



# [12] 发明专利说明书

专利号 ZL 200610058578.8

[45] 授权公告日 2009 年 11 月 18 日

[11] 授权公告号 CN 100561976C

[22] 申请日 2006.3.22

[21] 申请号 200610058578.8

[30] 优先权

[32] 2005.3.22 [33] US [31] 11/088,030

[73] 专利权人 罗技欧洲公司

地址 瑞士莫尔日河畔

[72] 发明人 阿龙·斯坦里奇 肯·埃尔贝斯

里米·齐默尔曼 菲利普·德帕兰斯

[56] 参考文献

CN1523848A 2004.8.25

WO2004/064356A2 2004.7.29

WO03/107628A2 2003.12.24

STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Rosenberg et al. Network Working Group, RFC 3489. 2003

审查员 董振兴

[74] 专利代理机构 北京律盟知识产权代理有限公司

代理人 王允方 刘国伟

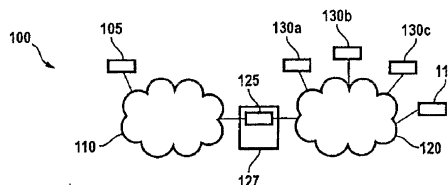
权利要求书 7 页 说明书 16 页 附图 4 页

## [54] 发明名称

用于使数据包穿越网络地址转换装置的方法和装置

## [57] 摘要

一种由一网络地址转换 (NAT) 装置后面的一内部计算机特征化所述 NAT 装置的方法, 其包括创建复数个套接口; 分别将所述复数个套接口绑定到复数个端口; 将用户数据报协议 (UDP) 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器, 其中每个 STUN 请求与所述套接口中的一个相关联; 如果没有从所述 STUN 服务器接收到回应, 那么确定所述 NAT 装置确实支持 UDP 数据包; 且如果从所述 STUN 服务器中的每一个接收到一回应, 那么确定所述 NAT 装置的一组 NAT 特征。



1. 一种由一网络地址转换 NAT 装置后面的一内部计算机特征化所述 NAT 装置的方法，所述方法包含：
  - 创建复数个套接口；
  - 分别将所述复数个套接口绑定到复数个端口；
  - 将用户数据报协议 UDP 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；
  - 如果没有从所述 STUN 服务器接收到回应，那么确定所述 NAT 装置不支持 UDP 数据包；和
  - 如果从所述 STUN 服务器中的每一个接收到一回应，那么确定所述 NAT 装置的一组 NAT 特征；
  - 其中所述 STUN 为 UDP 对 NAT 的简单穿越。
2. 根据权利要求 1 所述的方法，其中所述回应至少包括一第一回应和在所述第一回应后接收到的一第二回应。
3. 根据权利要求 2 所述的方法，其进一步包含：
  - 如果在所述第一回应中接收到的一第一映射端口小于在所述第二回应中接收到的一第二映射端口，且如果所述第二映射端口减去所述第一映射端口小于一选定数目，那么确定所述 NAT 装置的一端口指配行为是递增；且
  - 如果所述第一映射端口大于或等于所述第二映射端口且/或如果所述第一映射端口减去所述第二映射端口大于或等于所述选定数目，那么确定所述 NAT 装置的所述端口指配行为是随机。
4. 根据权利要求 3 所述的方法，其中所述复数个套接口包括至少一第一套接口和一第二套接口，其分别与包括在所述复数个端口中的一第一端口和一第二端口相关联。
5. 根据权利要求 4 所述的方法，其进一步包含：
  - 如果所述 NAT 装置的一端口指配行为是递增，如果所述第一映射端口与所述第一端口相同，且如果所述第二映射端口与所述第二端口相同，那么确定所述 NAT 装置的所述端口指配行为是内外递增；和
  - 如果所述 NAT 装置的一端口指配行为是随机，如果所述第一映射端口与所述第一端口相同，且如果所述第二映射端口与所述第二端口相同，那么确定所述 NAT 装置的所述端口指配行为是内外随机。

6. 根据权利要求 1 所述的方法，其中：

所述复数个 STUN 服务器至少包括第一、第二和第三 STUN 服务器，且传输所述复数个 STUN 请求的所述步骤包括：

将一第一 STUN 请求和一第二 STUN 请求传输到所述第一 STUN 服务器；

将一第三 STUN 请求传输到所述第二 STUN 服务器；和

将一第四 STUN 请求传输到所述第三 STUN 服务器，

其中所述第一 STUN 请求与所述复数个套接口中的一第一套接口相关联，且所述第二、第三和第四 STUN 请求与所述复数个套接口中的一第二套接口相关联。

7. 根据权利要求 6 所述的方法，其进一步包含：如果从所述第一 STUN 服务器接收到至少一个回应且没有从所述第二 STUN 服务器接收到一回应，那么确定所述 NAT 装置的一进入数据包过滤特征为异常。

8. 根据权利要求 6 所述的方法，其进一步包含：

从所述第一 STUN 服务器接收一第一回应，其中所述第一回应包括由所述 NAT 装置映射的且与所述第二套接口相关联的一第一映射端口；

从所述第二 STUN 服务器接收一第二回应，其中所述第二回应包括由所述 NAT 装置映射的且与所述第二套接口相关联的一第二映射端口；

如果所述第一映射端口与所述第二映射端口相同，那么确定所述 NAT 装置的一端口分配行为是锥形；和

如果所述第一映射端口与所述第二映射端口不相同，那么确定所述 NAT 装置的所述端口分配行为是端口敏感对称。

9. 根据权利要求 8 所述的方法，其进一步包含：

从所述第三 STUN 服务器接收一第三回应，其中所述第三回应包括由所述 NAT 装置映射的且与所述第二套接口相关联的一第三映射端口；

如果所述第一映射端口小于所述第二映射端口，

如果所述第二映射端口小于所述第三映射端口，

如果所述第一映射端口与所述第二映射端口之间的差值小于一选定端口增量，且

如果所述第二映射端口与所述第三映射端口之间的差值小于所述选定端口增量，

那么将一单套接口增量设定为所述第二映射端口与所述第三映射端口之间的差值；

其中，所述第二映射端口与所述第三映射端口之间的差值由所述第三映射端口减去所述第二映射端口得到，且所述第一映射端口与所述第二映射端口之间的差值由

所述第二映射端口减去所述第一映射端口得到。

10. 根据权利要求 8 所述的方法，其进一步包含：

从所述第三 STUN 服务器接收一第三回应，其中所述第三回应包括由所述 NAT 装置映射的且与所述第二套接口相关联的一第三映射端口；

如果所述第一映射端口小于所述第二映射端口，

如果所述第二映射端口小于所述第三映射端口，

如果所述第一映射端口与所述第二映射端口之间的差值小于一选定端口增量，且

如果所述第二映射端口与所述第三映射端口之间的差值小于所述选定端口增量，

那么将一单套接口增量设定为所述第二映射端口与所述第三映射端口之间的差值；

否则，

如果所述第二映射端口小于所述第三映射端口，且

如果所述第二映射端口与所述第三映射端口之间的差值小于一选定端口增量，

那么将所述单套接口增量设定为所述第二映射端口与所述第三映射端口之间的差值；

其中，所述第二映射端口与所述第三映射端口之间的差值由所述第三映射端口减去所述第二映射端口得到，且所述第一映射端口与所述第二映射端口之间的差值由所述第二映射端口减去所述第一映射端口得到。

11. 根据权利要求 10 所述的方法，其中所述第一套接口和所述第二套接口分别与包括在所述复数个端口中的一第一端口和一第二端口相关联，且该方法进一步包含：通过一反向通道将一组端口预测信息传输到一外部计算机，其中所述端口预测信息包括所述单套接口增量、所述端口分配行为、所述第一端口、所述第二端口、所述第一映射端口、所述第二映射端口和所述第三映射端口中的一者或多者。

12. 根据权利要求 11 所述的方法，其进一步包含：

所述外部计算机基于包括在所述一组 NAT 特征中的一个或一个以上要素预测所述 NAT 将选择的一组随后端口；和

将一组数据包从所述外部计算机传输到使用所述随后端口的所述 NAT 装置和所述内部计算机。

13. 根据权利要求 11 所述的方法，其进一步包含：

如果所述端口分配行为是锥形，那么经由所述第一映射端口将数据包从所述外部

计算机发送到所述内部计算机。

14. 根据权利要求 11 所述的方法，其进一步包含：如果所述端口分配行为是端口敏感对称，那么经由所述内部计算机的一 IP 地址和复数个预测端口将数据包从所述外部计算机发送到所述内部计算机，其中所述复数个预测端口是由所述 NAT 装置映射的一最后端口与增量的和，所述增量包括所述单套接口增量的数倍。
15. 根据权利要求 14 所述的方法，其中如果所述数据包中的至少一个穿越所述 NAT 装置到达所述内部计算机，那么在所述内部计算机与所述外部计算机之间建立一对等连接。
16. 根据权利要求 1 所述的方法，其进一步包含：通过一反向通道将所述一组 NAT 特征传输到一外部计算机。
17. 根据权利要求 16 所述的方法，其进一步包含：
  - 所述外部计算机基于所述一组 NAT 特征预测所述 NAT 将映射的一组随后端口；
  - 和
  - 经由所述随后端口将一组数据包从所述外部计算机传输到所述 NAT 装置和所述内部计算机。
18. 一种计算机系统，其经配置以特征化一网络地址转换 NAT 装置，以使得所述计算机经由一内部网络而耦合到所述 NAT 装置，且所述计算机在所述 NAT 装置后面，所述计算机系统包含：
  - 一 web 启用装置，其经配置以：
    - 创建复数个套接口；
    - 分别将所述复数个套接口绑定到复数个端口；
    - 将用户数据报协议 UDP 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；
    - 如果没有从所述 STUN 服务器接收到回应，那么确定所述 NAT 装置不支持 UDP 数据包；和
    - 如果从所述 STUN 服务器接中的每一个收到一回应，那么确定所述 NAT 装置的一组 NAT 特征；
    - 其中所述 STUN 为 UDP 对 NAT 的简单穿越。
19. 一种计算机系统，其包含：
  - 一第一网络；
  - 所述第一网络上的一第一网络地址转换 NAT 装置；

所述第一网络上的至少一第一 web 启用装置，其中

所述第一 web 启用装置操作地耦合到所述第一 NAT 装置且操作地在所述第一 NAT 装置后面，且

所述第一 web 启用装置经配置以：

创建复数个套接口；

分别将所述复数个套接口绑定到复数个端口；

将用户数据报协议 UDP 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；且

如果从所述 STUN 服务器中的每一个接收到一回应，那么确定所述第一 NAT 装置的一组 NAT 特征；

其中所述 STUN 为 UDP 对 NAT 的简单穿越。

20. 根据权利要求 19 所述的计算机系统，其进一步包含：

一第二网络，其操作地耦合到所述 NAT 装置；和

至少一第二 web 启用装置，其耦合到所述第二网络并经配置以从所述第一 web 启用装置接收所述一组 NAT 特征，其中

基于所述 NAT 特征，所述第二 web 启用装置经配置以预测由所述第一 NAT 装置映射的一组随后映射端口，并在所述一组随后映射端口上将一组数据包发送到所述第一 NAT 装置，

如果所述数据包中的一个被发送到由所述 NAT 装置映射的一随后映射端口，那么此数据包经配置以穿越所述 NAT 装置。

21. 根据权利要求 20 所述的计算机系统，其进一步包含：

所述第二网络上的一第二 NAT 装置，其中

所述第二 web 启用装置在所述第二 NAT 装置后面，且

所述第二 web 启用装置经配置以：

创建另外复数个套接口；

分别将所述另外复数个套接口绑定到另外复数个端口；

将用户数据报协议 UDP 数据包中的另外复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述另外复数个套接口中的一个相关联；且

如果从所述 STUN 服务器中的每一个接收到一回应，那么确定所述第二 NAT 装置的一组 NAT 特征。

22. 根据权利要求 21 所述的计算机系统，其进一步包含：

一第三网络，其安置在所述第一 NAT 装置与所述第二 NAT 装置之间。

23. 根据权利要求 22 所述的计算机系统，其中所述第三网络是因特网。

24. 根据权利要求 23 所述的计算机系统，其进一步包含操作地耦合到所述第二网络并经配置以接收所述 STUN 请求的复数个 STUN 服务器。

25. 一种由一防火墙装置后面的一内部计算机特征化所述防火墙装置的方法，所述方法包含：

创建复数个套接口；

分别将所述复数个套接口绑定到复数个端口；

将用户数据报协议 UDP 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；

如果没有从所述 STUN 服务器接收到回应，那么确定所述防火墙装置不支持 UDP 数据包；和

如果从所述 STUN 服务器中的每一个接收到一回应，那么确定所述防火墙装置的一组防火墙特征；

其中所述 STUN 为 UDP 对 NAT 的简单穿越。

26. 根据权利要求 25 所述的方法，其中所述回应包括至少一第一回应和在所述第一回应后接收到的一第二回应。

27. 一种计算机系统，其包含：

一第一网络；

所述第一网络上的一防火墙装置；

所述第一网络上的至少一第一 web 启用装置，其中

所述第一 web 启用装置操作地耦合到所述防火墙装置且操作地在所述防火墙装置后面，且

所述第一 web 启用装置经配置以：

创建复数个套接口；

分别将所述复数个套接口绑定到复数个端口；

将用户数据报协议 UDP 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；且

如果从所述 STUN 服务器中的每一个接收到一回应，那么确定所述防火墙装置的一组防火墙特征；

其中所述 STUN 为 UDP 对 NAT 的简单穿越。

28. 根据权利要求 27 所述的计算机系统，其进一步包含：

一第二网络，其操作地耦合到所述防火墙装置；和

至少一第二 web 启用装置，其耦合到所述第二网络并经配置以从所述第一 web 启用装置接收所述一组防火墙特征，其中

基于所述防火墙特征，所述第二 web 启用装置经配置以预测由所述防火墙装置映射的一组随后映射端口，并在所述一组随后映射端口上将一组数据包发送到所述防火墙装置，

如果所述数据包中的一个被发送到由所述防火墙装置映射的一随后映射端口，那么此数据包经配置以穿越所述防火墙装置。



## 用于使数据包穿越网络地址转换装置的方法和装置

### 技术领域

本发明涉及计算机网络中的通信，且更明确地说，本发明涉及一种使数据包穿越网络地址转换装置的系统和方法。

### 背景技术

由于近年来因特网的使用已在增长，所以新指配的可用因特网协议（IP）地址迅速下降。更具体地说，当前由 IP 第 4 版（IPv4）指定的指配给新的因特网用户的因特网协议（IP）地址的数目迅速下降。IPv4 指定每个 IP 地址使用 4 个字节。指定 16 字节 IP 定址的较新的 IP 第 6 版（IPv6）已将实施用于因特网用途，但不期望在接下来的几年中实施。

由于 IPv6 不计划用于接下来的几年内，且由于可用 IP 地址在下降，所以已经研究出临时解决办法通过使用已开发出的有限数目的当前可用 IP 地址来增加可连接到因特网的计算机的数目。提供到因特网的计算机连接的一个临时解决办法包括将 IP 地址暂时指配到连接计算机。此解决办法包括在因特网连接期间将一 IP 地址指配到一计算机且在因特网连接已结束后取消指配所述 IP 地址。

提供到因特网的计算机连接的其它临时解决办法包括使用网络地址转换（NAT）技术。NAT 技术包括将用于一个网络内的 IP 地址转换为另一网络内使用的不同 IP 地址。一个网络通常是指内部网络且通常包括局域网（LAN）、广域网（WAN）或可由公司、教育机构、政府机关或类似组织使用的类似网络。其它网络通常是指外部网络且可为 LAN、WAN、因特网或其它网络类型。当前 NAT 技术使用三组内部 IP 地址，其可保留用于内部网络且不用于外部网络上。通常，NAT 装置将外发数据包中的内部 IP 地址映射到一个或一个以上映射 IP 地址且不将引入数据包中的映射 IP 地址映射回内部 IP 地址中。举例来说，随着数据包离开内部网络（例如，公司 LAN），数据包通过 NAT 装置，其将内部 IP 地址（例如，10.0.0.1）映射到公司的映射 IP 地址（例如，198.60.42.12）。

NAT 装置通常还将由部网络上的内部计算机使用的内部端口映射到外部网络上使用的外部端口（有时称作映射的）。端口转换通常被称作网络端口转换（NPT）。为方便起见，本文所使用的术语 NAT 包括 NPT。

虽然 NAT 经配置以允许若干内部计算机经由单映射 IP 地址而连接外部网络，但这

些内部计算机中的一个或一个以上可能不知道其在一 NAT 装置“后面”（即，NAT 装置通信地耦合在内部计算机与外部计算机之间）或可能不知道内部计算机前面的 NAT 装置的特征。如果内部计算机不知道其是否在一 NAT 装置后面或不知道所述内部计算机前面的 NAT 装置的特征，那么可能妨碍内部计算机从外部计算机接收通信（例如，数据包）。举例来说，从外部计算机发送到内部计算机的数据包可能丢弃，因为内部计算机可能不能够通知外部计算机 NAT 装置的特征。更具体地说，如果外部计算机使用 NAT 装置不接受的端口，那么外部计算机发送的数据包可能被 NAT 装置丢弃。即，数据包将不穿越 NAT 装置。如果，或者，内部计算机可将内部计算机前面的 NAT 装置的特征传送到外部计算机，那么外部计算机可使用所述信息来发送数据包，所述数据包具有将允许数据包由 NAT 装置传递到内部计算机的适当选定的 IP 地址和端口号。

因此，需要一种用于特征化 NAT 装置以使改进的数据包穿越 NAT 装置的系统和方法。

## **发明内容**

本发明提供用于网络通信的计算机网络，且更明确地说，提供由网络地址转换（NAT）装置后面的内部计算机特征化所述 NAT 装置的系统和方法。

根据一个实施例，操作所述内部计算机的方法包括创建复数个套接口，和分别将所述复数个套接口绑定到复数个端口。复数个 STUN（UDP 对 NAT 的简单穿越）请求以 UDP（用户数据报协议）数据包的形式被传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联。如果没有从 STUN 服务器接收到回应，那么内部计算机断定 NAT 装置确实支持 UDP 数据包，且如果从所述 STUN 服务器中的每一个接收到一回应，那么内部计算机断定所述 NAT 装置的一组 NAT 特征。

根据一特定实施例，复数个 STUN 服务器至少包括第一、第二和第三 STUN 服务器。传输所述复数个 STUN 请求的步骤包括：i) 将第一 STUN 请求和第二 STUN 请求传输到第一 STUN 服务器；ii) 将第三 STUN 请求传输到第二 STUN 服务器；和 iii) 将第四 STUN 请求传输到第三 STUN 服务器。第一 STUN 请求与所述复数个套接口中的第一套接口相关联，且第二、第三和第四 STUN 请求与所述复数个套接口中的第二套接口相关联。

根据另一实施例，所述方法进一步包括：如果从第一 STUN 服务器接收到至少一个回应，且没有从第二 STUN 服务器接收到一回应，那么确定 NAT 装置的进入数据包过滤特征为异常。根据另一实施例，所述方法进一步包括：i) 从第一 STUN 服务器接收第

一回应，其中所述第一回应包括由 NAT 装置映射的且与第二套接口相关联的第一映射端口；ii) 从第二 STUN 服务器接收第二回应，其中所述第二回应包括由 NAT 装置映射的且与第二套接口相关联的第二映射端口；iii) 如果第一映射端口与第二映射端口相同，那么确定 NAT 装置的端口分配行为是锥形；和 iv) 如果第一映射端口与第二映射端口相同，那么确定 NAT 装置的端口分配行为是端口敏感对称。

根据一个实施例，提供一计算机系统，其经配置以特征化计算机前面的网络地址转换 (NAT)。计算机系统包括一 web 启用装置，其经配置以：i) 创建复数个套接口；ii) 分别将所述复数个套接口绑定到复数个端口；iii) 将用户数据报协议 (UDP) 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；iv) 如果没有从 STUN 服务器接收到回应，那么确定 NAT 装置确实支持 UDP 数据包；和 v) 如果从 STUN 服务器中的每一个接收到一回应，那么确定 NAT 装置中的一组 NAT 特征。

根据另一实施例，提供一计算机系统，其包括第一网络；所述第一网络上的第一网络地址转换 (NAT) 装置；第一网络上的至少一第一 web 启用装置，其中第一 web 启用装置操作地耦合到第一 NAT 装置且操作地在第一 NAT 装置后面，且第一 web 启用装置经配置以：i) 创建复数个套接口；ii) 分别将所述复数个套接口绑定到复数个套接口；iii) 将用户数据报协议 (UDP) 数据包中的复数个 STUN 请求传输到复数个 STUN 服务器，其中每个 STUN 请求与所述套接口中的一个相关联；且 iv) 如果从 STUN 服务器中的每一个接收到一回应，那么确定第一 NAT 装置的一组 NAT 特征。

对此发明内容和以下具体实施方式中所描述的特点和优势的进一步理解并非无所不包的，且明确地说，根据说明书、附图和权利要求书，所属领域的一般技术人员将明了很多附加特点和优势。

## **附图说明**

图 1 是根据本发明的一个实施例的网络系统的简图；

图 2 是根据本发明的另一实施例的网络系统的简图；

图 3 是高阶层流程图，其具有用于使内部计算机确定其是否在 NAT 装置后面的步骤；

图 4 是高阶层流程图，其具有提供对确定由 NAT 装置指配的映射端口是递增还是随机的概观的步骤；

图 5 是高阶层流程图，其具有提供对确定 NAT 装置将端口指配为内外递增还是内

外随机的概观的步骤；

图 6 是高阶层流程图，其具有用于由内部计算机进一步特征化 NAT 装置的步骤；  
和

图 7 是高阶层流程图，其具有用于使内部计算机确定连续套接口之间的单套接口增量的步骤。

## **具体实施方式**

### 介绍和概观

本文中出于容易理解的目的而使用标题，且不应理解成限制本发明的所述实施例。另外，所附图式仅为说明的目的而描绘本发明的选定实施例。从以下讨论、权利要求书和所附图式中，所属领域的技术人员将易于认识到，在不脱离本发明的范畴和界限的前提下，可利用本文所揭示的结构和方法的替代实施例。

图 1 是根据本发明的一个实施例的网络系统 100 的简图。网络系统 100 包括：耦合到内部网络 110 的至少一个内部计算机 105；耦合到外部网络 120 的至少一个外部计算机 115；和将所述内部网络耦合到所述外部网络的网络地址转换（NAT）装置 125。所述内部计算机可包括个人计算机、服务器、主机或经配置以耦合到所述内部网络的任何 Web 启用装置。所述内部网络可包括局域网（LAN）、广域网（WAN）、虚拟 LAN 或类似网络。所述外部计算机可包括个人计算机、服务器、主机或经配置以耦合到所述外部网络的任何 Web 启用装置。所述外部网络可包括 LAN、WAN、虚拟 LAN、因特网或类似网络。

根据一个实施例，内部计算机 105 经配置以检测并特征化 NAT 装置 125。对 NAT 装置的特征的确定允许内部计算机和外部计算机建立对等通信链路以用于交换 UDP 数据包。内部计算机和外部计算机可交换 UDP 数据包以用于对等文件传送。对等通常涉及在不使用数据包上载并接着传送到的中央服务器的前提下传送文件。

文件传送可包括传送多种文件类型，例如媒体文件（音频、视频、音频/视觉）、文本消息、语音消息（例如，用于 Web 电话）和类似物。

根据一个实施例，外部网络包括一组 STUN（UDP 到 NAT 的简单横跨）服务器 130。根据 STUN 协议操作的 STUN 服务器通常安置在 Web（例如，万维网）中以发现并特征化装置，例如 NAT 装置。虽然图 1 中所示的所述组的 STUN 服务器包括三个 STUN 服务器 130a、130b 和 130c（如本文所指），但一组可包括一个或一个以上部件。下文进一步详细描述 STUN 服务器。根据一些实施例，NAT 装置可形成另一电子系统 127（例如

防火墙装置、路由器或类似物)的一部分,或 NAT 装置可为独立装置,其可耦合到防火墙装置、路由器或类似物。根据一替代实施例,装置 125 可为防火墙装置且经配置以执行本文所述的方法。根据所述实施例,装置 127 可为防火墙的外壳或可为防火墙经配置以与其一起操作的路由器。

图 2 是根据本发明的另一实施例的网络系统 200 的简图。类似编号方案用于识别与图 1 中所示的那些元件相同或类似的元件。网络系统 200 与网络系统 100 不同之处在于外部计算机 125,类似于内部计算机 105,可能在 NAT 装置 205 之后。内部网络和外部网络可经由网络 210(例如另一 LAN、另一 WAN、因特网或类似物)而耦合。为说明性目的而描述前文所述的网络系统。所属领域的技术人员将知道经配置以如下文所述进行操作的很多网络系统,且这些其它网络系统均被认为在目前所述的本发明的范畴和界限内。根据一个实施例,外部网络 120 和网络 210 中的一者或两者可包括一组 STUN 服务器。根据一些实施例,NAT 装置 205 可形成另一电子系统 207(例如防火墙装置、路由器或类似物)的一部分,或 NAT 装置可为独立装置,其可耦合到防火墙装置、路由器或类似物。根据一替代实施例,装置 205 可为防火墙装置并经配置以执行本文所述的方法。根据所述实施例,装置 207 可为防火墙的外壳或可为防火墙经配置以与其一起操作的路由器。

根据一个实施例,内部计算机和/或外部计算机可不知道它们是否位于 NAT 装置后面且/或可不知道它们前面的 NAT 装置的特征。举例来说,内部计算机 105 可不知道 i) NAT 装置 125 的因特网协议(IP)地址分配行为;ii) NAT 装置的端口分配行为;iii) NAT 装置的端口指配行为;和/或 iv) NAT 装置的引入数据包过滤。如果内部计算机不知道其是否位于 NAT 装置后面或不知道所述内部计算机前面的所述 NAT 装置的特征,那么可能妨碍内部计算机接收从外部计算机发送的数据包。举例来说,如果内部计算机和外部计算机试图建立对等通信,那么如果这些计算机不知道 NAT 装置的前文所述的特征的话,从外部计算机发送到内部计算机的数据包可能被 NAT 装置 125 丢弃。本发明的实施例是针对这些问题和其它问题。

#### NAT 装置特征的描述

如上文简要描述,NAT 装置具有多种特征 i) 端口分配行为;ii) 端口指配行为;和 iii) 引入数据包过滤。下文详细描述这些特征。应了解,出于示范性目的而描述所述特征,且 NAT 装置可具有其它特征,计算机可经配置以根据本文所述的方法确定所述其它特征。

根据本发明的一个实施例,内部计算机和/或外部计算机经配置以确定它们关联 NAT

装置的特征并将所述特征的信息传输给其它计算机，以使得从一个计算机发送到另一计算机的数据包可穿越另一计算机的 NAT 装置而不被丢弃。下文详细描述由内部计算机和/或外部计算机执行的用来确定这些特征的方法。

现在进一步详细描述端口分配行为。端口分配行为包括由 NAT 装置使用的一组规则，其用于当来自内部网络的数据包被发送到外部网络时映射端口。三个主要端口分配行经描述并包括：i) 锥形；ii) 地址敏感对称；和 iii) 端口敏感对称。

锥形：由计算机（例如，内部计算机）从相同内部 IP 地址和端口（即，ip:端口）发送的数据包被 NAT 装置映射到相同外部 ip:端口。映射通常指 NAT 装置将内部网络上的由内部计算机使用的 IP 地址和/或端口转换为外部网络上使用的 IP 地址和/或端口。映射通常还指 NAT 装置将从外部网络接收的 IP 地址和端口转换为内部网络上的由内部计算机使用的 IP 地址和端口。根据锥形特征，映射从内部 ip:端口（假定 A）发送到目标计算机 ip:端口（假定 D）的数据包，以使得 A 被映射到 X，其中 X 是 NAT 装置的 ip:端口。如果内部计算机使用 ip:端口 A 来将数据包发送到不同目标 ip:端口（假定 E），那么 NAT 装置维持相同的 A 到 X 映射。即，NAT 装置使用相同 IP 地址和端口来将数据包发送到 ip:端口 D 和 ip:端口 E。因此如果数据包由 ip:端口 D 和 ip:端口 E 发送到 ip:端口 X，那么从 ip:端口 D 和 ip:端口 E 返回的数据包将穿越 NAT 装置（即，由 NAT 装置导向 ip:端口 A 处的内部计算机）。如果使用除了 ip:端口 D 和 ip:端口 E 之外的 ip:端口的外部计算机试图将数据包发送到 ip:端口 A 上的内部计算机，那么 NAT 装置将丢弃这些数据包。IP 地址和端口通常称为套接口。更具体地说，套接口是 IP 地址和端口的描述符。如所属领域中所广泛了解，每个端口与用于标识所述端口的端口号相关联，且端口有时由它们的相关端口号来称谓。

地址敏感对称：由计算机（例如，内部计算机）从相同内部 IP 地址和端口发送到相同目标 IP 地址的数据包被 NAT 装置映射到相同映射 IP 地址和端口。即如果目标 IP 地址保持相同，但是目标端口改变，那么 NAT 装置使用相同映射。如果目标 IP 地址改变，那么 NAT 装置产生新的端口映射。举例来说，从使用 ip:端口（假定 A）的内部计算机发送到外部 ip:端口（假定 D:M）的数据包被 NAT 装置映射，以使得 A 被映射到 X，且 X 映射到 D，其中 X 是 NAT 装置的 ip:端口。地址敏感对称 NAT 装置在映射中包括目标 IP 地址但不包括目标端口。如果内部计算机使用 ip:端口 A 来将数据包发送到不同目标 ip:端口（假定 D:N），那么 NAT 装置维持 A 映射到 X 且 X 映射到 D 的相同映射。如果内部计算机使用 ip:端口 A 来将数据包发送到不同目标 ip:端口（假定 J:K），那么 NAT 装置创建新的映射，以使得 A 映射到 ip:端口（假定 Y），且 Y 映射到 J。

端口敏感对称：由计算机（例如，内部计算机）从相同内部 IP 地址和端口发送到相同目标 IP 地址和端口的数据包被映射到相同映射 IP 地址和端口。即，如果目标 IP 地址或目标端口改变，那么 NAT 装置创建新的端口映射。举例来说，从使用 ip:端口 A 的内部计算机发送到使用 ip:端口 D:M 的外部计算机的数据包的套接口被 NAT 装置映射，以使得 A 映射到 X，且 X 映射到 D:M，其中 X 是 NAT 装置的 ip:端口。端口敏感对称 NAT 装置在映射中包括目标 IP 地址和端口。如果内部计算机使用 ip:端口 A 来将数据包发送到不同目标 ip:端口 D:N，那么创建新的映射，其中 A 映射到 Y，且 Y 映射到 D:N。

端口指配行为包括由 NAT 装置使用的一组规则，其用于指配外部端口映射。四个主要端口指配行为经描述并包括：i) 递增；ii) 随机；iii) 内外递增和 iv) 内外随机。

递增：如果产生内部 ip:端口到外部 ip:端口的新的映射，那么 NAT 装置递增地选择下一可用外部端口。举例来说，NAT 装置可将外部端口递增 1、2、5 或类似数目以用于新的映射。递增外部端口的 NAT 装置通常经配置以存储一表，其由 NAT 装置维持以存储并追踪外部端口的状态。

随机：如果 NAT 装置创建内部 ip:端口到外部 ip:端口的新的映射，那么 NAT 装置从一队列中选择下一可用外部端口。所述队列包括可指配的端口号。重新指配的端口号返回到所述队列。由于端口号并非以固定次序重新指配，所以这些端口号并非以固定次序进入所述队列。因此，在指配若干个端口号后，随后的端口号的指配实质上是随机的。

内外递增：内部计算机使用的内部端口与 NAT 装置映射的外部端口相同。举例来说，内部地址和端口可为 192.168.1.1:5000 且由 NAT 装置映射的外部地址和端口可为 64.3.3.3:5000。如果 NAT 装置为相同的内部端口产生新的映射，那么 NAT 装置会使端口号递增一固定增量，例如 1、2、3 等等。即，如果 NAT 装置为相同内部端口产生不同的外部端口，那么 NAT 装置应用上文所述的递增规则以产生外部端口。举例来说，初始内部地址和端口可为 192.168.1.1:7000，且 NAT 装置映射的外部地址和端口可为 64.3.3.3:7000，且初始内部地址和端口 192.168.1.1:7000 的随后映射可为外部地址和端口 64.3.3.3:7001，其中端口 7000 递增 1 到 7001。

内外随机：内部端口与外部端口相同。想到外部端口为由 NAT 装置映射以用于外部网络上的端口。如果 NAT 装置为相同内部端口产生新的外部端口映射，那么 NAT 装置应用上文所述的随机规则以产生新的外部端口映射。

引入数据包过滤通常指由 NAT 装置使用的一组规则，其用于允许数据包从外部计算机通过 NAT 装置穿越到内部计算机或阻挡数据包从外部计算机通过 NAT 装置穿越到内部计算机。三个主要引入数据包过滤行为包括：i) 无引入数据包过滤；ii) 地址敏感

数据包过滤；和 iii) 端口敏感数据包过滤。

无引入数据包过滤：经配置以不过滤引入数据包的 NAT 装置通常不会使引入数据包起源于其的计算机生效。即，使用 ip:端口（假定 D）的任何外部计算机可通过将数据包发送到由 NAT 装置分配的映射的 ip:端口 X 来将数据包发送到使用 ip:端口（假定 A）的内部计算机。

地址敏感数据包过滤：NAT 装置的数据包过滤，其经配置以检验包括于引入数据包中的 IP 地址来确定数据包是否应被允许穿越 NAT 装置而进入内部网络。使用 ip:端口（假定 D:M）的任何外部计算机可通过将引入数据包发送到由 NAT 装置分配的映射 ip:端口（假定 X）来将所述数据包发送到使用 ip:端口（假定 A）的内部计算机，但仅在使用 ip:端口 A 的内部计算机先前已将一数据包发送到使用 IP 地址 D 的外部计算机时。

端口敏感数据包过滤：NAT 装置的数据包过滤，其经配置以检验包括于引入数据包中的 IP 地址和端口来确定数据包是否应被允许穿越 NAT 装置而进入内部网络。使用 ip:端口（假定 D:M）的任何外部计算机可通过将引入数据包发送到由 NAT 装置分配的映射 ip:端口（假定 X）来将所述数据包发送到使用 ip:端口（假定 A）的内部计算机，但仅在使用 ip:端口 A 的内部计算机先前已将一数据包发送到 ip:端口 D:M 上的外部计算机时。

除前文所述的主要引入数据包过滤规则之外，NAT 装置可经配置以使用被称作异常数据包过滤的第二数据包过滤规则。所述异常数据包过滤可启用或禁用，且可应用到地址敏感数据包过滤和/或端口敏感数据包过滤中。

异常数据包过滤：NAT 装置的数据包过滤，其经配置以在第一数据包从 ip:端口（假定 D:M）上的目标计算机到达后修改引入数据包过滤，以使得仅允许来自 D:M 的数据包被允许穿越 NAT 装置而进入内部网络。

### NAT 装置分类

如上文简要描述，内部计算机 105 和外部计算机 115 中的一者或两者可经配置以确定这些计算机前面的个别 NAT 装置的前文所述的特征。内部计算机和外部计算机中的一者或两者可进一步经配置以确定它们是否位于 NAT 装置后面。举例来说，内部计算机和外部计算机可经配置以确定它们是否位于相同网络上的相同 NAT 装置后面。内部计算机和外部计算机前面的 NAT 装置的经确定的特征的信息（或关于缺少 NAT 装置的信息）经彼此发送，以使得数据包可由这些计算机进行交换而所述数据包不被 NAT 装置丢弃。由于内部计算机和/或外部计算机经配置以使用经传送的信息来预测可由 NAT 装置映射的下一端口，所以所述信息在本文被称作端口预测信息。如果正确预测下一映



射端口，那么计算机可将数据包发送到所述由 NAT 装置使用的下一映射端口，且所发送的数据包将穿越 NAT 装置并到达所希望的计算机接收端。

图 3 是高阶层流程图，其具有让内部计算机确定其是否在 NAT 装置后面的步骤。虽然以下描述讨论由内部计算机执行的流程图步骤，但外部计算机也可经配置以执行所述流程图的步骤来确定其是否在 NAT 装置后面。

根据一个实施例，内部计算机经配置以产生一套接口（假定 L0），并将所述套接口绑定到一端口。L0 的内部 IP 地址和绑定到 L0 的本地端口由内部计算机存储。为方便起见，绑定到 L0 的本地端口被称作 L0 端口号。所述端口可由内部计算机随机选择。举例来说，内部计算机可选择 0 与 65535 之间的端口。根据一个实施例，内部计算机经配置以选择从 5000 到 65535（包括 5000 和 65535）的端口。如果内部计算机运行 Microsoft™ Windows™ 操作系统，那么通过选择 5000 或 5000 以上的一端口，Windows™ 操作系统将类似地选择 5000 或 5000 以上的端口。在产生套接口 L0 并选择端口后，内部计算机经配置以将 STUN 请求发送到 STUN 服务器 130a（步骤 300）。可根据用户数据报协议（UDP）或所属领域的技术人员将易于知道的其它协议来发送所述 STUN 请求。

通常，STUN 服务器经配置以将回应发送回将 stun 请求发送到所述 STUN 服务器的内部计算机（步骤 305）。所述回应包括从其发送 STUN 请求的映射 IP 地址和映射端口。因此，回应包括由 NAT 装置从发送 STUN 请求的计算机所使用的内部 IP 地址和端口映射的映射 IP 地址和映射端口。

在 STUN 请求从内部计算机发送到 STUN 服务器后，内部计算机经配置以等待 STUN 服务器的回应。如果从 STUN 服务器接收到回应，那么由内部计算机存储映射 IP 地址和映射端口（步骤 310）。为方便起见，L0 套接口的映射端口在本文被称作 E0 端口号。进一步回应接收到来自 STUN 服务器的回应，内部计算机经配置以设定内部旗标，其指示 NAT 装置支持 UDP 数据包或用于特征化的其它数据包类型。

内部计算机经配置以比较内部 IP 地址与映射 IP 地址（步骤 320）。如果内部 IP 地址与映射 IP 地址相同，那么内部计算机经配置以断定其不在 NAT 装置后面。否则，如果内部 IP 地址与映射 IP 地址不同，那么内部计算机经配置以断定其在 NAT 装置后面。具体地说，如果这些 IP 地址不同，那么内部计算机可断定 NAT 装置已经将内部计算机使用的内部 IP 地址映射到外部网络上的 NAT 装置使用的映射 IP 地址（有时称作外部 IP 地址）

或者，如果内部计算机在预定时间间隔中（例如，在约 250 毫秒内或几乎 250 毫秒时）不从 STUN 服务器接收一回应，那么内部计算机经配置以重新发送 STUN 请求（步

骤 300)。STUN 请求可在预定时间周期内(例如 3 秒)以预定时间间隔重复发送到 STUN 服务器。如果在所述预定时间周期后,没有从 STUN 服务器接收到回应,那么本地计算机经配置以断定 NAT 装置不具有 UDP 网络能力(步骤 325)。即,UDP 数据包被 NAT 装置阻挡。如果内部计算机断定 NAT 装置不支持 UDP 数据包,那么 NAT 装置的特征化被中断。内部计算机可经配置以设定一内部旗标以指示 NAT 装置不支持 UDP 数据包(例如,UPD 支持=假)或用于特征化过程的其它数据包类型。如果在预定时间周期内从 STUN 服务器接收到回应,那么内部计算机执行上文的存储步骤 310 和比较步骤 315。

根据一个实施例,使用由内部计算机产生的另一套接口(假定 L1)的内部计算机可重复流程图的步骤。内部计算机可经配置以将新的端口(假定 L1 端口号)绑定到 L1 套接口。所述 L1 端口号可由内部计算机随机产生。可由内部计算机存储套接口 L1 的内部 IP 地址和 L1 端口号。如果内部计算机不接收对在预定时间周期内发送到 STUN 服务器 130a 的 STUN 请求的回应,那么设定内部旗标以指示 NAT 装置不支持 UDP 数据包(例如,UPD 支持=假)或由内部计算机用于特征化 NAT 装置的接着由内部计算机使用的其它数据包类型。如果内部计算机从 STUN 服务器接收到回应,那么由内部计算机设定内部旗标以指示 NAT 装置支持 UDP 数据包(例如,UPD 支持=真)或由内部计算机使用的其它数据包类型。同样,由内部计算机存储通过 STUN 服务器的回应而返回到内部计算机的映射 IP 地址和映射端口。为方便起见,L0 套接口的映射端口被称作 E1 端口号。

根据一个实施例,内部计算机经配置以比较 E0 端口号与 E1 端口号来确定由 NAT 装置指配的映射端口是递增的还是随机的。上文详细描述了递增和随机的端口指配。

图 4 是高阶层流程图,其具有提供前文所述的比较的概观的步骤。在 400 处,内部计算机确定 E0 端口号是否小于 E1 端口号,并计算 E1 端口号与 E0 端口号之间的差值。如果 E0 端口号小于 E1 端口号,且 E1 端口号与 E0 端口号之间的差值小于选定端口增量(例如,20、10、5 或类似数目),那么内部计算机经配置以确定 NAT 装置以递增的方式指配端口(上文详细描述),否则确定 NAT 装置随机地指配端口。内部计算机经配置以设定旗标(例如,套接口间端口指配行为)以依据前文所述的比较结果(例如,套接口间端口指配行为=递增或随机)来指示 NAT 装置经配置而以递增方式或随机方式指配端口。

在确定 NAT 装置是以随机方式还是以递增方式指配端口后,内部计算机经配置以确定 NAT 装置是将端口指配为内外递增还是内外随机(上文详细描述 NAT 装置的内外特征)。

图 5 是高阶层流程图,其具有提供前文所述的对 NAT 装置特征的确定的概观的步

骤。在 500 处，内部计算机经配置以确定 E0 端口号是否与 L0 端口号相同，且 E1 端口号是否与 L1 端口号相同。如果这些端口相同，那么在 505 处，内部计算机检查按序指配的套接口的端口指配行为是否为递增的方式。如果这些端口相同，且端口指配行为是递增的方式，那么内部计算机（步骤 510）经配置以断定 NAT 装置的端口指配行为是内外递增（上文详细描述）。或者，如果这些端口相同，但端口指配行为是随机的，那么内部计算机（步骤 515）经配置以断定端口指配行为是内外随机的（上文详细描述）。如果 E0 端口号与 L0 端口号，和/或 E0 端口号与 E1 端口号不相同，那么内部计算机（步骤 520）经配置以断定端口指派行为是随机的且不是内外递增（步骤 525），或递增的且不是内外随机的（步骤 530）。套接口间端口指配行为可由内部计算机修改以反映前文所述的比较结果。举例来说，套接口间端口指配行为可依据比较结果而被设定为内外随机或内外递增。

根据一个实施例，在针对 L0 和 L1 套接口的 STUN 请求发送到 STUN 服务器 130b 后，内部计算机经配置以根据图 3 的流程图的步骤通过使用（例如）套接口 L1 将 STUN 请求发送到 STUN 服务器 130b。如果内部计算机在预定时间周期内不从 STUN 服务器 130b 接收回应，那么内部计算机经配置以断定 NAT 为异常 NAT 装置（上文详细描述）。由内部计算机存储 NAT 装置的此特征的信息（例如，异常=真）。如果从 STUN 服务器接收到回应，那么内部计算机经配置以存储根据回应而返回的映射端口。此映射端口称作 E2 端口号。

根据另一实施例，内部计算机经配置以根据图 3 的流程图的步骤通过使用（例如）套接口 L1 将另一 STUN 请求发送到 STUN 服务器 130c。如果内部计算机在预定时间周期内不从 STUN 服务器 130c 接收回应，那么内部计算机经配置以确认 NAT 装置为异常 NAT 装置。如果从 STUN 服务器接收到回应，那么内部计算机经配置以存储根据回应而返回的映射端口。此映射端口称作 E3 端口号。

图 6 是高阶层流程图，其具有使内部计算机进一步特征化 NAT 装置的步骤。在 600 处，如果确定 NAT 装置为异常 NAT 装置，那么内部计算机经配置以停止特征化所述 NAT 装置，且断定端口分配行为和端口指配行为是未知的。可设定与特征相关联的旗标以反映 NAT 装置的这些未知特征。在 605 处，内部计算机经配置以比较 E1 端口号与 E2 端口号。如果这些端口号相同（610），那么确定 NAT 装置的端口分配行为是锥形（上文详细描述）。如果这些端口号不相同（615），那么确定端口分配行为是端口敏感的。

图 7 是高阶层流程图，其具有让内部计算机确定连续套接口之间的单套接口增量的步骤。即，所述步骤由内部计算机执行以确定由 NAT 装置映射的连续映射端口的递增

值（例如，1、5、10等）。在700处，内部计算机经配置以确定：

- i) E1 端口号是否小于 E2 端口号；
- ii) E2 端口号是否小于 E3 端口号；
- iii) E1 端口号与 E2 端口号之间的差值是否小于选定端口增量（例如，20、10、5或类似数目）；和
- iv) E2 端口号与 E3 端口号之间的差值是否小于选定端口增量（例如，20、10、5或类似数目）。

如果内部计算机从上文的四个比较中得到正的查找结果，那么内部计算机经配置以确认 NAT 装置以递增方式映射外部端口（步骤 705）。另外，内部计算机经配置以将连续套接口的单套接口增量设定为 E3 端口号减去 E2 端口号（步骤 710）。如果内部计算机从上文的四个比较中的一个或一个以上中得到负的查找结果，那么在 715 处，内部计算机经配置以确定：

- i) E2 端口号是否小于 E3 端口号；和
- ii) E2 端口号与 E3 端口号之间的差值是否小于选定端口增量（例如，20、10、5或类似数目）。

如果内部计算机从前文的两个比较中得到正的查找结果，那么内部计算机确认 NAT 装置以递增的方式映射外部端口（步骤 705）。另外，内部计算机经配置以将连续套接口的单套接口增量设定为 E3 端口号减去 E2 端口号（步骤 710）。如果内部计算机从前文的两个比较中的一个或两个中得到负的查找结果，那么内部计算机经配置以断定 NAT 装置以随机方式映射端口（步骤 720），且将单套接口增量设定为未知（步骤 725）。

在执行前文所述的对 NAT 装置的特征的确定中的一个或多个后，内部计算机经配置以根据对特征的确定而设定若干内部旗标并设定若干内部变量。所述内部旗标和所述内部变量被称作端口预测信息。所述端口预测信息包括：

- i) UDP 预测的外部端口号；
- ii) UDP 预测的内部端口号；
- iii) 映射 IP 地址
- iv) 内部 IP 地址；
- v) 单套接口增量；
- vi) 端口分配行为（例如，锥形、端口敏感对称等），和
- vii) UDP 预测的套接口。

所述 UDP 预测的外部端口号是内部计算机预测 NAT 装置将创建的下一映射端口。

UDP 预测的内部端口号是内部计算机预测其将创建的下一端口。所述映射 IP 地址由外部网络上的 NAT 装置使用。所述内部 IP 地址由内部网络上的内部计算机使用。所述单套接口增量是由 NAT 装置创建的连续映射端口和/或连续映射 IP 地址之间的预测增量。上文详细描述所述端口分配行为。所述 UDP 预测的套接口是内部计算机将使用的预测套接口。

下文描述 8 组替代端口预测信息。一旦端口预测信息由内部计算机确定，内部计算机就可经配置以将端口预测信息传送到外部计算机，以使得外部计算机可使用所述信息来将数据包发送到映射端口，所述映射端口的数据包将穿越 NAT 装置。下文详细描述端口预测信息的传输。

根据端口预测信息的第一实施例，如果内部计算机确定 NAT 装置不支持 UDP 数据包或用于特征化 NAT 装置的其它数据包，那么内部计算机经配置以断定与外部计算机的 UDP 对等连接是不可能的，且可经配置以建立与外部计算机通信的另一方法。

根据端口预测信息的第二实施例，如果内部计算机确定其不在 NAT 装置后面，且所述 NAT 装置为异常 NAT 装置，那么内部计算机经配置以产生新的套接口（假定 L2）并将所述套接口绑定到随机端口（例如，5000 与 65535 之间的端口）。接着内部计算机存储绑定到套接口 L2 的本地端口号（例如）作为 L2 端口号。另外，因为没有安置 NAT 装置，所以内部计算机经配置以将 UDP 预测的外部端口号设定为 L2 端口号，以将 L2 端口号映射到映射端口号。内部计算机进一步经配置以将 UDP 预测的内部端口号设定为 L2 端口号。

根据端口预测信息的第三实施例，如果内部计算机确定其不在 NAT 装置后面，且所述 NAT 装置不是异常 NAT 装置，那么内部计算机经配置以将 UDP 预测外部端口号设定为 L1 端口号，且经配置以将 UDP 预测的内部端口号设定为 L1 端口号。

根据端口预测信息的第四实施例，如果内部计算机确定其在 NAT 装置后面，且所述 NAT 装置具有锥形的端口分配行为，那么内部计算机经配置以将 UDP 预测的外部端口号设定为 E1 端口号；将 UDP 预测的套接口设定为 L1 套接口；且将 UDP 预测的内部端口号设定为 L1 端口号。

根据端口预测信息的第五实施例，如果内部计算机确定其在 NAT 装置后面，所述 NAT 装置具有非锥形的端口分配行为，且套接口间端口指配行为是内外的，那么内部计算机经配置以产生新的套接口（假定 2）并将所述套接口 L2 绑定到端口号（例如，随机端口号）（假定 L2 端口号），内部计算机经配置以存储所述端口号。接着内部计算机经配置以将 UDP 预测的外部端口号设定为 L2 端口号，将 UDP 预测的套接口设定为 L2，

且将 UDP 预测的内部端口号设定为 L2 端口号。

根据端口预测信息的第六实施例，如果内部计算机确定其在 NAT 装置后面，所述 NAT 装置具有非锥形的端口分配行为，端口指配行为是递增且非内外的，那么内部计算机经配置以预测将由 NAT 装置创建的下一映射端口。

为详细阐述，如果 E1 端口号与 E2 端口号之间的差值与 E2 端口号与 E3 端口号之间的差值相同，那么内部计算机经配置以将 UDP 预测的外部端口号设定为 E3 端口号加上单套接口增量（即，E3 端口号减去 E2 端口号）。另外，内部计算机经配置以将 UDP 预测套接口设定为 L1，并将 UDP 预测的内部端口号设定为 L1 端口号。

或者，如果 E1 端口号与 E2 端口号之间的差值与 E2 端口号与 E3 端口号之间的差值不相同，那么内部计算机经配置以将 UDP 预测的外部端口号设定为 E3 端口号加上单套接口增量（即，E3 端口号减去 E2 端口号），另外，内部计算机经配置以将 UDP 预测的套接口设定为 L1 套接口，并将 UDP 预测的内部端口号设定为 L1 端口号。

根据端口预测信息的第七实施例，如果内部计算机确定其在 NAT 装置后面，所述 NAT 装置具有非锥形的端口分配行为，端口指配行为是递增且非内外的，那么内部计算机经配置以产生新的套接口（假定 L2），并将所述新的套接口绑定到端口号（例如，随机端口号）（假定 L2 端口号），内部计算机经配置以存储所述端口号。接着内部计算机经配置以将 UDP 预测的外部端口号设定为 E1 端口号加上单套接口增量（即，E3 端口号减去 E2 端口号），将 UDP 预测的套接口设定为 L2，且将 UDP 预测的内部端口号设定为 L2 端口号。

根据端口预测信息的第八实施例，如果内部计算机确定其在 NAT 装置后面，所述 NAT 装置具有非锥形的端口分配行为，端口指配行为不是递增且非内外的，那么内部计算机经配置以将 UDP 预测的外部端口号设定为 E0 端口号，将 UDP 预测的套接口设定为 L0，且将 UDP 预测的内部端口号设定为 E0 端口号。

根据一个实施例，内部计算机经配置以将端口预测信息传输到外部计算机以与外部计算机建立 UDP 对等通信链路。所述端口预测信息可通过内部计算机与外部计算机之间的反向通道传送以确保端口预测信息不会被与外部计算机相关联的 NAT 装置阻挡。所述反向通道是经由一通信链路（可为有线或无线）连接两个对等物的通信装置。反向通道通常由一服务器作主机。两个对等物均可经由通信链路连接到服务器，其有助于端口预测信息的传送。端口预测信息可由外部计算机用于确定内部计算机是否在 NAT 装置后面，或预测将由 NAT 装置创建的下一端口以将数据包发送到预测的端口。在接收到端口预测信息后或在接收到此信息前，外部计算机可经配置以确定外部计算机前面的

NAT 装置（例如 NAT 装置 205）的特征。外部计算机可执行前文的高阶层流程图中的一个或一个以上的步骤以确定 NAT 装置的特征或存在。外部计算机接着可设定一组内部旗标和内部变量（即，端口预测信息），并将此端口预测信息传输到内部计算机。

根据一个实施例，如果内部计算机和外部计算机从所接收的端口预测信息确定它们具有相同的映射 IP 地址，那么内部计算机和外部计算机都在相同的 NAT 装置后面。这些计算机接着将经配置以将 UDP 预测的内部端口号用于数据包共享。根据前文所述的实施例，如果数据包穿越 NAT 装置，那么在内部与外部计算机之间建立对等通信链路。

根据替代实施例，如果外部计算机确定内部计算机在具有锥形端口分配行为的 NAT 装置后面，那么由外部计算机用于将数据包发送到内部计算机的端口是 UDP 预测的外部端口号。内部计算机可类似地经配置以将数据包发送到外部计算机前面的 NAT 装置的 UDP 预测的端口号。根据前文所述的实施例，如果数据包穿越 NAT 装置，那么在内部与外部计算机之间建立对等通信链路。

或者，如果外部计算机确定内部计算机在对称的 NAT 装置后面，那么外部计算机可经配置以基于从内部计算机接收到的端口预测信息中的由外部计算机接收的单套接口增量而使用复数个不同端口将数据包发送到内部计算机。举例来说，外部计算机可经配置以经由五个不同端口将五个数据包发送到内部计算机。所述五个不同端口可包括 UDP 预测的外部端口号加上单套接口增量、UDP 预测的外部端口号加上两倍的单套接口增量、UDP 预测的外部端口号加上三倍的单套接口增量等等。内部计算机可类似地经配置以使用预测的端口号的增量将若干数据包发送到外部计算机。根据前文所述的实施例，如果数据包穿越 NAT 装置，那么在内部与外部计算机之间建立对等通信链路。

应了解，上文所述的实例和实施例仅为了说明性目的，且所属领域的技术人员将提出参照所述实例和实施例的各种修改或改变，且所述各种修改和改变包括于此申请案的精神和界限以及所附权利要求书的范畴内。举例来说，本文所述的防火墙装置可经配置以大体上类似于以各种方式描述的 NAT 装置操作，尽管防火墙装置不可经配置以执行网络地址转换且其可或不可经配置以执行端口地址转换。所属领域的技术人员广泛了解防火墙装置的功能且本文将不再作详细描述，除了应注意防火墙装置经配置以在网络阶层、应用层阶层和类似阶层处操作以阻挡数据包通过防火墙，除非它们匹配一组规则。防火墙管理者可界定所述组规则或所述组规则可为一组默认规则。所述规则可包括本文所述的数据包过滤规则（例如，异常规则）。根据另一实例，本文所述的一个或一个以上 NAT 装置可经配置以与一个或一个以上防火墙装置一起操作以执行 NAT 并提供防火墙过滤。所属领域的技术人员广泛了解 NAT 装置与防火墙装置的相互操作且本文将不

---

再作进一步详细描述。因此，不应将上文的描述看作限制由权利要求书界定的本发明的范畴。



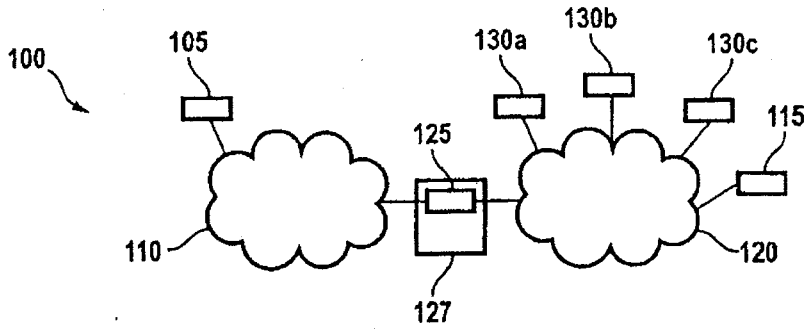


图 1

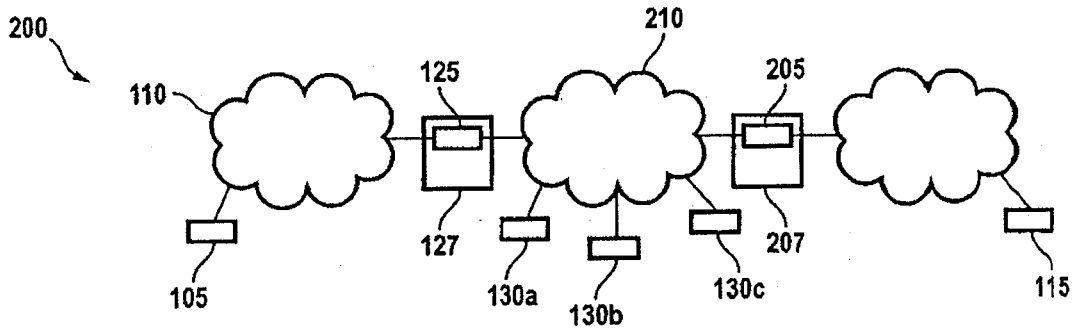


图 2

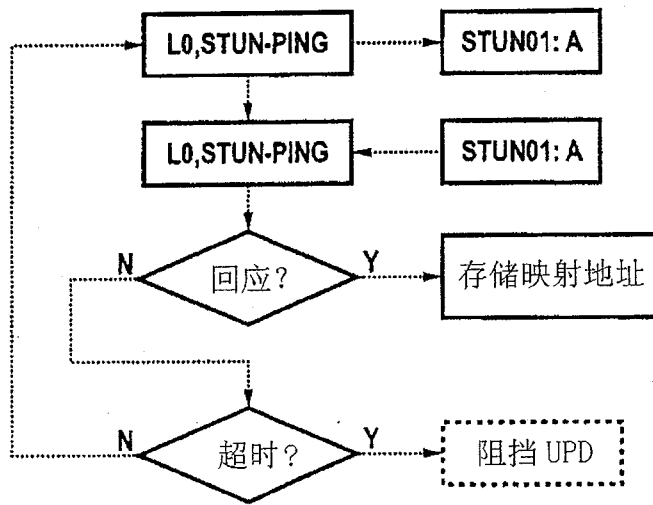


图 3

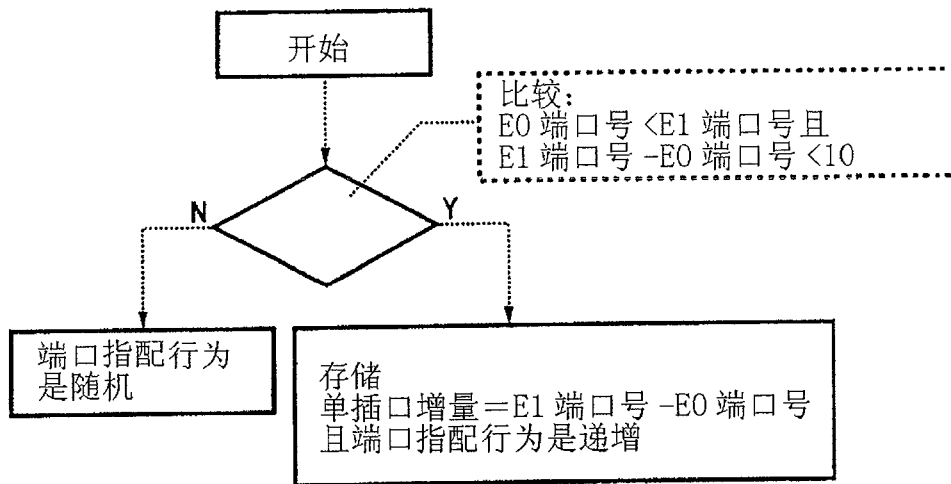


图 4

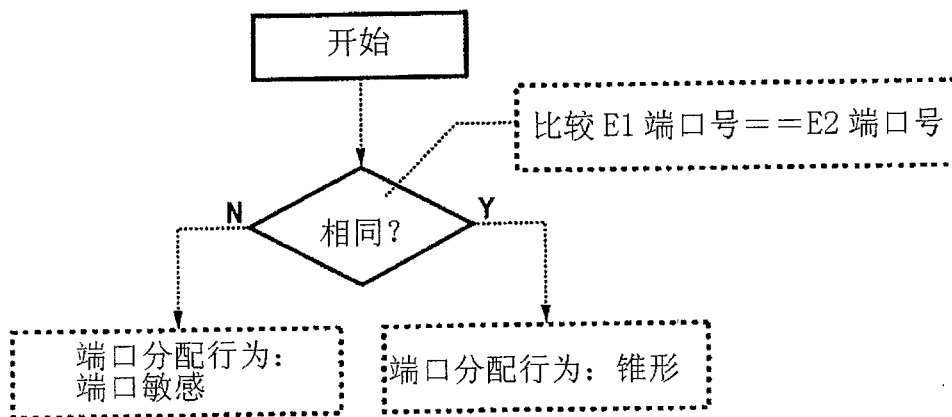


图 6

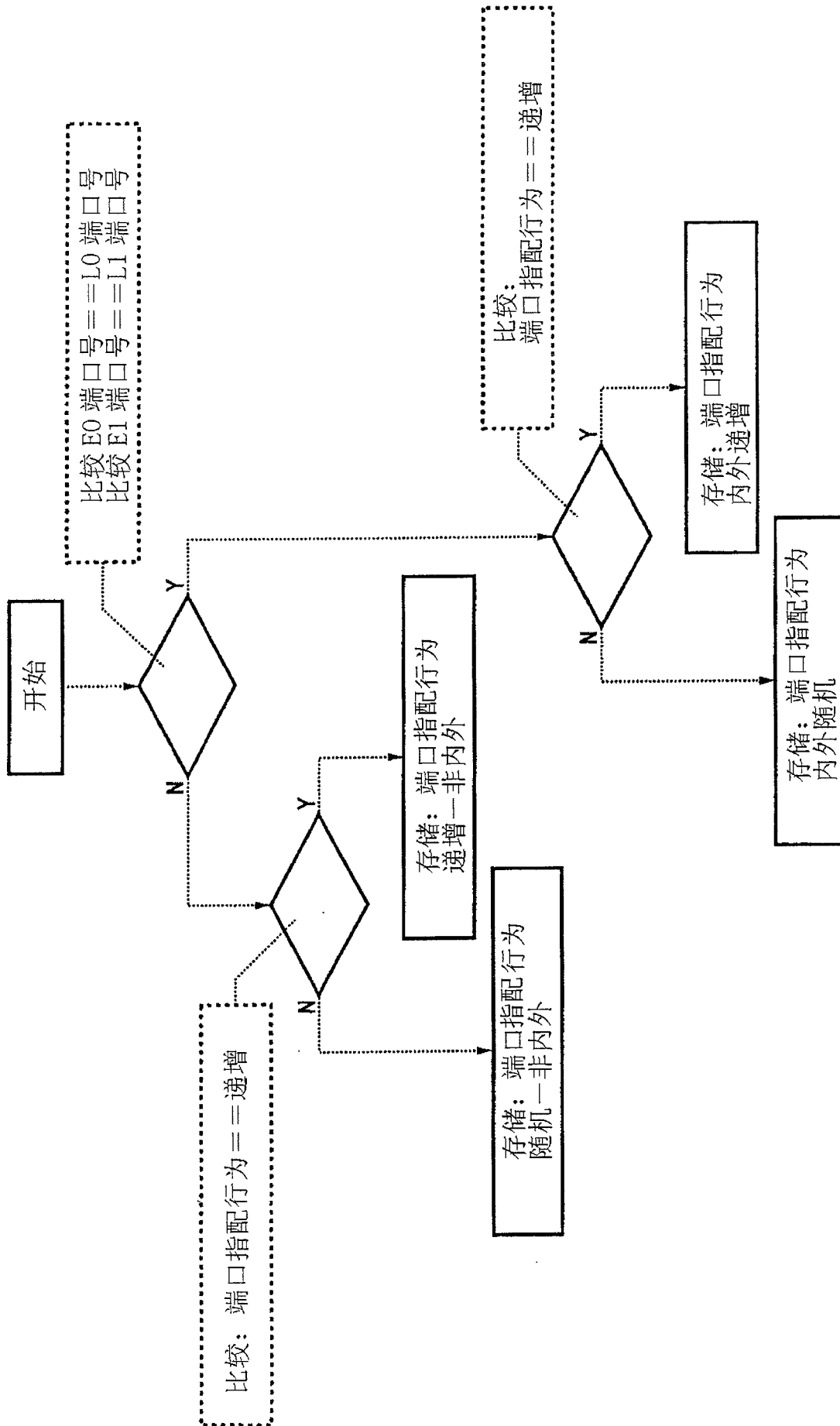


图 5

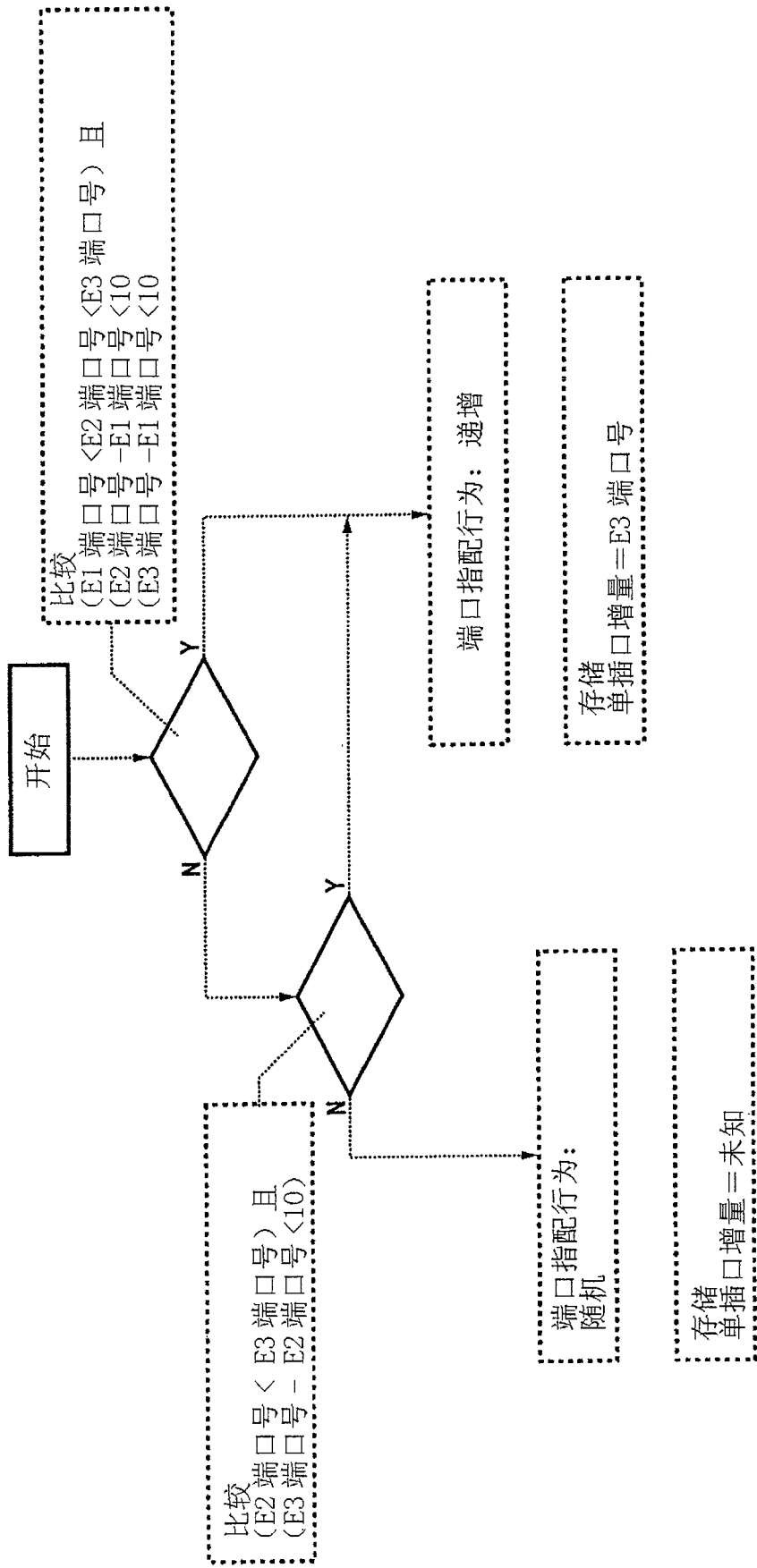


图 7