(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 105681268 B
(45)授权公告日 2019.09.24

(21)申请号 201410677400.6

(22)申请日 2014.11.21

(65)同一申请的已公布的文献号
申请公布号 CN 105681268 A

(43)申请公布日 2016.06.15

(73)专利权人 南京中兴软件有限责任公司
地址 210012 江苏省南京市雨花台区宁南街道紫荆花路68号

(72)发明人 李锐 钟小武 廖俊锋

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 梁丽超 韩建伟

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

(56)对比文件
CN 102396250 A,2012.03.28,
CN 101483606 A,2009.07.15,
CN 102098237 A,2011.06.15,
CN 102256329 A,2011.11.23,
WO 2011053040 A3,2011.10.27,

审查员 王丹

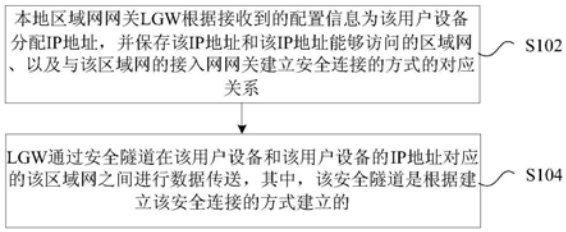
权利要求书1页 说明书6页 附图3页

(54)发明名称

数据传送方法及装置

(57)摘要

本发明公开了一种数据传送方法及装置,其中,该方法包括:本地区域网网关LGW根据用户设备的认证信息为该用户设备分配IP地址,并保存该IP地址和该IP地址能够访问的区域网、以及与该区域网的接入网网关建立安全连接的方式的对应关系;该LGW通过安全隧道在该用户设备和该用户设备的IP地址对应的该区域网之间进行数据传送,其中,该安全隧道是根据建立该安全连接的方式建立的。通过本发明,解决了相关技术中并没有考虑不同用户访问不同区域网的问题,不同用户根据分配的IP地址访问不同的区域网。



CN 105681268 B

1.一种数据传送方法,其特征在于,包括:

本地区域网网关LGW根据接收到的配置信息为用户设备分配IP地址,并保存所述IP地址和所述IP地址能够访问的区域网、以及与所述区域网的接入网网关建立安全连接的方式的对应关系;

所述LGW通过安全隧道在所述用户设备和所述用户设备的IP地址对应的所述区域网之间进行数据传送,其中,所述安全隧道是根据建立所述安全连接的方式建立的;

其中,在所述LGW保存所述对应关系之前,所述方法还包括:所述LGW将用于认证所述用户设备的认证信息转发给认证服务器;所述LGW接收所述认证服务器返回的所述配置信息,其中,所述返回的信息中包括:为所述用户设备分配的接入IP地址、以及所述IP地址能够接入的区域网、以及与所述区域网的接入网网关建立安全连接的方式。

2.根据权利要求1所述的方法,其特征在于,在所述LGW将用于认证所述用户设备的认证信息转发给认证服务器之前,所述方法还包括:

所述LGW接收来自核心网的所述认证信息,其中,所述认证信息是所述用户设备选择区域网接入点名称之后输入的。

3.根据权利要求1至2中任一项所述的方法,其特征在于,与所述区域网的接入网网关建立连接的方式包括以下至少之一:

IPSec方式、SSL方式、TLS方式。

4.根据权利要求1至2中任一项所述的方法,其特征在于,所述方法还包括:

所述LGW接收到所述用户设备不在服务范围的通知;

所述LGW删除所述对应关系。

5.一种数据传送装置,其特征在于,应用于本地区域网网关LGW,包括:

分配模块,用于根据接收到的配置信息为用户设备分配IP地址,并保存所述IP地址和所述IP地址能够访问的区域网、以及与所述区域网的接入网网关建立安全连接的方式的对应关系;

数据传送模块,用于通过安全隧道在所述用户设备和所述用户设备的IP地址对应的所述区域网之间进行数据传送,其中,所述安全隧道是根据建立所述安全连接的方式建立的;

其中,所述装置还包括:转发模块,用于将用于认证所述用户设备的认证信息转发给认证服务器;第一接收模块,用于接收所述认证服务器返回的所述配置信息,其中,所述返回的信息中包括:为所述用户设备分配的接入IP地址、以及所述IP地址能够接入的区域网、以及与所述区域网的接入网网关建立安全连接的方式。

6.根据权利要求5所述的装置,其特征在于,所述装置还包括:

第二接收模块,用于接收来自核心网的所述认证信息,其中,所述认证信息是所述用户设备选择区域网接入点名称之后输入的。

7.根据权利要求5至6中任一项所述的装置,其特征在于,与所述区域网的接入网网关建立连接的方式包括以下至少之一:

IPSec方式、SSL方式、TLS方式。

8.根据权利要求5至6中任一项所述的装置,其特征在于,所述装置还包括:

第三接收模块,用于接收到所述用户设备不在服务范围的通知;

删除模块,用于删除所述对应关系。

数据传送方法及装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种数据传送方法及装置。

背景技术

[0002] LTE提出异构网络(Heterogeneous Network，简称为HN)的概念，从而演进了一些新技术，3GPP(3rd Generation Partnership Project:第三代合作项目)也对此技术进行专门的研究，比如本地业务交换本地IP接入(Local IP Access，简称为LIPA)，以及数据分流(SIPTO:Selected IP Traffic Offload，可选IP业务分流)等，将本地或者低价值的数据业务直接交换，分流到Internet，而不是再送回到核心网转发，避免大量低价值的业务对核心网的冲击。

[0003] LIPA是基于家庭级基站(Home eNodeB，简称为HeNB)网络提出的，其核心思想是将本地网络的通信数据直接从HeNB就分流出去，从而减轻了核心网络的负荷和传输成本。LIPA技术可以进一步演化为区域网的概念，即在一个有限的区域部署一个本地的无线网络，无线网络用户在认证后访问本地区域网络资源，也可以访问Internet资源，访问本地网络不需要计费或者另外计费，用户可以不更换终端访问企业内网，只需要换一个访问节点名称(Access Point Name，简称为APN)即可。

[0004] 用户终端(User Equipment，简称为UE)都是基于标准的IP数据，移动用户接入到区域本地网后，需要严格的限制权限。如多家公司共享一个HeNB，A公司用户绝对不能访问B公司网络，同理B公司员工也不能访问A公司网络。另外在一家公司内，普通员工不能访问财务等敏感部门，只有高级授权用户才能访问，对于一些临时来访客户，在满足客户基本需求前提下，需要尽可能限制客户的可访问资源。

[0005] 发明人发现，区域内部有线网络组网复杂，需要隔离内部用户，把不同用户划分到不同的区域网中，例如，划分到不同的虚拟本地网络(Virtual Local Area Network，简称为VLAN)。但是，在相关技术中并没有考虑不同用户访问不同区域网的问题。

发明内容

[0006] 本发明提供了一种数据传送方法及装置，以至少解决相关技术中并没有考虑不同用户访问不同区域网的问题。

[0007] 根据本发明的一个方面，提供了一种数据传送方法，包括：本地区域网网关LGW根据接收到的配置信息为所述用户设备分配IP地址，并保存所述IP地址和所述IP地址能够访问的区域网、以及与所述区域网的接入网网关建立安全连接的方式的对应关系；所述LGW通过安全隧道在所述用户设备和所述用户设备的IP地址对应的所述区域网之间进行数据传送，其中，所述安全隧道是根据建立所述安全连接的方式建立的。

[0008] 进一步地，在所述LGW保存所述对应关系之前，所述方法还包括：所述LGW将用于认证所述用户设备的认证信息转发给认证服务器；所述LGW接收所述认证服务器返回的所述配置信息，其中，所述返回的信息中包括：为所述用户设备分配的接入IP地址、以及所述IP

地址能够接入的区域网、以及与所述区域网的接入网网关建立安全连接的方式。

[0009] 进一步地，在所述LGW将用于认证所述用户设备的认证信息转发给认证服务器之前，所述方法还包括：所述LGW接收来自核心网的所述认证信息，其中，所述认证信息是所述用户设备选择区域网接入点名称之后输入的。

[0010] 进一步地，与所述区域网的接入网网关建立连接的方式包括以下至少之一：IPSec方式、SSL方式、TLS方式。

[0011] 进一步地，所述方法还包括：所述LGW接收到所述用户设备不在服务范围的通知；所述LGW删除所述对应关系。

[0012] 根据本发明的另一方面，提供了一种数据传送装置，应用于本地区域网网关LGW，包括：分配模块，用于根据接收到的配置信息为所述用户设备分配IP地址，并保存所述IP地址和所述IP地址能够访问的区域网、以及与所述区域网的接入网网关建立安全连接的方式的对应关系；数据传送模块，用于通过安全隧道在所述用户设备和所述用户设备的IP地址对应的所述区域网之间进行数据传送，其中，所述安全隧道是根据建立所述安全连接的方式建立的。

[0013] 进一步地，所述装置还包括：转发模块，用于将用于认证所述用户设备的所述配置转发给认证服务器；第一接收模块，用于接收所述认证服务器返回的信息，其中，所述返回的信息中包括：为所述用户设备分配的接入IP地址、以及所述IP地址能够接入的区域网、以及与所述区域网的接入网网关建立安全连接的方式。

[0014] 进一步地，所述装置还包括：第二接收模块，用于接收来自核心网的所述认证信息，其中，所述认证信息是所述用户设备选择区域网接入点名称之后输入的。

[0015] 进一步地，与所述区域网的接入网网关建立连接的方式包括以下至少之一：IPSec方式、SSL方式、TLS方式。

[0016] 进一步地，所述装置还包括：第三接收模块，用于接收到所述用户设备不在服务范围的通知；删除模块，用于删除所述对应关系。

[0017] 通过本发明，采用本地区域网网关LGW根据接收到的配置信息为所述用户设备分配IP地址，并保存所述IP地址和所述IP地址能够访问的区域网、以及与所述区域网的接入网网关建立安全连接的方式的对应关系；所述LGW通过安全隧道在所述用户设备和所述用户设备的IP地址对应的所述区域网之间进行数据传送，其中，所述安全隧道是根据建立所述安全连接的方式建立的，解决了相关技术中并没有考虑不同用户访问不同区域网的问题，不同用户根据分配的IP地址访问不同的区域网。

附图说明

[0018] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0019] 图1是根据本发明实施例的数据传送方法的流程图；

[0020] 图2是根据本发明实施例的数据传送装置的框图；

[0021] 图3是根据本发明优选实施例的数据传送装置的框图一；

[0022] 图4是根据本发明优选实施例的数据传送装置的框图二；

[0023] 图5是根据本发明优选实施例的数据传送装置的框图三；

[0024] 图6是根据本发明实施例的区域网组网示意图；

[0025] 图7是根据本发明实施例的UE接入区域网的示意图。

具体实施方式

[0026] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0027] 在本实施例中提供了一种数据传送方法，图1是根据本发明实施例的数据传送方法的流程图，如图1所示，该流程包括如下步骤：

[0028] 步骤S102，本地区域网网关LGW根据接收到的配置信息为该用户设备分配IP地址，并保存该IP地址和该IP地址能够访问的区域网、以及与该区域网的接入网网关建立安全连接的方式的对应关系；

[0029] 步骤S104，LGW通过安全隧道在该用户设备和该用户设备的IP地址对应的该区域网之间进行数据传送，其中，该安全隧道是根据建立该安全连接的方式建立的。

[0030] 通过上述步骤，通过安全隧道在用户设备和该用户设备的IP地址对应的区域网之间进行数据传送，从而可以根据IP地址和该IP地址能够访问的区域网、以及与该区域网的接入网网关建立安全连接的方式的对应关系控制用户设备的访问权限，解决了相关技术中并没有考虑不同用户访问不同区域网的问题，不同用户根据分配的IP地址访问不同的区域网。

[0031] 为了更加安全，该配置信息可以是在认证完成之后发送的，对用户设备的认证可以有多种方式，例如，在而一个可选的实施方式中，在LGW保存该对应关系之前，该LGW还可以将用于认证该用户设备的认证信息转发给认证服务器；该LGW接收该认证服务器返回的该配置信息，其中，该返回的信息中包括：为该用户设备分配的接入IP地址、以及该IP地址能够接入的区域网、以及与该区域网的接入网网关建立安全连接的方式。

[0032] 在LGW将用于认证该用户设备的认证信息转发给认证服务器之前，该LGW还可以接收来自核心网的该认证信息，其中，该认证信息是该用户设备选择区域网接入点名称之后输入的。

[0033] 与区域网的接入网网关建立连接的方式可以有很多种，在一个可选的实施例中，与该区域网的接入网网关建立连接的方式可以包括以下至少之一：IPSec方式、SSL方式、TLS方式。

[0034] 在一个可选的实施例中，用户设备不在服务范围的情况下，LGW接收到该用户设备不在服务范围的通知，并删除该对应关系，释放了资源，节约了储存空间。

[0035] 本发明实施例还提供了一种数据传送装置，应用于本地区域网网关LGW，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0036] 图2是根据本发明实施例的数据传送装置的框图，如图2所示，包括：分配模块22和数据传送模块24，下面对各个模块进行简要说明。

[0037] 分配模块22，用于根据接收到的配置信息为该用户设备分配IP地址，并保存该IP地址和该IP地址能够访问的区域网、以及与该区域网的接入网网关建立安全连接的方式的

对应关系；

[0038] 数据传送模块24，用于通过安全隧道在该用户设备和该用户设备的IP地址对应的该区域网之间进行数据传送，其中，该安全隧道是根据建立该安全连接的方式建立的。

[0039] 图3是根据本发明优选实施例的数据传送装置的框图一，如图3所示，该装置还包括：

[0040] 转发模块32，用于将用于认证该用户设备的认证信息转发给认证服务器；

[0041] 第一接收模块34，用于接收该认证服务器返回的该配置信息，其中，该返回的信息中包括：为该用户设备分配的接入IP地址、以及该IP地址能够接入的区域网、以及与该区域网的接入网网关建立安全连接的方式。

[0042] 图4是根据本发明优选实施例的数据传送装置的框图二，如图4所示，该装置还包括：

[0043] 第二接收模块42，用于接收来自核心网的该认证信息，其中，该认证信息是该用户设备选择区域网接入点名称之后输入的。

[0044] 在一个可选的实施例中，可以通过以下至少之一确定与该区域网的接入网网关建立连接的方式：IPSec方式、SSL方式、TLS方式。

[0045] 图5是根据本发明优选实施例的数据传送装置的框图三，如图5所示，该装置还包括：

[0046] 第三接收模块52，用于接收到该用户设备不在服务范围的通知；

[0047] 删除模块54，用于删除该对应关系。

[0048] 下面结合可选实施例对本发明实施例进行进一步说明。

[0049] LIPA引入了一个本地网关(Local Gateway，简称为LGW)的网络逻辑节点，HeNB数据汇聚到LGW后再做分流处理，实际应用中，LGW和HeNB可以是同一物理实体，也可以为单独物理实体。

[0050] 用户接入区域网，用户在UE上选择接入区域网APN，输入用户名密码，核心网将区域网的用户认证信息给LGW，LGW转发给认证服务器认证。

[0051] 用户鉴权，LGW在区域网内部部署，访问LGW的认证服务器也在区域网内。LGW将UE请求数据发送给认证服务器，认证协议一般为标准的Radius协议(但不限于Radius协议)，LGW发送给认证服务器的认证信息包括身份唯一标识(Identity，简称为UE ID)，一般为全球用户识别卡(Universal Subscriber Identity Module，简称为USIM)的国际移动用户识别码(International Mobile Subscriber Identification Number，简称为IMSI)号，或者手机号码、UE接入APN的用户名、密码等。

[0052] 接入权限分配，认证服务器收到认证请求后，返回给UE和LGW预先规划的信息，返回用户接入本地网络的用户IP、接入网关IP、接入权限、认证方式，加密算法等。

[0053] 接入网关处理，区域网接入网关需要对接入的报文做过滤处理，对于敏感访问区域，推荐使用强鉴权和加密处理。如在LGW和接入网关之间建立IP安全(IP Security，简称为IPSec)隧道或者安全套接层/传输层安全(Secure Sockets Layer/Transport Layer Security，简称为SSL/TLS)等，IPSec隧道内，只有特定范围的报文(指定范围的IP、协议、端口)才能访问区域网，其余报文直接丢弃。

[0054] 用户UE访问本地网络，UE访问区域网络，LGW在转发数据时，先查询UE访问本地网

络对应的网关IP，接入权限，认证方式和加密算法等。如果是IPSec方式，LGW和认证服务器分配的的接入网关之间建立IPSec隧道，如果是其余安全接入方式(如SSL/TLS)，LGW根据协议和接入网关之间建立对应的安全连接。对于UE发送给区域网的报文，LGW加密发送给接入网关，接入网关解密后再转发给内部网络。对于区域网到UE的报文，接入网关加密后转发给LGW，LGW解密后，根据UE的IP转发给对应的UE。

[0055] 释放资源，当UE切换或离开基站时，LGW同步删除之前保留的UE和安全隧道映射表。

[0056] 对于某些大写字楼，每一楼层可能有多家规模较小的公司，因为占地面积小，这些公司会共用一个基站(大部分都是Femto级别的小站)，所以室内的网络部署可能是公共方如物业公司提供。物业公司提供的多家公司的共享网络，则需要隔离不同公司的访问权限，如A公司员工不能访问B公司的网络，同理B公司的员工不能访问A公司的网络。

[0057] 物业公司在部署HeNB和LGW时，可以考虑LGW和不同公司的网关之间建立安全隧道，不同公司用户通过安全隧道访问公司内网。

[0058] 对于某大型企业，部门较多，一些公共部门宣传广告部门每个用户都可以访问，但是类似财务部门则只能限制某些高级用户才能接入。LGW可以和不同部门的接入服务器协商规则，如访问公共宣传资料，直接明文访问不加密；访问财务等其它敏感部门，需要LGW和接入网关之间做认证加密处理。

[0059] 图6是根据本发明实施例的区域网组网示意图，如图6所示，区域网是在一个有限的区域部署一个本地的无线网络，可以是不同公司，或者不同楼层的网络，用户接入区域网内部不需要更换UE，也不需要基站更改频段，只需要修改接入的APN。

[0060] 区域网需要核心网支持本地交换等功能，区域网认证服务器放置在区域网内，UE的接入权限，IP、接入网关、认证方式、加密算法等都由区域网认证服务器来分配，推荐不同公司或者不同楼层使用不同接入网关隔离。

[0061] 图7是根据本发明实施例的UE接入区域网的示意图，如图7所示，UE选择区域网APN，用户输入认证信息后，核心网将区域网的用户认证信息给LGW，LGW转发给认证服务器认证。

[0062] 用户接入认证包括以下步骤：

[0063] S702，LGW把认证数据发送给认证服务器，认证服务器认证用户信息，认证通过后，分配UE的接入IP、接入权限和认证方式，主要包括UE的用户IP、接入网关、认证方式、加密算法等信息；

[0064] S704，LGW收到认证信息后，将用户IP分配给对应UE，保存对应UE的IP，按照认证服务器分配的认证方式、加密算法等与接入网关建立安全连接；

[0065] S706，LGW接收到UE发送给区域网的数据，查询保存的UE和IP和安全隧道的对应关系，如果需要加密，则根据协商的秘钥将数据加密发送给接入网关，接入网关把报文解密，发送给内部网络；如果有区域网内部报文发送给UE，接入网关根据协商的秘钥加密报文，发送给LGW，LGW解密后根据IP转发给不同UE；

[0066] S708，如果是同LGW下UE数据互传，则直接在LGW转发，不需要认证加密处理。如果UE切换，离开基站，或者掉电等，基站检测出UE不在服务范围后通知LGW删除之前对应的UE和、IP对应关系，也拆除预先建立的隧道连接；

[0067] S710,UE访问本地网络。

[0068] 本可选实施例中的LGW需要实现的以下功能,需要说明的是,以下的功能可以通过不同的模块实现。

[0069] 认证功能,LGW需要封装认证信息报文给认证服务器,完成UE接入的认证功能。

[0070] 安全连接功能,LGW需要和接入网关之间建立安全的连接,保证用户数据可靠传送。

[0071] UE和IP、安全隧道映射列表,LGW需要保存每个接入区域网UE对应的IP和安全隧道的映射关系,将UE的数据在协商好的安全隧道发送,发给对应的接入网关。接收区域网到UE的数据包时,将数据包解密转发给对应的UE。

[0072] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。

[0073] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

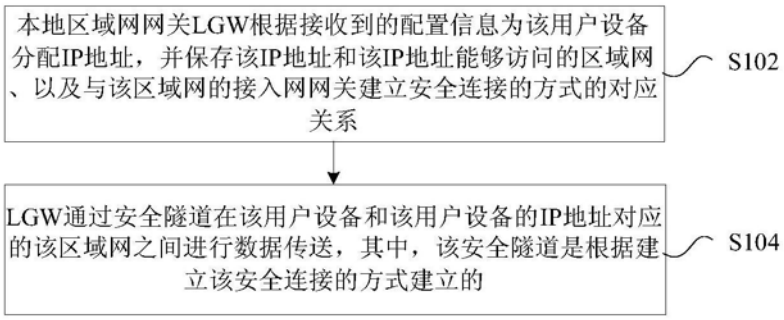

本地区域网网关LGW根据接收到的配置信息为该用户设备分配IP地址，并保存该IP地址和该IP地址能够访问的区域网、以及与该区域网的接入网网关建立安全连接的方式的对应关系
S102
LGW通过安全隧道在该用户设备和该用户设备的IP地址对应的该区域网之间进行数据传送，其中，该安全隧道是根据建立该安全连接的方式建立的
S104

图1


分配模块22
数据传送模块24

图2


转发模块32
第一接收模块34
分配模块22
数据传送模块24

图3


第二接收模块42
转发模块32
第一接收模块34
分配模块22
数据传送模块24

图4


分配模块22
数据传送模块24
第三接收模块52
删除模块54

图5

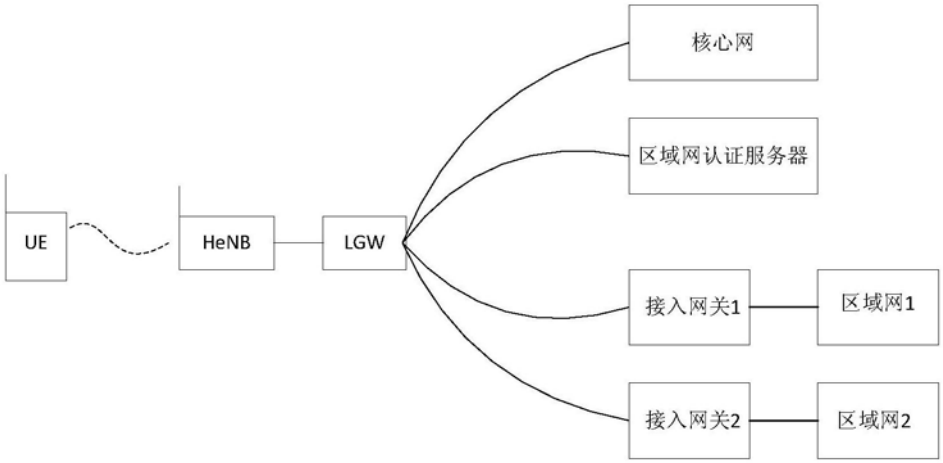

核心网
区域网认证服务器
UE
HeNB
LGW
接入网关1
区域网1
接入网关2
区域网2

图6

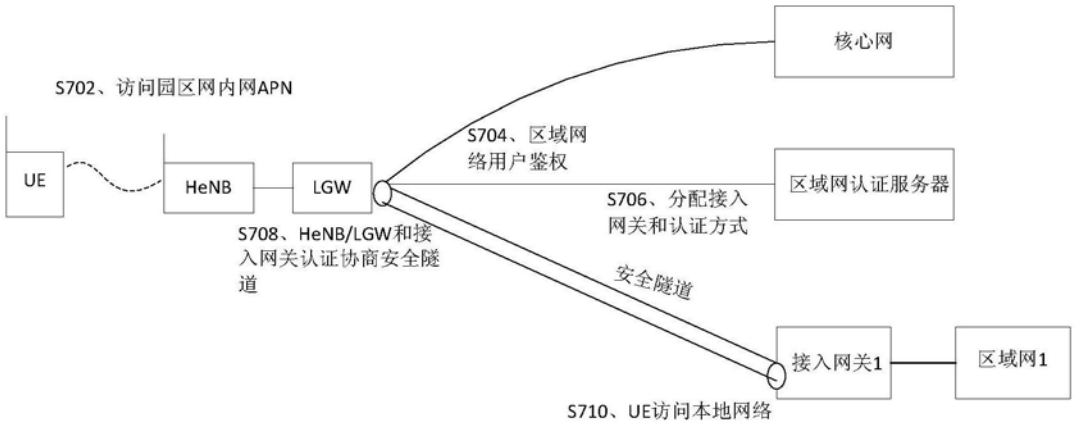

核心网
S702、访问园区网内网APN
UE
HeNB
LGW
S704、区域网络用户鉴权
区域网认证服务器
S706、分配接入网关和认证方式
S708、HeNB/LGW和接入网关认证协商安全隧道
安全隧道
接入网关1
区域网1
S710、UE访问本地网络

图7