(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 101572729 B
(45)授权公告日 2012.02.01

(21)申请号 200910139354.3

(22)申请日 2009.05.04

(73)专利权人 成都市华为赛门铁克科技有限公司
地址 611731 四川省成都市高新区西部园区清水河片区

(72)发明人 王雨晨

(74)专利代理机构 深圳市深佳知识产权代理事务所（普通合伙）44285
代理人 彭愿洁 李文红

(51)Int.Cl.
H04L 29/12(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101151849 A,2008.03.26,
CN 1747436 A,2006.03.15,
CN 1476204 A,2004.02.18,

审查员 苏宁

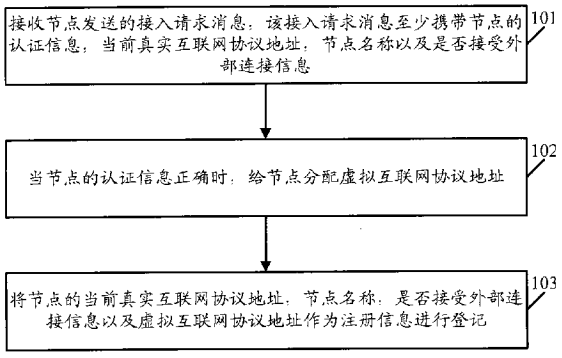
权利要求书 2 页 说明书 13 页 附图 6 页

(54)发明名称

一种虚拟专用网节点信息的处理方法及相关设备、系统

(57)摘要

本发明实施例涉及通信技术领域，公开了一种虚拟专用网节点信息的处理方法及设备，该方法包括：接收节点发送的接入请求消息，该接入请求消息至少携带节点的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息；当所述节点的认证信息正确时，如果是，则给节点分配虚拟互联网协议地址；将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记。本发明实施例使得节点在加入虚拟专用网时，无需调整其它节点的配置，从而使得虚拟专用网可以支持动态变化的网络结构，提高了虚拟专用网的灵活性。



CN 101572729 B

1. 一种虚拟专用网节点信息的处理方法，其特征在于，包括：

接收节点发送的接入请求消息，该接入请求消息至少携带所述节点的认证信息，节点名称以及是否接受外部连接信息；所述节点至少包括第一节点和第二节点；

当所述节点的认证信息正确时，将所述节点的节点名称，是否接受外部连接信息作为注册信息进行登记；

接收第一节点发送的查询消息，所述查询消息中携带第二节点的节点名称；

根据所述第二节点的节点名称查询所述第二节点的注册信息；

向所述第一节点发送所述第二节点的注册信息，所述第二节点的注册信息中至少携带第二节点是否接受外部连接的信息；

若所述第二节点不接受外部连接，且所述第一节点不接受外部连接，则分别接收所述第一节点和第二节点发送的建立网络隧道请求；

分别向所述第一节点和第二节点发送建立网络隧道响应，从而分别建立与所述第一节点和第二节点之间的网络隧道；

利用与所述第一节点和第二节点之间的网络隧道，为所述第一节点和第二节点互相传递信息。

2. 根据权利要求 1 所述的方法，其特征在于，该方法还包括：

接收第一节点发送的查询消息，所述查询消息中携带第一节点的节点名称；

根据所述第一节点的节点名称查询所述第一节点的注册信息；

向所述第一节点发送所述第一节点的注册信息，所述第一节点的注册信息中至少携带第一节点是否接受外部连接的信息。

3. 一种虚拟专用网节点信息的处理设备，其特征在于，包括：

第一接收单元，用于接收节点发送的接入请求消息，该接入请求消息至少携带所述节点的认证信息、节点名称以及是否接受外部连接信息；所述节点至少包括第一节点和第二节点；

判断单元，用于判断所述节点的认证信息是否正确；

登记单元，用于当所述判断单元判断所述节点的认证信息正确时，将所述节点的节点名称、是否接受外部连接信息作为注册信息进行登记；

第二接收单元，用于接收第一节点发送的查询消息，所述查询消息中携带第二节点的节点名称；

查询单元，用于根据所述第二节点的节点名称查询所述第二节点的注册信息；

第一发送单元，用于向所述第一节点发送所述第二节点的注册信息，所述第二节点的注册信息至少携带第二节点的是否接受外部连接的信息；

若所述第二节点不接受外部连接，且所述第一节点不接受外部连接，则所述处理设备还包括：

第三接收单元，用于接收所述第一节点发送的建立网络隧道请求，以及所述第二节点发送的建立网络隧道请求；

第二发送单元，用于向所述第一节点发送建立网络隧道响应，从而建立与所述第一节点之间的网络隧道，向所述第二节点发送建立网络隧道响应，从而建立与所述第二节点之间的网络隧道；

转发控制单元，用于接收所述第一节点发送给所述第二节点的信息，并转发给所述第二节点，以及接收所述第二节点发送给所述第一节点的信息，并转发给所述第一节点。

4. 根据权利要求 3 所述的处理设备，其特征在于，

所述第二接收单元，用于接收第一节点发送的查询消息，所述查询消息中携带第一节点的节点名称；

所述查询单元，用于根据所述第一节点的节点名称查询所述第一节点的注册信息；

所述第一发送单元，用于向所述第一节点发送所述第一节点的注册信息，所述第一节点的注册信息至少携带第一节点的是否接受外部连接的信息。

5. 一种虚拟专用网系统，其特征在于，包括：

虚拟专用网节点信息的处理设备和至少两个虚拟专用网节点设备；

第一虚拟专用网节点设备，用于获取自身的认证信息、节点名称以及是否接受外部连接信息，并将所述认证信息、节点名称以及是否接受外部连接信息放入接入请求消息之后，发送给所述虚拟专用网节点信息的处理设备；向所述虚拟专用网节点信息的处理设备发送查询消息，所述查询消息中携带第二虚拟专用网节点设备的节点名称；接收返回的第二虚拟专用网节点设备的注册信息，当根据注册信息中携带的第二虚拟专用网节点设备是否接受外部连接的信息确定所述第二虚拟专用网节点设备不接受外部连接，且所述第一虚拟专用网节点设备不接受外部连接，则向所述虚拟专用网节点信息的处理设备发送建立网络隧道请求，接收到建立网络隧道响应后，建立与所述虚拟专用网节点信息的处理设备的网络隧道；

所述虚拟专用网节点信息的处理设备，用于接收所述第一虚拟专用网节点设备或第二虚拟专用网节点设备发送的接入请求消息，该接入请求消息至少携带发送所述接入请求消息的虚拟专用网节点设备的认证信息、节点名称以及是否接受外部连接信息；当判断所述认证信息正确时，将所述第一虚拟专用网节点设备或第二虚拟专用网节点设备的节点名称、是否接受外部连接信息作为注册信息进行登记；接收第一虚拟专用网节点设备发送的查询消息，返回第二虚拟专用网节点设备的注册信息，所述注册信息至少携带第二虚拟专用网节点设备是否接受外部连接的信息，若所述第二虚拟专用网节点设备不接受外部连接，且所述第一虚拟专用网节点设备不接受外部连接，则分别接收所述第一虚拟专用网节点设备和第二虚拟专用网节点设备发送的建立网络隧道请求；分别向所述第一虚拟专用网节点设备和第二虚拟专用网节点设备发送建立网络隧道响应，从而分别建立与所述第一虚拟专用网节点设备和第二虚拟专用网节点设备之间的网络隧道；利用与所述第一虚拟专用网节点设备和第二虚拟专用网节点设备之间的网络隧道，为所述第一虚拟专用网节点设备和第二虚拟专用网节点设备互相传递信息。

一种虚拟专用网节点信息的处理方法及相关设备、系统

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种虚拟专用网节点信息的处理方法及相关设备、系统。

背景技术

[0002] 目前，不同的节点设备之间通过一个公用网络（通常是因特网）灵活而安全地动态组建虚拟专用网(VPN,Virtual Private Network)的技术应用日益广泛。VPN网络可以帮助远程用户、公司分支机构、商业伙伴及供应商与公司的内部网建立可信的安全连接，并保证数据的安全传输。

[0003] 在现有的VPN网络中，每一个节点上预先配置其它所有节点的注册信息，比如，配置其它节点设备的当前真实互联网协议(IP，Internet Protocol)，虚拟IP地址以及是否接受外部连接信息等。根据其它节点的注册信息，节点可以和其它节点建立相应的网络隧道。比如，当其它节点接受外部连接信息时，可以根据其它节点的真实IP地址与其它节点建立直连通道模式下的网络隧道；当其它节点不接受外部连接信息时，可以根据其它节点的虚拟IP地址与其它节点建立虚拟交换模式下的网络隧道。

[0004] 发明人发现，在现有的VPN网络中，当加入一个节点时，需要在加入的节点上配置其它原有节点的注册信息；同时，还需要调整其它原有节点的配置；当一个节点脱离网络时，也需要调整其它原有节点的配置，即在现有的VPN网络中节点的加入或脱离，必然会导致其它节点相应调整自身配置，因此，现有的VPN网络一般只适用于拓扑结构和网络配置较为固定的环境，灵活性较差。

发明内容

[0005] 本发明实施例提供了一种虚拟专用网节点信息的处理方法及相关设备、系统，可以提高VPN网络的灵活性。

[0006] 为实现上述目的，本发明实施例提供如下技术方案：

[0007] 本发明实施例提供了一种虚拟专用网节点信息的处理方法，包括：

[0008] 接收节点发送的接入请求消息，该接入请求消息至少携带所述节点的认证信息，节点名称以及是否接受外部连接信息；

[0009] 将所述节点的节点名称，是否接受外部连接信息作为注册信息进行登记；

[0010] 接收第一节点发送的查询消息，所述查询消息中携带第二节点的节点名称；

[0011] 根据所述第二节点的节点名称查询所述第二节点的注册信息；

[0012] 向所述第一节点发送所述第二节点的注册信息，所述第二节点的注册信息中至少携带第二节点是否接受外部连接的信息；

[0013] 若所述第二节点不接受外部连接，且所述第一节点不接受外部连接，则分别接收所述第一节点和第二节点发送的建立网络隧道请求；

[0014] 分别向所述第一节点和第二节点发送建立网络隧道响应，从而分别建立与所述第

一节点和第二节点之间的网络隧道；

[0015] 利用与所述第一节点和第二节点之间的网络隧道，为所述第一节点和第二节点互相传递信息。

[0016] 本发明实施例提供了一种虚拟专用网节点信息的处理设备，包括：

[0017] 第一接收单元，用于接收节点发送的接入请求消息，该接入请求消息至少携带所述节点的认证信息、节点名称以及是否接受外部连接信息；

[0018] 判断单元，用于判断所述节点的认证信息是否正确；

[0019] 登记单元，用于将所述节点节点名称、是否接受外部连接信息作为注册信息进行登记；

[0020] 第二接收单元，用于接收第一节点发送的查询消息，所述查询消息中携带第二节点的节点名称；

[0021] 查询单元，用于根据所述第二节点的节点名称查询所述第二节点的注册信息；

[0022] 第一发送单元，用于向所述第一节点发送所述第二节点的注册信息，所述第二节点的注册信息至少携带第二节点的是否接受外部连接的信息；

[0023] 若所述第二节点不接受外部连接，且所述第一节点不接受外部连接，则所述处理设备还包括：

[0024] 第三接收单元，用于接收所述第一节点发送的建立网络隧道请求，以及所述第二节点发送的建立网络隧道请求；

[0025] 第二发送单元，用于向所述第一节点发送建立网络隧道响应，从而建立与所述第一节点之间的网络隧道，向所述第二节点发送建立网络隧道响应，从而建立与所述第二节点之间的网络隧道；

[0026] 转发控制单元，用于接收所述第一节点发送给所述第二节点的信息，并转发给所述第二节点，以及接收所述第二节点发送给所述第一节点的信息，并转发给所述第一节点。

[0027] 本发明实施例提供了一种虚拟专用网节点设备，包括：

[0028] 获取单元，用于获取自身的认证信息，节点名称以及是否接受外部连接信息；

[0029] 发送单元，用于将所述认证信息，节点名称以及是否接受外部连接信息放入接入请求消息后，发送给虚拟专用网节点信息的处理设备。

[0030] 本发明实施例提供了一种虚拟专用网系统，包括：

[0031] 虚拟专用网节点信息的处理设备和至少虚拟专用网节点设备；

[0032] 第一所述虚拟专用网节点设备，用于获取自身的认证信息、节点名称以及是否接受外部连接信息，并将所述认证信息、节点名称以及是否接受外部连接信息放入接入请求消息之后，发送给所述虚拟专用网节点信息的处理设备；向所述虚拟专用网节点信息的处理设备发送查询消息，所述查询消息中携带第二虚拟专用网节点设备的节点名称；接收返回的第二虚拟专用网节点设备的注册信息，当根据注册信息中携带的第二虚拟专用网节点设备是否接受外部连接的信息确定所述第二虚拟专用网节点设备不接受外部连接，且所述第一虚拟专用网节点设备不接受外部连接，则向所述虚拟专用网节点信息的处理设备发送建立网络隧道请求，接收到建立网络隧道响应后，建立与所述虚拟专用网节点信息的处理设备的网络隧道；

[0033] 所述虚拟专用网节点信息的处理设备，用于接收所述虚拟专用网节点设备发送的

接入请求消息，该接入请求消息至少携带所述虚拟专用网节点设备的认证信息、节点名称以及是否接受外部连接信息；并将所述虚拟专用网节点设备的节点名称、是否接受外部连接信息作为注册信息进行登记；接收第一虚拟专用网节点设备发送的查询消息，返回第二虚拟专用网节点设备的注册信息，所述注册信息至少携带第二虚拟专用网节点设备是否接受外部连接的信息，若所述第二虚拟专用网节点设备不接受外部连接，且所述第一虚拟专用网节点设备不接受外部连接，则分别接收所述第一虚拟专用网节点设备和第二虚拟专用网节点设备发送的建立网络隧道请求；分别向所述第一虚拟专用网节点设备和第二虚拟专用网节点设备发送建立网络隧道响应，从而分别建立与所述第一虚拟专用网节点设备和第二虚拟专用网节点设备之间的网络隧道；利用与所述第一虚拟专用网节点设备和第二虚拟专用网节点设备之间的网络隧道，为所述第一虚拟专用网节点设备和第二虚拟专用网节点设备互相传递信息。

[0034] 与现有的技术相比，本发明实施例采用了虚拟专用网节点信息的处理设备对 VPN 节点的注册信息进行集中登记，避免了在每一个 VPN 节点上配置其它 VPN 节点的注册信息，当加入一个 VPN 节点时，只需在虚拟专用网节点信息的处理设备上对加入的 VPN 节点的注册信息进行登记即可，无需调整其它 VPN 节点的配置，从而使得 VPN 可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

附图说明

[0035] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0036] 图 1 为本发明实施例中提供的一种虚拟专用网节点信息的处理方法的流程图；

[0037] 图 2 为本发明实施例中提供的一种查询节点注册信息的方法的流程图；

[0038] 图 3 为本发明实施例中提供的一种虚拟专用网节点通信方法的流程图；

[0039] 图 4 为本发明实施例中提供的一种虚拟专用网节点信息的处理方法的流程图；

[0040] 图 5 为本发明实施例中提供的一种虚拟专用网节点信息的处理设备的结构图；

[0041] 图 6 为本发明实施例中提供的一种虚拟专用网节点信息的处理设备的结构图；

[0042] 图 7 为本发明实施例中提供的一种虚拟专用网节点信息的处理设备的结构图；

[0043] 图 8 为本发明实施例中提供的一种虚拟专用网节点设备的结构图；

[0044] 图 9 为本发明实施例中提供的一种虚拟专用网系统的结构图；

[0045] 图 10 为本发明实施例中提供的一种虚拟专用网的示意图；

[0046] 图 11 为本发明实施例中提供的一种查询节点注册信息的方法流程图；

[0047] 图 12 为本发明实施例中提供的一种虚拟专用网节点通信方法的流程图；

[0048] 图 13 为本发明实施例中提供的一种虚拟专用网节点通信方法的流程图。

具体实施方式

[0049] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于

本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0050] 实施例一：

[0051] 请参阅图 1，图 1 为本发明实施例一提供的一种虚拟专用网节点信息的处理方法的流程图。如图 1 所示，该方法可以包括：

[0052] 101：接收节点发送的接入请求消息，该接入请求消息至少携带节点的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息；

[0053] 其中，本实施例及后续实施例中所说的节点包括但不限于移动手机，掌上电脑，个人电脑，服务器以及网关等等。

[0054] 优选地，本实施例及后续实施例中所说的节点认证信息包括但不限于节点的账号和口令；其中，节点的认证信息是由服务提供商预先根据节点期望接入的 VPN 网络的需要（如，节点数量以及 VPN 网络拓扑结构等）而提供的。

[0055] 举例来说，节点的当前真实互联网协议地址可以是节点在因特网中的互联网协议（IP，Internet Protocol）地址，或者是节点在因特网中的 IP 地址与传输控制协议（TCP，Transmission Control Protocol）/ 用户数据报协议（UDP，User Datagram Protocol）端口组合后的地址，或者是节点在因特网中的以网页地址（URL，Uniform Resource Locator）表示的其他服务地址。

[0056] 当然，接入请求消息除了携带节点的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息之外，还可以携带节点的其它相关信息。

[0057] 102：当所述节点的认证信息正确时，给节点分配虚拟互联网协议地址；

[0058] 如果上述 101 中接收到的节点的认证信息为节点的账号和口令，那么在 102 中可以判断节点的账号和口令是否都正确，如果节点的账号和口令都正确，则为该节点分配虚拟互联网协议地址，并将分配的虚拟 IP 地址发送给节点；

[0059] 反之，如果节点的账号和口令不完全正确，则不再为节点分配虚拟 IP 地址，此时，可以给节点发送错误信息，并关闭网络连接。

[0060] 103：将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记。

[0061] 其中，将当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记，可以实现对节点的注册信息的集中管理，这样，每一个节点上无需再配置其它节点的注册信息，方便后续节点查询其它节点以及本节点的注册信息。

[0062] 举例来说、在上述步骤 103 将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记之后，本发明实施例提供的虚拟专用网节点信息的处理方法还可以允许节点进行注册信息的查询。请一并参阅图 2，图 2 为本发明实施例一提供的一种查询节点注册信息的方法的流程图，如图 2 所示，该方法可以包括如下步骤：

[0063] 201：接收第一节点发送的查询消息，该查询消息中携带第二节点的节点名称和 / 或第二节点的当前真实互联网协议地址；

[0064] 202：根据第二节点的节点名称和 / 或第二节点的当前真实互联网协议地址查询

第二节点的注册信息；

[0065] 203：向第一节点发送第二节点的注册信息，第二节点的注册信息至少携带第二节点的是否接受外部连接的信息。

[0066] 本发明实施例提供的虚拟专用网节点信息的处理方法允许第一节点查询第二节点的注册信息，为了确切地获知第一节点需要查询的第二节点的注册信息，要求第一节点发送的查询消息中需要携带有用于识别第二节点的信息，由于每一个节点的名称以及当前真实互联网协议地址是不相同的，所以第一节点发送的查询消息中可以携带第二节点的名称和 / 或第二节点的当前真实互联网协议地址。

[0067] 当然，第一节点发送的查询消息中还可以携带其他用于识别第二节点的信息，本发明实施例在此不做限定。

[0068] 举例来说、在上述步骤 103 将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记之后，本发明实施例提供的虚拟专用网节点信息的处理方法还可以包括如下步骤：

[0069] 接收第一节点发送的查询消息，该查询消息中携带第一节点的节点名称和 / 或第一节点的当前真实互联网协议地址；

[0070] 根据第一节点的节点名称和 / 或第一节点的当前真实互联网协议地址查询第一节点的注册信息；

[0071] 向第一节点发送第一节点的注册信息，第一节点的注册信息至少携带第一节点的是否接受外部连接的信息。

[0072] 本发明实施例提供的虚拟专用网节点信息的处理方法允许第一节点查询第一节点的注册信息，同样，要求第一节点发送的查询消息中需要携带有用于识别第一节点的信息，比如第一节点的名称和 / 或第一节点的当前真实互联网协议地址等等。

[0073] 举例来说，在第一节点在查询到第二节点以及第一节点的注册信息后，如果发现第二节点不接受外部连接，且第一节点不接受外部连接，则本发明实施例提供的虚拟专用网节点信息的处理方法还可以利用与第一节点和第二节点之间的网络隧道，为第一节点和第二节点互相传递信息。请一并参阅图 3，图 3 为本发明实施例一提供的一种虚拟专用网节点通信方法的流程图，如图 3 所示，该方法可以包括如下步骤：

[0074] 301：分别接收第一节点和第二节点发送的建立网络隧道请求；

[0075] 302：分别向第一节点和第二节点发送建立网络隧道响应，从而分别建立与所述第一节点和第二节点之间的网络隧道；

[0076] 303：利用与第一节点和第二节点之间的网络隧道，为第一节点和第二节点互相传递信息。

[0077] 其中，第二节点在发送建立网络隧道请求之前，需要接收第一节点发送的提示消息，该提示消息是第一节点在发现第二节点不接受外部连接，且第一节点不接受外部连接的情况发送的，用于提示第二节点需要和第一节点建立虚拟通道模式下的间接网络连接。

[0078] 其中，第一节点发送的建立网络隧道请求是以第一节点的虚拟互联网协议地址发送的，第二节点发送的建立网络隧道请求是以第二节点的虚拟互联网协议地址发送的。

[0079] 举例来说，在第一节点查询到第二节点以及第一节点的注册信息后，如果发现第二节点接受外部连接，则第一节点可以主动向第二节点发送建立网络隧道请求；第一节点

接收第二节点发送的响应后，建立与第二节点之间的直连通道模式下的直连网络隧道。

[0080] 其中，第一节点与第二节点之间是以当前真实互联网协议地址进行消息的发送的。

[0081] 举例来说，在第一节点查询到第二节点以及第一节点的注册信息后，如果发现第二节点不接受外部连接，而第一节点接受外部连接，则第一节点可以主动向第二节点发送用于提示第二节点向第一节点建立网络隧道的消息；第一节点接收第二节点发送的建立网络隧道请求，并向第二节点发送响应后，建立与第二节点之间的直连通道模式下的直连网络隧道。

[0082] 其中，第一节点与第二节点之间是以当前真实互联网协议地址进行消息的发送的。

[0083] 本发明实施例可以对节点的注册信息进行集中登记，避免了在 VPN 网络的每一个节点上配置其它节点的注册信息，当加入一个节点时，只需对加入的节点的注册信息进行登记即可，无需调整其它节点的配置，从而使得 VPN 网络可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

[0084] 实施例二：

[0085] 请参阅图 4，图 4 为本发明实施例二提供的一种虚拟专用网节点信息的处理方法的流程图。根据本发明实施例提供的方法，需要在因特网上预先部署一个虚拟专用网节点信息的处理设备。其中，该虚拟专用网节点信息的处理设备应该具有当前真实互联网协议地址，可以是该虚拟专用网节点信息的处理设备在因特网中的 IP 地址，或者是在因特网中的 IP 地址与 TCP/UDP 端口组合后的地址，或者在因特网中以 URL 表示的其他服务地址。如图 2 所示，该方法可以包括：

[0086] 401：虚拟专用网节点信息的处理设备接收节点发送的接入请求信息。

[0087] 其中，节点发送的接入请求信息是根据已知的虚拟专用网节点信息的处理设备的当前真实互联网协议地址发送的。

[0088] 节点发送的接入请求信息可以携带但不限于节点当前真实互联网协议地址，以及认证信息等等。

[0089] 本实施例及后续实施例中所说的节点认证信息包括但不限于节点的账号和口令；其中，节点的认证信息是由服务提供商预先根据节点期望接入的 VPN 网络的需要（如，节点数量以及 VPN 网络拓扑结构等）而提供的。

[0090] 402：虚拟专用网节点信息的处理设备接收到节点发送的接入请求信息后，判断节点认证信息是否正确，如果正确，则执行 403；反之，则执行 406。

[0091] 如果上述 402 中虚拟专用网节点信息的处理设备判断节点的账号和口令是否都正确，则为节点分配虚拟互联网协议地址，并将分配的虚拟互联网协议地址发送给节点；

[0092] 反之，如果节点的账号和口令不完全正确，则不再为节点分配虚拟互联网协议地址，此时，可以给节点发送错误信息，并关闭网络连接。

[0093] 403：为节点分配虚拟互联网协议地址，并发送给节点。

[0094] 当节点的认证信息正确后，虚拟专用网节点信息的处理设备可以给节点分配虚拟互联网协议地址，其中，每一个节点被分配的虚拟互联网协议地址是互不相同的。

[0095] 另外，当虚拟专用网节点信息的处理设备可以和其他不同的 VPN 网络之间建立路

由与访问控制策略时，虚拟专用网节点信息的处理设备的功能和行为在 VPN 网络内的节点看来如同一个虚拟的路由器或者防火墙。这样，虚拟专用网节点信息的处理设备在给节点分配虚拟互联网协议地址的时候，可以进一步给节点分配 VPN 网络内虚拟网关的虚拟互联网协议地址等信息。

[0096] 其中，节点在接收到虚拟专用网节点信息的处理设备发送的虚拟互联网协议地址之后，可以对节点内的虚拟网卡进行相应的配置，然后再向虚拟专用网节点信息的处理设备发送注册信息。

[0097] 需要说明的是，节点发送注册信息是在节点和虚拟专用网节点信息的处理设备之间建立的安全通道内进行协议封装，并传输到虚拟专用网节点信息的处理设备。其中，节点和虚拟专用网节点信息的处理设备之间建立的安全通道是在虚拟专用网节点信息的处理设备向节点发送虚拟互联网协议地址完成后建立的。

[0098] 404 ：接收节点发送的请求注册信息，该请求注册信息中携带有该节点的注册信息，包括当前真实互联网协议地址、虚拟互联网协议地址以及节点名称等等。

[0099] 405 ：登记该节点的注册信息。

[0100] 406 ：虚拟专用网节点信息的处理设备向节点返回错误信息并关闭此网络连接。

[0101] 本实施例与上述实施例一的区别在于，在实施例一中，节点在发送接入请求消息，该接入请求消息至少携带节点的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息 ；这样，当虚拟专用网节点信息的处理设备判断节点的认证信息正确之后，可以给节点分配虚拟互联网协议地址，并且直接将节点的当前真实互联网协议地址，节点名称以及是否接受外部连接信息和虚拟互联网协议地址进行登记 ；而本实施例中，节点在接收到虚拟专用网节点信息的处理设备分配的虚拟互联网协议地址之后，再将节点的当前真实互联网协议地址，节点名称以及是否接受外部连接信息和虚拟互联网协议地址等作为注册信息发送给的虚拟专用网节点信息的处理设备进行登记。

[0102] 本发明实施例可以对节点的注册信息进行集中登记，避免了在 VPN 网络的每一个节点上配置其它节点的注册信息，当加入一个节点时，只需对加入的节点的注册信息进行登记即可，无需调整其它节点的配置，从而使得 VPN 网络可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

[0103] 实施例三 ：

[0104] 请参阅图 5，为本发明实施例三提供的一种虚拟专用网节点信息的处理设备的结构图 ；本发明实施例提供的虚拟专用网节点信息的处理设备部署在因特网中，具有真实的互联网协议地址。如图 5 所示，该虚拟专用网节点信息的处理设备可以包括 ：

[0105] 第一接收单元 501，用于接收节点发送的接入请求消息，该接入请求消息至少携带节点的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息 ；

[0106] 举例来说，节点认证信息包括但不限于节点的账号和口令 ；其中，节点的认证信息是由服务提供商预先根据节点期望接入的 VPN 网络的需要（如，节点数量以及 VPN 网络拓扑结构等）而提供的。

[0107] 判断单元 502，用于判断节点的认证信息是否正确 ；

[0108] 分配单元 503，用于在判断单元 302 判断所述节点的认证信息正确时，给节点分配虚拟互联网协议地址 ；

[0109] 登记单元 504，用于将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记。

[0110] 请一并参阅图 6，图 6 为本发明实施例三提供的另一种虚拟专用网节点信息的处理设备的结构图。图 6 所示的虚拟专用网节点信息的处理设备是在图 3 所示的虚拟专用网节点信息的处理设备的基础之上，进一步包括：

[0111] 第二接收单元 505，用于在登记单元 504 将节点的当前真实互联网协议地址、节点名称、是否接受外部连接信息以及虚拟互联网协议地址等信息作为注册信息进行登记之后，接收第一节点发送的查询消息，该查询消息中携带第二节点的节点名称和 / 或第二节点的当前真实互联网协议地址；

[0112] 查询单元 506，用于根据第二节点的节点名称和 / 或第二节点的当前真实互联网协议地址查询第二节点的注册信息；

[0113] 第一发送单元 507，用于向第一节点发送所述第二节点的注册信息，所述第二节点的注册信息至少携带第二节点的是否接受外部连接的信息。

[0114] 图 6 所示的虚拟专用网节点信息的处理设备允许第一节点查询第二节点的注册信息，为了确切地获知第一节点需要查询的第二节点的注册信息，要求第一节点发送的查询消息中需要携带有用于识别第二节点的信息，由于每一个节点的名称以及当前真实互联网协议地址是不相同的，所以第一节点发送的查询消息中可以携带第二节点的名称和 / 或第二节点的当前真实互联网协议地址。

[0115] 当然，第一节点发送的查询消息中还可以携带其他用于识别第二节点的信息，本发明实施例在此不做限定。

[0116] 其中，第二接收单元 505 还用于在登记单元 504 将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记之后，接收第一节点发送的查询消息，该查询消息中携带第一节点的节点名称和 / 或第一节点的当前真实互联网协议地址；

[0117] 查询单元 506 还用于根据第一节点的节点名称和 / 或第一节点的当前真实互联网协议地址查询第一节点的注册信息；

[0118] 第一发送单元 507 还用于向第一节点发送第一节点的注册信息，所述第一节点的注册信息至少携带第一节点的是否接受外部连接的信息。

[0119] 图 6 所示的虚拟专用网节点信息的处理设备允许第一节点查询第一节点的注册信息，同样，要求第一节点发送的查询消息中需要携带有用于识别第一节点的信息，比如第一节点的名称和 / 或第一节点的当前真实互联网协议地址等等。

[0120] 请一并参阅图 7，图 7 为本发明实施例三提供的另一种虚拟专用网节点信息的处理设备的结构图。图 7 所示的虚拟专用网节点信息的处理设备是在图 5 所示的虚拟专用网节点信息的处理设备的基础之上，进一步包括：

[0121] 第三接收单元 508，用于在第一发送单元 507 向第一节点发送第二节点的注册信息，以及向第一节点发送第一节点的注册信息之后，接收第一节点发送的建立网络隧道请求；

[0122] 其中，第一节点发送的建立网络隧道请求是第一节点在接收到第一发送单元 507 发送的第二节点以及第一节点的注册信息后，发现第二节点不接受外部连接，且第一节点

不接受外部连接的情况下发送的。

[0123] 第二发送单元 509，用于向第一节点发送建立网络隧道响应，从而建立与第一节点之间的网络隧道；

[0124] 第三接收单元 508 还用于在第一发送单元 507 向第一节点发送第二节点的注册信息，以及向第一节点发送所述第一节点的注册信息之后，接收第二节点发送的建立网络隧道请求；

[0125] 其中，第二节点在发送建立网络隧道请求之前，需要接收第一节点发送的提示消息，该提示消息是第一节点在发现第二节点不接受外部连接，且第一节点不接受外部连接的情况发送的，用于提示第二节点需要和第一节点建立虚拟通道模式下的间接网络连接。

[0126] 第二发送单元 509 还用于向第二节点发送建立网络隧道响应，从而建立与所述第二节点之间的网络隧道；

[0127] 其中，第一节点发送的建立网络隧道请求是以第一节点的虚拟互联网协议地址发送的，第二节点发送的建立网络隧道请求是以第二节点的虚拟互联网协议地址发送的。

[0128] 转发控制单元 510，用于接收第一节点发送给第二节点的信息，并转发给第二节点，以及接收第二节点发送给所述第一节点的信息，并转发给第一节点。

[0129] 本发明实施例提供的虚拟专用网节点信息的处理设备可以对节点的注册信息进行集中登记，避免了在 VPN 网络的每一个节点上配置其它节点的注册信息，当加入一个节点时，只需对加入的节点的注册信息进行登记即可，无需调整其它节点的配置，从而使得 VPN 网络可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

[0130] 实施例四：

[0131] 请参阅图 8，图 8 为本发明实施例四提供的一种虚拟专用网节点设备的结构图。本发明实施例提供的虚拟专用网节点设备包括但不限于移动手机，掌上电脑，个人电脑，服务器以及网关等等。如图 8 所示，该虚拟专用网节点设备可以包括：

[0132] 获取单元 801，用于获取自身的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息；

[0133] 发送单元 802，用于将自身的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息放入接入请求消息后，发送给虚拟专用网节点信息的处理设备。

[0134] 本实施例中所述的虚拟专用网节点信息的处理设备与上述实施例三介绍的虚拟专用网节点信息的处理设备的结构和功能完成相同，本实施例在此不再复述。

[0135] 优选地，本发明实施例的虚拟专用网节点设备还可以包括：

[0136] 接收单元 803，用于接收虚拟专用网节点信息的处理设备发送的虚拟互联网协议地址。

[0137] 本发明实施例提供的虚拟专用网节点设备可以主动将自身的认证信息、当前真实互联网协议地址、节点名称以及是否接受外部连接信息发送给虚拟专用网节点信息的处理设备，向虚拟专用网节点信息的处理设备主动进行注册。通过虚拟专用网节点信息的处理设备的对节点设备的认证信息、当前真实互联网协议地址、节点名称以及是否接受外部连接信息集中注册的方法，避免了在虚拟专用网节点设备上配置其它节点的注册信息，并且，当加入节点时，也无需节点设备自身额外配置，从而使得 VPN 网络可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

[0138] 实施例五：

[0139] 请参阅图 9，图 9 为本发明实施例五提供的一种虚拟专用网系统的结构图。如图 9 所示，该虚拟专用网系统可以包括：

[0140] 虚拟专用网节点设备 901 和虚拟专用网节点信息的处理设备 902；其中，

[0141] 虚拟专用网节点设备 901，用于获取自身的认证信息、当前真实互联网协议地址、节点名称以及是否接受外部连接信息，并将自身的认证信息、当前真实互联网协议地址、节点名称以及是否接受外部连接信息放入接入请求消息之后，发送给虚拟专用网节点信息的处理设备 902；

[0142] 虚拟专用网节点信息的处理设备 902，用于接收虚拟专用网节点设备 901 发送的接入请求消息，该接入请求消息至少携带虚拟专用网节点设备 901 的认证信息、当前真实互联网协议地址、节点名称以及是否接受外部连接信息；当判断虚拟专用网节点设备 901 的认证信息正确时，给虚拟专用网节点设备 901 分配虚拟互联网协议地址；并将虚拟专用网节点设备 901 的当前真实互联网协议地址、节点名称、是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记。

[0143] 本发明实施例提供的虚拟专用网系统可以对节点的注册信息进行集中登记，避免了在 VPN 网络的每一个节点上配置其它节点的注册信息，当加入一个节点时，只需对加入的节点的注册信息进行登记即可，无需调整其它节点的配置，从而使得 VPN 网络可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

[0144] 实施例六：

[0145] 请参阅图 10，为本发明实施例六提供的一种虚拟专用网的示意图。如图 10 所示，虚拟专用网包括了虚拟专用网节点信息的处理设备以及名称分别为 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 的 6 个节点。其中，节点 NID-2 和 NID-4 分别处在 NAT 设备 1 和 NAT 设备 2 内。

[0146] 当虚拟专用网节点信息的处理设备接收到节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 分别发送的接入请求消息之后，如果判断节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 分别发送的接入请求消息携带的认证信息都正确的时，虚拟专用网节点信息的处理设备分别向节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 发送分配的虚拟地址；并将节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 分别发送的接入请求消息中携带的节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 的当前真实互联网协议地址，虚拟互联网协议地址，以及节点名称作为注册信息进行登记。这样节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 分别可以和虚拟专用网节点信息的处理设备之间通过建立的网络隧道连接，构成 VPN 网络内的独立节点；另外，与虚拟专用网节点信息的处理设备互联的节点也可作为一个网关，将本地局域网内的其他节点接入该 VPN 网络中，如图 10 中的节点 NID-5。

[0147] 在虚拟专用网节点信息的处理设备上登记节点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 的注册信息之后，点 NID-1，NID-2，NID-3，NID-4，NID-5，NID-6 通过网络隧道与虚拟专用网节点信息的处理设备组成一个虚拟的内部网络，该虚拟网络内部的网络拓扑结构可以为星型网络结构。

[0148] 本发明实施例提供的虚拟专用网可以对节点的注册信息进行集中登记，避免了在 VPN 网络的每一个节点上配置其它节点的注册信息，当加入一个节点时，只需对加入的节点

的注册信息进行登记即可，无需调整其它节点的配置，从而使得 VPN 网络可以支持动态变化的网络结构，提高了 VPN 网络的灵活性。

[0149] 实施例七：

[0150] 请参阅图 11，图 11 为本发明实施例七提供的一种查询节点注册信息的方法流程图。本实施例是在前述实施例进行了节点的注册信息登记的基础之上进行的。本实施例以第一节点查询第二节点的注册信息为例，介绍本发明实施例提供的查询 VPN 注册信息的方法。如图 11 所示，该方法可以包括：

[0151] 1101、第一节点通过与虚拟专用网节点信息的处理设备建立的网络隧道，向虚拟专用网节点信息的处理设备发送用于查询第二节点的注册信息的消息；

[0152] 举例来说，第一节点向虚拟专用网节点信息的处理设备发送用于查询第二节点的注册信息的消息中可以携带第二节点的节点名称和 / 或第二节点的当前真实互联网协议地址等信息。

[0153] 1102、虚拟专用网节点信息的处理设备查询已注册的所有节点的注册信息，如果查询失败，说明第二节点尚未接入 VPN 网络，虚拟专用网节点信息的处理设备向第一节点发送错误信息；

[0154] 1103、虚拟专用网节点信息的处理设备查询已注册的所有节点的注册信息，如果查询成功，说明第二节点已经连接进入 VPN 网络，虚拟专用网节点信息的处理设备将把第二节点的注册信息发送给第一节点。

[0155] 举例来说，第二节点的注册信息至少包括第二节点的是否接受外部连接的信息。

[0156] 其中，如果第二节点接受外部连接的信息，则第一节点可以根据第二节点的当前真实的互联网协议地址与第二节点建立直连通道模式下的直连网络隧道；反之，如果第二节点不接受外部连接，则第一节点可以根据第二节点的虚拟互联网协议地址与第二节点建立虚拟交换模式下的间接网络隧道。

[0157] 如果，第一节点已知第二节点的当前真实互联网协议地址和虚拟互联网协议地址，则 1103 中的虚拟专用网节点信息的处理设备发送的第二节点的注册信息可以是第二节点的是否接受外部连接的信息。

[0158] 本发明实施例中虚拟专用网节点信息的处理设备允许第一节点查询第二节点的注册信息，为了确切地获知第一节点需要查询的第二节点的注册信息，要求第一节点发送的查询消息中需要携带有用于识别第二节点的信息，由于每一个节点的名称以及当前真实互联网协议地址是不相同的，所以第一节点发送的查询消息中可以携带第二节点的名称和 / 或第二节点的当前真实互联网协议地址。当然，第一节点发送的查询消息中还可以携带其他用于识别第二节点的信息，本发明实施例在此不做限定。

[0159] 实施例八：

[0160] 请参阅图 12，图 12 为本发明实施例八提供的一种 VPN 网络节点通信方法的流程图。本实施例是在前述实施例进行了节点的注册信息登记以及节点的注册信息查询的基础之上进行的。本实施例以第一节点和第二节点进行通信为例，介绍本发明实施例提供的 VPN 网络节点通信方法。如图 12 所示，该方法可以包括：

[0161] 1201、第一节点查询到第二节点的虚拟互联网协议地址之后，构造一个发送给第二节点的“网内通信报文”并发送给第一节点的虚拟网卡；

[0162] 需要说明的是，在 VPN 网络中，每一个节点都具有一个虚拟网卡和真实网卡。其中，虚拟网卡的作用是根据虚拟互联网协议地址发送网内通信报文；真实网卡的作用是根据当前真实互联网协议地址发送网内通信报文。

[0163] 1202、第一节点的虚拟网卡将“网内通信报文”进行封装，添加虚拟专用网节点信息的处理设备的当前真实互联网协议地址，形成“封装报文 -1”，将此报文使用第一节点的当前真实互联网协议地址经由第一节点的真实网卡发送给虚拟专用网节点信息的处理设备；

[0164] 1203、虚拟专用网节点信息的处理设备接收到“封装报文 -1”后对其进行解析，获得其内部的“网内通信报文”；

[0165] 1204、虚拟专用网节点信息的处理设备将“网内通信报文”进行封装，添加第二节点的当前真实互联网协议地址，形成“封装报文 -2”，并将其通过第二节点当前所使用的网络隧道发送给第二节点；

[0166] 虚拟专用网节点信息的处理设备根据“网内通信报文”携带的第二节点的虚拟互联网协议地址，得知“网内通信报文”需要转发给第二节点；

[0167] 举例来说，虚拟专用网节点信息的处理设备还可以查询第二节点的当前真实互联网协议地址，以及第二节点当前所使用的网络隧道等信息。

[0168] 1205、第二节点在接收到“封装报文 -2”后，将通过虚拟网卡对“封装报文 -2”进行拆封，获得其内部的“网内通信报文”。

[0169] 至此，第一节点通过虚拟专用网节点信息的处理设备进行中转，与第二节点完成了一次通信。上述流程中的报文封装 / 拆封对于第一节点、第二节点中的网络应用都是透明的，网络应用会认为是在直接使用第一节点与第二 VPN 节点的虚拟 IP 地址进行通信。

[0170] 由于第一节点向第二节点发送“网内通信报文”与第二节点向第一节点发送“网内通信报文”的过程完全相同，本实施例在此不作复述。

[0171] 本发明实施例提供的虚拟专用网节点信息的处理设备可以在对节点的注册信息进行集中登记的基础之上，接收第一节点发送的信息转发给对应的第二节点，并将第二节点发送的信息转发给对应的第一节点，从而可以建立第一节点和第二节点之间的间接网络通道。

[0172] 实施例九：

[0173] 请参阅图 13，图 13 为本发明实施例九提供的一种 VPN 网络节点通信方法的流程图。本实施例是在前述实施例进行了节点的注册信息登记以及节点的注册信息查询的基础之上进行的。本实施例以第一节点和第二节点进行通信为例，介绍本发明实施例提供的 VPN 网络节点通信方法。如图 13 所示，该方法可以包括：

[0174] 1301、第一节点向虚拟专用网节点信息的处理设备查询到第二节点的虚拟互联网协议地址之后，构造一个发送给第二节点的“网内通信报文”并发送给第一节点的虚拟网卡；

[0175] 1302、第一节点的虚拟网卡将“网内通信报文”进行封装，添加第二节点的当前真实互联网协议地址，形成“封装报文”，将此报文使用第一节点的当前真实互联网协议地址经由其真实网卡发送给第二节点；

[0176] 1303、第二节点在接收到“封装报文”后，将通过第二节点的虚拟网卡对其进行解

析，获得其内部的“网内通信报文”；

[0177] 1304、第二节点将“网内通信报文”提交网络应用程序。

[0178] 至此，第一节点通过与第二节点之间直接通过当前真实互联网协议地址进行网络连接，使双方的网络应用完成了一次使用第一点与第二节点的当前真实互联网协议地址进行通信的过程。

[0179] 上述流程中的报文封装 / 拆封对于第一节点、第二节点中的网络应用都是透明的，网络应用会认为是在直接使用第一节点与第二节点的虚拟互联网协议地址进行通信。

[0180] 本发明实施例提供的虚拟专用网节点信息的处理设备可以给第一节点发送第一节点查询的第二节点的注册信息，以使第一节点和第二节点之间可以建立直连网络隧道。

[0181] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：只读存储器 (ROM，Read-Only Memory)，随机存取器 (RAM，Random-Access Memory) 磁碟或者光盘等各种可以存储程序代码的介质。

[0182] 以上对本发明实施例所提供的一种虚拟专用网节点信息的处理方法及相关设备、系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

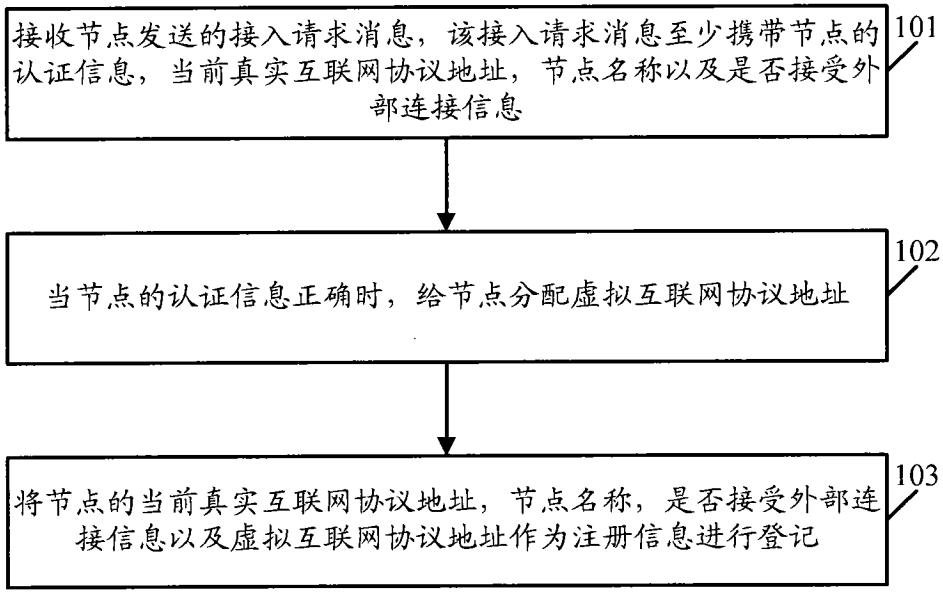

接收节点发送的接入请求消息，该接入请求消息至少携带节点的认证信息，当前真实互联网协议地址，节点名称以及是否接受外部连接信息
101
当节点的认证信息正确时，给节点分配虚拟互联网协议地址
102
将节点的当前真实互联网协议地址，节点名称，是否接受外部连接信息以及虚拟互联网协议地址作为注册信息进行登记
103

图 1

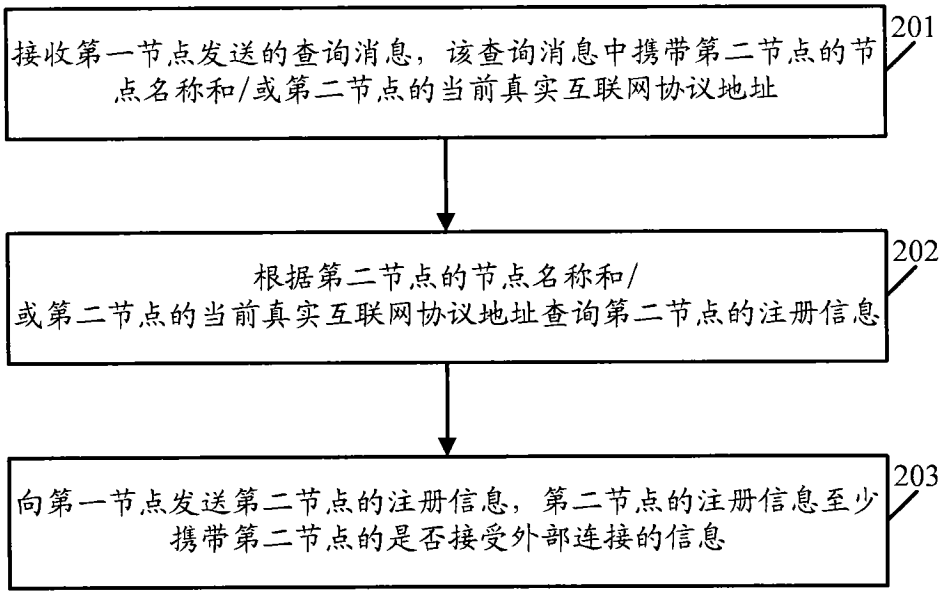

接收第一节点发送的查询消息，该查询消息中携带第二节点的节点名称和/或第二节点的当前真实互联网协议地址
201
根据第二节点的节点名称和/
或第二节点的当前真实互联网协议地址查询第二节点的注册信息
202
向第一节点发送第二节点的注册信息，第二节点的注册信息至少携带第二节点的是否接受外部连接的信息
203

图 2

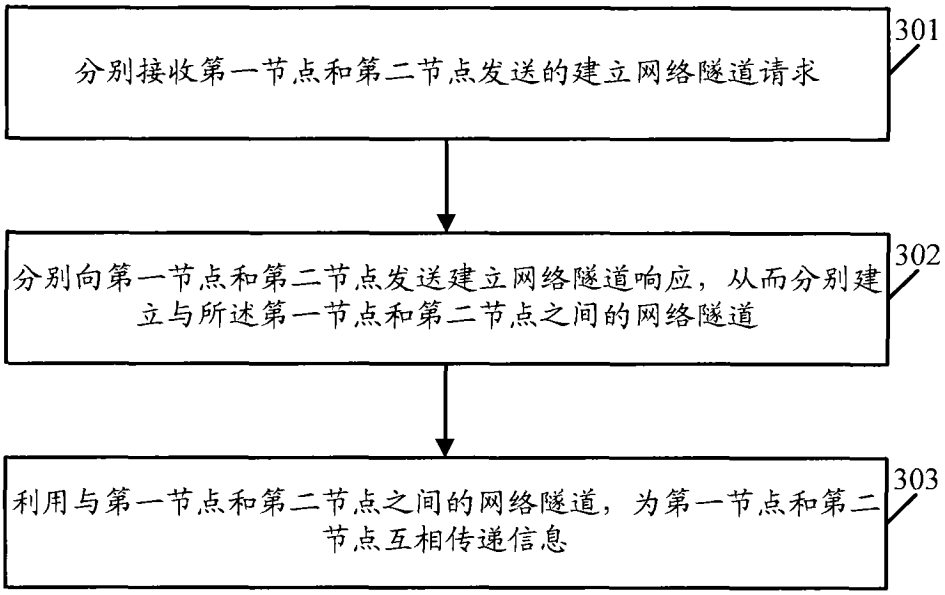

分别接收第一节点和第二节点发送的建立网络隧道请求
301
分别向第一节点和第二节点发送建立网络隧道响应，从而分别建立与所述第一节点和第二节点之间的网络隧道
302
利用与第一节点和第二节点之间的网络隧道，为第一节点和第二节点互相传递信息
303

图 3

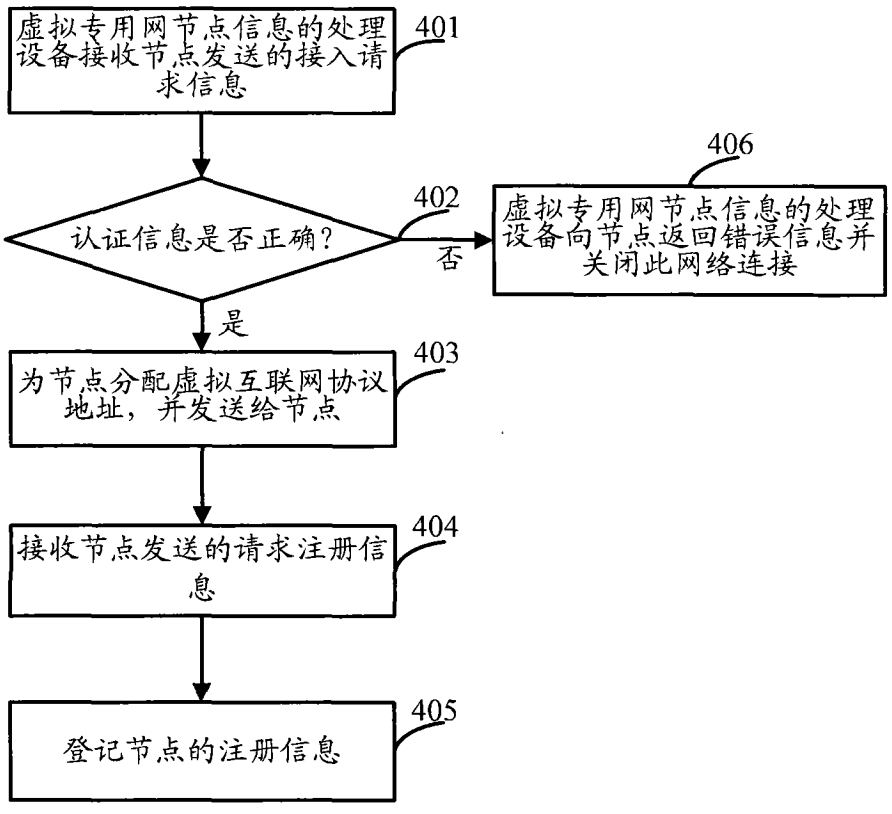

虚拟专用网节点信息的处理设备接收节点发送的接入请求信息
401
认证信息是否正确？
402
否
406
虚拟专用网节点信息的处理设备向节点返回错误信息并关闭此网络连接
是
为节点分配虚拟互联网协议地址，并发送给节点
403
接收节点发送的请求注册信息
404
登记节点的注册信息
405

图 4

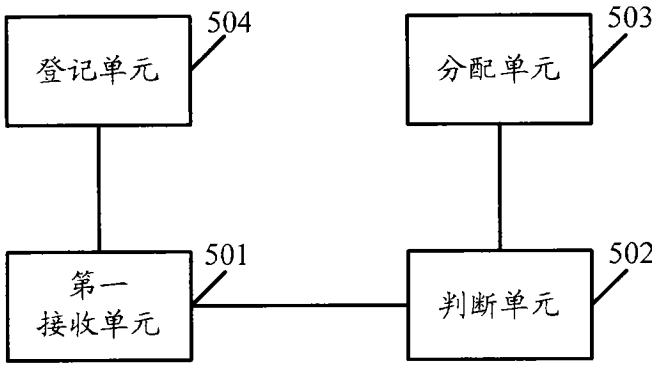

登记单元
504
分配单元
503
第一
接收单元
501
判断单元
502

图 5

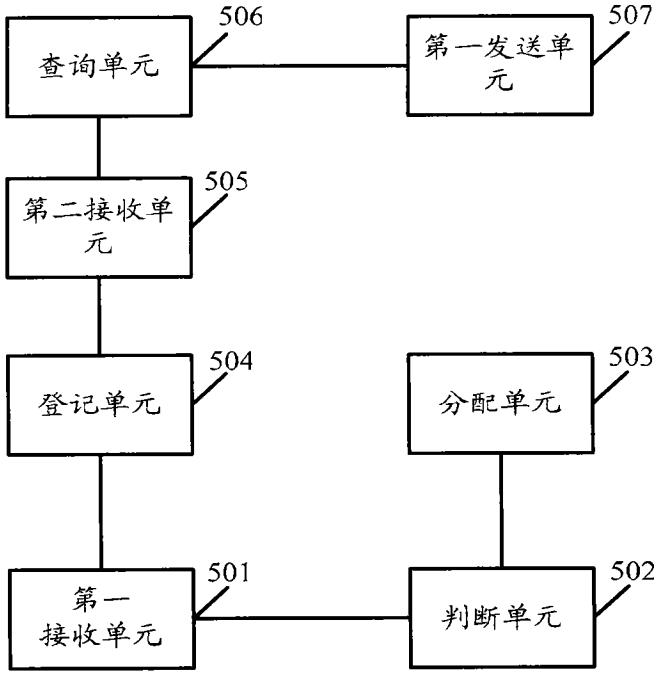

查询单元
506
第一发送单
元
507
第二接收单
元
505
登记单元
504
分配单元
503
第一
接收单元
501
判断单元
502

图 6

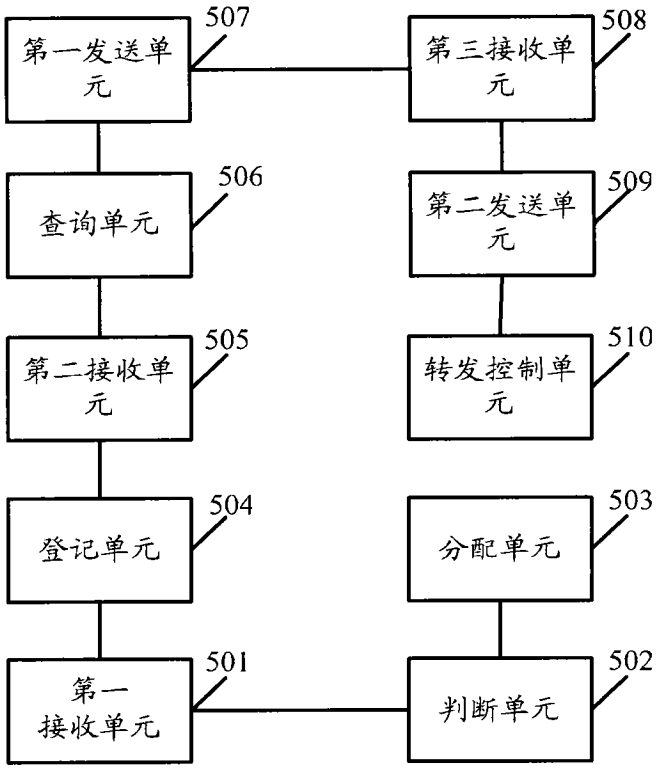

第一发送单元
507
第三接收单元
508
查询单元
506
第二发送单元
509
第二接收单元
505
转发控制单元
510
登记单元
504
分配单元
503
第一接收单元
501
判断单元
502

图 7

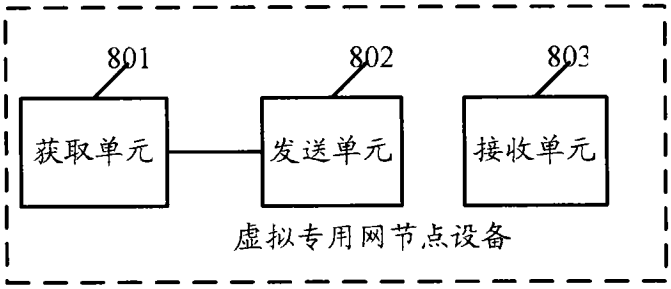

801
802
803
获取单元
发送单元
接收单元
虚拟专用网节点设备

图 8

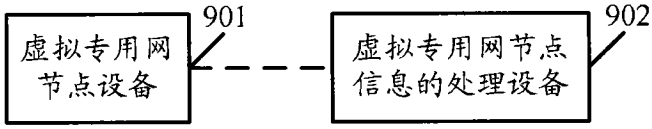

虚拟专用网节点设备
901
虚拟专用网节点信息的处理设备
902

图 9

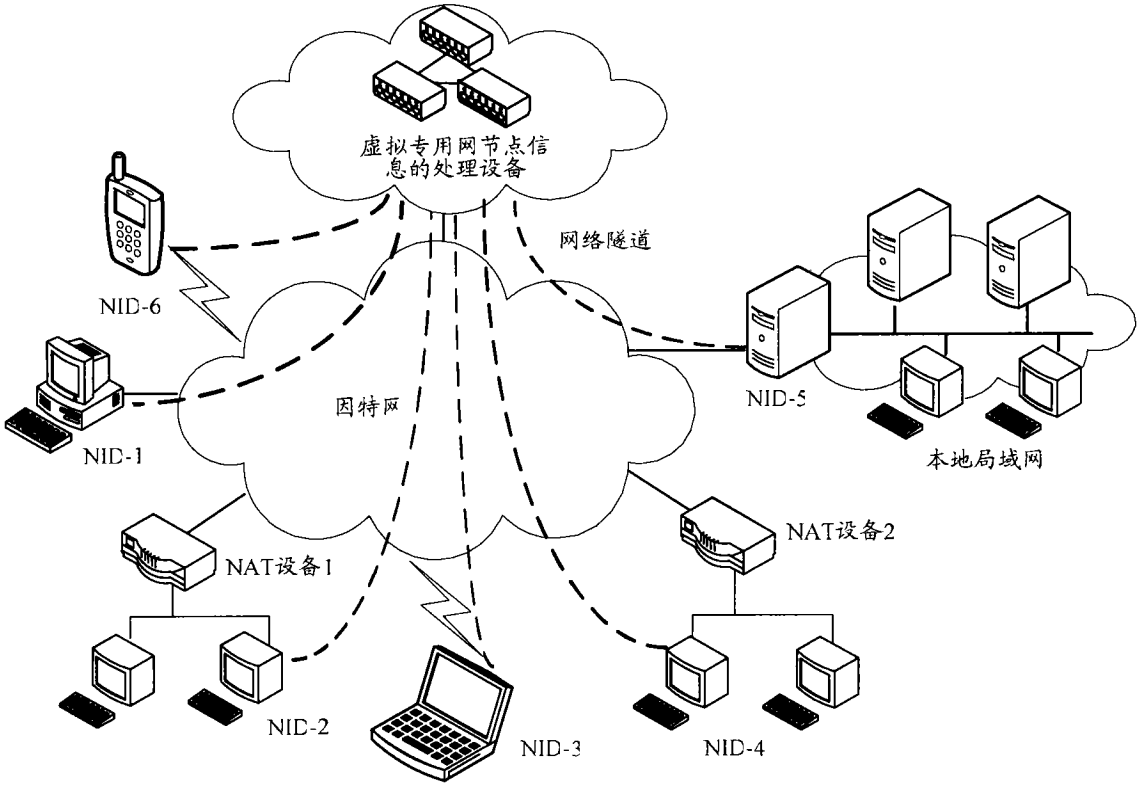

虚拟专用网节点信息的处理设备
网络隧道
NID-6
因特网
NID-5
NID-1
本地局域网
NAT设备2
NAT设备1
NID-2
NID-3
NID-4

图 10

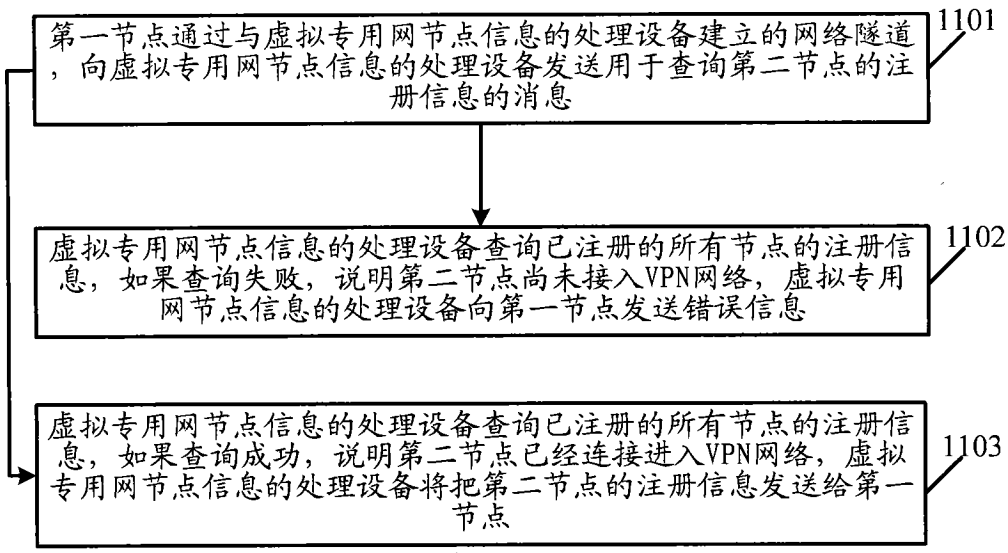

第一节点通过与虚拟专用网节点信息的处理设备建立的网络隧道，向虚拟专用网节点信息的处理设备发送用于查询第二节点的注册信息的消息
1101
虚拟专用网节点信息的处理设备查询已注册的所有节点的注册信息，如果查询失败，说明第二节点尚未接入VPN网络，虚拟专用网节点信息的处理设备向第一节点发送错误信息
1102
虚拟专用网节点信息的处理设备查询已注册的所有节点的注册信息，如果查询成功，说明第二节点已经连接进入VPN网络，虚拟专用网节点信息的处理设备将把第二节点的注册信息发送给第一节点
1103

图 11

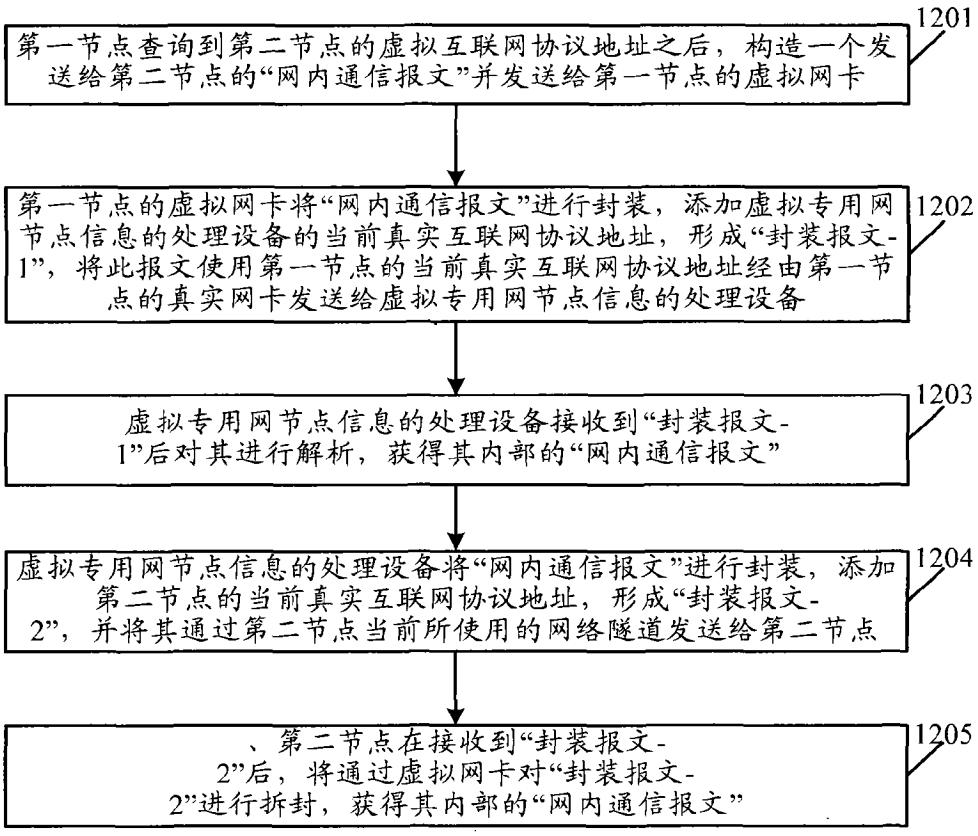

第一节点查询到第二节点的虚拟互联网协议地址之后，构造一个发送给第二节点的“网内通信报文”并发送给第一节点的虚拟网卡
1201
第一节点的虚拟网卡将“网内通信报文”进行封装，添加虚拟专用网节点信息的处理设备的当前真实互联网协议地址，形成“封装报文-1”，将此报文使用第一节点的当前真实互联网协议地址经由第一节点的真实网卡发送给虚拟专用网节点信息的处理设备
1202
虚拟专用网节点信息的处理设备接收到“封装报文-1”后对其进行解析，获得其内部的“网内通信报文”
1203
虚拟专用网节点信息的处理设备将“网内通信报文”进行封装，添加第二节点的当前真实互联网协议地址，形成“封装报文-2”，并将其通过第二节点当前所使用的网络隧道发送给第二节点
1204
、第二节点在接收到“封装报文-2”后，将通过虚拟网卡对“封装报文-2”进行拆封，获得其内部的“网内通信报文”
1205

图 12

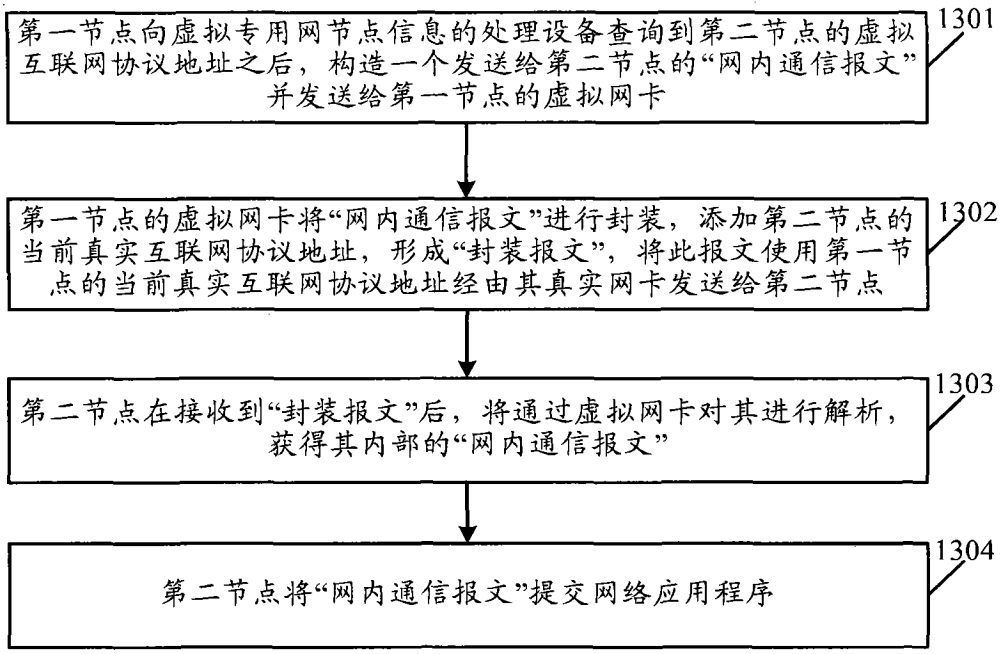

第一节点向虚拟专用网节点信息的处理设备查询到第二节点的虚拟互联网协议地址之后，构造一个发送给第二节点的“网内通信报文”并发送给第一节点的虚拟网卡
1301
第一节点的虚拟网卡将“网内通信报文”进行封装，添加第二节点的当前真实互联网协议地址，形成“封装报文”，将此报文使用第一节点的当前真实互联网协议地址经由其真实网卡发送给第二节点
1302
第二节点在接收到“封装报文”后，将通过虚拟网卡对其进行解析，获得其内部的“网内通信报文”
1303
第二节点将“网内通信报文”提交网络应用程序
1304

图 13