(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 101164321 B
(45)授权公告日 2012.10.03

(21)申请号 200680013714.X

(22)申请日 2006.04.11

(30)优先权数据
05447093.5 2005.04.25 EP

(85)PCT申请进入国家阶段日
2007.10.23

(86)PCT申请的申请数据
PCT/EP2006/061525 2006.04.11

(87)PCT申请的公布数据
WO2006/114367 EN 2006.11.02

(73)专利权人 汤姆森许可贸易公司
地址 法国布洛涅－比郎库尔

(72)发明人 德克·范德波尔 蒂埃里·杜特里

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 戎志敏

(51)Int.Cl.
*H04L 29/12*(2006.01)
*H04L 29/14*(2006.01)

(56)对比文件
EP 1349349 A2,2003.10.01, 说明书第[0013]-[0014]段以及附图1、3、6、8.
CN 1538706 A,2004.10.20, 全文.

审查员 张博

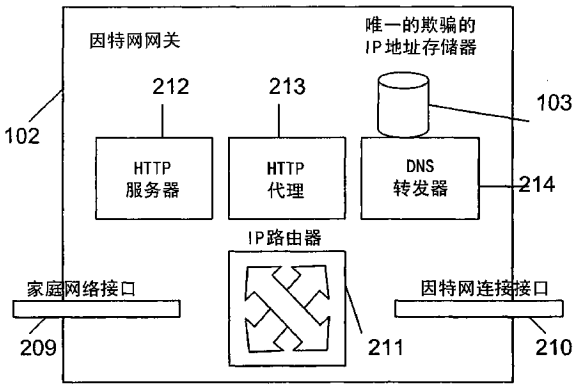
权利要求书 2 页 说明书 6 页 附图 3 页

(54)发明名称

用于管理资源地址请求的方法及关联的网关设备

(57)摘要

本发明涉及一种网关设备，包括：连接到第一设备的装置以及连接到第二设备的装置，以便根据由所述第一设备提供的网络资源标识符，获得真实的网络地址；以及提供虚假的网络地址的装置，用于在不能提供真实的网络地址的情况下，响应由所述第一设备提供的网络资源标识符来提供虚假的网络地址。所述提供虚假网络地址的装置适于针对不同的网络资源标识符提供不同的虚假网络地址－当所述真实的网络地址可用时，对于不同的虚假地址所做的请求使得所述第一设备能够获得相对应的真实的网络地址。本发明还涉及一种关联的方法。




CN 101164321 B

1. 一种网关设备 (102)，包括连接到包括至少一个第一设备 (101，107) 的第一网络 (108) 的装置；以及连接到包括至少一个第二设备 (106) 的第二网络 (104) 的装置，以便获得真实的网络地址，所述真实的网络地址是所述第二网络上的网络资源标识符的网络地址，所述网关设备还包括：

提供虚假的网络地址的装置，用于在不能从所述至少一个第二设备获得真实的网络地址的情况下，响应由所述第一设备提供的网络资源标识符来提供虚假的网络地址；所述提供虚假的网络地址的装置适于针对不同的网络资源标识符提供不同的虚假的网络地址；

装置，用于一旦能够获得真实的网络地址，则对于已经针对其提供了虚假的网络地址的之前接收到的网络资源标识符中的每一个，获取真实的网络地址，并将所述真实的网络地址转发到请求所述真实网络地址的所述至少一个第一设备。

2. 根据权利要求 1 所述的设备，还包括服务器部件，用于根据虚假的网络地址，对由所述第一设备所做的请求提供响应。

3. 根据权利要求 2 所述的设备，其中，所述响应包括描述无真实的网络地址的原因的信息。

4. 根据权利要求 3 所述的设备，还包括重定向装置，用于基于真实的网络地址已经被确定的虚假的网络地址，根据来自所述第一设备的请求将所述第一设备重定向到所述真实的网络地址。

5. 根据权利要求 1 所述的设备，还包括存储器 (103)，用于存储虚假的网络地址和其各自的网络资源标识符。

6. 根据权利要求 5 所述的设备，其中，一旦确定了真实的网络地址，所述存储器还存储与网络资源标识符相对应的真实的网络地址。

7. 根据以上权利要求中的任一项所述的设备，其中第一网络是局域网，第二网络是因特网，网络地址是因特网协议地址，以及网络资源标识符是统一资源定位器。

8. 一种用于管理从位于第一网络 (108) 中的至少一个第一设备 (101，107) 到位于第二网络 (104) 中的至少一个第二设备 (106) 的网络资源地址请求的方法，所述方法由连接在所述第一设备 (101，107) 和所述第二设备 (106) 之间的网关设备 (102) 执行，所述方法包括：

接收来自所述第一设备 (101，107) 的用于获取与网络资源标识符相对应的真实的网络地址的请求，所述真实的网络地址是所述第二网络上所述网络资源标识符的网络地址；

确定所述至少一个第二设备 (106) 是否能够提供所述真实的网络资源地址；

在否定情况下，向所述第一设备提供虚假的网络资源地址，其中针对每一个不同的网络资源标识符提供不同的虚假的网络地址；

一旦能够获得真实的网络地址，则对于已经针对其提供了虚假的网络地址的之前接收到的网络资源标识符中的每一个，获取真实的网络地址，并将所述真实的网络地址转发到请求所述真实网络地址的所述至少一个第一设备。

9. 根据权利要求 8 所述的方法，还包括步骤：基于虚假的网络地址，从所述第一设备 (101，107) 接收请求，以及作为响应，将所述第一设备 (101，107) 重定向到所述第一设备 (101，107) 可访问的服务器 (212)。

10. 根据权利要求 9 所述的方法，其中，所述可访问的服务器 (212) 提供关于导致无真

实的网络地址的错误状态的信息。

11. 根据权利要求 8 所述的方法，还包括步骤：当基于虚假网络地址接收到来自所述第一设备的请求时，建立所述网关和由与所述虚假的网络地址相对应的所述真实的网络地址所识别的设备之间的连接。

12. 根据权利要求 8 所述的方法，还包括步骤：存储接收到的标识符及其关联的虚假的网络资源地址，并且当获得真实的网络地址时，存储接收到的标识符及与接收到的标识符相对应的真实的网络地址。

# 用于管理资源地址请求的方法及关联的网关设备

## 技术领域

[0001] 本发明涉及一种用于管理例如来自 Web 浏览器应用程序的网络资源地址请求的方法，以及一种用于执行该方法的网关设备。本发明能够用于连接 LAN 到 IP 网络的网关中，但是不局限于这样的情境。

## 背景技术

[0002] 当配备有浏览器应用程序的客户端计算机需要接入因特网服务器以便获得例如所谓的“网页”，时，其需要知道与提供该页面的服务器相对应的因特网协议 (IP) 地址。通常，浏览器最初知道所谓的 URL（统一资源定位器）或者 FQDN（正式域名）。

[0003] 根据由客户端计算机提供的 URL 或 FQDN，诸如域名系统服务器的设备执行将 URL 或者 FQDN 翻译为实际的 IP 地址。

[0004] 一旦浏览器知道主持 (host) 网页的设备的 IP 地址，即 Web 服务器，则建立到该 IP 地址的连接，并使用例如 HTTP 协议（超文本链接标记语言）发送对于所需的信息的请求。该 Web 服务器利用 HTML（超文本链接标记语言）网页、画面或者一些其他数据来进行响应。

[0005] 例如，当客户端计算机连接到局域网或者其它类型的网络并且通过网关设备连接到因特网时，该地址翻译可以在该网关设备上执行。

[0006] 当不可能连接到 DNS 服务器时，会出现问题，例如在网关设备和因特网之间的连接中断。在这种情况下，浏览器不能获得 IP 地址。这造成浏览器显示错误消息，诸如例如“主机名不能解析”。

[0007] 为了向用户通知该问题的本质，并最终建议解决方案，已知的是使该网关设备执行所谓的“欺骗 (spoofing)”。该机制在于使网关设备给浏览器返回虚假的 IP 地址，使浏览器相信到 DNS 服务器的连接已经建立。然后，该网关设备截获对于到欺骗地址的连接的任何请求和行为，好像该网关设备是 Web 服务器。当网关设备接收到来自浏览器的请求时，于是网关能够返回解释问题本质的 HTML 页面，例如因为给出了错误的口令或者因为一些其他原因而不存在因特网连通性 (connectivity)。

[0008] 还已知的是，当 DNS 服务器宣布 URL 或 FQDN 未知时，产生欺骗的地址。这样做的目的在于使客户端发送请求到 Web 服务器。如果没有获得地址将不会建立连接以发送请求。

[0009] 不但浏览器或者其它应用程序，而且其它诸如操作系统的客户端部件也可以执行所谓的 DNS 高速缓存。DNS 高速缓存保持 URL 或 FQDN 与 IP 地址之间的关联。因而应用程序不需要再次请求 IP 地址，致使更快访问相对应的信息。

[0010] 然而，当结合上述欺骗机制时，DNS 高速缓存的出现会导致问题。实际上，一旦恢复了到 DNS 服务器的连接，应用程序就应该停止使用欺骗的 IP 地址，并再次继续从 DNS 服务器请求 URL 的实际 IP 地址。应用程序记住欺骗 / 虚假的 IP 地址的事实导致应用程序不再访问最初请求的网站的结果，这是因为其不再请求真实的地址。

[0011] 在某些应用程序中已知的是，关闭应用程序将导致清除 (purging)DNS 高速缓存。

## 发明内容

[0012] 本发明涉及一种网关设备，包括连接到第一设备的装置以及连接到第二设备的装置，以便根据所述第一设备提供的网络资源标识符来获得网络地址，所述网关设备还包括：

[0013] 提供虚假的网络地址的装置，用于在不能提供真实的网络地址情况下，响应由所述第一设备提供的网络资源标识符来提供虚假的网络地址；

[0014] 所述网关设备的特征在于，提供虚假的网络地址的装置适于对不同的网络资源标识符提供不同的虚假的网络地址。

[0015] 一旦这种真实的地址是可用的，则这种不同的虚假的地址能够用于提供与最初的资源标识符相对应的真实的地址。

[0016] 根据本发明的实施例，该设备还包括服务器部件，用于根据虚假的网络地址，对所述第一设备所做的请求提供响应。

[0017] 根据本发明的实施例，所述响应包括描述无真实的网络地址的原因的信息。

[0018] 根据本发明的实施例，该设备还适于针对之前被提供了虚假的网络地址的网络资源标识符，确定真实的网络地址。

[0019] 根据本发明的实施例，该设备还包括重定向装置，用于基于真实的网络地址已经被确定的虚假的网络地址，根据来自所述第一设备的请求，将所述第一设备重定向到所述真实的网络地址。

[0020] 根据本发明的实施例，该设备还包括用于存储虚假的网络地址和其相应网络资源标识符的存储器。

[0021] 根据本发明的实施例，一旦确定了真实的网络地址，所述存储器还存储与网络资源标识符相对应的所述真实的网络地址。

[0022] 本发明还涉及一种用于管理从第一设备到第二设备的网络资源地址请求的方法，所述方法由连接在所述第一设备和所述第二设备之间的网关设备执行，所述方法包括：

[0023] 接收来自所述第一设备的资源标识符；

[0024] 确定所述第二设备是否能够提供与所述资源标识符相对应的真实的网络资源地址；

[0025] 在肯定情况下，提供所述真实的网络资源地址；

[0026] 在否定情况下，提供虚假的网络资源地址，其中所述提供的虚假的网络资源地址与所述接收的资源标识符唯一地关联。

[0027] 根据本发明的实施例，该方法还包括步骤：基于虚假的网络地址，接收来自所述第一设备的请求，以及作为响应，将所述第一设备重定向到由所述第一设备可访问的服务器。

[0028] 根据本发明的实施例，所述服务器提供关于导致无真实的网络地址的错误状态的信息。

[0029] 根据本发明的实施例，该方法包括步骤：一旦能够获得真实的网络地址，针对已经被提供了虚假的网络地址的、之前接收到的资源标识符，获得这种真实的网络地址。

[0030] 根据本发明的实施例，该方法包括步骤：当基于虚假的网络地址接收到来自所述第一设备的请求时，建立所述网关和由与所述虚假的网络地址相对应的所述真实的网络地址所识别的设备之间的连接。

[0031] 根据本发明的实施例，该方法包括步骤：存储接收到的标识符及其关联的虚假的网络资源地址，以及当获得真实的网络地址时，存储接收到的标识符及其相对应的真实的网络地址。

## 附图说明

[0032] 将参考附图在特定实施例中详细描述本发明。本发明不应局限于实施例的详细描述。

[0033] 图 1 是使用本发明实施例所述的网关设备连接的局域网和因特网的示意图；

[0034] 图 2 是网关设备的功能部件的示意图；

[0035] 图 3 是描述根据本发明实施例的客户端应用程序、网关设备的部件和 DNS 服务器之间的通信的消息序列图；

[0036] 图 4 描述了一个表，所述表指示了根据本发明，在没有与 DNS 服务器连通的时间间隔期间网关设备已经接收到请求之后该网关设备的地址高速缓冲存储器的内容；以及

[0037] 图 5 描述了一旦重新建立连通性以及“真实”或实际的 IP 地址被确定时图 4 的表。

## 具体实施方式

[0038] 图 1 描述了作为本实施例描述对象的网关 102，网关 102 将局域网 108 与因特网 104 相连。客户端计算机 101 与该局域网相连，客户端计算机 101 具有需要诸如 Web 浏览器之类的需要因特网接入的应用程序 107。图 1 示出了与因特网相连的一个 DNS 服务器 106 和 Web 服务器 105，当然可以连接更多的 DNS 服务器和 Web 服务器，除这两种服务器的设备之外的其他设备也可以连接到因特网。网关 102 包括存储器 103，其目的稍后描述。根据本示例，该存储器为半导体类型或者其等同类型。因特网应用程序 107 也可以不同于浏览器，并可以运行在除计算机以外的设备上。例如，因特网应用程序 107 可以是具有电子节目指南应用程序的支持 IP 的音频 / 视频解码器。应该注意的是，网关 102 可以直接位于设备 101 中，在这种情况下，实质上不存在局域网。

[0039] 图 2 示出了网关设备 102 的各种功能部件，网关设备 102 包括分别将该网关设备连接到局域网和因特网的接口 209 和 210。例如，该局域网可以是以太网或者 IEEE802.11b 类型的无线网络。

[0040] 此外，网关设备 102 包括 HTTP 服务器 212，HTTP 服务器 212 是与 Web 服务器类似的应用程序，管理和提供与例如网关设备的内部配置相对应的网页。

[0041] 根据本实施例，HTTP 服务器 212 还提供信息给请求欺骗的 IP 地址的设备。

[0042] HTTP 代理 213 充当网络 108 中客户端应用程序的代理服务器。HTTP 代理 213 接收客户端应用程序表示 (formulated) 的请求，适当时将请求转发到诸如服务器 105 的真实的服务器，还将该真实的服务器的任何响应传输回该客户端应用程序。只要涉及 Web 服务器，HTTP 代理充当客户端应用程序。

[0043] DNS 转发器 214 是处理从客户端应用程序 107 接收到的 DNS 查询 (query) 的部件，并将其转发到因特网中的一个或多个 DNS 服务器。该部件检测是否从该 DNS 服务器接收到有效响应，并将该响应发送回客户端应用程序。根据本实施例，当因为各种原因不能获得正确的 DNS 服务器响应时，DNS 转发器还是产生“欺骗”或“虚假”IP 地址并将其发送到客户

端应用程序的部件。代替使用仅仅一个欺骗 / 虚假的 IP 地址来响应 DNS 请求，当需要这种欺骗的地址时，网关设备的 DNS 转发器针对 DNS 请求中所接收到的每个新 URL 或 FQDN，发送不同的欺骗 IP 地址。

[0044] IP 路由器部件 211 向局域网、网关的其它部件以及因特网转发 IP 分组，并转发来自局域网、网关的其它部件以及因特网的 IP 分组。

[0045] 网关设备 102 还包含存储器 103，已经在涉及图 1 时简要提及。响应发送 URL 或 FQDN，存储器 103 将由 DNS 转发器确定的欺骗的 IP 地址与相应的 URL 或 FQDN 一起存储。因此，网关 102 能够确定对于所接收的给定 URL/FQDN 发送哪个欺骗的 IP 地址，反之亦然。

[0046] 在下面，将假定当检测到不存在因特网连通性时网关设备发送欺骗的地址。当然也可以考虑其它情况。

[0047] 图 4 给出了在接收到来自客户端应用程序 107 的两个请求之后的存储器 103 的内容的示例。假定 DNS 转发器确定对于这两个请求，没有接收到正确的 DNS 服务器响应，因此，两个不同的欺骗 IP 地址被发送回客户端应用程序 107。“实际 IP 地址”一栏指示客户端应用程序所期望的真实的地址，在此阶段保持为空。

[0048] 一旦网关设备可以建立到 DNS 服务器的连接，网关设备检查存储器 103 的内容并针对其存储器中那些之前不能被确定实际 IP 地址的每一对欺骗的 IP 地址和 URL 或者 FQDN，将对于实际 IP 地址的请求发送到 DNS 服务器。

[0049] 图 5 示出了一旦确定了实际 IP 地址时存储器的状态。

[0050] 在本实施例中，存储器存储多达 32 个条目。当列表满时，循环 (round robin) 机制删除最陈旧的条目。根据不同的实施例，使用期限 (time-to-live) 参数与每个条目相关联。

[0051] 当网关设备从客户端应用程序接收到包含欺骗的 IP 地址之一作为目的地地址的请求时 ( 即客户端应用程序尝试建立连接 )，网关设备在其高速缓冲存储器 103 中查找对于欺骗的地址，是否已经高速缓存实际的 IP 地址。

[0052] 如果存在这样的实际 IP 地址，则利用实际 IP 地址来替代请求中的欺骗的 IP 地址，并且网关设备建立与实际的 IP 地址所识别的正确服务器的连接，并将最初的请求转发到该服务器。

[0053] 如果在高速缓冲存储器中不存在这样的实际 IP 地址，网关设备将诸如 HTML 网页之类的适当消息返回到客户端应用程序。只要网关设备能够确认，该消息或者页面优选地包括无实际 IP 地址的原因标识符。例如，网关设备可以执行测试来确定错误状态的原因。换而言之，HTTP 协议使服务器能够使用新的 URL 将客户端重定向到其它位置。

[0054] 图 3 是消息交换和客户端应用程序、网关设备的部件、DNS 服务器以及 Web 服务器的动作的详细图。

[0055] 下面描述不同的步骤 :

[0056] 步骤 1 :客户端设备上的 web 浏览器 ( 更准确而言，浏览器上操作系统的行为 ) 发送 DNS 查询到 DNS 转发器，请求与 web 站点 URL( 例如 www.xyz.com) 相对应的 IP 地址。

[0057] 步骤 2 :网关设备的 DNS 转发器检测不存在到因特网的连通性 ( 作为结果，到实际的 DNS 服务器的连通性 )。

[0058] 步骤 3 :DNS 转发器决定利用欺骗的 / 虚假的 IP 地址进行响应。DNS 转发器利用

欺骗的 IP 地址和 URL/FQDN 之间的唯一关联来更新其高速缓存 / 表。

[0059] 步骤 4 :因为 web 浏览器认为 web 站点的地址是欺骗 / 虚假的 IP 地址,web 浏览器建立了到 web 站点的连接。网关设备 102“截获”该连接请求,建立了到该网关的 HTTP 代理模块的连接。web 浏览器发送对于该网址的 HTTP 请求。

[0060] 步骤 5 :HTTP 代理检测到欺骗的 / 虚假的 IP 地址。该部件查询 DNS 转发器以得知是否存在与该欺骗 IP 地址相对应的实际的 IP 地址。

[0061] 步骤 6 :DNS 转发器检查其高速缓存 / 表,得知与该欺骗的 IP 地址相关的 URL/FQDN 没有被解析为实际的 IP 地址。DNS 转发器告知 HTTP 代理不存在实际的 IP 地址。

[0062] 步骤 7 :得知不存在与该欺骗的 IP 地址相关的实际的 IP 地址,HTTP 代理将 web 浏览器重定向到由网关设备的 HTTP 服务器主持的网页 :该网页对 web 浏览器指示了新的 URL。

[0063] 步骤 8 :现在,web 浏览器建立了到网关设备的连接,并将对于网页的 HTTP 请求发送到网关的本地服务器。

[0064] 步骤 9 :HTTP 服务器网页检测到不存在因特网连通性,或能够进行其它的诊断测试。

[0065] 步骤 10 :HTTP 服务器基于由网关设备执行的诊断测试,使用 HTMP 页面进行响应以解释该问题,例如包含解决因特网连通性问题的可能方案。

[0066] 步骤 11 :用户进行校正的行为(例如重新连接线缆或者校正因特网连接口令)并按压按钮或者点击屏幕上的链接。例如,这触发了将校正后的口令发送回 HTTP 服务器。

[0067] 步骤 12 :现在 HTTP 服务器检测到再次建立了因特网连接。当建立因特网连接时,由网关动态地重新获得 DNS 服务器的地址。网关还一起接收因特网地址和一个或多个 DNS 服务器的地址。

[0068] 步骤 13 :因特网连通性的建立触发了网关设备的 DNS 转发部件针对已经被发送了“欺骗的”/ 虚假的 IP 地址的 URL 发送 DNS 查询。DNS 转发部件向因特网上 DNS 服务器的地址发送这些查询。

[0069] 步骤 14 :DNS 服务器利用与 URL 相对应的实际或者“真实”的 IP 地址进行响应。

[0070] 步骤 15 :DNS 转发器利用欺骗的 IP 地址、URL(FQDN) 以及实际的 IP 地址来更新其高速缓存 / 表。

[0071] 步骤 16 :得知再次建立了因特网连通性,因特网网关 HTTP 服务器将 Web 服务器再次重定向到最初请求的 web 站点。该 HTTP 服务器记得之前在 HTTP 代理和 HTTP 服务器之间交换的最初请求的 web 站点的 URL。

[0072] 步骤 17 :现在,web 浏览器使用高速缓存的最初的 web 站点与欺骗的 / 虚假的 IP 地址间的关系并再次连接到欺骗的 / 虚假的 IP 地址。网关设备“截获”该连接,所以实际上建立了到网关设备的 HTTP 代理模块的连接。

[0073] 步骤 18 :HTTP 代理部件查询 DNS 转发器部件,以得知是否存在与欺骗的 IP 地址相对应的实际的 IP 地址。

[0074] 步骤 19 :DNS 转发器部件利用在步骤 14 中从 DNS 服务器接收到的实际的 IP 地址进行响应。

[0075] 步骤 20 :HTTP 代理利用实际的 IP 地址来替代欺骗的 IP 地址并建立到请求网页的

Web 服务器的连接。

[0076] 步骤 21 :Web 服务器利用请求的 HTML 网页进行响应。

[0077] 步骤 22 :现在，HTTP 代理将从 Web 服务器接收到的响应转发到客户端计算机 web 浏览器。在客户端计算机的用户自动接收请求的 web 站点。因此，客户端应用程序接入正确的服务器，虽然其继续使用欺骗的 IP 地址。

[0078] 应该注意的是，大部分操作系统包括其自己的 DNS 高速缓存。这是一种模块，该模块记得具有使用期限 (ttl) 参数的 DNS 结果 ( 与 IP 地址相对应的 URL/FQDN)。在操作系统“之上”或者“上”运行的应用程序，例如 web 浏览器也具有其自己的缓存。但是他们不考虑 ttl 参数。

[0079] 在变体实施例中，检查对于欺骗的地址在存储器 103 中真实的地址是否可用的步骤由 IP 路由器 211 来执行，而不是 HTTP 代理 213。同样，由真实的 IP 地址来替代欺骗的 IP 地址的步骤可以由该 IP 路由器来执行 ( 步骤 20)。HTTP 代理检查存在欺骗的 IP 地址并当检测到这样的地址时将客户端应用程序重定向到本地 HTTP 服务器。HTTP 代理不查询存储器 103 中的表。该实施例不仅提供了对于 web 浏览器不正确记得 ( 错误的 ) 地址的常见问题的解决方案，还可适用于在其自己的 DNS 缓存中记得地址的其它程序。

[0080] 虽然实施例的描述基于因特网协议网络的执行，本发明可以适于标识符由地址来替代并且在这种结构中高速缓存响应可能造成问题的其它情境中。

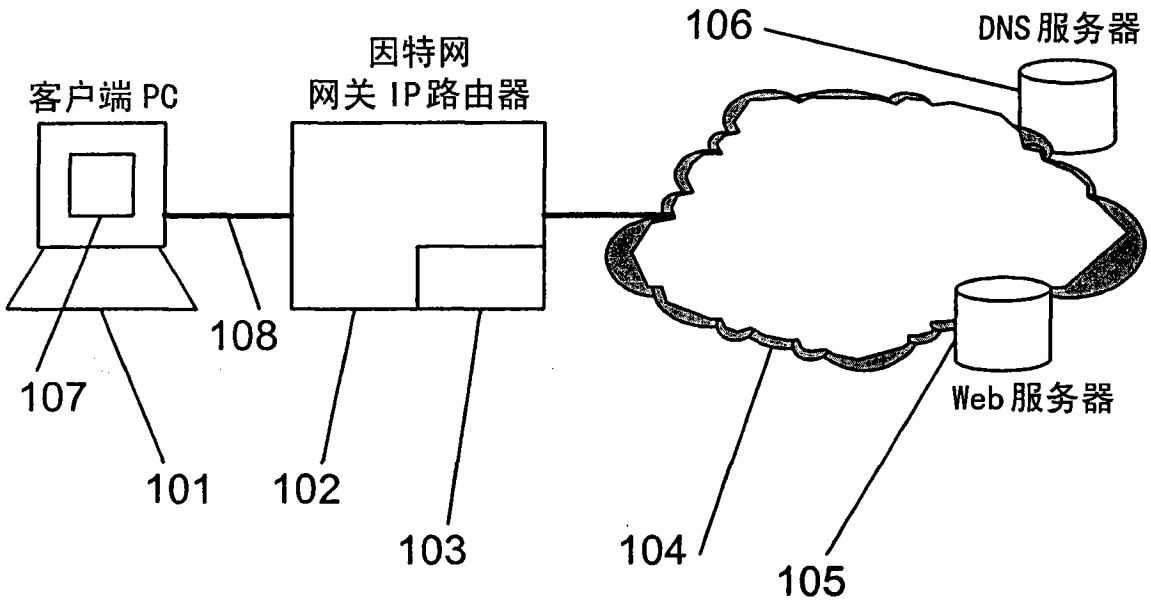

106
DNS服务器
因特网
网关 IP路由器
客户端 PC
108
107
101
102
103
104
105
Web服务器

图 1

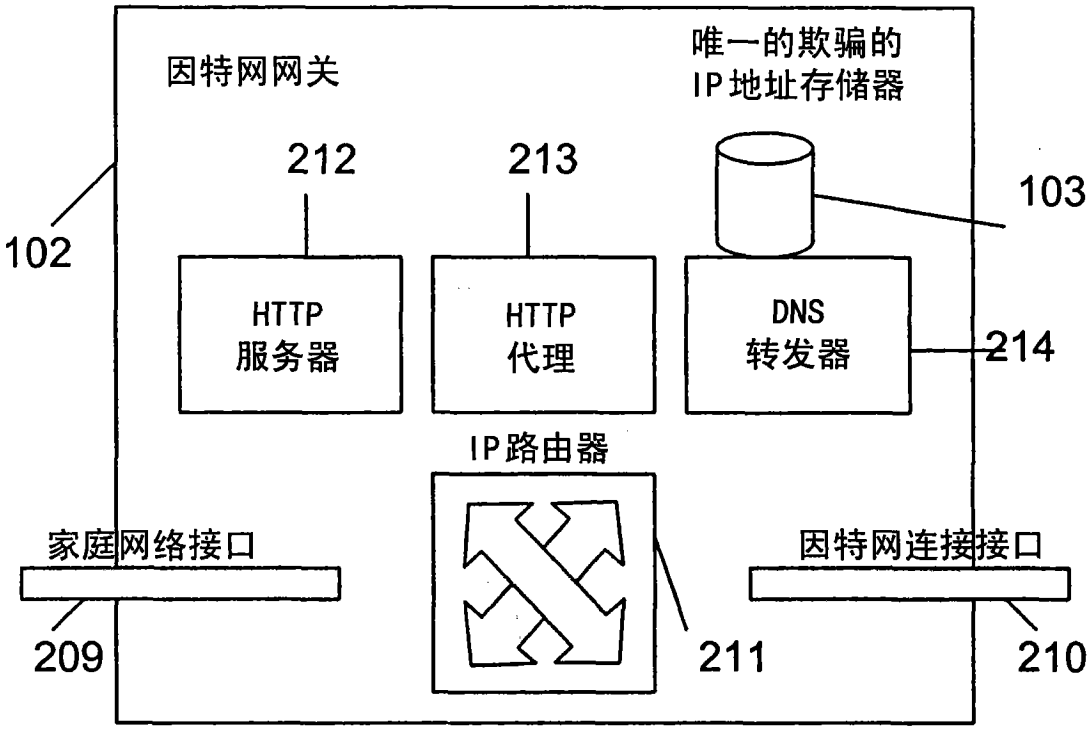

因特网网关
唯一的欺骗的
IP地址存储器
212
213
103
102
HTTP
服务器
HTTP
代理
DNS
转发器
214
IP路由器
家庭网络接口
因特网连接接口
209
211
210

图 2

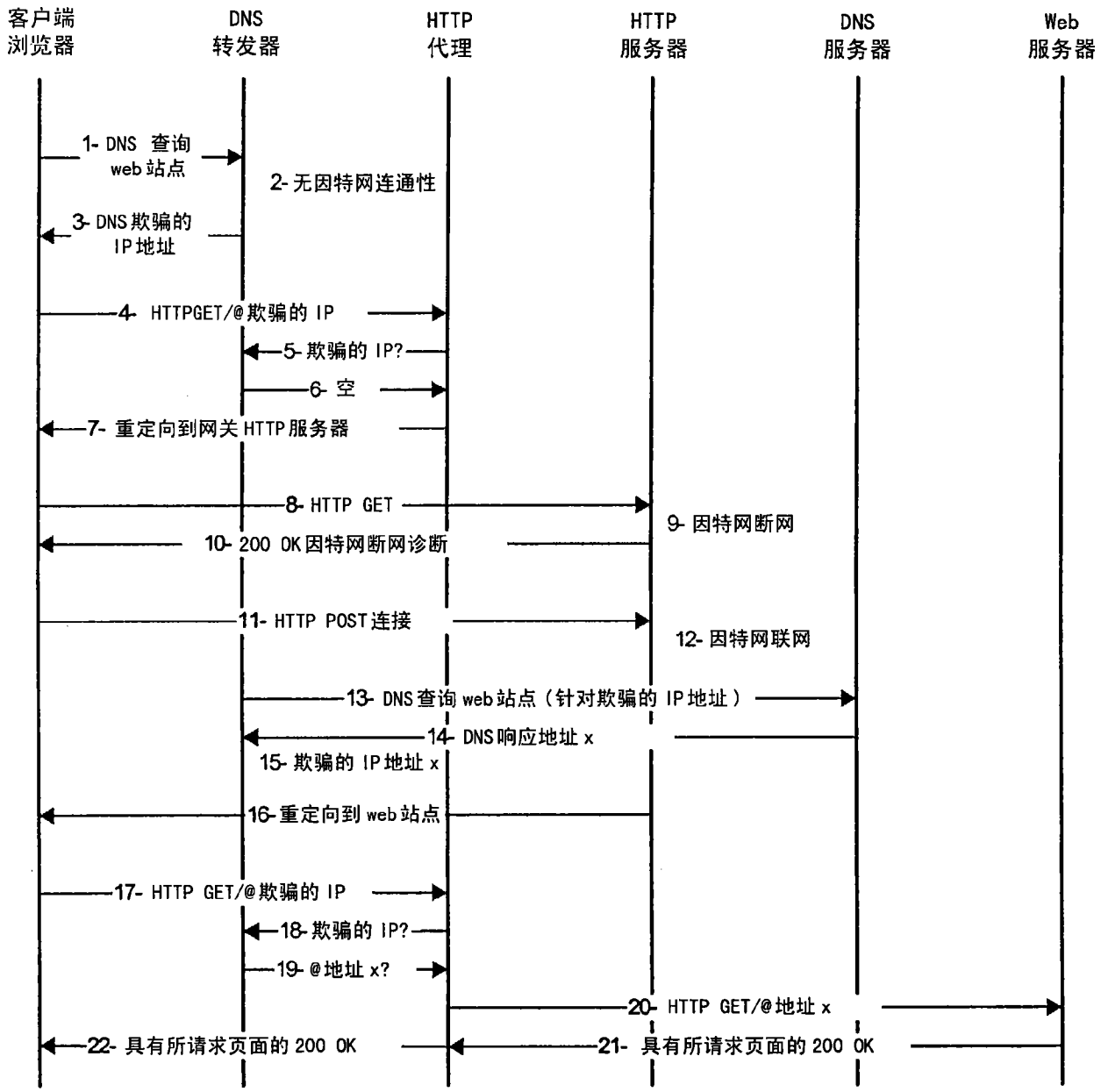

客户端
浏览器
DNS
转发器
HTTP
代理
HTTP
服务器
DNS
服务器
Web
服务器
1- DNS 查询
web 站点
2- 无因特网连通性
3- DNS 欺骗的
IP 地址
4- HTTPGET/@欺骗的 IP
5- 欺骗的 IP?
6- 空
7- 重定向到网关 HTTP 服务器
8- HTTP GET
9- 因特网断网
10- 200 OK 因特网断网诊断
11- HTTP POST 连接
12- 因特网联网
13- DNS 查询 web 站点（针对欺骗的 IP 地址）
14- DNS 响应地址 x
15- 欺骗的 IP 地址 x
16- 重定向到 web 站点
17- HTTP GET/@欺骗的 IP
18- 欺骗的 IP?
19- @地址 x?
20- HTTP GET/@地址 x
21- 具有所请求页面的 200 OK
22- 具有所请求页面的 200 OK

图 3

| 欺骗的 IP | FQDN / URL | 实际的 IP |
|---|---|---|
| a.b.c.d | Proxy.xyz.be | 空 |
| e.f.g.h | www.abc.be | 空 |

图 4

| 欺骗的 IP | FQDN / URL | 实际的 IP |
|---|---|---|
| a.b.c.d | Proxy.xyz.be | 80.200.248.199 |
| e.f.g.h | www.abc.be | 216.239.57.104 |

图 5