

# (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局



(43) 国际公布日  
2011年10月6日 (06.10.2011)

PCT

(10) 国际公布号  
WO 2011/120276 A1

- (51) 国际专利分类号:  
H04W 76/00 (2009.01)
- (21) 国际申请号: PCT/CN2010/076142
- (22) 国际申请日: 2010年8月19日 (19.08.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201010140579.3 2010年3月29日 (29.03.2010) CN
- (71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): **赵凝霞 (ZHAO, Ningxia)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 **吴强 (WU, Qiang)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 **吴波 (WU, Bo)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (74) 代理人: 北京派特恩知识产权代理事务所(普通合伙) (CHINA PAT INTELLECTUAL PROPERTY

OFFICE); 中国北京市海淀区知春路 113 号 0717 室, Beijing 100086 (CN)。

- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

### 本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

(54) Title: METHOD AND SYSTEM FOR ESTABLISHING CONNECTION BETWEEN TERMINALS

(54) 发明名称: 一种终端实现连接建立的方法及系统

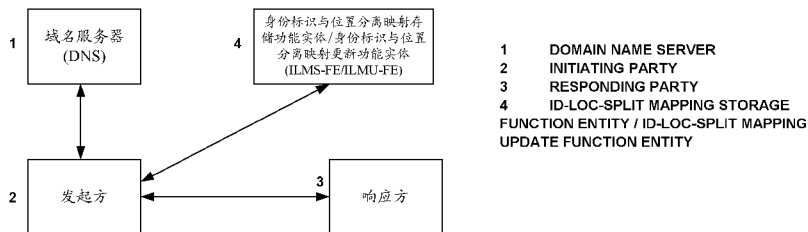


图 4 / Fig. 4

(57) Abstract: A method and a system for establishing a connection between terminals are provided in the present invention. The method includes: an initiating party queries a domain name server (DNS) and obtains the address of the mapping server associated with a responding party; the initiating party, using the Node ID of the responding party, queries the mapping server associated with the responding party and obtains the location information of the responding party; the initiating party establishes the connection with the responding party. In the method of the present invention, the location of the opposite user can be obtained by using the Node ID and the connection can be established between the initiating party and the responding party, which ensures the connection establishment between terminals in the case of split of transfer and control, as well as the connection reliability.

[见续页]

WO 2011/120276 A1

---

**(57) 摘要:**

本发明提供了一种终端实现连接建立的方法及系统。该方法包括：发起方通过域名服务器（DNS）查询，获得响应方所在映射服务器的地址；发起方利用响应方的 Node ID 向响应方所在映射服务器查询，获得响应方的位置信息；发起方与响应方建立连接。本发明方法中，使用 Node ID 获得对端用户的位置，在发起方与响应方之间直接建立连接，不仅实现了传输与控制分离的情况下，终端建立连接的过程，而且保证了连接的可靠性。

## 一种终端实现连接建立的方法及系统

### 技术领域

本发明涉及下一代网络中身份标识与位置分离（IPSPLIT, ID/locator separation in NGN）技术，尤其涉及一种 IPSPLIT 网络中，终端实现连接建  
5 立的方法及系统。

### 背景技术

当前，因特网的各层结构中，除了物理层以外，各层协议实体均有自己的名字空间，分别是：链路层的介质访问控制（MAC, Media Access Control）地址、网络层的 IP 地址、传输层的 IP 地址和端口号，以及应用层的  
10 域名。在上述名字空间中，MAC 地址只要求在子网内唯一，端口号只要求在主机内部唯一，这样，因特网中存在两个重要的全局名字空间，即 IP 地址和域名。域名和 IP 地址中间通过域名服务器（DNS, Domain Name Server）实现解析。在这样的名字空间结构中，IP 地址具有双重功能，既作为网络层的通信终端主机网络接口在网络拓扑中的位置标识，又作为传输  
15 层主机网络接口的身份标识。

传输控制协议/因特网协议（TCP/IP）设计之初并没有考虑主机移动的情况，但是，随着下一代网络（NGN, Next Generation Networks）的发展，用户移动性（mobility）和主机多穴性（multi homing）的问题越来越普遍，这种 IP 地址的语义过载缺陷日益明显。当主机的 IP 地址发生变化时，不仅  
20 路由要发生变化，通信终端主机的身份标识也会发生变化。对于路由的变化是可以接受的，但是主机身份标识的变化却会导致应用和连接的中断。

为了支持用户移动性和主机多穴性，更好地支持通话的连续性，业界提出了下一代网络中身份标识与位置分离（IPSPLIT, ID/locator separation in

NGN) 技术。在 IPSPLIT 技术中, 采用主机标识符 (Node ID) 作为主机的身份标识, 主机标识符用于全球唯一地标识每台连接到 Internet 的主机, 其目的是将传输层与网络层分开, 为 Internet 提供一个安全的主机移动和多宿主的方法; 进一步地, 提供一个加密的主机标识命名空间, 更容易地对通信双方进行认证, 从而实现安全的、可信任的网络系统。在 IPSPLIT 网络中, IP 地址仅表示通信终端主机在网络拓扑中的路由位置。IPSPLIT 技术解决 IP 地址的语义过载问题, 将 IP 地址的双重功能进行分离, 实现对多移动性、多家乡性、IP 地址动态重分配及不同网络区域之间的互访等问题的支持。

图 1 为现有 IPSPLIT 网络体系的架构示意图, 图 1 中加粗单点划线表示控制信号, 加粗双点划线表示管理信号, 加粗虚线表示媒体流。如图 1 所示, IPSPLIT 网络体系架构包括网络接入控制部分、身份标识与位置分离控制部分、身份标识与位置分离映射部分、资源控制部分、传输部分、业务控制功能部分和用户终端/用户网络部分。其中, 网络接入控制部分为接入 NGN 网络的用户终端/用户网络提供注册、鉴权授权、地址分配、参数配置、位置管理等功能, 例如图 1 中所示的网络附着控制功能 (NACF, Network Attachment Control Functions)。身份标识与位置分离控制功能 (ILCF, Id-loc- control functions) 进行身份标识与位置分离 ID/LOC 映射的存储和动态更新。资源控制部分基于策略和网络资源状态, 完成用户终端/用户网络接入网络时接纳控制、资源预留等功能, 例如 ITU-T NGN 网络中资源接纳控制功能 (RACF, Resource and Admission Control Functions), NGN 中接入管理功能 (Access management Functions)。传输部分完成信息的传输功能, 例如 ITU-T NGN 网络中传输功能 (Transport Functions)。业务控制功能 (Service Control Functions) 部分属于业务层 (Service stratum) 中的一部分, 在业务层次上完成注册、鉴权授权、资源控制等功能, 例如 ITU-T NGN

网络中业务终端认证和鉴权过程。用户终端/用户网络部分向用户提供网络接入功能，例如 ITU-T NGN 网络中用户设备（UE，User Equipment）。

图 2 为现有 IPSPLIT 的体系功能框架示意图，如图 2 所示，其中，NACF 包含如下功能实体：

5 传输层用户配置功能实体（TUP-FE，Transport User Profile Functional Entity），负责保存与传输层面相关的用户信息；

认证和鉴权功能实体（TAA-FE，Transport Authentication and Authorization Functional Entity），用于提供传输层鉴权和认证功能，基于用户信息对用户的网络接入执行鉴权和授权检查；

10 接入管理功能实体（AM-FE，Access Management Functional Entity），用于对用户发起的网络接入请求进行翻译转换，将分配 IP 地址和其它网络配置参数的请求发送给 NAC-FE；

15 传输层位置管理功能实体（TLM-FE，Transport Location Management Functional Entity），用于注册分配给用户的 IP 地址和 NAC-FE 提供的其它网络位置信息；

网络接入管理功能实体（NAC-FE，Network Access Configuration Functional Entity），用于向用户终端分配 IP 地址，同时可能向用户终端分配其他网络配置参数，如 DNS 服务器的地址、信令代理的地址等；

20 身份标识与位置分离映射存储功能实体（ILMS-FE，Id-loc-split mapping storage function entity），作为 NGN 中用户身份标识与位置分离映射存储实体，用于存储用户身份标识 Node ID 与一个或多个位置 LOC 的映射；

身份标识与位置分离映射更新功能实体（ILMU-FE，Id-loc-split mapping update function entity），作为 NGN 中用户身份标识与位置分离映射更新实体，用于实现用户身份标识 Node ID 与一个或多个位置 LOC 的映射的更新。

25 传输功能包含的功能实体如下：

身份标识与位置分离映射功能实体 (ILM-FE, Id-loc-split mapping function entity), 作为 NGN 中用户身份标识与位置分离系统的映射数据库实体, 用于实现用户身份标识 Node ID 与一个或多个位置 LOC 的映射;

策略执行功能实体 (PE-FE, Policy enforcement functional entity), 是传输层策略执行的功能实体。

业务控制功能包含的功能实体为业务层用户配置功能实体 (SUP-FE, Service User Profile Functional Entity), 用于负责配置业务层用户信息。

UE 包含的功能有身份标识与位置分离映射功能 (ILMF, Id-loc-Mapping functions)。

10 基于主机的 IPSPLIT 采用的是 端点标识协议 (HIP, Node Identity Protocol) 协议。HIP 协议是端到端的协议, 图 3 为采用 HIP 协议的主机连接建立过程的示意图, 如图 3 所示, 采用 HIP 协议的主机连接建立过程包括: 当发起方要发起对响应方的 HIP 连接时, 发起方主机先在会和服务器 (Rendezvous Server, 简称为 RVS 服务器) 中注册自己的 IP 地址和身份标识 Node ID<sub>I</sub>, 发起方通过查询目录服务器 DNS, 获得响应方所在的 RVS 服务器的地址。

发起方发送认证包 I1 到响应方所在的 RVS 服务器, 其中至少携带有发起方的身份标识 Node ID<sub>I</sub> 和响应方的身份标识 Node ID<sub>R</sub>, RVS 服务器查找响应方主机当前的 IP 地址, RVS 服务器将相应的认证包 I1 转发到响应方, 响应方回复 R1 消息即响应消息。从第三个包开始, 如图中的 I2 消息和 R2 消息, 能够在基本交换中携带发送数据。

但是, 现有技术中, 没有基于主机的 IPSPLIT 的 HIP 连接建立的实现方法。

## 发明内容

25 有鉴于此, 本发明的主要目的在于提供一种终端实现连接建立的方法

及系统，能够在 IPSPLIT 网络中，传输与控制分离的情况下，实现终端建立连接的过程。

为达到上述目的，本发明的技术方案是这样实现的：

一种终端实现连接建立的方法，应用在下一代网络中的身份标识与位置分离的 IPSPLIT 网络中，在发起方完成注册认证后，该方法还包括：

发起方通过域名服务器 DNS 查询，获得响应方所在映射服务器的地址；

发起方发送 ID/LOC 映射查询消息给所述映射服务器，获得响应方的位置信息；所述映射服务器保存终端的身份标识与位置映射；

发起方根据获得的所述位置信息与响应方建立连接。

10 所述发起方和响应方建立连接包括：

所述发起方发送携带有自身所在位置的位置信息的消息给响应方；

所述响应方对接收到的消息验证后，更新本地关联与自身地址之间的映射关系并向所述发起方所在位置返回响应消息；所述发起方向响应方回复响应确认消息；

15 所述响应方收到响应确认消息后，确认对所述发起方所在位置验证成功，建立与所述发起方之间的连接。

在所述发起方向响应方发送的消息中，还携带有所述发起方的身份标识符、所述响应方的身份标识符及安全参数索引；

20 所述响应方向发起方所在位置返回的响应消息中，携带有用于对所述发起方所在位置的位置信息进行验证的响应参数，及安全参数索引。

所述发起方向响应方发送的消息中还携带有所述发起方所在位置的位置信息生命期。

所述发送方向响应方发送消息后，如果在预设时间段内未收到来自响应方的响应，该方法还包括：

25 所述发起方重新发送所述携带有自身所在位置的位置信息的消息。

所述响应方所在映射服务器为身份标识与位置分离映射存储功能实体 ILMS-FE 或身份标识与位置分离映射更新功能实体 ILMU-FE。

一种终端实现连接建立的系统，该系统至少包括发起方、DNS、映射服务器和响应方，其中，

5 发起方，用于通过域名服务器 DNS 查询，获得响应方所在映射服务器的地址；发送 ID/LOC 映射查询消息给所述映射服务器，获得响应方的位置信息；根据获得的所述位置信息与响应方建立连接；

DNS，用于接收发起方的查询，提供响应方所在映射服务器的地址；

映射服务器，用于接收发起方的查询，通过身份标识与位置映射查询，  
10 获得响应方的位置信息并返回给发起方；保存终端的身份标识与位置映射即 ID/LOC 映射；

响应方，用于与发起方建立连接。

所述发起方，还用于与响应方使用安全封装协议 ESP 通道，执行数据封装发送或解封操作。

15 所述映射服务器为身份标识与位置分离映射存储功能实体 ILMS-FE，或身份标识与位置分离映射更新功能实体 ILMU-FE。

从上述本发明提供的技术方案可以看出，包括发起方通过域名服务器（DNS）查询，获得响应方所在映射服务器的地址；发起方通过响应方所在映射服务器，通过 ID/LOC 映射查询查找到响应方的地址；发起方和响应方通过基本交换，建立连接。本发明方法中，业务的访问使用身份标识符 Node ID，终端连接过程通过身份标识符找到对端用户的位置，并在发起方  
20 与响应方之间直接建立连接，不仅实现了传输与控制分离的情况下，终端建立连接的过程，而且保证了连接的可靠性。

## 附图说明

25 图 1 为现有 IPSPLIT 网络体系的架构示意图；



图 2 为现有 IPSPLIT 的体系功能框架示意图;

图 3 为现有采用 HIP 协议的主机连接建立过程的示意图;

图 4 为本发明终端实现连接建立的方法的流程示意图;

图 5 为本发明终端实现连接建立的方法的实施例的流程图。

## 5 具体实施方式

图 4 为本发明终端实现连接建立的方法的流程示意图, 如图 4 所示, 在 IPSPLIT 网络中, 当发起方要发起对响应方的连接时, 在发起方完成注册认证后, 包括:

首先, 发起方通过 DNS 查询, 获得响应方所在映射服务器的地址;

10 然后, 发起方通过响应方所在映射服务器, 通过 ID/LOC 映射查询, 利用响应方的身份标识符 Node ID 查找到响应方的位置信息 (LOC); 所述映射服务器保存终端的身份标识与位置映射即 ID/LOC 映射。

最后, 发起方根据获得的所述位置信息与响应方建立连接。

15 进一步地, 发送方和响应方通过 IPsec 封装式安全协议 (ESP) 通道, 执行将数据封装发送或解封操作。具体实现属于现有技术, 这里不再赘述。

在 IPSPLIT 网络中, 应用和业务层与身份标识符相映射, 当终端因位置发生改变时身份标识符不变, 从而业务和应用不会中断, 本发明方法中, 业务的访问使用身份标识符 Node ID, 终端连接过程通过身份标识符找到对端用户, 不仅实现了传输与控制分离的情况下, 终端建立连接的过程, 而且保证了连接的可靠性。

20

针对本发明方法, 还提供一种终端实现连接建立的系统, 如图 4 所示, 至少包括发起方、DNS、映射服务器和响应方, 其中,

发起方, 用于通过域名服务器 DNS 查询, 获得响应方所在映射服务器的地址; 发送 ID/LOC 映射查询消息给所述映射服务器, 获得响应方的位置  
25 信息; 根据获得的所述位置信息与响应方建立连接;

DNS, 用于接收发起方的查询, 提供响应方所在映射服务器的地址;

映射服务器, 用于接收发起方的查询, 通过身份标识与位置映射查询, 利用响应方的身份标识符 Node ID 查找到响应方的位置信息并返回给发起方; 保存终端的身份标识与位置映射即 ID/LOC 映射;

5        响应方, 用于与发起方建立连接。

发起方, 还用于与响应方使用安全封装协议 (ESP) 通道, 执行数据封装发送或解封等操作。

图 5 为本发明终端实现连接建立的方法的实施例的流程图, 图 5 中假设发起方为 UE1, 响应方为 UE2, 当 UE1 完成注册认证后, UE1 开始进行连接建立过程, 如图 5 所示, 包括以下步骤:

10        步骤 500: UE1 查询 DNS 服务器, 获得 UE2 所在映射服务器的 IP 地址。本步骤中, 映射服务器指 ILMS-FE 或 ILMU-FE。

步骤 501: UE1 向 UE2 所在映射服务器发送 ID/LOC 映射查询 (ID/LOC mapping query), 其中携带有 UE2 的身份标识符。

15        步骤 502: UE2 所在映射服务器, 利用 UE2 的身份标识符查询获得 UE2 的 LOC 信息, 并将获得的 UE2 的 LOC 信息携带在 ID/LOC 映射响应 (ID/LOC mapping response) 中返回给 UE1。UE2 所在映射服务器保存终端的身份标识与位置映射即 ID/LOC 映射。

步骤 503: UE1 与 UE2 连接建立, 具体包括:

20        UE1 发送携带有自身所在位置的 LOC 信息的信息给 UE2, 在该消息中, 还携带有 UE1 的身份标识符 Node ID1 和 UE2 的身份标识符 Node ID2 以及安全参数索引, 同时参数中包含 UE1 所在位置的 LOC 信息的生命期。UE1 发送该消息后, 等待来自 UE2 的确认。进一步地, 如果在预设时间段内未收到来自 UE2 的响应, 可以进行重发。

25        UE2 收到 UE1 发送的消息并验证后, 更新本地关联与 UE2 地址之间的

映射关系并向 UE1 所在位置（由 UE1 所在位置的 LOC 信息指示）返回响应消息。同时，UE2 为了对 UE1 所在位置的 LOC 信息进行验证，会在响应消息中携带响应参数，响应消息中还应携带有安全参数索引。

5 UE1 处理来自 UE2 的响应消息并向 UE2 回复响应确认消息。UE2 收到响应确认消息后，认为对 UE1 所在位置的 LOC 信息验证成功完成，建立 UE1 与 UE2 之间的连接。

需要说明的是，发起方与响应方之间的验证具体实现可以采用现有多种方式实现，这里并不用于限定本发明保护范围。本发明强调的是，业务的访问使用身份标识符，终端连接过程通过身份标识符找到对端用户的位置，并在发起方与响应方之间直接建立连接。

10 UE1 与 UE2 之间建立连接后，UE1 与 UE2 使用 ESP 通道，执行数据封装发送或解封等操作。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

## 权利要求书

1、一种终端实现连接建立的方法，应用在下一代网络中的身份标识与位置分离的 IPSPLIT 网络中，发起方完成注册认证后，其特征在于，该方法还包括：

- 5       发起方通过域名服务器 DNS 查询，获得响应方所在映射服务器的地址；  
发起方发送 ID/LOC 映射查询消息给所述映射服务器，获得响应方的位置信息，其中，所述映射服务器保存终端的身份标识与位置映射；  
发起方与响应方建立连接。

- 2、根据权利要求 1 所述的方法，其特征在于，所述发起方和响应方建立连接包括：

所述发起方发送携带有自身所在位置的位置信息的信息给响应方；

所述响应方对接收到的消息验证后，更新本地关联与自身地址之间的映射关系并向所述发起方所在位置返回响应消息；所述发起方向响应方回复响应确认消息；

- 15       所述响应方收到响应确认消息后，确认对所述发起方所在位置验证成功，建立与所述发起方之间的连接。

3、根据权利要求 2 所述的方法，其特征在于，在所述发起方向响应方发送的消息中，还携带有所述发起方的身份标识符、所述响应方的身份标识符以及安全参数索引；

- 20       所述响应方向发起方所在位置返回的响应消息中，携带有用于对所述发起方所在位置的位置信息进行验证的响应参数，及安全参数索引。

4、根据权利要求 3 所述的方法，其特征在于，所述发起方向响应方发送的消息中还携带有所述发起方所在位置的位置信息的生命期。

- 25       5、根据权利要求 4 所述的方法，其特征在于，所述发送方向响应方发送消息后，如果在预设时间段内未收到来自响应方的响应，该方法还包括：

所述发起方重新发送所述携带有自身所在位置的位置信息的信息。

6、根据权利要求 1 所述的方法，其特征在于，所述响应方所在映射服务器为身份标识与位置分离映射存储功能实体 ILMS-FE 或身份标识与位置分离映射更新功能实体 ILMU-FE。

5 7、一种终端实现连接建立的系统，其特征在于，该系统至少包括发起方、DNS、映射服务器和响应方，其中，

发起方，用于通过域名服务器 DNS 查询，获得响应方所在映射服务器的地址；发送 ID/LOC 映射查询消息给所述映射服务器，获得响应方的位置信息；根据获得的所述位置信息与响应方建立连接；

10 DNS，用于接收发起方的查询，提供响应方所在映射服务器的地址；

映射服务器，用于接收发起方的查询，通过身份标识与位置映射查询，获得响应方的位置信息并返回给发起方；保存终端的身份标识与位置映射即 ID/LOC 映射；

响应方，用于与发起方建立连接。

15 8、根据权利要求 7 所述的系统，其特征在于，所述发起方，还用于与响应方使用安全封装协议 ESP 通道，执行数据封装发送或解封操作。

9、根据权利要求 7 或 8 所述的系统，其特征在于，所述映射服务器为身份标识与位置分离映射存储功能实体 ILMS-FE，或身份标识与位置分离映射更新功能实体 ILMU-FE。

20

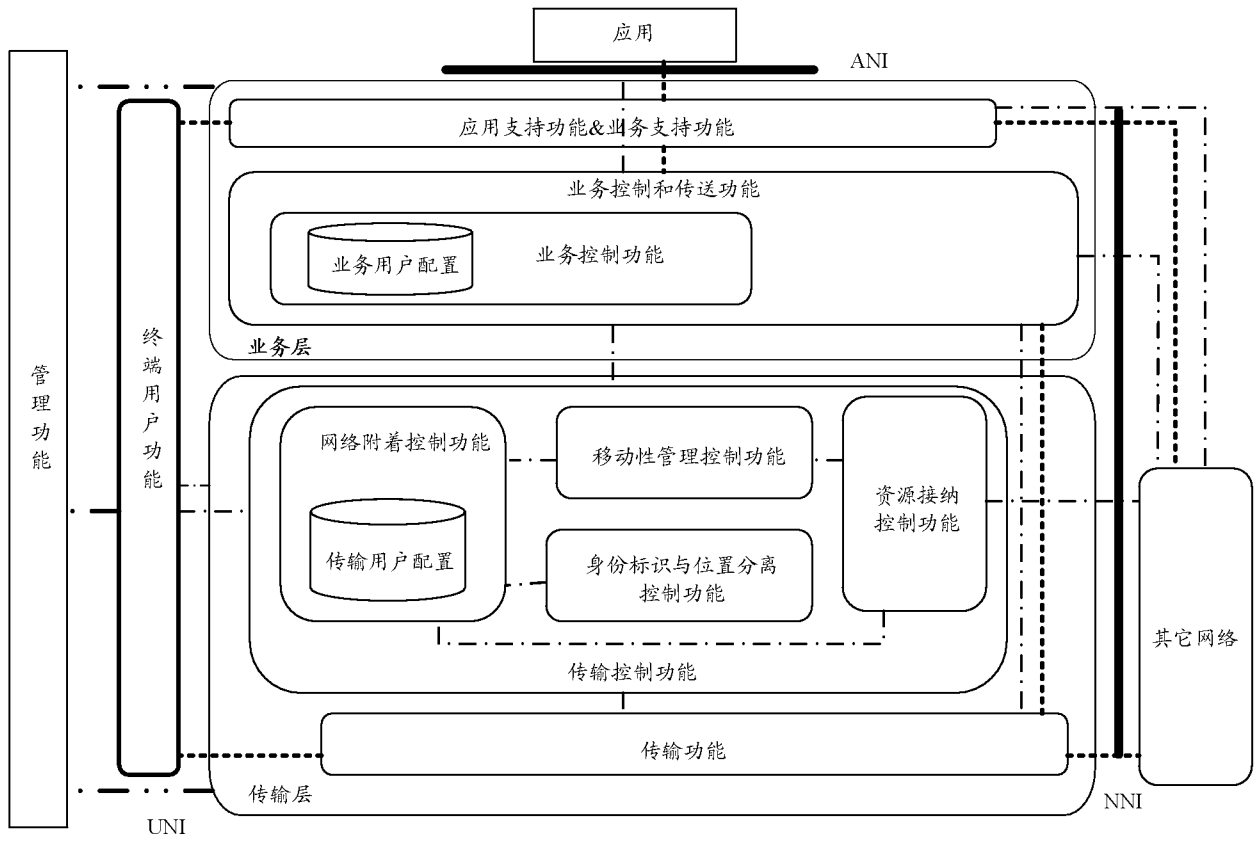


图 1

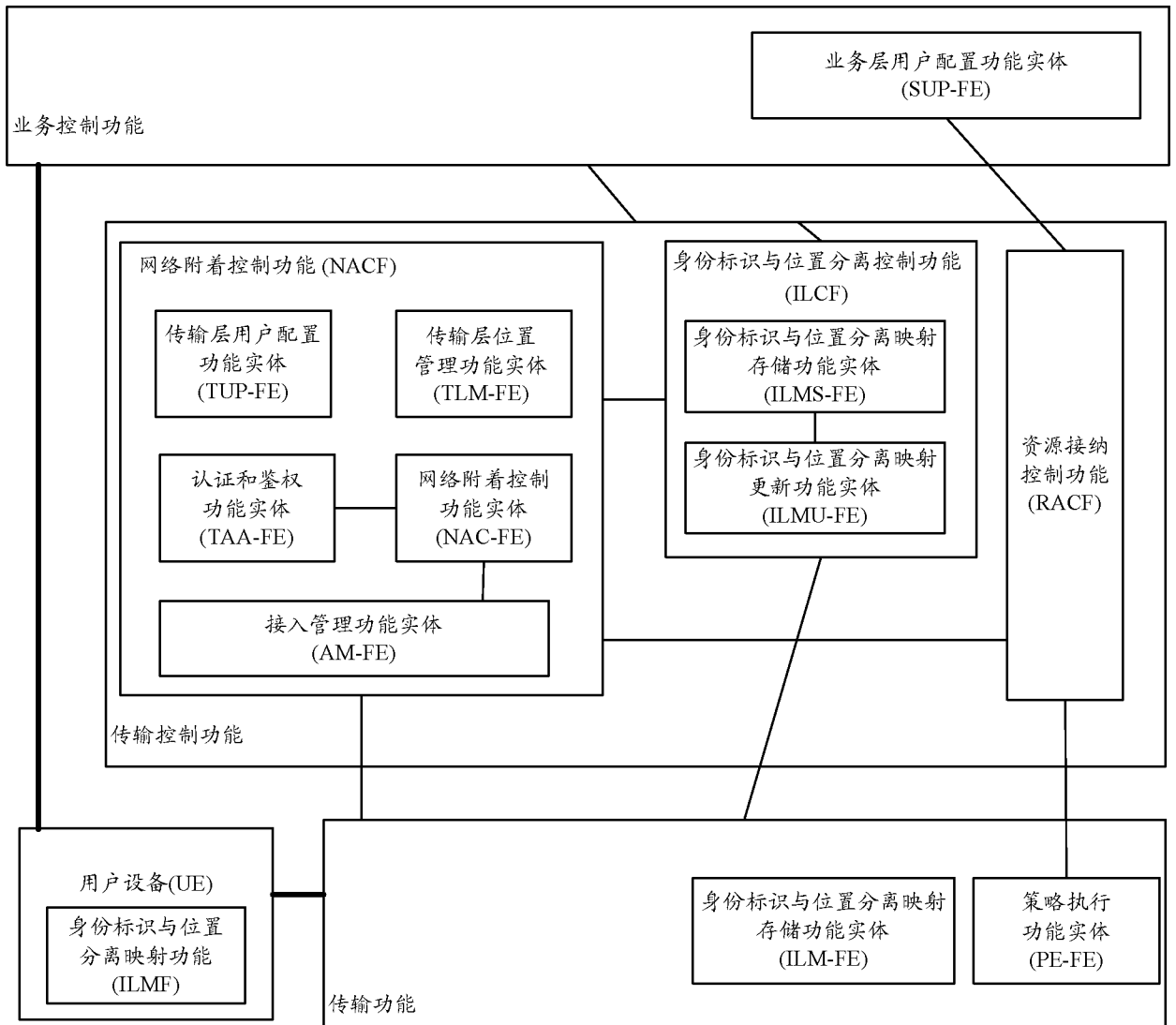


图 2

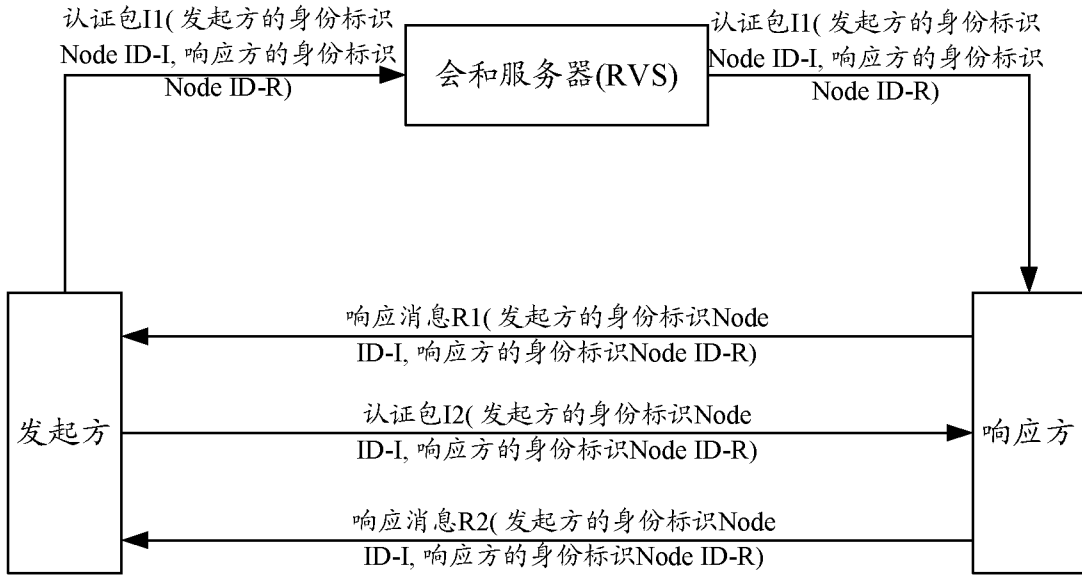


图 3

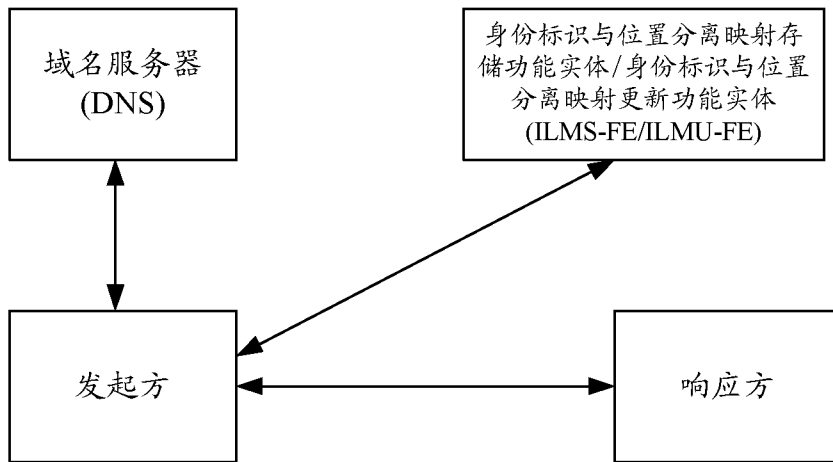


图 4



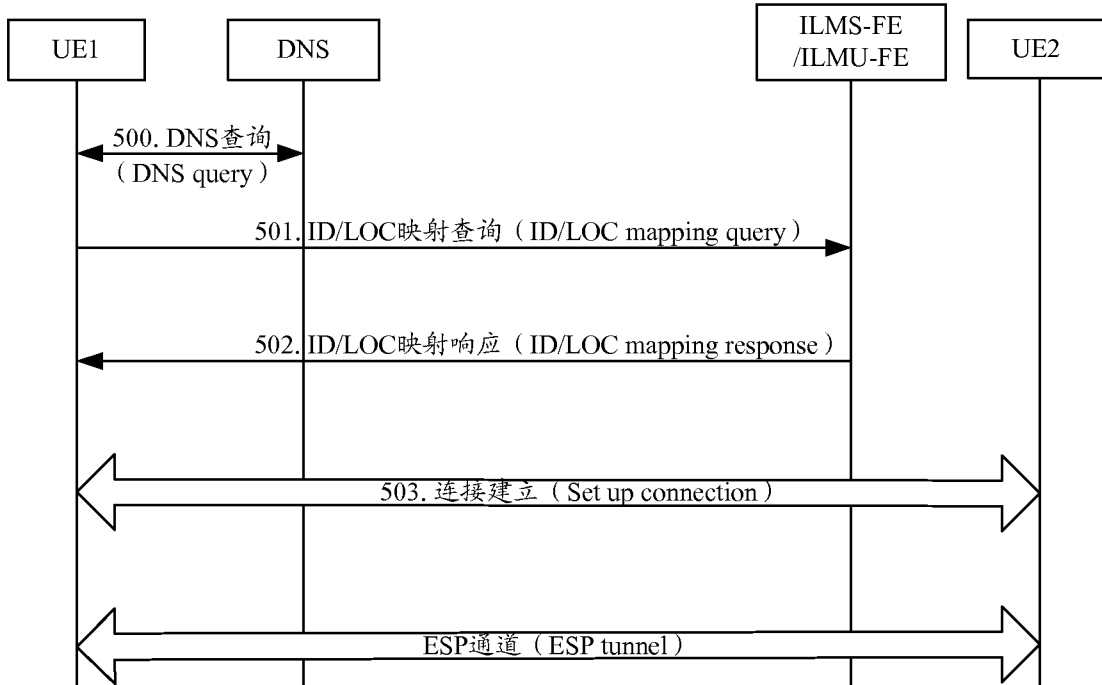


图 5

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/076142

## A. CLASSIFICATION OF SUBJECT MATTER

H04W76/00(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L; H04W; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRS, CNKI, WPI, EPODOC; NGN, ID, identity, Loc, location, position, separat+, split, address, map+, server, connect+, DNS, IP, terminal, node, ILMU, ILMU

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1801764A (UNIV BEIJING JIAOTONG) 12 Jul. 2006(12.07.2006) the description page 6 line 10-page 11 line 7, figs. 1-2	1-9
A	CN101656765A (ZTE CORP) 24 Feb. 2010(24.02.2010) the whole document	1-9
A	US2008005275A1 (BAILEY S W et al.) 03 Jan. 2008(03.01.2008) the whole document	1-9

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>“&amp;” document member of the same patent family</p>
--	---

Date of the actual completion of the international search  
15 Dec. 2010(15.12.2010)

Date of mailing of the international search report  
**06 Jan. 2011 (06.01.2011)**

Name and mailing address of the ISA/CN  
The State Intellectual Property Office, the P.R.China  
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China  
100088  
Facsimile No. 86-10-62019451

Authorized officer  
**CAO, Juan**  
Telephone No. (86-10)62411251

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/CN2010/076142

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1801764A	12.07.2006	CN100428719C	22.10.2008
CN101656765A	24.02.2010	None	
US2008005275A1	03.01.2008	WO0195137A2	13.12.2001
		US2002032787A1	14.03.2002
		AU6535001A	17.12.2001
		AU2001265350A8	06.10.2005
		US7233978B2	19.06.2007

国际检索报告

国际申请号  
**PCT/CN2010/076142**

<b>A. 主题的分类</b>		
H04W76/00(2009.01)i		
按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类		
<b>B. 检索领域</b>		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L; H04W; G06F		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CPRS,CNKI,WPI,EPODOC: 下一代网络、NGN、身份、标识、位置、分离、IPSPLIT、DNS、域名服务器、映射、服务器、ILMS、ILMU、查询、地址、IP、连接、终端; NGN, ID, identity, Loc, location, position, separat+, split, address, map+, server, connect+, DNS, IP, terminal, node, ILMS, ILMU		
<b>C. 相关文件</b>		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN1801764A (北京交通大学) 12.7 月 2006(12.07.2006)	1-9
A	CN101656765A (中兴通讯股份有限公司) 24.2 月 2010(24.02.2010) 全文	1-9
A	US2008005275A1 (BAILEY S W et al.) 03.1 月 2008(03.01.2008) 全文	1-9
<input type="checkbox"/> 其余文件在 C 栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 15.12 月 2010(15.12.2010)		国际检索报告邮寄日期 <b>06.1 月 2011 (06.01.2011)</b>
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员  <b>曹娟</b> 电话号码: (86-10) <b>62411251</b>

国际检索报告  
关于同族专利的信息

国际申请号  
**PCT/CN2010/076142**

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1801764A	12.07.2006	CN100428719C	22.10.2008
CN101656765A	24.02.2010	无	
US2008005275A1	03.01.2008	WO0195137A2	13.12.2001
		US2002032787A1	14.03.2002
		AU6535001A	17.12.2001
		AU2001265350A8	06.10.2005
		US7233978B2	19.06.2007