

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04L 12/54

H04L 12/66 H04L 29/02

[12] 发明专利申请公开说明书

[21] 申请号 02111483.8

[43] 公开日 2002 年 11 月 20 日

[11] 公开号 CN 1380773A

[22] 申请日 2002.4.25 [21] 申请号 02111483.8

[71] 申请人 复旦大学

地址 200433 上海市邯郸路 220 号

[72] 发明人 凌 力

[74] 专利代理机构 上海正旦专利代理有限公司

代理人 陆 飞

权利要求书 2 页 说明书 8 页 附图 1 页

[54] 发明名称 一种增强的 NAT-PT 协议方案

[57] 摘要

本发明属计算机网络技术领域,具体为一种能够实现 IPV4 和 IPV6 两类网络高效互访的 ENAT-PT 协议,由 ENAT、NAPT、PT 三部分构成。它成功地解决了 IPV4 网络和 IPV6 网络的互访,并可用少量的 IPV4 地址就支持网络互连。

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

1、一种支持 IPv4 和 Ipv6 两类网络互访的 ENAT-PT 协议，其特征在于由三个部分组成：

- (1) ENAT，增强的 NAT 机制，处理入站会话；
- (2) NAPT，处理出站会话；
- (3) PT，两种协议之间的转换；

其中，ENAT 的基本方法如下：会话建立前，源节点 H1 发起一个 DNS 请求到 DNS 服务器请求获得 H2 的地址，ENAT-PT 网关截获 DNS 响应，并从地址池中取得一个未被绑定的临时 IPv4 地址 REG1 与返回 H2 的地址 ADDR2 绑定到一起，同时将 REG1 作为 H2 的地址返回给 H1，V4 主机 H1 以 REG1 作为服务器地址发起会话请求，ENAT-PT 网关在会话建立后就释放临时 IPv4 地址，而非在会话结束后才释放临时地址。

2、根据权利要求 1 所述的 ENAT-PT 协议，其特征在于为了区分到不同 V6 节点的不同会话，ENAT 引入会话参数并维护一个会话表；ENAT-PT 网关截获到某个会话的第一个数据包以后，在会话表中建立起一个新的表项，该表项的形式为：V4 主机地址、V4 主机端口、映射地址、V6 主机地址、V6 主机端口。

3、根据权利要求 2 所述的 ENAT-PT 协议，其特征在于 ENAT 的具体步骤如下：

- (1) V4 客户机在需要访问 V6 主机时使用 DNS 查询 V6 的 IP 地址；
- (2) 截获 DNS 的响应，从空闲的临时地址池中选择一个 V4 地址 REG1，将 DNS 中 V6 主机的地址 IV6 替换为 REG1，返回给 V4 客户，同时建立地址绑定(IV6, REG1)放入绑定列表；

(3) 关收到 V4 的数据报后，根据报文参数检查会话表，

(a)如果有该会话的会话项，则进行协议转换操作，将报文转换为 IPv6 格式，将会话项中的 IV6 地址作为 V6 的目标地址；

(b)如果没有相关会话项，则根据报文的 IPv4 目的地址查询绑定列表，

①如果没有相关绑定，则转换失败；

②如果有绑定，

(A)如果是 TCP 连接建立报文或 UDP 或 ICMP 报文则根据报文信息和绑定，在会话表中建立会话项 (V4 主机地址，V4 主机端口，映射地址，V6 主机地址，V6 主机端口)，释放该绑定，并进行协议转换；

(B)否则是错误或超时报文，丢弃；

(c)如果是结束报文则，释放会话项；

- (4) 网关收到 V6 的数据报后，根据报文参数检查会话表，如果有会话项则进行协议转换，将报文转换为 IPv4 格式，将会话项中的 REG1 地址作为 V4 的源地址，系统通过超时机制来回收资源：当绑定超时是，要释放绑定，使得地址可重用，当会话超时时释放会话项。

4、根据权利要求 3 所述的 ENAT-PT 协议，其特征在于通过扩展 NAPT 的映射参数，使 ENAT 在进行端口映射时采用源地址、源端口、目的地址、目的端口四个参数来映射一个数据包，从而统一 ENAT 和 NAPT 对报文的处理过程。

一种增强的 NAT-PT 协议方案

技术领域

本发明属计算机网络技术领域，具体为一种能够实现 IPv4 网络和 IPv6 网络高效互访的增强型 NAT-PT 协议。

背景技术

虽然 IP 因其简洁性在诸多网络协议的竞争中取得的胜利，在网络中尤其是互连网中得到广泛的应用，但随着技术的进步和网络应用的快速发展，IPv4 也面临众多的挑战，如地址空间过小，协议处理仍然相对复杂，对服务质量支持差，安全性差等问题。为了应对 IPv4 面临的问题，IETF 设计了下一代互联网协议 IPv6。尽管 IPv6 继承了 IPv4 的众多优点，但两者有显著差异。由于 IPv4 网络现存的资源数量巨大，设备种类繁多，将不可能在短时期内实现向 IPv6 的迁移，两类网络将长期共存。实现两类网络间的互访是 IPv6 成功应用的重要方面。为了实现互访，需要解决两个问题。1) 两类报文协议间的互相转换即协议翻译(PT—Protocol Translation)。2) 实现 IPv4 与 IPv6 两个地址域的转换即地址翻译网络(NAT—Network Address Translation)。IP 网络是采用 IP 地址实现数据报文传递的，由于 IPv4 采用 32 位地址，IPv6 采用 128 位地址，需要在两类网络节点互访时，实现地址翻译。现有的方案：NAT-PT (NAT 协议翻译，RFC 2766) 定义了将 IPv4 数据包转换为公共 IPv6 数据包的方法。NAT-PT 最重要的两种形式是双向 NAT-PT 和 NAPT-PT。

双向 NAT-PT 同时支持出站会话和入站会话。在双向 NAT-PT 模型中，一个 IPv6 地址在会话建立前静态地绑定到一个临时 IPv4 地址，或者在会话建立的时候动态地映射到一个临时 IPv4 地址。对于入站会话，在会话建立前，源节点发起一个 DNS 请求(假定所有 IPv6 节点的域名是全局唯一的)。NAT-PT 网关获得从 DNS 服务器返回的 IPv6 地址后，将其动态的绑定到一个临时 IPv4 地址，或者查找静态绑定表找到该 V6 地址所对应的映射地址，之后，NAT-PT 根据映射关系对 IP 包头中的地址进行转换。

NAPT-PT (Network Address Port Translation-Protocol Translation) 是一种改进的 NAT-PT 模型。NAPT-PT 的基本原理是：对于从 IPv6 发起的会话，NAPT-PT 在将 IPv6 地址映射成 IPv4 地址的同时，将 IP 包中客户端端口映射成某个临时 IPv4 地址的一个未用端口。这样，每个临时 IPv4 地址上最多可以同时建立达 63000 个会话(端口号 0~1023 保留)，从而节省 IPv4 地址。

尽管双向 NAT-PT 可以支持 IPv4 与 IPv6 节点的互访，但是由于一个临时 IPv4 地址只能绑定到一个 IPv6 节点上，对于大型网络的互访需要大量的临时 IPv4 地址存放在临时地址池中。这将使得 IPv4 地址资源紧张的问题更加严重。NAPT-PT 采用端口复用技术可以节约大量的 IPv4 地址，但是其只支持 IPv6 节点访问 IPv4 网络。

发明内容

本发明的目的在于提出一种既支持 IPv4 和 IPv6 两类网络互访，又不需要大量临时 IPv4 地址的协议方案。

为了便于叙述，先将本发明涉及的常用的术语与标记介绍如下：

定义 1. SA, S-port, DA, D-port: 分别表示源地址、源端口、目标地址、目标端口。它们是一个会话的参数。

定义 2. 会话 (Session), 进站会话(Inbound Session), 出站会话(Outbound Session): 会话定义为客户与服务器一个交互过程的所有数据流，其含义约略相当于一个 TCP/UDP 连接或 ICMP 查询。在 ENAT-PT 中，它们被当作一个处理单元来进行地址翻译。TCP/UDP 会话可由参数 (SA, S-port, DA, D-port) 来标识，而 ICMP 查询会话则由 (SA, ICMP query ID, DA) 唯一的标识。进站会话表示从 V4 节点发起的会话，而出站会话表示由 V6 节点发起的会话。会话的方向 (进站或出站) 由发起的节点决定，而非数据包的流动方向。

定义 3. 进站数据包(Inbound packet), 出站数据包(Outbound packet): 进站数据包表示流向发起会话的节点的数据包，而出站数据包表示从发起该会话的节点流出的数据包。例如一个 telnet 会话，出站数据包通常携带终端的键盘输入信息，而进站数据包则携带服务器返回的显示信息。

本发明提出的支持 IPv4 和 IPv6 两类网络互访的协议，可记为 ENAT-PT (Enhanced NAT-PT) 协议。它分为三个部分：

- (1) ENAT: 增强的 NAT 机制，处理进站会话；
- (2) NAPT: 处理出站会话；
- (3) PT: 实现 IPv4 和 Ipv6 两种协议之间的转换。

其中，NAPT 和 PT 有现有的方案，遵循相关标准。ENAT 的基本方法如下：如图 1 所示，设 H1 为 IPv4 主机，地址为 ADDR1 (V4 地址)；H2 为 IPv6 主机，地址为 ADDR2 (V6 地址)。对于进站会话，会话建立前，源节点 H1 发起一个 DNS 请求 (请求获得 H2 的地址) 到 DNS 服务器。ENAT-PT 网关截获 DNS 响应，并从地址池中取得一个未被绑定的临时 IPv4 地址 REG1 (V4 地址) 与返回 H2 的地址 ADDR2 绑定到一起，同时将 REG1 作为 H2 的

地址返回给 H1。V4 主机 H1 以 REG1 作为服务器地址发起会话请求。

对于以上 DNS 解析过程，ENAT 与传统的 NAT（仅指 V4 地址与 V6 地址的翻译）的入站会话的过程完全相同。与传统的 NAT 不同的是，ENAT-PT 网关在会话建立后就释放临时 IPv4 地址，而非在会话结束后才释放临时地址，通过该方法可以实现临时地址的复用。但是采用该方法可能使得一个临时地址对应多个 V6 节点。为了区分到不同 V6 节点的不同会话，ENAT 引入会话参数并维护一个会话表。ENAT-PT 网关截获到某个会话的第一个数据包以后，在会话表中建立起一个新的表项，该表项的形式为 V4 主机地址、V4 主机端口、映射地址、V6 主机地址、V6 主机端口。在本例中，假设 V4 主机获得 H2 的映射地址 (REG1) 以后发起一个到 V6 的会话，源端口为 PORT1，目标端口为 PORT2，则会话表中对应该会话的表项为 (ADDR1, PORT1, REG1, ADDR2, PORT2)。会话建立以后，临时 IPv4 地址 REG1 与 V6 地址 ADDR2 的绑定关系即被释放。对于该会话后续的数据包，ENAT-PT 网关将查询会话表，并根据会话参数查询到 V6 节点的地址，然后对数据包头中的地址进行转换。会话表中的表项在其所对应的会话结束时被删除。

临时 IPv4 地址与 V6 地址的绑定关系在会话建立后立即被释放，并可重新绑定到另一个 V6 地址，因此同一个临时 IPv4 地址可以同时映射到任意多个不同的 V6 地址，从而大大的提高了临时 IPv4 地址的利用率。

图 2 是一个临时 IPv4 地址的状态图。它表明了一个临时 IPv4 地址被复用的详细情况。临时 IPv4 地址起始状态为 free。响应一个 DNS 请求时临时 IPv4 地址被绑定到一个 V6 地址，为 bind 状态。会话建立以后，会话表中记录了会话的相关信息，临时 IPv4 地址被释放，临时 IPv4 地址状态为 using 状态（会话表中至少有一个表项包含了该映射地址），此时该临时 IPv4 地址又可重新绑定到新的 V6 地址。当新的 V4 节点进行域名查询时，该临时 IPv4 地址又被绑定到新的 V6 节点，此时其状态为 bind and using。

根据上述方法，ENAT 的具体步骤如下：

- (1) 4 客户机在需要访问 V6 主机时使用 DNS 查询 V6 的 IP 地址；
- (2) 网关截获 DNS 的响应，从空闲的临时地址池中选择一个 V4 地址 REG1，将 DNS 中 V6 主机的地址 IV6 替换为 REG1，返回给 V4 客户，同时建立地址绑定(IV6, REG1)放入绑定列表；
- (3) 网关收到 V4 的数据报后，根据报文参数检查会话表：
 - (a)如果有该会话的会话项，则进行协议转换操作，将报文转换为 IPv6 格式，将会话项中的 IV6 地址作为 V6 的目标地址；
 - (b)如果没有相关会话项，则根据报文的 IPv4 目的地址查询绑定列表，

①如果没有相关绑定，则转换失败；

②如果有绑定，

(A)如果是 TCP 连接建立报文或 UDP 或 ICMP 报文则根据报文信息和绑定，在会话表中建立会话项（V4 主机地址，V4 主机端口，映射地址，V6 主机地址，V6 主机端口），释放该绑定，并进行协议转换；

(B)否则是错误或超时报文，丢弃；

(c)如果是结束报文则，释放会话项。

(4) 网关收到 V6 的数据报后，根据报文参数检查会话表。如果有会话项则进行协议转换，将报文转换为 IPv4 格式，将会话项中的 REG1 地址作为 V4 的源地址。

系统通过超时机制来回收资源：当绑定超时是，要释放绑定，使得地址可重用。当会话超时时释放会话项。

ENAT 仅适用于入站会话，而普通 NAPT 仅适用于出站会话。ENAT-PT 结合两者的功能，从而可以使用一个很小的地址池同时支持大量两个方向的会话。这可以有两种方法来实现，一种是普通 NAPT 与 ENAT 采用相互独立的临时 IPv4 地址池，分别独立的对入站会话和出站会话进行处理。二是两者使用相同的地址池和相同的会话表。由于采用分离的临时地址池需要更多的地址并且要求区分入站会话和出站会话，引入了新的运算。在 ENAT-PT 中采用第二种方法。在该方法中需要对普通的 NAPT 进行适当的修改。传统的 NAPT 仅使用（源地址、源端口）作为参数进行映射，而 ENAT 需要根据（源地址、源端口、目的地址、目的端口）进行处理。通过扩展 NAPT，使其在进行端口映射时采用(SA, S-port, DA, D-port)四个参数来映射一个数据包，从而统一了 ENAT 和 NAPT 对报文的处理过程。会话表的形式略有改动，需要加上“映射端口”一列。

协议转换 PT 用于实现 IPv4/v6 报文协议的相互转换。该部分遵循相关标准。

显著效果：

ENAT-PT 成功的解决了 IPv4、IPv6 两类网络间的互访，同时仅使用少量的 IPv4 地址就支持大网络的互连。对于 V6 节点访问 V4 网络时，ENAT-PT 模型采用修改过的 NAPT-PT 技术，使得一个临时 IPv4 地址可以支持 63000 个会话访问 IPv4 网络。采用 ENAT 支持 IPv4 节点访问 V6 网络。由于在 ENAT 中一个临时 IPv4 地址在一个 V4 节点到 V6 的会话建立后就释放了，该地址可以用作其它 V4 节点建立到 V6 网络新的会话，从而实现地址复用。从理论上说 ENAT 只使用一个临时 IPv4 地址就可以支持 V4 网络中所有节点访问 V6 网络。由于在支持 V4/V6 网络互访的网络地址转换协议中要求 DNS 记录的生存期为 0，即要求 V4 节点每次在建立与 V6 节点的会话时要进行 DNS 查询。在现有的大量应用中，有

些应用并没有完全按照 DNS 协议的要求进行设计，所以 ENAT 的效果有所退化，但其最终效果仍然比普通的 NAT 强很多。假设有 1 万个 V4 节点的 V4 网络与有 2 万个 V6 节点的 V6 网络互连，采用 100 个临时 IPv4 地址。对于普通的 NAT，只支持 V4 网络中的所有节点同时访问 100 个不同的 IPv6 节点，即 V6 网络资源的可访问率为 $100/20000=0.5\%$ 。但 ENAT 支持 V4 网络中的每一个节点至少可以访问 100 个不同的 IPv6 节点，即使每个 V4 节点访问的 V6 节点不同，依然可以成功访问。在这个网络拓普中，ENAT 理论上可以同时访问 $100*10000=1,000,000$ 个 V6 节点，即可以支持 V4 节点访问所有 V6 节点。由于每个节点在一段时间内访问的节点数目有限，采用 ENAT，使用一个 100 个 V4 临时地址，在绝大部分情况下可以正常支持互访，但采用普通的 NAT 显然是不能完成这个工作的。

在 ENAT-PT 方案中由于引入了传输层的信息，在信息处理量上比普通的 NAT 要大，但由于需要处理的总体信息量不大，并且处理方法规整，通过采用合适的数据结构，对互访的效率产生的影响极小。总之 ENAT-PT 是一个使用少量的 IPv4 地址就支持大 IPv4、IPv6 网络互连的高效方法。

附图说明

图 1 为 ENAT 基本模型图。

图 2 为 ENAT-PT 模型下临时 IPv4 地址的状态转换图。

图 3 为 ENAT-PT 入站会话操作图示。

图中标号：H1 为 IPv4 主机，H2 为 Ipv6 主机，*Free*: 初始状态，*Bind*: 地址被绑定到一个 IPv6 节点上，*Using*: 当绑定的 IPv6 节点建立了会话，*Bind and Using*: 地址被绑定到一个 IPv6 节点上，同时有 IPv6 节点使用该地址建立了会话。

具体实施方式

下面通过实施例进一步说明 ENAT-PT 的操作过程。如图 3 所示，临时 IPv4 地址池中含有两个 V4 地址：202.120.224.1 和 202.120.224.2。临时 IPv4 地址 202.120.224.1 被静态的绑定到 DNS 服务器。DNS 服务器的作用如前所述。ENAT-PT 网关截获所有数据包并作相关的地址转换等处理。以下的例子展示了如何在一个注册 IP 地址 202.120.224.2 上建立多个入站会话。

会话 1 节点 A 发起到节点 B 的会话

在域名解析过程中，DNS 服务器返回节点 B 的地址 (FEDC:BA98::7654:3210)，此地址在网关 G 中被绑定到临时 IPv4 地址 202.120.224.2 (临时 IPv4 地址状态为 bind，见图 2)。网关 G 将临时 IPv4 地址 202.120.224.2 作为节点 B 的地址返回给 A。

(1) 出站数据包 (从 V4 主机流出的数据包)

出站数据包会话参数 (未经 ENAT-PT 转换时) 如下:

SA = 202.120.225.9, S-port = 1024, DA = 202.120.224.2, D-port = 23. (S1)

ENAT-PT 网关截获会话第一个数据包以后, 在会话表中建立如下表项 (表 1), 其中的映射端口对于 ENAT 没有实质意义只是为了统一与 NAT 的操作, 其值与 V6 端口相同。表项建立后释放临时 IPv4 地址 202.120.224.2 与 V6 地址 FEDC:BA98::7654:3210 的绑定关系 (临时 IPv4 地址状态为 using, 见图 2)。

表 1 会话表 (1)

V4 主机地址	V4 端口	映射地址	映射端口	V6 主机地址	V6 端口
202.120.225.9	1024	202.120.224.2	23	FEDC:BA98::7654:3210	23

对于其他的出站数据包 (非第一个数据包), ENAT-PT 网关根据数据包参数 (SA, S-port, DA, D-port) 与会话表中参数 (V4 主机地址, V4 端口, 映射地址, 映射端口 (V6 端口)) 进行匹配, 并据此找到实际目标主机 (V6) 地址 FEDC:BA98::7654:3210。因此, 出站数据包经过 ENAT-PT 网关后将被转换成以下形式

SA = PREFIX: 202.120.225.9, S-port = 1024, DA = FEDC:BA98::7654:3210, D-port = 23. (S2)

PREFIX::/96 是一个规定的 V6 地址前缀, 长度为 96 位。PREFIX 可任意指定, 如 aaaa:bbbb:cccc:dddd:eeee:ffff。在 ENAT-PT 网关所在的 IPv6 域中, 所有包含此前缀的 V6 地址都被路由到 ENAT-PT 网关。

(2) 进站数据包 (从 V6 主机返回的数据包)

ENAT-PT 网关截获的进站数据包参数如下:

SA = FEDC:BA98::7654:3210, S-port = 23, DA = PREFIX:202.120.225.9, D-port = 1024. (S3)

ENAT-PT 网关查询会话表, 方法是对进站数据包的特征参数 (SA, S-port, DA, D-port) 和表项 (V6 主机地址, V6 端口, V4 主机地址, V4 端口) 进行匹配, 以查找 SA (V6 地址) 所映射的临时 IPv4 地址。该临时 IPv4 地址将作为转换后数据包的源地址, 目标地址 DA 则被去掉前缀 PREFIX, 端口号保持不变。进站数据包中的地址信息将被 ENAT-PT 网关转换成以下形式

SA = 202.120.224.2, S-port = 23, DA = 202.120.225.9, D-port = 1024. (S4)

会话 2 节点 A 发起到节点 C 的会话

当一个临时 IPv4 地址被释放以后即可被绑定到另一个 V6 地址。假设节点 A 在发起第一个连接之后又发起另一个到 V6 节点 C (地址 FEDC:BA98::7654:3211) 的连接 (如图 3)。网关返回节点 C 的映射地址 202.120.224.2 给节点 A (临时 IPv4 地址状态为 bind and using, 见图 2), 此会话参数为

SA = 202.120.225.9, S-port = 2002, DA = 202.120.224.2, D-port = 80. (S5)

ENAT-PT 网关在截获此会话第一个数据包以后, 会话表如下。

表 2 会话表 (2)

V4 主机地址	V4 端口	映射地址	映射端口	V6 主机地址	V6 端口
202.120.225.9	1024	202.120.224.2	23	FEDC:BA98::7654:3210	23
202.120.225.9	2002	202.120.224.2	80	FEDC:BA98::7654:3211	80

由于记录了会话的参数, ENAT-PT 网关有足够的信息分辨两个会话的数据包, 并正确地进行地址转换和转发。出站数据包将被转换成

SA = PREFIX:202.120.225.9, S-port = 2002, DA = FEDC:BA98::7654:3211, D-port = 80.(S6)

入站数据包参数为

SA = FEDC:BA98::7654:3211, S-port = 80, DA = PREFIX:202.120.225.9, D-port = 2002 (S7)

它们将被转换为如下形式

SA =202.120.224.2, S-port = 80, DA =202.120.225.9, D-port = 2002.(S8)

NAPT 与 ENAT 的协作

会话 3 节点 B 发起到节点 A 的会话

假设 V6 节点 B 发起一个到 V4 节点 A 的连接, 参数如下:

SA = FEDC:BA98::7654:3210, S-port = 2300, DA = PREFIX:202.120.225.9, D-port =80.(S9)

由于是 V6 到 V4 的会话, 将采用 NAPT 进行处理。网关选择一个可用的临时 IPv4 地址进行映射, 在该例中节点 B 的地址被映射到临时 IPv4 地址 202.120.224.2, 网关将选择一个未用的端口, 例如 1024 作为客户端 (节点 B) 的源端口, 进行会话表, 见表 3。对于出站数据包, 会话参数见 (S9) 式。转换后参数如下

SA=202.120.224.2,S-port=1024,DA=202.120.225.9,D-port=80.(S10)

入站数据包参数为

SA=202.120.225.9,S-port=80,DA=202.120.224.2,D-port=1024.(S11)

转换后参数为

SA=PREFIX:202.120.225.9,S-port=2002,DA=FEDC:BA98::7654:3210,D-port=2300.(S12)

Table 3 会话表 (3)

V4 节点地址	V4 端口	转换地址	映射 端口	V6 节点地址	V6 端口
202.120.225.9	1024	202.120.224.2	23	FEDC:BA98::7654:3210	23
202.120.225.9	2002	202.120.224.2	80	FEDC:BA98::7654:3211	80
202.120.225.9	80	202.120.224.2	1024	FEDC:BA98::7654:3210	2300

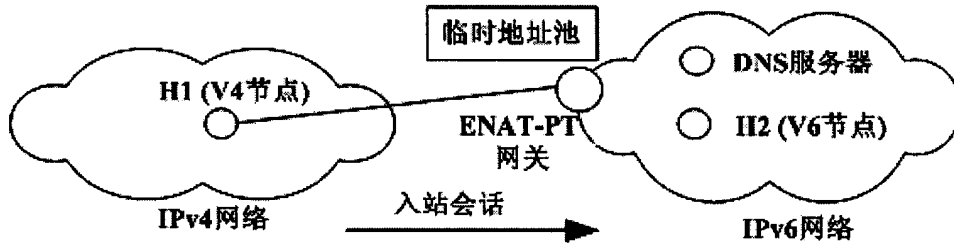


图 1

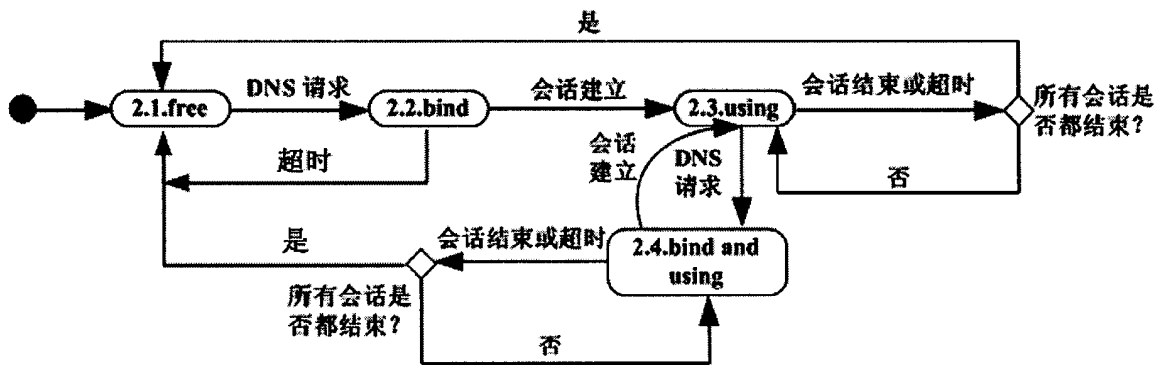


图 2

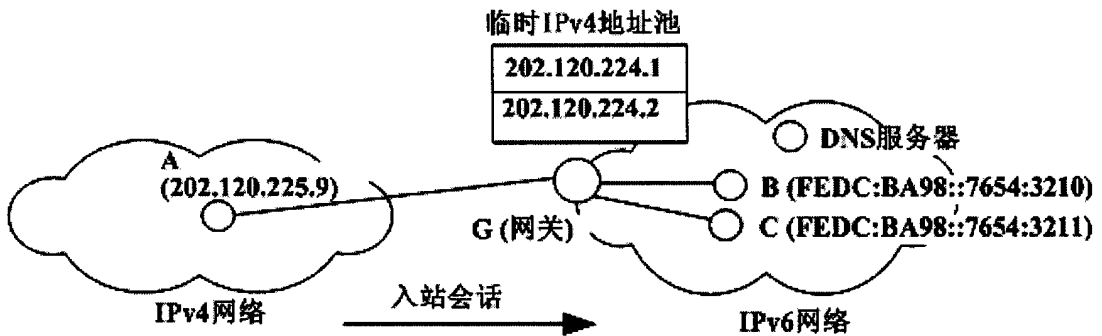


图 3