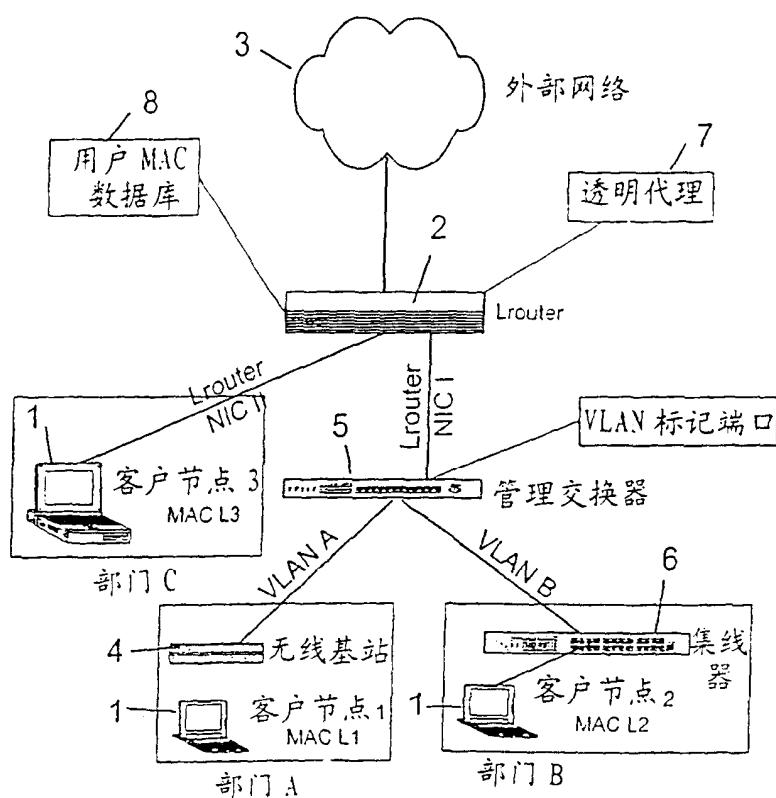
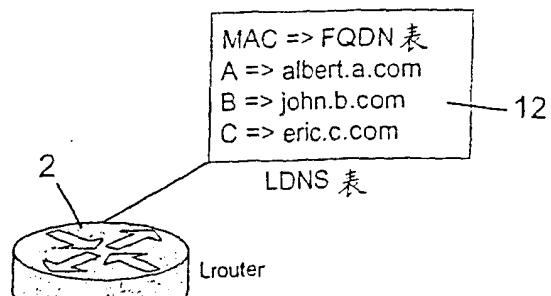


图 1



初始阶段

图 4

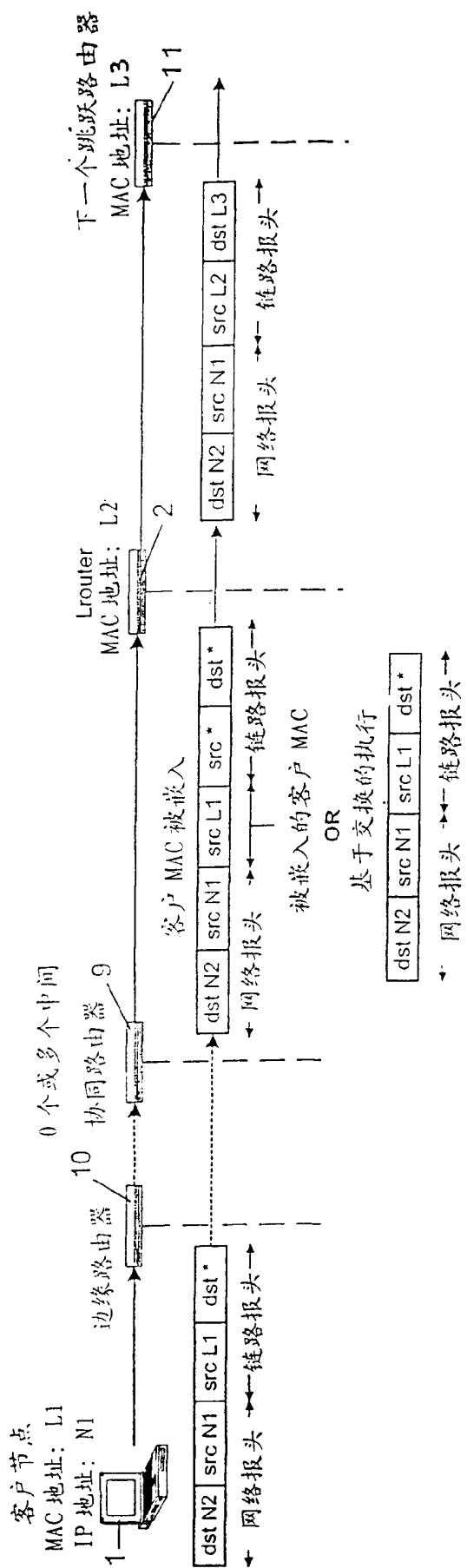


图 2

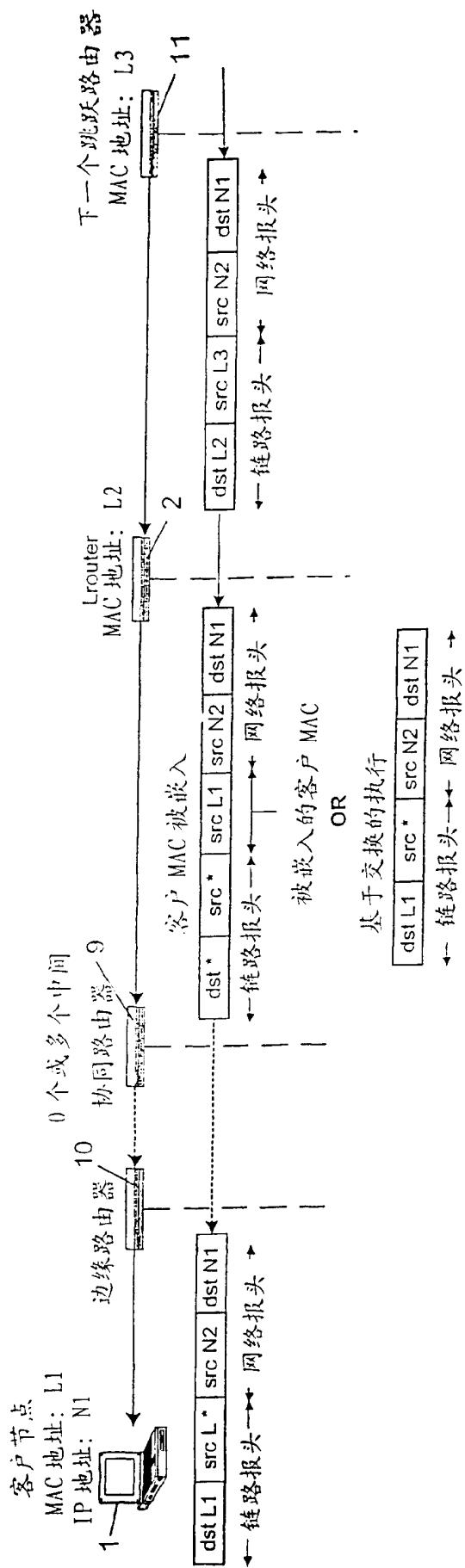


图 3

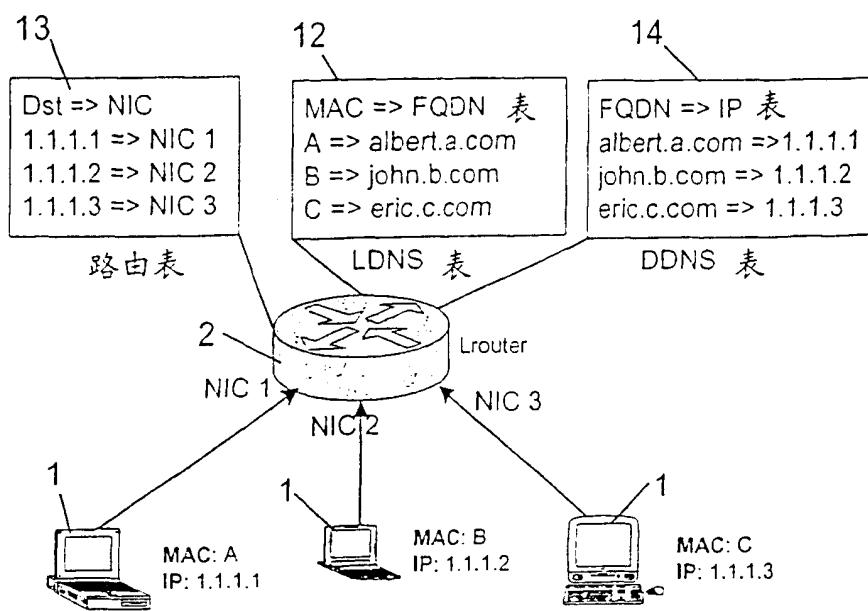


图 5

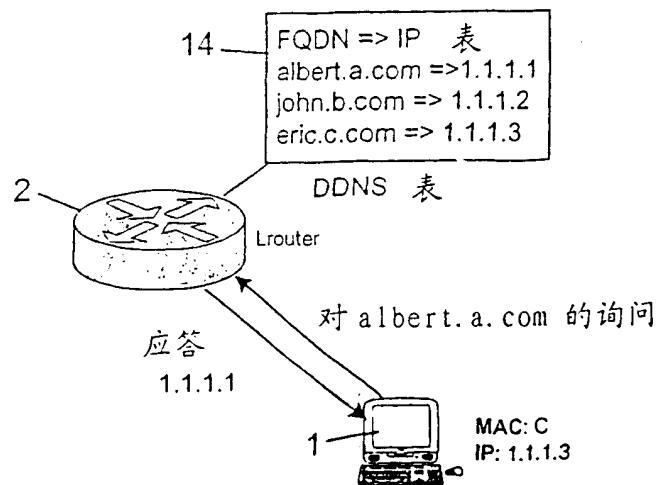


图 6

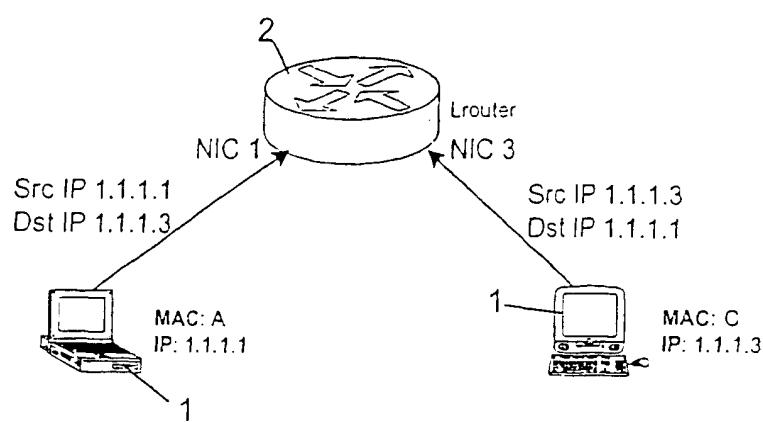


图 7

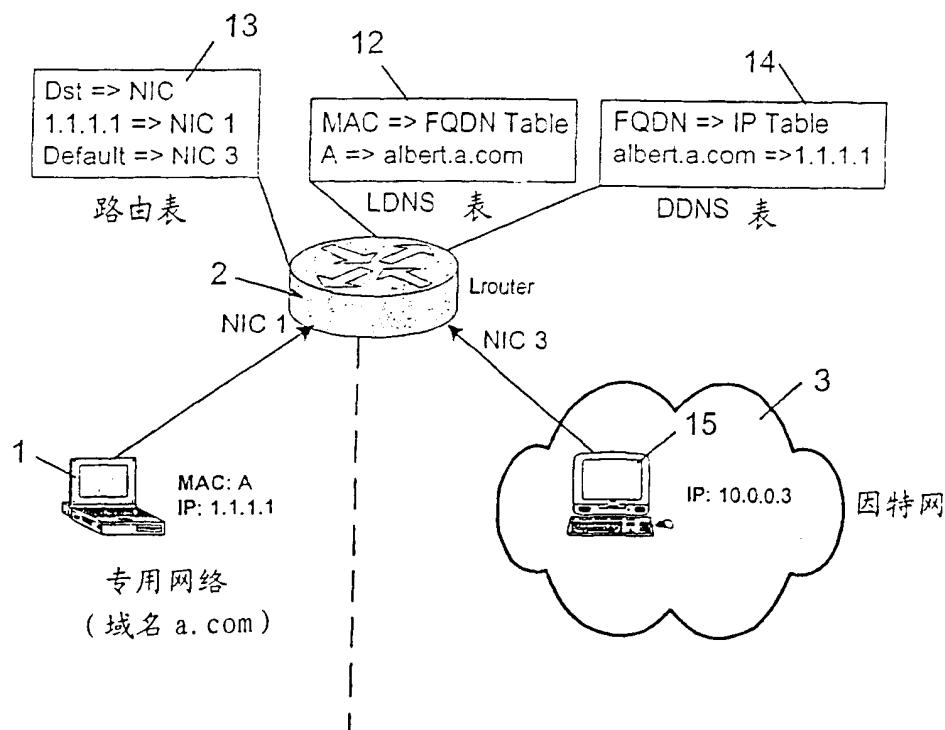


图 8

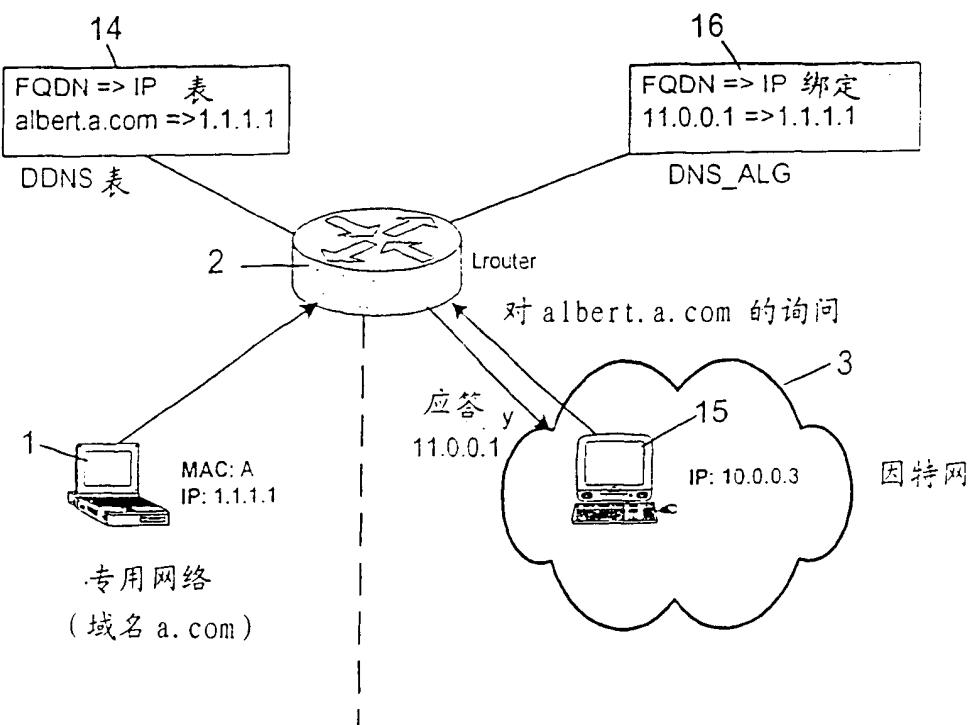


图 9

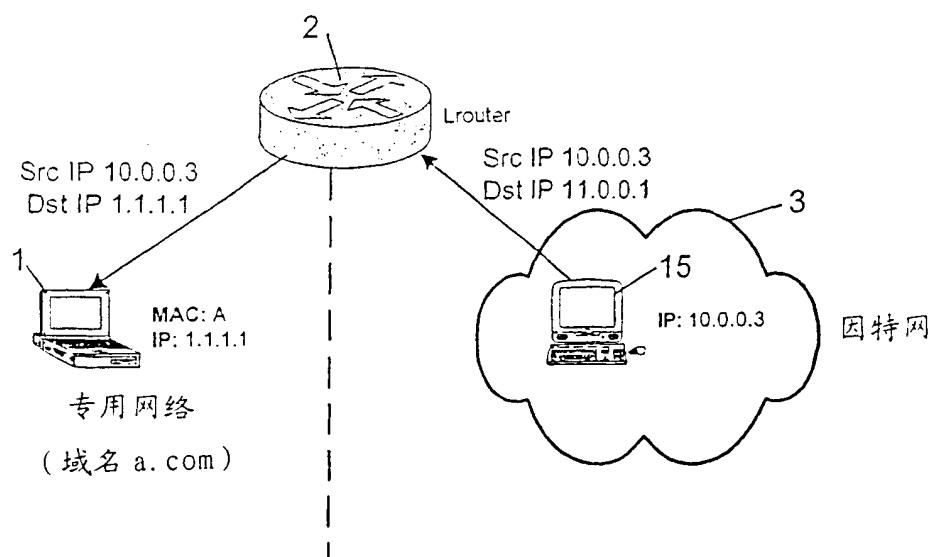


图 10

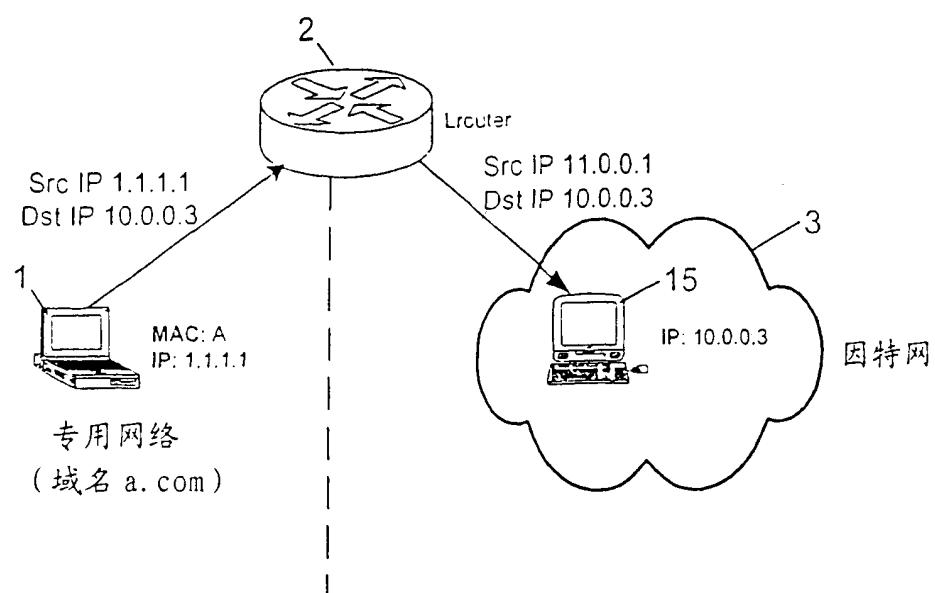


图 11

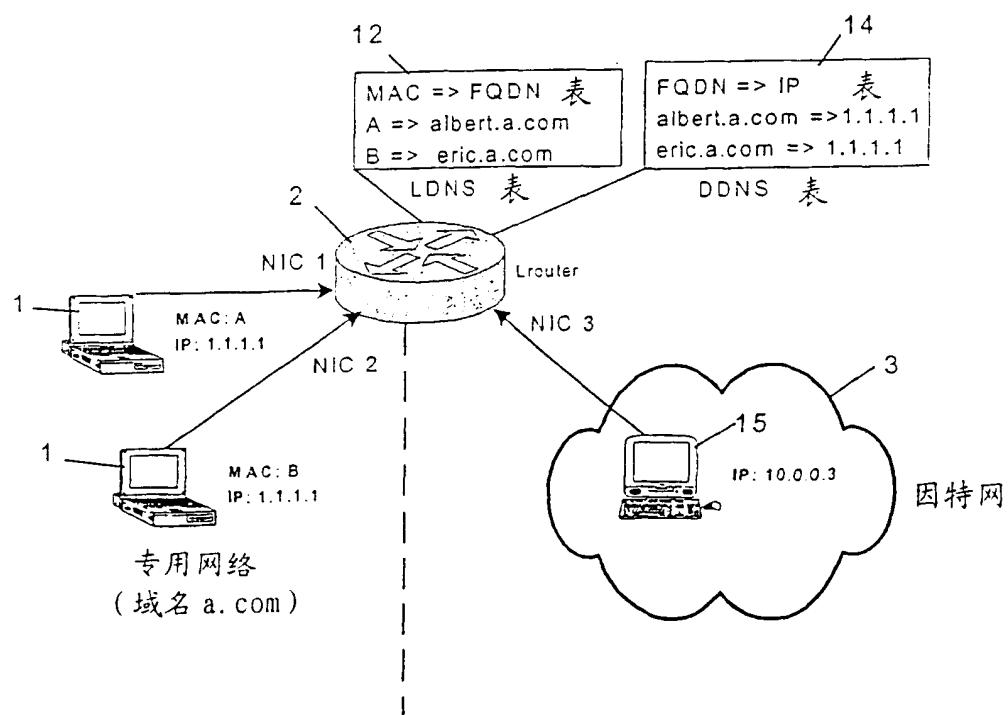


图 12

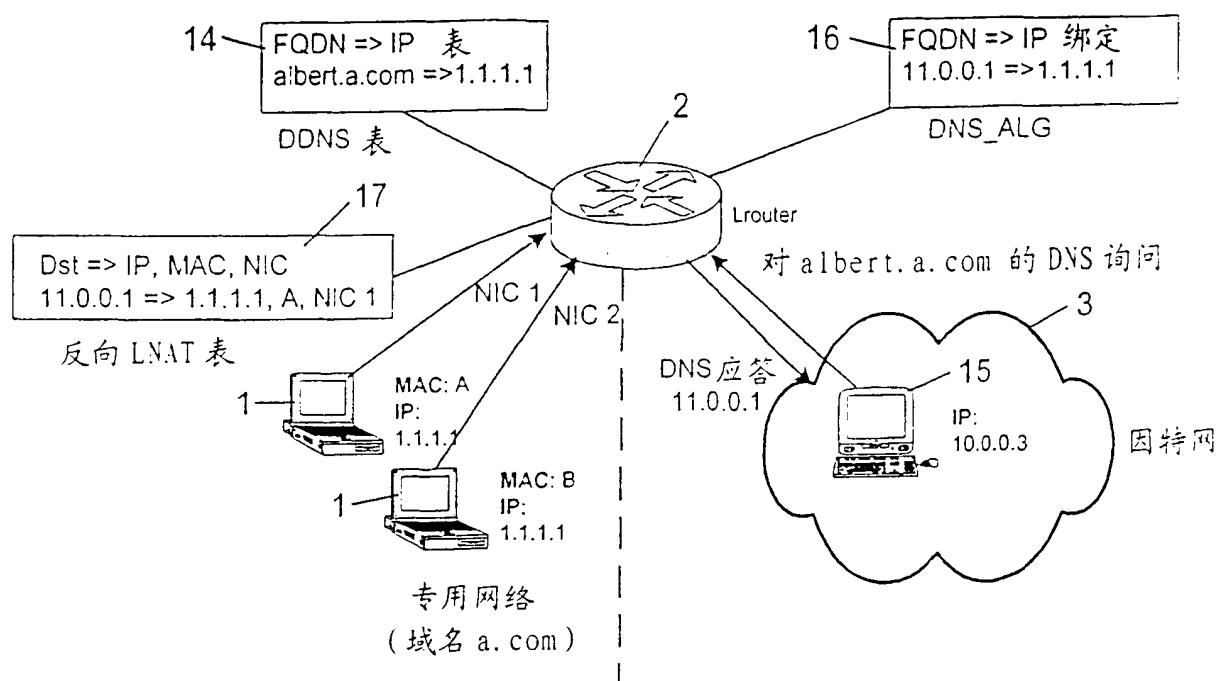


图 13

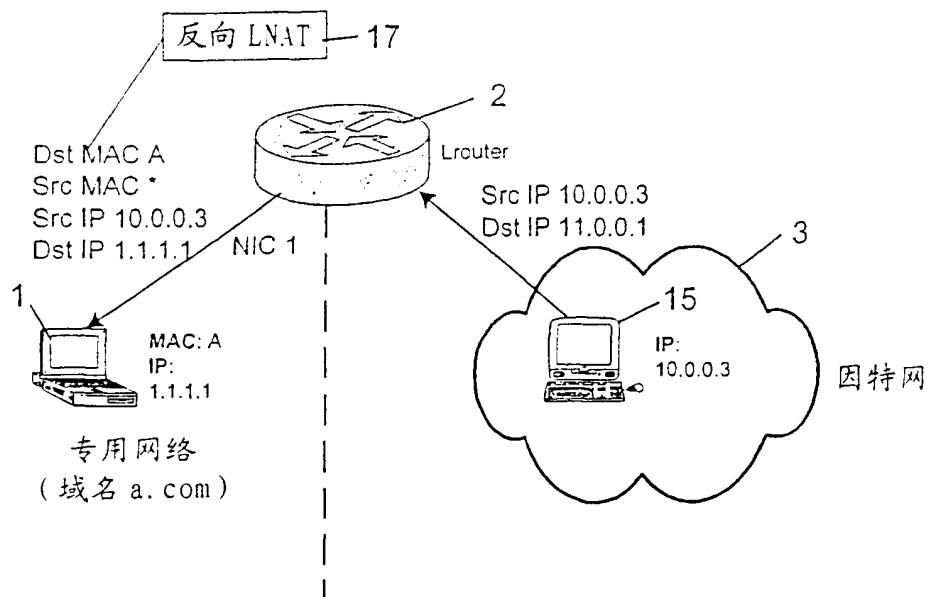


图 14

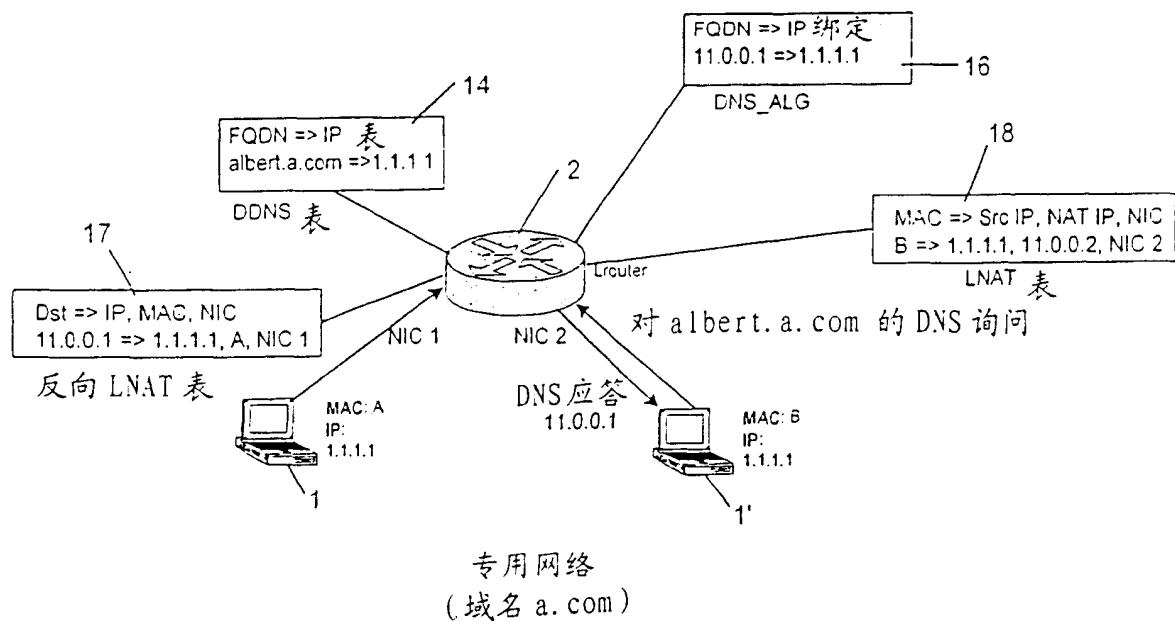


图 15

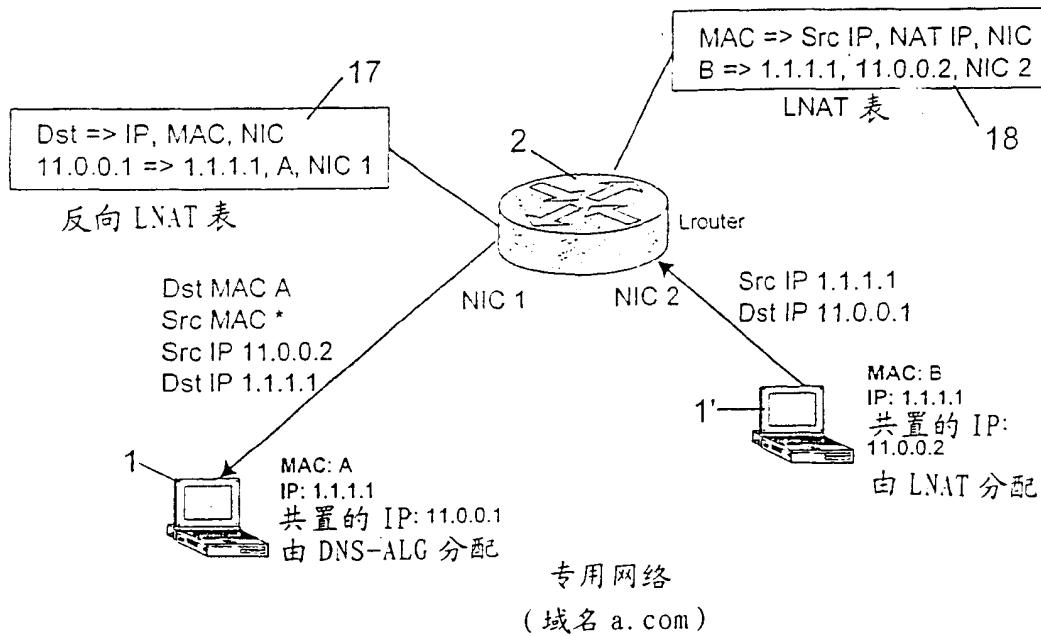


图 16

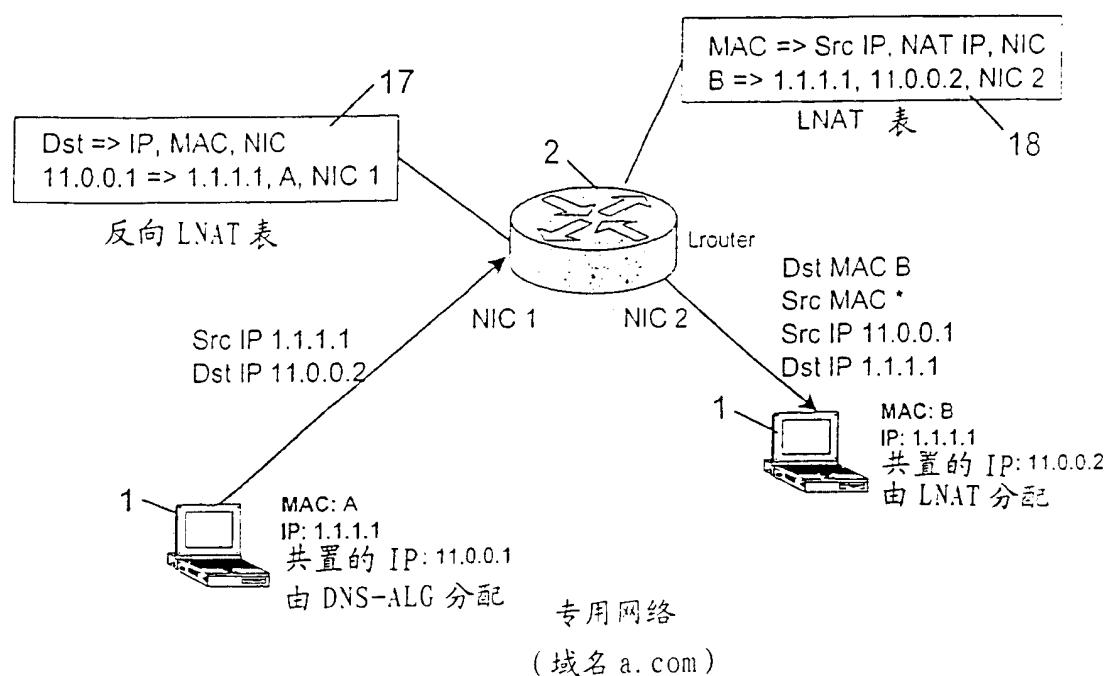


图 17