(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 107819888 B
(45)授权公告日 2020.03.31

(21)申请号 201610825244.2

(22)申请日 2016.09.14

(65)同一申请的已公布的文献号
申请公布号 CN 107819888 A

(43)申请公布日 2018.03.20

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 王建军 王晓波 王宏磊 刘骥刚

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲

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

(56)对比文件
CN 104426656 A,2015.03.18,
CN 103248472 A,2013.08.14,
CN 1949762 A,2007.04.18,
CN 102883076 A,2013.01.16,
US 2013145464 A1,2013.06.06,
CN 104426656 A,2015.03.18,

审查员 曹荣珍

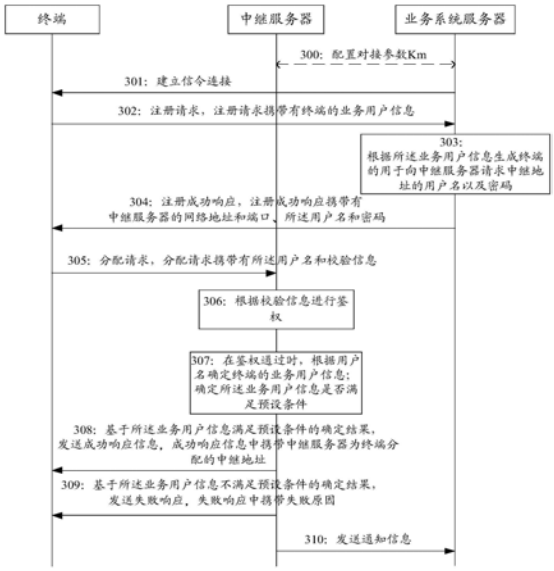
权利要求书3页 说明书12页 附图4页

(54)发明名称

一种分配中继地址的方法、装置以及网元

(57)摘要

一种分配中继地址的方法、装置以及网元，该方法包括：中继服务器接收终端发送的分配请求，分配请求中携带终端的用于向中继服务器请求中继地址的用户名和校验信息；其中，所述用户名与终端的用于向业务系统服务器请求注册的业务用户信息相关；中继服务器根据校验信息对所述用户名进行鉴权；在鉴权通过时，中继服务器根据所述用户名确定所述业务用户信息；中继服务器确定所述业务用户信息是否满足预设条件；中继服务器基于所述业务用户信息满足所述预设条件的确定结果，向终端发送成功响应信息，成功响应信息中携带中继服务器为终端分配的中继地址。通过该方法，可以提高网络的安全性。



CN 107819888 B

1.一种分配中继地址的方法,其特征在于,包括:

中继服务器接收终端发送的分配请求,所述分配请求中携带所述终端的用于向所述中继服务器请求中继地址的用户名和校验信息;其中,所述用户名与所述终端的用于向业务系统服务器请求注册的业务用户信息相关;

所述中继服务器根据所述校验信息对所述用户名进行鉴权;

在鉴权通过时,所述中继服务器根据所述用户名确定所述业务用户信息;

所述中继服务器确定所述业务用户信息是否满足预设条件;

所述中继服务器基于所述业务用户信息满足所述预设条件的确定结果,向所述终端发送成功响应信息,所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。

2.如权利要求1所述的方法,其特征在于,所述中继服务器确定所述业务用户信息是否满足预设条件,包括:

所述中继服务器确定所述业务用户信息已获得的总资源数;

所述中继服务器确定所述总资源数未超过所述业务用户信息的预设的最大资源数。

3.如权利要求1或2所述的方法,其特征在于,所述方法还包括:

所述中继服务器基于所述业务用户信息不满足所述预设条件的确定结果,向所述终端发送失败响应,所述失败响应中携带失败原因。

4.如权利要求3所述的方法,其特征在于,在所述中继服务器向所述终端发送失败响应后,所述方法还包括:

所述中继服务器接收到所述终端多次发送的分配请求,以请求分配中继地址;

所述中继服务器将所述业务用户信息加入黑名单并拒绝提供服务。

5.如权利要求3所述的方法,其特征在于,在所述中继服务器向所述终端发送失败响应后,所述方法还包括:

所述中继服务器向所述业务系统服务器发送通知信息,以通知所述系统业务服务器所述业务用户信息对应的用户异常。

6.一种分配中继地址的方法,其特征在于,包括:

业务系统服务器接收终端发送的注册请求,所述注册请求携带所述终端的业务用户信息;

所述业务系统服务器根据所述业务用户信息生成所述终端的用于向中继服务器请求中继地址的用户名;其中,所述用户名用于所述中继服务器根据所述用户名确定所述业务用户信息,并在确定所述业务用户信息满足预设条件时向所述终端分配中继地址;

所述业务系统服务器向所述终端发送注册成功响应,所述注册成功响应中携带所述中继服务器的网络地址和端口、所述用户名。

7.如权利要求6所述的方法,其特征在于,所述方法还包括:

所述业务系统服务器接收所述中继服务器发送的通知信息,所述通知信息中包括所述业务用户信息;

所述业务系统服务器将所述业务用户信息对应的用户加入黑名单并拒绝提供服务,或,所述业务系统服务器为所述用户重新生成用于向所述中继服务器请求中继地址的用户名并将重新生成的用户名发送给所述终端。

8.一种分配中继地址的装置,其特征在于,包括:

接收单元，用于接收终端发送的分配请求，所述分配请求中携带所述终端的用于向中继服务器请求中继地址的用户名和校验信息；其中，所述用户名与所述终端的用于向业务系统服务器请求注册的业务用户信息相关；

处理单元，用于根据所述校验信息对所述用户名进行鉴权；在鉴权通过时，根据所述用户名确定所述业务用户信息；所述中继服务器确定所述业务用户信息是否满足预设条件；

发送单元，用于基于所述业务用户信息满足所述预设条件的确定结果，向所述终端发送成功响应信息，所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。

9.如权利要求8所述的装置，其特征在于，所述处理单元用于：确定所述业务用户信息已获得的总资源数；确定所述总资源数未超过所述业务用户信息的预设的最大资源数。

10.如权利要求8或9所述的装置，其特征在于，所述发送单元还用于：基于所述业务用户信息不满足所述预设条件的确定结果，向所述终端发送失败响应，所述失败响应中携带失败原因。

11.如权利要求10所述的装置，其特征在于，所述接收单元还用于：在所述发送单元向所述终端发送失败响应后，接收到所述终端多次发送的分配请求，以请求分配中继地址；

所述处理单元还用于：将所述业务用户信息加入黑名单并拒绝提供服务。

12.如权利要求10所述的装置，其特征在于，所述发送单元还用于：在向所述终端发送失败响应后，向所述业务系统服务器发送通知信息，以通知所述系统业务服务器所述业务用户信息对应的用户异常。

13.一种分配中继地址的装置，其特征在于，包括：

接收单元，用于接收终端发送的注册请求，所述注册请求携带所述终端的业务用户信息；

处理单元，用于根据所述业务用户信息生成所述终端的用于向中继服务器请求中继地址的用户名；其中，所述用户名用于所述中继服务器根据所述用户名确定所述业务用户信息，并在确定所述业务用户信息满足预设条件时向所述终端分配中继地址；

发送单元，用于向所述终端发送注册成功响应，所述注册成功响应中携带所述中继服务器的网络地址和端口、所述用户名。

14.如权利要求13所述的装置，其特征在于，所述接收单元还用于：接收所述中继服务器发送的通知信息，所述通知信息中包括所述业务用户信息；

所述处理单元还用于将所述业务用户信息对应的用户加入黑名单并拒绝提供服务，或，为所述用户重新生成用于向所述中继服务器请求中继地址的用户名并将重新生成的用户名通过所述发送单元发送给所述终端。

15.一种网元，其特征在于，包括：

存储器，用于存储计算机可执行程序代码；

接收器，

发送器，以及

处理器，与所述存储器、所述接收器和所述发送器耦合；

其中所述程序代码包括指令，当所述处理器执行所述指令时，所述指令使所述网元执行以下操作：通过所述接收器接收终端发送的分配请求，所述分配请求中携带所述终端的用于向所述网元请求中继地址的用户名和校验信息；其中，所述用户名与所述终端的用于

向业务系统服务器请求注册的业务用户信息相关;根据所述校验信息对所述用户名进行鉴权;在鉴权通过时,根据所述用户名确定所述业务用户信息;确定所述业务用户信息是否满足预设条件;基于所述业务用户信息满足所述预设条件的确定结果,通过所述发送器向所述终端发送成功响应信息,所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。

16.一种网元,其特征在于,包括:

存储器,用于存储计算机可执行程序代码;

接收器,

发送器,以及

处理器,与所述存储器、所述接收器和所述发送器耦合;

其中所述程序代码包括指令,当所述处理器执行所述指令时,所述指令使所述网元执行以下操作:通过所述接收器接收终端发送的注册请求,所述注册请求携带所述终端的业务用户信息;根据所述业务用户信息生成所述终端的用于向中继服务器请求中继地址的用户名,所述用户名用于所述中继服务器根据所述用户名确定所述业务用户信息,并在确定所述业务用户信息满足预设条件时向所述终端分配中继地址;通过所述发送器向所述终端发送注册成功响应,所述注册成功响应中携带所述中继服务器的网络地址和端口、所述用户名。

一种分配中继地址的方法、装置以及网元

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种分配中继地址的方法、装置以及网元。

背景技术

[0002] 在现有技术中，多种业务系统中均部署了使用中继方式穿越网络地址转换(英文：Traversal Using Relays around NAT(英文:Network Address Translation)，简称：TURN)服务器，例如物联网(英文:Internet of Things，简称:IoT)业务系统、网页实时通信(英文:Web Real-Time Communication，简称:WebRTC)业务系统。

[0003] TURN服务器是用来实现防火墙和/或NAT穿越的网元。

[0004] TURN服务器使用中转的方式实现位于两个不同NAT网元后的客户端通信。TURN服务器会为每个连接到该服务器的客户端都分配一个中继地址，该中继地址专用于该客户端的消息中转。

[0005] 在现有技术中，TURN服务器为客户端分配中继地址的流程如下：在客户端与业务系统建立信令连接后，客户端会向业务系统发送注册请求，注册请求中携带业务用户名userX。业务系统在接收到注册请求后，为该客户端生成一个TURN用户名和密码，该TURN用户名由随机数加一个有效期组成，密码由事先配置的对接参数、TURN用户名加密生成。然后业务系统发送注册成功响应给客户端，注册成功响应中携带TURN服务器的网络地址和端口，以及TURN用户名和密码。

[0006] 接下来，客户端向TURN服务器发起分配请求，该分配请求中携带TURN用户名和消息完整性校验值，该消息完整性校验值由消息内容和TURN密码计算得到。然后TURN根据分配请求中的TURN用户名和本地配置的对接参数，通过相同的加密算法，重新计算出TURN密码，并通过重新计算出的TURN密码和消息内容重新计算出新的消息完整性校验值。TURN服务器验证分配请求中的消息完整性校验值和新的消息完整性校验值是否一致，以及有效期是否超出，若两个消息完整性校验值一致且有效期未超出，则鉴权通过，否则鉴权失败。若鉴权通过，TURN服务器向客户端发送分配的中继地址。

[0007] 然而，在现有技术的分配中继地址的方法中，若某个客户端的TURN用户名和密码泄露或被恶意使用，反复发起分配请求，TURN服务器的分配资源将被快速耗尽。因此，现有技术中的分配中继地址的方法，存在安全漏洞，安全性较低。

发明内容

[0008] 本发明提供一种分配中继地址的方法、装置以及网元，用以解决现有技术中分配中继地址的方法的安全性较低的技术问题。

[0009] 第一方面，本发明实施例提供一种分配中继地址的方法。该方法从中继服务器的角度进行描述。在该方法中，中继服务器接收终端发送的分配请求，所述分配请求中携带所述终端的用于向所述中继服务器请求中继地址的用户名和校验信息；其中，所述用户名与

所述终端的用于向业务系统服务器请求注册的业务用户信息相关。中继服务器在接收到分配请求后，根据所述校验信息对所述用户名进行鉴权。在鉴权通过时，中继服务器根据所述用户名确定所述业务用户信息。然后中继服务器确定所述业务用户信息是否满足预设条件；并基于所述业务用户信息满足所述预设条件的确定结果，向所述终端发送成功响应信息，所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。因为中继服务器因为会根据业务用户信息来判定是否进行中继地址的分配，所以不会随意分配中继地址，所以不会出现因为用户名和密码泄露而造成的中继服务器的资源被快速耗尽的情况。因此，在本发明实施例的分配中继地址的方法中，现有的安全漏洞得以弥补，提高了系统安全性。

[0010] 在一个可能的设计中，中继服务器确定所述业务用户信息是否满足预设条件，包括：中继服务器确定所述业务用户信息已获得的总资源数。然后中继服务器确定所述总资源数未超过所述业务用户信息的预设的最大资源数。因为每个业务系统的用户对中继地址的数量的需求是不同的，所以可以通过已获得的资源数控制是否继续分配中继地址，所以通过该方法可以较精确的控制中继地址的分配，既能保证每个用户的资源够用又能防止资源被恶意消耗。

[0011] 在一个可能的设计中，所述中继服务器基于所述业务用户信息不满足所述预设条件的确定结果，向所述终端发送失败响应，所述失败响应中携带失败原因。通过该方法告知终端申请中继地址失败的原因，使得用户可以及时采取相应的措施进行应对，避免影响业务的正常进行。

[0012] 在一个可能的设计中，在所述中继服务器向所述终端发送失败响应后，所述中继服务器接收到所述终端多次发送的分配请求，以请求分配中继地址。那么中继服务器将所述业务用户信息加入黑名单并拒绝提供服务。通过该方法可以识别被恶意攻击的情况，并在被攻击的情况下，及时停止中继地址的分配，减少资源的恶意消耗。

[0013] 在一个可能的设计中，在所述中继服务器向所述终端发送失败响应后，中继服务器向所述业务系统服务器发送通知信息，以通知所述系统业务服务器所述业务用户信息对应的用户异常。通过该方法可以及时告知业务系统异常的用户，使得业务系统服务器及时采取相应的应对措施，阻止继续被恶意攻击。

[0014] 第二方面，本发明实施例提供一种分配中继地址的方法。该方法从业务系统服务器的角度进行描述。在该方法中，业务系统服务器接收终端发送的注册请求，所述注册请求携带所述终端的业务用户信息。业务系统服务器在接收到所述注册请求周，根据所述业务用户信息生成所述终端的用于向中继服务器请求中继地址的用户名。然后业务系统服务器向所述终端发送注册成功响应，所述注册成功响应中携带所述中继服务器的网络地址和端口、所述用户名。因为业务系统服务器在为终端生成用户名时，就是根据终端的业务用户信息生成的，所以便于在终端向中继服务器申请中继地址时，中继服务器根据用户名确定业务用户信息，并根据业务用户信息判断是否给所述终端分配中继地址。

[0015] 在一个可能的设计中，业务系统服务器还接收所述中继服务器发送的通知信息，所述通知信息中包括所述业务用户信息。业务系统服务器在接收到通知信息后，将所述业务用户信息对应的用户加入黑名单并拒绝提供服务，或，业务系统服务器为所述用户重新生成用于向所述中继服务器请求中继地址的用户名并将重新生成的用户名发送给所述终

端。通过该方法，业务系统服务器可以及时采取相应的措施，阻止恶意攻击的情况继续发生。

[0016] 第三方面，本发明实施例提供一种分配中继地址的方法。该方法从终端的角度进行描述。在该方法中，终端向业务系统服务器发送注册请求，所述注册请求携带所述终端的业务用户信息。然后终端接收所述业务系统服务器返回的注册成功响应，所述注册成功响应消息中携带中继服务器的网络地址和端口、用户名，所述用户名用于在所述中继服务器进行中继地址分配，所述用户名与所述业务用户信息相关。通过该方法，终端可以获取到与业务用户信息相关的用户名。

[0017] 在一个可能的设计中，终端设备向所述中继服务器发送分配请求，所述分配请求中携带所述用户名和校验信息。然后终端设备接收所述中继服务器发送的成功响应信息，所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。通过该方法，因为在请求分配中继地址时，使用的用户名与业务用户信息相关，所以便于中继服务器通过用户名确定业务用户信息，进而通过业务用户信息判定是否分配中继地址。

[0018] 第四方面，本发明实施例提供一种分配中继地址的装置。具体的，该装置可以为中继服务器。该装置具有实现上述方法设计中中继服务器的功能。这些功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的单元。

[0019] 在一个可能的设计中，作为中继服务器的分配中继地址的装置的具体结构可包括接收单元、处理单元以及发送单元。接收单元、处理单元以及发送单元可执行上述方法中的相应功能。

[0020] 第五方面，本发明实施例提供一种分配中继地址的装置。具体的，该装置可以为业务系统服务器。该装置具有实现上述方法设计中业务系统服务器的功能。这些功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的单元。

[0021] 在一个可能的设计中，作为业务系统服务器的分配中继地址的装置的具体结构可包括接收单元、处理单元以及发送单元。接收单元、处理单元以及发送单元可执行上述方法中的相应功能。

[0022] 第六方面，本发明实施例提供一种分配中继地址的装置，具体的，该装置可以为终端。该装置具有实现上述方法设计中终端的功能。这些功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的单元。

[0023] 在一个可能的设计中，作为业务请求设备的分配中继地址的装置的具体结构可包括发送单元以及接收单元。接收单元以及发送单元可执行上述方法中的相应功能。

[0024] 第七方面，本发明实施例提供一种网元。该网元可以为中继服务器。该网元包括：存储器，用于存储计算机可执行程序代码；接收器，发送器，以及处理器，与所述存储器、所述接收器和所述发送器耦合；其中所述程序代码包括指令，当所述处理器执行所述指令时，所述指令使所述网元执行上述中继服务器执行的方法。

[0025] 第八方面，本发明实施例提供一种网元。该网元可以为业务系统服务器。该网元包括：存储器，用于存储计算机可执行程序代码；接收器，发送器，以及处理器，与所述存储器、所述接收器和所述发送器耦合；其中所述程序代码包括指令，当所述处理器执行所述指令

时，所述指令使所述网元执行上述业务系统服务器执行的方法。

[0026] 第九方面，本发明实施例提供一种网元。该网元可以为终端，包括：存储器，用于存储计算机可执行程序代码；接收器，发送器，以及处理器，与所述存储器、所述接收器和所述发送器耦合；其中所述程序代码包括指令，当所述处理器执行所述指令时，所述指令使所述网元执行上述终端执行的方法。

[0027] 第十方面，本发明实施例提供一种计算机存储介质，用于存储为上述第四方面所描述的分配中继地址的装置或第七方面所描述的网元所用的计算机软件指令，并包含用于执行上述方面所设计的程序。

[0028] 第十一方面，本发明实施例提供一种计算机存储介质，用于存储为上述第五方面所描述的分配中继地址的装置或第八方面所描述的网元所用的计算机软件指令，并包含用于执行上述方面所设计的程序。

[0029] 第十二方面，本发明实施例提供一种计算机存储介质，用于存储为上述第六方面所描述的分配中继地址的装置或第九方面所描述的网元所用的计算机软件指令，并包含用于执行上述方面所设计的程序。

附图说明

[0030] 图1为本发明实施例提供的一种网络系统的架构图；

[0031] 图2为本发明实施例提供的一种网元的结构图；

[0032] 图3为本发明实施例提供的一种分配中继地址的方法的流程图；

[0033] 图4为本发明实施例提供的一种数据转发方法的流程图；

[0034] 图5为本发明实施例提供的第一种分配中继地址的装置的功能框图；

[0035] 图6为本发明实施例提供的第二种分配中继地址的装置的功能框图。

具体实施方式

[0036] 本发明提供一种分配中继地址的方法、装置以及网元，用以解决现有技术中分配中继地址的方法的安全性较低的技术问题。

[0037] 下面将结合本发明实施例中的附图，本发明实施例中的技术方案进行描述。

[0038] 本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0039] 为便于说明本发明实施例中的分配中继地址的方法，下面先介绍一种网络系统，本发明实施例中的分配中继地址的方法可以应用在该系统中。如图1所示，为本发明实施例提供的一种网络系统的结构图，本发明实施例基于现有的网络系统，在终端向业务系统服务器注册时，业务系统服务器根据终端的业务用户信息，为终端生成用于向中继服务器请求中继地址的用户名。然后终端向中继服务器发起分配请求时，携带该用户名，中继服务器能够根据该用户名获取到终端的业务用户信息，并判断该业务用户信息是否满足预设条件，只有在业务用户信息满足预设条件时，才会为该业务用户信息对应的终端分配中继地址。通过该方法，可以避免中继服务器仅通过校验信息进行鉴权，在鉴权通过时，就会无条件的分配中继地址的情况，所以在某个终端的用户名和密码泄露或被恶意使用，反复发起

分配请求时，中继服务器因为会根据业务用户信息来判定，所以不会随意分配中继地址，所以不会出现因为用户名和密码泄露而造成的中继服务器的资源被快速耗尽的情况。因此，在本发明实施例的网络系统中，现有的安全漏洞得以弥补，提高了系统安全性。

[0040] 具体的，为实现本发明的目的，本发明实施例提供的一个结构图包括以下功能部件：

[0041] 终端，能够支持TURN客户端的所有设备，或者，软件和/或硬件，需要向中继服务器申请中继地址。

[0042] 业务系统服务器，用于业务系统用户权限管理的服务器，每个终端需要向业务系统服务器申请用于向中继服务器请求中继地址的用户名和密码。

[0043] 中继服务器，负责对终端的分配请求进行鉴权，并在鉴权通过，以及业务用户信息满足预设条件时，为终端分配中继地址；然后利用为终端分配的中继地址为终端进行数据转发。

[0044] 在实际运用中，图1所示的业务系统可以是物联网(英文：Internet of Things，简称：IoT)系统，也可以是网页实时通信系统，对应的，业务系统服务器可以是IoT系统服务器，也可以是WebRTC系统服务器；终端也可以是IoT系统的客户端，终端也可以是WebRTC系统的客户端。当然，在实际应用中，业务系统和终端也可以是其它业务系统和终端，本发明不作具体限定。

[0045] 中继服务器例如为TURN服务器，在实际运用中，也可以是其它与TURN服务器工作原理相同的中继服务器。

[0046] 图2显示了本发明实施例中的一种网元的结构示意图。这一网元例如为图1中的通信系统中的一个部件，例如终端、中继服务器、业务系统服务器。如图2所示，该通信设备包括：处理器10、发送器20、接收器30、存储器40。存储器40、发送器20和接收器30和处理器10可以通过总线进行连接。当然，在实际运用中，存储器40、发送器20和接收器30和处理器10之间可以不是总线结构，而可以是其它结构，例如星型结构，本申请不作具体限定。

[0047] 可选的，处理器10具体可以是通用的中央处理器或特定应用集成电路(英文：Application Specific Integrated Circuit，简称：ASIC)，可以是一个或多个用于控制程序执行的集成电路，可以是使用现场可编程门阵列(英文：Field Programmable Gate Array，简称：FPGA)开发的硬件电路，可以是基带处理器。

[0048] 可选的，处理器10可以包括至少一个处理核心。

[0049] 可选的，存储器40可以包括只读存储器(英文：Read Only Memory，简称：ROM)、随机存取存储器(英文：Random Access Memory，简称：RAM)和磁盘存储器中的一种或多种。存储器40用于存储处理器10运行时所需的数据和/或指令。存储器40的数量可以为一个或多个。

[0050] 在图1所示的架构中，中继服务器可以为每个业务系统的用户预设一个最大资源数，即中继服务器可以为每个业务系统的每个用户分配的中继地址的数量的最大值。通常来讲，每个业务系统不同，需求的资源数也可以不相同，所以中继服务器可以根据每个业务系统的实际需求为每个业务系统中配置不同的最大资源数，对于同一业务系统中的所有用户而言，每个用户的最大资源数即为该业务系统的最大资源数。例如为IoT业务系统配置的最大资源数为10个，那么IoT业务系统中的用户X和用户Y的最大资源数均为10个。再例如为

WebRTC业务系统配置的最大资源数为15个，那么WebRTC业务系统的用户M和用户N的最大资源数均为15个。

[0051] 需要说明的是，物理上为一个单独的中继服务器，即可以对接一个业务系统，也可以对接多个业务系统。在对接多个业务系统的情况下，中继服务器可以设计为多个相互独立的逻辑模块，每个逻辑模块对接一个业务系统，所以每个逻辑模块可以单独为对接的业务系统设置最大资源数。若多个业务系统对接的为同一个逻辑模块，即中继服务器被设计为一个逻辑模块，但可以对接多个业务系统，那么该逻辑模块可以为每个业务系统配置不同的最大资源数，并且该逻辑模块可以识别用户属于哪个业务系统。

[0052] 接下来，请同时参考图3所示，图3为本发明实施例提供的一种分配中继地址的方法的流程图，也可以理解为图1所示架构中各个功能部件的信息交互示意图。

[0053] 其中，步骤300：配置对接参数Km。对接参数Km因不同的业务系统而不同。对接参数Km可以作为中继服务器和业务系统服务器的共享密钥，用来进行加密运算，具体的使用方式将在后续步骤中介绍。

[0054] 作为一个例子，可以是中继服务器和业务系统服务器通过协商确定两者之间使用的对接参数Km。在实际运用中，也可以是通过其它方式在中继服务器和业务系统服务器之间配置对接参数Km，本发明不作具体限定。

[0055] 需要说明的是，在图3中，步骤300是用虚线表示的，虚线表示的含义为该步骤为可选步骤。因为对接参数Km可以是协议约定好的，也可以不使用对接参数Km，所以可以不执行步骤300。

[0056] 步骤301：业务系统服务器和终端之间建立信令连接。具体的，可以是终端先发起建立信令连接请求，也可以是业务系统服务器主动发起建立信令连接请求，经过二者协商之后，建立信令连接。对于不同的业务系统，建立信令连接的过程可以不同，该部分内容为本领域技术人员所熟知的内容，所以在此不再赘述。

[0057] 需要说明的是，步骤301可以周期性的执行，也可以是在终端每次重新联网时执行，也可以是在每次终端和业务系统服务器需要进行信息交互时执行。

[0058] 在建立信令连接之后，接下来可以执行步骤302：终端向业务系统服务器发送注册请求，所述注册请求携带所述终端的业务用户信息；对应的，业务系统服务器接收终端发送的注册请求。

[0059] 具体的，业务用户信息可以是终端在业务系统中的账号、用户名或昵称，或者是其它可以唯一识别终端上运行的某个业务系统的客户端的用户信息。

[0060] 可选的，业务系统服务器在接收到终端发送的注册请求之后，还对业务用户信息进行鉴权，例如判断是否为合法用户。在鉴权通过后，执行步骤303。当然，在实际运用中，也可以不对业务用户信息进行鉴权就直接执行步骤303。

[0061] 步骤303：业务系统服务器根据所述业务用户信息生成终端的用于向中继服务器请求中继地址的用户名以及密码。

[0062] 作为一个例子，业务系统服务器可以使用对接参数Km作为密钥的可逆加密算法对业务用户信息进行加密得到用于在中继服务器请求分配中继地址的用户名。可逆加密算法例如为高级加密标准(英文：Advanced Encryption Standard，简称：AES)。当然，在实际运用中，也可以采用其它可逆加密算法，本发明不作具体限定。

[0063] 可选的，业务系统服务器还可以根据当前系统时间加上有效时长生成一个有效期，然后将有效期也作为用户名的一部分。换言之，用户名既包括对业务用户信息加密生成的字符串，也包括有效期的字符串。

[0064] 举例来说，业务用户信息为userX，通过公式AES(userX,Km)得到字符串Tid。再根据当前系统时间加上有效时长，例如5s，生成有效期Texp，则用户名为Tid:Texp。

[0065] 当然，在实际运用中，也可以是用户名包括业务用户信息和其它字符串，例如在业务用户信息之前，之后，或者前后补入其它字符串作为最终的用户名，补入的字符串可以是前述所描述的有效期。举例来说，业务用户信息为userX，有效期为2016090500，那么用户名就可以为TURNuserX2016090500。

[0066] 作为一个例子，业务系统服务器将对接参数Km和用户名作为参数，使用哈希(Hash)加密算法进行加密得到密码。举例来说，密码Tpwd＝Hash(Km,Tid:Texp)。

[0067] 当然，在实际运用中，也可以通过其它方式获得密码，本发明不作具体限定。

[0068] 在生成用户名以及密码之后，接下来执行步骤304：业务系统服务器向终端发送注册成功响应，注册成功响应中携带中继服务器的网络地址和端口、所述用户名和密码。

[0069] 具体的，中继服务器的网络地址例如为网络协议(英文：Internet Protocol，简称：IP)地址。终端可以根据中继服务器的网络地址和端口获知自己需要向哪个中继服务器和端口请求中继地址。

[0070] 在终端接收到业务系统服务器发的注册成功响应之后，就可以作为客户端向注册成功响应中携带的中继服务器的网络地址和端口发送分配请求，即执行步骤305。分配请求中携带注册成功响应中返回的用户名和校验信息。

[0071] 对应的，中继服务器接收终端发送的分配请求，所述分配请求中携带所述终端的用于向所述中继服务器请求中继地址的用户名和校验信息。

[0072] 可选的，校验信息可以是前述注册成功响应中携带的密码。

[0073] 可选的，校验信息可以是消息完整性校验值，消息完整性校验值可以通过国际互联网工程任务组(英文：The Internet Engineering Task Force，简称：IETF)一系列以编号排定的文件(英文：Request For Comments，简称：RFC)5766协议的规则计算得到，例如将分配请求中除了消息完整性校验值之外的消息内容和密码进行哈希计算，得到的值即为消息完整性校验值。

[0074] 当然，在实际运用中，校验信息还可以是其它校验信息，本发明不作具体限定。

[0075] 当中继服务器接收到终端发送的分配请求之后，执行步骤306：中继服务器根据所述校验信息对所述用户名进行鉴权。

[0076] 具体的，根据校验信息的不同，进行鉴权的方式也不同。举例来说，如果校验信息为密码，那么中继服务器就会采用与业务系统服务器计算密码相同的算法重新计算密码，例如依然采用公式Hash(Km,Tid:Texp)重新计算密码，得到新密码Tpwd1。然后对比自己计算出的密码Tpwd1与分配请求中携带的密码Tpwd，若两者一致，则表征鉴权通过；若两者不一致，则表征鉴权未通过。

[0077] 再举例来说，若校验信息为消息完整性校验值，那么中继服务器可以按照上述算法计算得到新密码Tpwd1，然后再根据相同的哈希算法，对分配请求中除了消息完整性校验值之外的消息内容和新密码Tpwd1进行哈希计算，得到新的消息完整性校验值。然后对比分

配请求中携带的消息完整性校验值和新的消息完整性校验值，若两者一致，则表征鉴权通过；若果不一致，则表征鉴权失败。

[0078] 可选的，若用户名中包含了有效期，那么还需要查看有效期是否超过当前时间，如果超过则鉴权失败，若未超过，则表征鉴权通过。

[0079] 在鉴权通过时，接下来执行步骤307：中继服务器根据所述用户名确定所述业务用户信息；中继服务器确定所述业务用户信息是否满足预设条件。

[0080] 因为用户名和业务用户信息相关，所以可以通过用户名确定出业务用户信息。通过用户名确定出业务用户信息的具体的确定方式和根据业务用户信息生成用户名时的生成方式相关。通常来讲，通过用户名确定出业务用户信息的方式与根据业务用户信息生成用户名的方式相反。举例来说，在前文描述中，可以使用对接参数Km通过可逆加密算法AES对业务用户信息，例如账号useX进行加密得到用户名或者用户名的部分字符串，例如Tid，那么在步骤307中，就可以使用对接参数Km通过可逆加密算法AES对Tid进行逆向解密计算出业务用户信息，例如账号userX。

[0081] 在确定出业务用户信息之后，中继服务器确定业务用户信息是否满足预设条件。需要说明的是，在实际运用中，预设条件可以根据实际需求设置成不同的形式，并且预设条件的设置原则为通过业务用户信息与预设条件相比较，能够确定出是否应该给该业务用户信息对应的客户端分配中继地址。因此，对于预设条件的设置可以有多种实现方式。举例来说，确定业务用户信息是否满足预设条件，可以包括：确定所述业务用户信息是否位于黑名单上。具体的，例如在网络上会有一些恶意账户，将这些恶意账户整理成黑名单，那么中继服务器就可以查询业务用户信息是否位于该黑名单上，如果业务用户信息位于该黑名单上，则表示业务用户信息不满足预设条件；反之，则表示业务用户信息满足预设条件。

[0082] 再举例来说，中继服务器确定所述业务用户信息是否满足预设条件，包括：中继服务器确定所述业务用户信息已获得的总资源数；中继服务器确定所述总资源数未超过所述业务用户信息的预设的最大资源数。若所述总资源数未超过所述预设的最大资源数，则表征所述业务用户信息满足预设条件。若所述总资源数超过所述预设的最大资源数，则表征所述业务用户信息不满足预设条件。

[0083] 具体的，如前所述，中继服务器可以事先为每个业务系统的所有用户预设一个可以申请的中继地址的最大量，例如10，所以在每次为该业务用户信息对应的用户分配中继地址之后，就记录该业务用户信息对应的用户已获得的总资源数，即成功申请中继地址的次数。然后在步骤307中，在鉴权通过后，就给该业务用户信息已获得的资源数上加1，得到总资源数，例如9，然后再比较总资源数9和预设的最大资源数10的大小。

[0084] 若所述业务用户信息满足所述预设条件，则执行步骤308：中继服务器基于所述业务用户信息满足所述预设条件的确定结果，向终端发送成功响应信息，成功响应信息中携带中继服务器为终端分配的中继地址。

[0085] 举例来说，当业务用户信息没有位于黑名单上，则表示该分配请求不是恶意攻击，所以可以给该业务用户信息对应的用户分配中继地址。

[0086] 再例如，当总资源数小于或等于最大资源数时，说明还在允许申请的量的范围内，所以可以给该业务用户信息对应的用户分配中继地址。

[0087] 通过该方法，可以避免中继服务器仅通过校验信息进行鉴权，在鉴权通过时，就会

无条件的分配中继地址的情况，所以在某个终端的用户名和密码泄露或被恶意使用，反复发起分配请求时，中继服务器因为会根据业务用户信息来判定，所以不会随意分配中继地址，所以不会出现因为用户名和密码泄露而造成的中继服务器的资源被快速耗尽的情况。因此，在本发明实施例的中继地址分配方法，使得现有的安全漏洞得以弥补，提高了系统安全性。

[0088] 可选的，中继地址在为终端分配中继地址之后，可以保存中继地址和终端的地址之间的映射关系，便于后续对终端的数据进行转发，这部分内容将在后面描述。

[0089] 若所述业务用户信息不满足所述预设条件，可以执行步骤309：中继服务器基于所述业务用户信息不满足所述预设条件的确定结果，向所述终端发送失败响应，所述失败响应中携带失败原因。具体的，失败原因可以是业务用户信息位于黑名单上，或者是申请的资源数超限。通过该方法使得用户得知申请失败的原因，进而采取相对应的处理措施，例如重新去业务系统服务器进行注册，进而获得新的用户名和密码。

[0090] 可选的，在中继服务器向终端发送失败响应之后，可以执行步骤310：中继服务器向所述业务系统服务器发送通知信息，以通知所述系统业务服务器所述业务用户信息对应的用户异常。

[0091] 相应的，业务系统服务器接收中继服务器发送的通知信息，所述通知信息中包括所述业务用户信息；业务系统服务器将所述业务用户信息对应的用户加入黑名单并拒绝提供服务，或，业务系统服务器为所述用户重新生成用于向所述中继服务器请求中继地址的用户名并将重新生成的用户名发送给所述终端；或业务系统服务器通知终端重新进行注册，进而再为该终端生成新的用户名和密码。

[0092] 通过该方法可以在出现非法请求中继地址时，可以回溯到具体的业务用户，并且采取相应的措施，防止恶意攻击，而不像现有技术中，对于这种攻击，因为当前的TURN用户名都是临时分配的随机数，所以无法追踪到具体的业务用户，所以TURN服务器只能跟踪到源网络地址和端口，进行源网络地址的防攻击，如果黑客或者恶意用户使用大量不同的源网络地址和端口，反复发起分配请求，TURN服务器将无法防止此类攻击。因此，本发明实施例中的分配中继地址的方法，可以防堵安全漏洞，提高安全性。

[0093] 可选的，在中继服务器向终端发送失败响应后，所述方法还包括：中继服务器接收到所述终端多次发送的分配请求，以请求分配中继地址；中继服务器将所述业务用户信息加入黑名单并拒绝提供服务。本文中的多次表示“至少两次”。

[0094] 具体的，若在中继服务器向终端发送失败响应后，如果该用户仍继续申请中继地址，就很可能是恶意攻击，所以中继服务器可以将该业务用户信息加入黑名单并拒绝提供服务，以此防止资源被恶意消耗。因此，当再次接收到分配请求，分配请求中携带该用户名，那么就直接拒绝提供服务。

[0095] 因为在本发明实施例中，是将该业务用户信息加入黑名单中，并不是像现有技术中将终端的网络地址和端口加入黑名单中，一旦将终端的网络地址和端口加入黑名单，那么运行在该终端上的其它业务系统的用户将也无法申请中继地址，所以本发明实施例中的方法更加合理。

[0096] 可选的，步骤310中的发送通知信息也可以是在中继服务器确定所述业务用户信息不满足预设条件后发送。

[0097] 接下来请参考图4所示，为在终端请求到中继地址之后，终端和目的终端之间的数据转发流程图。

[0098] 步骤401：终端会生成并发送第一数据包给中继服务器，第一数据包包括源网络地址：终端的地址，目的网络地址：目的终端的地址以及数据。

[0099] 具体的，第一数据包例如是符合TURN协议的报文，TURN报文头可以包括源网络地址：终端的地址，目的网络地址：目的终端的地址；报文正文包括数据。

[0100] 步骤402：中继服务器根据终端的地址查询地址映射表，确定终端对应的中继地址；生成第二数据包，第二数据包包括源网络地址：中继地址，目的网络地址：目的终端的地址以及所述数据。

[0101] 具体的，在前述分配中继地址的流程中，当中继服务器为终端分配中继地址之后，可以保存中继地址和终端的地址的地址映射表，所以在步骤402中，当中继服务器接收到第一数据包时，就可以在数据包的包头获取到终端的地址，然后在地址映射表中查找到与该终端的地址对应的中继地址。进一步，可以将第一数据包中的源网络地址替换为中继地址，得到第二数据包。可选的，也可以是封装成符合其它传输协议的报文，例如第二数据包为符合用户数据报协议(英文：User Datagram Protocol，简称：UDP)的报文，在UDP的报文头中，源网络地址为中继地址，目的网络地址为目的终端的地址。

[0102] 在第二数据包生成之后，执行步骤403。

[0103] 步骤403：发送第二数据包。对于目的终端而言，终端是透明的，目的终端认为是在和中继服务器进行通信，所以目的终端在回复时，目的网络地址为中继地址。

[0104] 步骤404：目的终端生成第三数据包并发送第三数据包给中继服务器，第三数据包包括源网络地址：目的终端的地址，目的网络地址：中继地址以及数据。

[0105] 具体的，第三数据包可以是一个UDP报文。

[0106] 在中继服务器接收到第三数据包时，执行步骤405。

[0107] 步骤405：中继服务器根据中继地址查询地址映射表，确定中继地址对应的终端的地址；生成第四数据包，第四数据包包括源网络地址：目的终端的地址，目的网络地址：终端的地址以及数据。

[0108] 具体的，第四数据包例如为符合TURN协议的报文。

[0109] 在生成第四数据包之后，执行步骤406：中继服务器发送第四数据包给终端。如此完成了一次终端和目的终端之间的通信。

[0110] 可选的，图2所示的网元可以为图1中的部分或全部元件，用以实现如图3及图4所示的方法中的部分步骤或全部步骤，具体的配置可以依据实际需要确定。

[0111] 具体的，当图2所示的网元为中继服务器时，处理器10执行存储器40上存储的计算机可执行程序代码中包括的指令时，所述指令使得网元执行以下操作：通过接收器30接收终端发送的分配请求，所述分配请求中携带所述终端的用于向所述网元请求中继地址的用户名和校验信息；其中，所述用户名与所述终端的用于向业务系统服务器请求注册的业务用户信息相关；根据所述校验信息对所述用户名进行鉴权；在鉴权通过时，根据所述用户名确定所述业务用户信息；确定所述业务用户信息是否满足预设条件；基于所述业务用户信息满足所述预设条件的确定结果，通过发送器20向所述终端发送成功响应信息，所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。

[0112] 进一步的，以上作为中继服务器的网元包含的处理器10所执行操作的具体实现方式可以参照图3和图4的实施例的中由中继服务器执行的对应步骤，本发明实施例不再赘述。

[0113] 作为另一种可选方式，当图2所示的网元为业务系统服务器时，处理器10执行存储器40上存储的计算机可执行程序代码中包括的指令时，所述指令使得网元执行以下操作：通过接收器30接收终端发送的注册请求，所述注册请求携带所述终端的业务用户信息；根据所述业务用户信息生成所述终端的用于向中继服务器请求中继地址的用户名；通过发送器20向所述终端发送注册成功响应，所述注册成功响应中携带所述中继服务器的网络地址和端口、所述用户名。

[0114] 进一步的，以上作为业务系统服务器的网元包含的处理器10所执行操作的具体实现方式可以参照图3和图4的实施例的中由业务系统服务器执行的对应步骤，本发明实施例不再赘述。

[0115] 图5本发明实施例提供的第一种分配中继地址的装置的简化功能框图。该业务部署装置包括：接收单元501、处理单元502以及发送单元503。

[0116] 其中，接收单元501，用于接收终端发送的分配请求，所述分配请求中携带所述终端的用于向中继服务器请求中继地址的用户名和校验信息；其中，所述用户名与所述终端的用于向业务系统服务器请求注册的业务用户信息相关；处理单元502，用于根据所述校验信息对所述用户名进行鉴权；在鉴权通过时，根据所述用户名确定所述业务用户信息；所述中继服务器确定所述业务用户信息是否满足预设条件；发送单元503，用于基于所述业务用户信息满足所述预设条件的确定结果，向所述终端发送成功响应信息，所述成功响应信息中携带所述中继服务器为所述终端分配的中继地址。

[0117] 可选的，处理单元502用于：确定所述业务用户信息已获得的总资源数；确定所述总资源数未超过所述业务用户信息的预设的最大资源数，若所述总资源数未超过所述预设的最大资源数，则表征所述业务用户信息满足预设条件。

[0118] 可选的，发送单元503还用于：基于所述业务用户信息不满足所述预设条件的确定结果，向所述终端发送失败响应，所述失败响应中携带失败原因。

[0119] 可选的，接收单元501还用于：在发送单元503向所述终端发送失败响应后，接收到所述终端多次发送的分配请求，以请求分配中继地址；处理单元502还用于：将所述业务用户信息加入黑名单并拒绝提供服务。

[0120] 可选的，发送单元503还用于：在向所述终端发送失败响应后，向所述业务系统服务器发送通知信息，以通知所述系统业务服务器所述业务用户信息对应的用户异常。

[0121] 图6为本发明实施例提供的第二种分配中继地址的装置的简化功能框图。该业务部署装置包括：接收单元601、处理单元602以及发送单元603。

[0122] 具体的，接收单元601，用于接收终端发送的注册请求，所述注册请求携带所述终端的业务用户信息；处理单元602，用于根据所述业务用户信息生成所述终端的用于向中继服务器请求中继地址的用户名；发送单元603，用于向所述终端发送注册成功响应，所述注册成功响应中携带所述中继服务器的网络地址和端口、所述用户名。

[0123] 可选的，接收单元601还用于：接收所述中继服务器发送的通知信息，所述通知信息中包括所述业务用户信息；处理单元602还用于将所述业务用户信息对应的用户加入黑

名单并拒绝提供服务，或，为所述用户重新生成用于向所述中继服务器请求中继地址的用户名并将重新生成的用户名通过发送单元603发送给所述终端。

[0124] 需要说明的是，分配中继地址的装置以功能单元的形式展示。在不受限制的情况下，本文所使用的术语“单元”可指执行一个或多个软件或固件程序的专用集成电路(ASIC)、电子电路、(共享、专用或组)处理器以及存储器，组合逻辑电路，和/或提供所述功能的其它合适的部件。

[0125] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0126] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0127] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0128] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0129] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

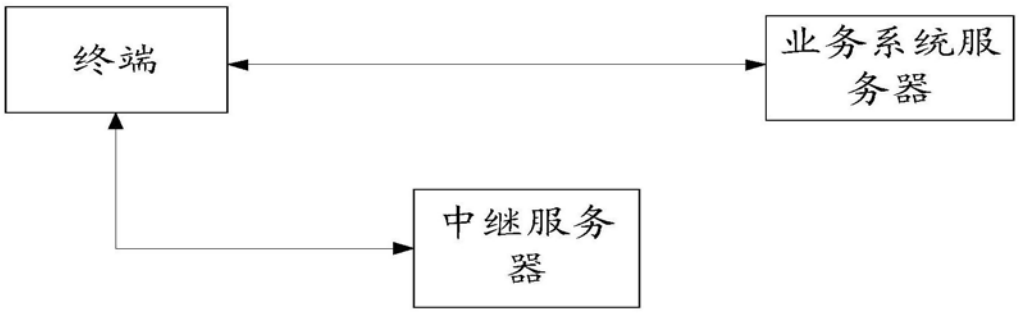


图1

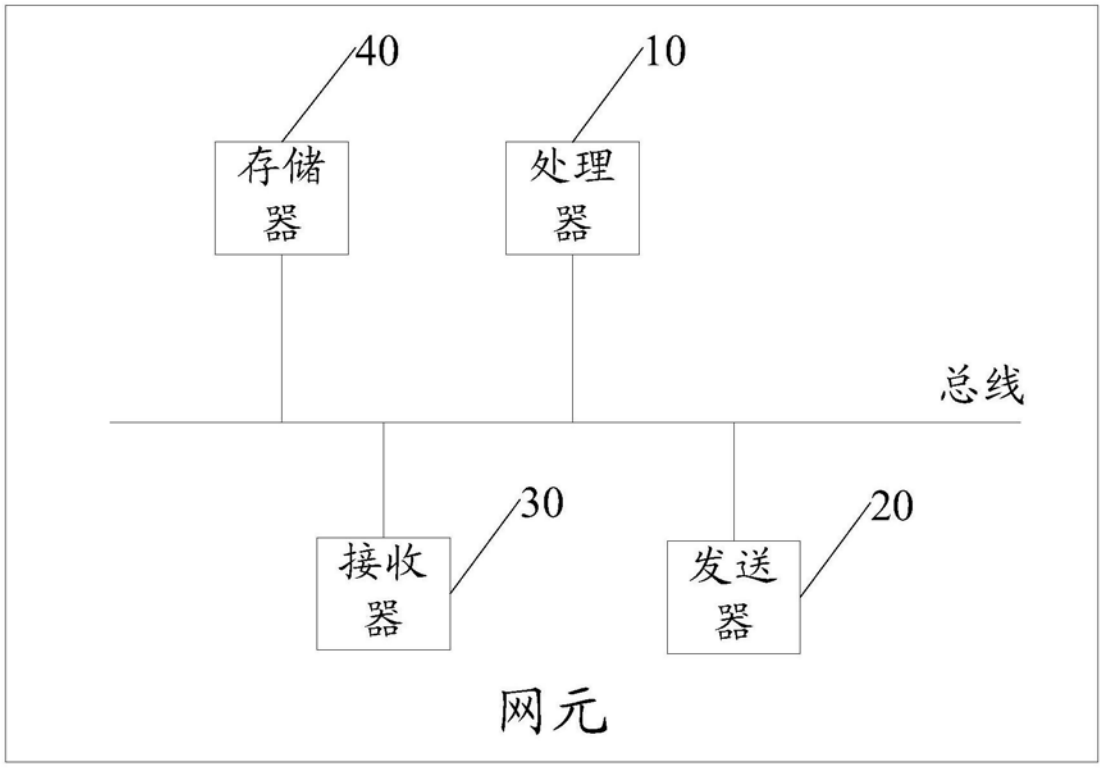


图2

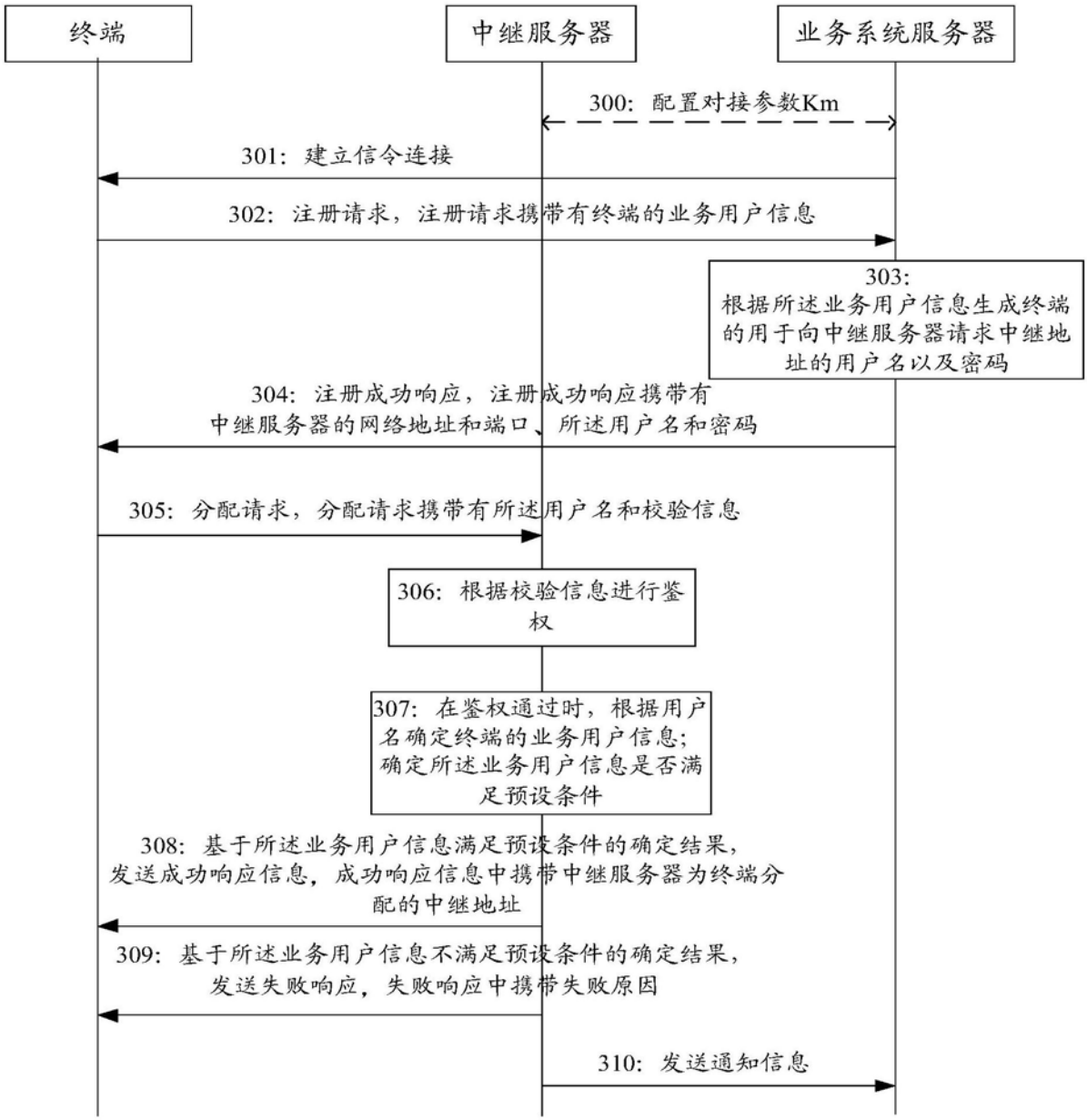

终端
中继服务器
业务系统服务器
300：配置对接参数Km
301：建立信令连接
302：注册请求，注册请求携带有终端的业务用户信息
303：
根据所述业务用户信息生成终端的用于向中继服务器请求中继地址的用户名以及密码
304：注册成功响应，注册成功响应携带有
中继服务器的网络地址和端口、所述用户名和密码
305：分配请求，分配请求携带有所述用户名和校验信息
306：根据校验信息进行鉴权
307：在鉴权通过时，根据用户名确定终端的业务用户信息；
确定所述业务用户信息是否满足预设条件
308：基于所述业务用户信息满足预设条件的确定结果，
发送成功响应信息，成功响应信息中携带中继服务器为终端分配的中继地址
309：基于所述业务用户信息不满足预设条件的确定结果，
发送失败响应，失败响应中携带失败原因
310：发送通知信息

图3

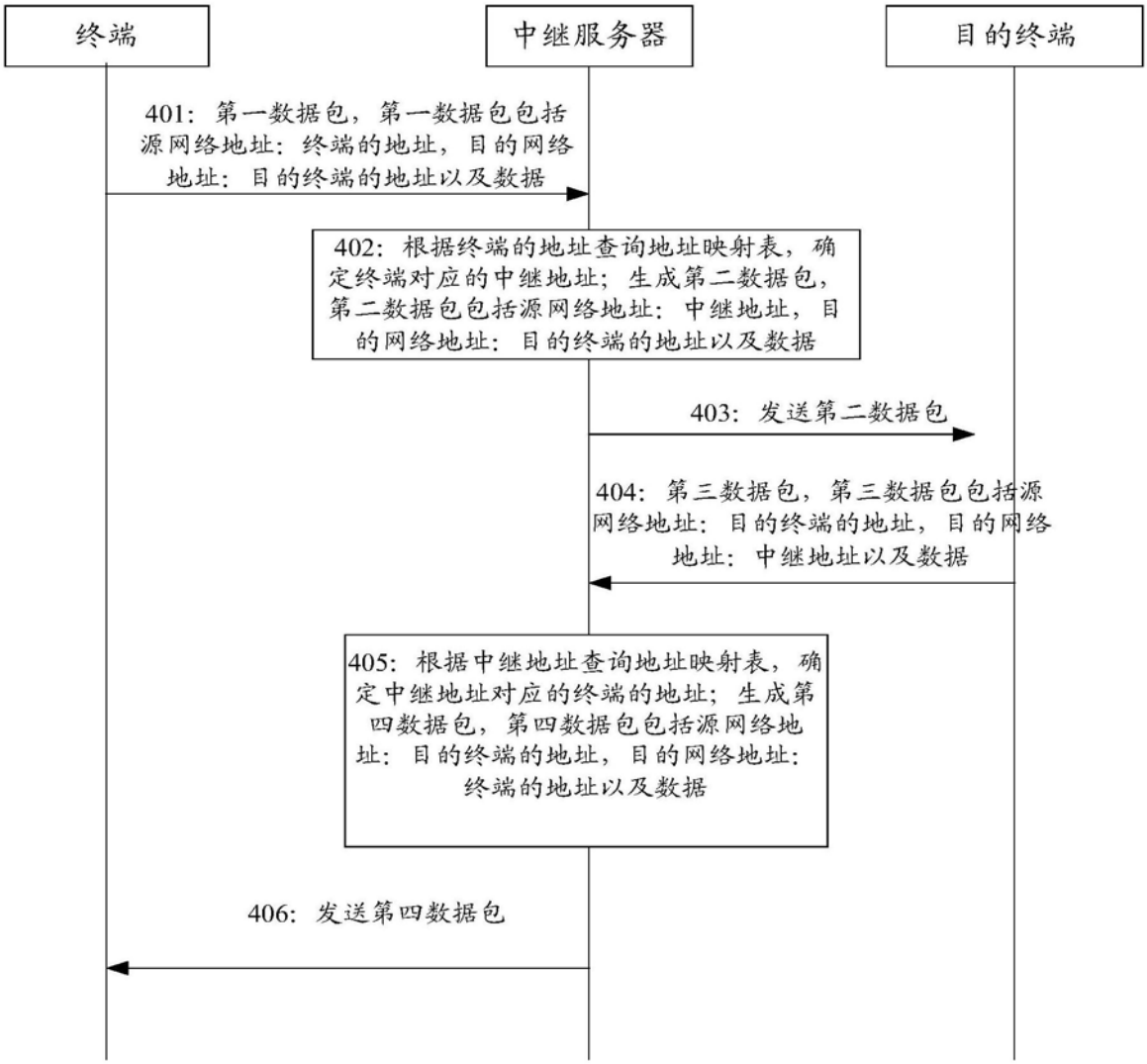

终端
中继服务器
目的终端
401：第一数据包，第一数据包包括源网络地址：终端的地址，目的网络地址：目的终端的地址以及数据
402：根据终端的地址查询地址映射表，确定终端对应的中继地址；生成第二数据包，第二数据包包括源网络地址：中继地址，目的网络地址：目的终端的地址以及数据
403：发送第二数据包
404：第三数据包，第三数据包包括源网络地址：目的终端的地址，目的网络地址：中继地址以及数据
405：根据中继地址查询地址映射表，确定中继地址对应的终端的地址；生成第四数据包，第四数据包包括源网络地址：目的终端的地址，目的网络地址：终端的地址以及数据
406：发送第四数据包

图4

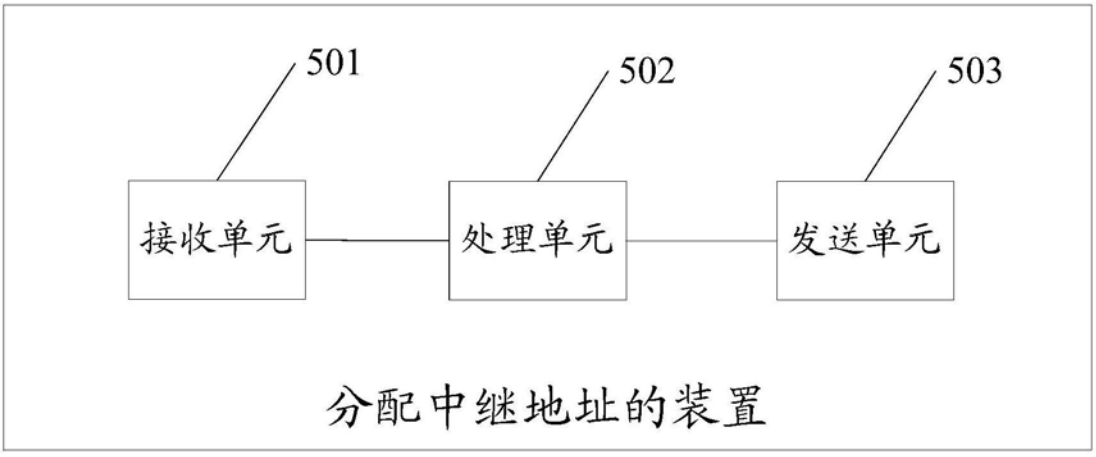

501
502
503
接收单元
处理单元
发送单元
分配中继地址的装置

图5

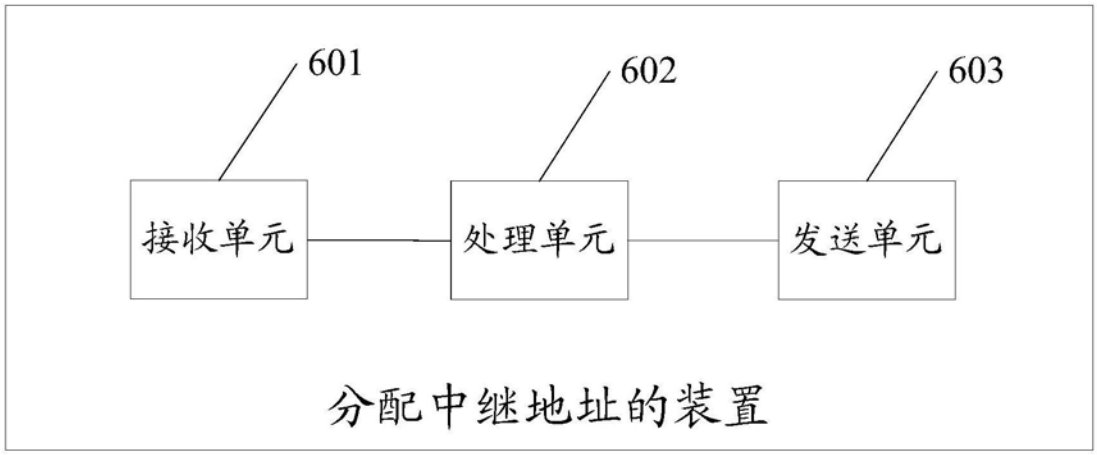


图6