(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
2017 年 6 月 29 日 (29.06.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/107033 A1

(51) 国际专利分类号:
H04L 12/717 (2013.01)

(21) 国际申请号: PCT/CN2015/098167

(22) 国际申请日: 2015 年 12 月 22 日 (22.12.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **北京大学深圳研究生院 (PEKING UNIVERSITY SHENZHEN GRADUATE SCHOOL)** [CN/CN]; 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。

(72) 发明人: **李挥 (LI, Hui)**; 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。 **刘慧玲 (LIU, Huiling)**; 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。 **于超琪 (YU, Chaoqi)**; 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。

(74) 代理人: **深圳市科吉华烽知识产权事务所（普通合伙） (SHENZHEN KINDWALF INTELLECTUAL PROPERTY FIRM)**; 中国广东省深圳市南山区深南西路深南花园裙楼 A 区四层 402 室, Guangdong 518057 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: IDENTITY-BASED CENTRALIZED-CONTROL NETWORK (ICCN) ARCHITECTURE

(54) **发明名称** : 一种基于身份的集中控制式网络体系架构 ICCN

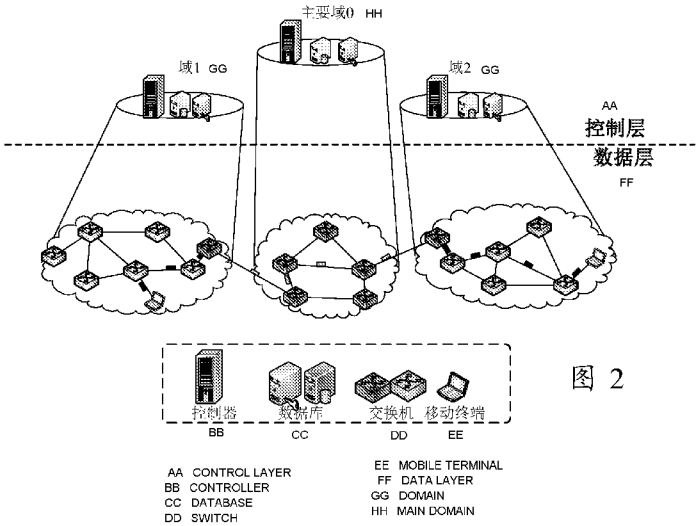

图 2

(57) **Abstract**: The present invention relates to the field of network protocols. Disclosed is a centralized identity network (CIN) routing protocol, comprising an application layer, a data link layer and a physical layer, and further comprising an identity/location layer, wherein the identity/location layer is located between the application layer and the data link layer; the identity/location layer decouples an identity attribute and a location attribute of an IP address; and the identity/location layer puts same in an identity location mapping database (ILMD) and an identity location mapping cache (ILMC) of a whole network. The beneficial effects of the present invention are that in the present invention, the compatibility of an identity and location separation network and a current IPv6 network is realized by way of adding an IPv6 expansion header, without modifying a host protocol stack; and a simple and effective method without a convergence server is proposed to deal with the problem of mobility.

(57) **摘要**:

[见续页]

WO 2017/107033 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明涉及网络协议领域，其公开了一种集中式身份网络路由协议 CIN：包括应用层、数据链路层和物理层，还包括身份/位置层，所述身份/位置层位于应用层和数据链路层之间；所述身份/位置层解耦 IP 地址的身份属性和位置属性；所述身份/位置层放入全网身份位置映射数据库 ILMD 和身份位置映射缓存 ILMC。本发明的有益效果是：本发明采用增加 Ipv6 扩展首部的方式实现身份位置分离网络与当前 IPv6 网络的兼容，且不需要修改主机协议栈；提出一种不需要汇聚服务器，简单且有效的方法应对移动性问题。

一种基于身份的集中控制式网络体系架构 ICCN

【技术领域】

本发明涉及网络协议领域，尤其涉及一种基于身份的集中控制式网络体系架构 ICCN。

【背景技术】

传统互联网中，终端地址即IP地址同时包含了身份信息和地址信息。身份标识通信终端，而地址用来在网络中路由。IP地址的二义性导致了一些问题，如路由扩展性，主机移动性等问题。为了解决这些问题，并且满足新一代网络的高速效率和普遍性的要求，已经有一些将身份信息和位置信息分离的解决方案被提出。解决方案主要有两种类型，一种基于主机，如HIP和SHIM6，另一种则是基于路由，如LISP。身份位置分离有着明显的优点：例如可在扩展性问题上一定程度的减缓BGP路由表的增长，给予移动性一定的支持。

软件定义网络（SDN）是一种自从美国斯坦福大学 Clean Slate 研究组提出后，就引起了学术界和工业界众多兴趣的新型网络架构样例。SDN 的核心思想是控制和转发分离思想，即 SDN 将所有控制逻辑，例如路由协议，防火墙，负载均衡配置等都从交换机中剥离出来放入 SDN 控制器中，只在交换机中留下转发功能，从而实现分离。在实现上，可编程接口像 OpenFlow 规定了控制器和交换机通信的标准方式，从而允许网络软件与硬件通信，并且各自独自开发发展。而 SDN 控制器则是在知道网络拓扑信息后会做出快速的决策决定，而无需考虑数据包在网络中的转发过程。并且在部署网络时，无需针对每个硬件进行配置，通过控制程序可以直接部署实现，并且使得调试和检测都更加容易。

LISP 是思科公司提出的一种在网络设备上实现身份与位置分离的协议。

它使用一部分 IP 地址作为终端标识（EID，Endpoint Identifier），

另一部分 IP 地址作为网络通信中的路由位置标识（RLOC，Routing Locators），终端通过 EID 来访问对端节点，而终端的位置标识 RLOC 由其连接的边界路由器决定。LISP 在设计时考虑了实现与部署的实际问题。它在保持了现有终端的网络协议架构不变的基础上，只改变了终端接入路由器的工作方式，因此对现有基础设施的修改较小，易于渐进部署。

LISP 是以隧道的形式在互联网的核心将数据从源 EID 的 RLOC 转发到目的 EID 的 RLOC。EID 与现有 IP 地址格式完全相同，可以使 32 位的 IPv4 地址，也可以是 128 位的 IPv6 地址，区别在于，EID 与网络拓扑无关，是扁平化标识，是根据 EID-to-RLOC 映射服务器的部署进行分配的。通信前，终端由 DNS 查询获得对端终端的 EID。RLOC 则是接入路由器 IPv4 或 IPv6 地址，用于在路由系统中实现数据包的存储和转发。RLOC 代表的是位置信息，按照网络拓扑结构进行分配，通信中，路由器通过查询 EID-to-RLOC 数据库获得与终端 EID 对应的 RLOC。互联网上两个终端在进行端到端的数据传输时，发送隧道路由器（ETR，Egress Tunnel Router）为每个数据包加上含有通过查询数据库得到的通信对端 EID 对应的 RLOC 的 LISP 报头，接收隧道路由器（ITR，Ingress Tunnel Router）在接收到数据包后去掉 LISP 报头，在转发给目的 EID。用这种方式，核心互联网没有必要知道本地 EID，只要知道 RLOC 就足以满足数据包的转发。

LISP 通信过程中的地址转换，即身份标识与位置标识的转换，是由映射机制提供了一对 EID 和 RLOC 的映射，并且维护了 RLOC 的地址可达状态。

LISP 的协议栈格式，以及数据包转发过程中的标识转换示意如图 1 所示。

LISP 在一定程度上改善了传统网络中 IP 地址的二义性问题，并且简化了渐进部署的难度。但是 LISP 仍存在诸多问题。

1） LISP 仍硬件具有较大的依赖性；

2） LISP 中，对于路由 ETR 和 ITR 而言，需要完成映射查询和转换功能，对于硬件路由器性能要求较高；

3） 此外 LISP 中映射更新的频率以及使用什么样的映射查询的算法都能影响网络中终端通信的效率；

4） 最后，当前互联网中，每一个终端可以给网络中任意终端发送数据包，虽然 LISP 在核心网络中将终端标识封装到了数据包的有效载荷中，但是中间人仍然可以解封装从而得到 EID，这就会产生 DDoS 攻击问题。

【发明内容】

为了解决现有技术中的问题，本发明提供了一种基于身份的集中控制式网络体系架构 ICCN，解决现有技术中对硬件要求很高的问题。

本发明提供了一种基于身份的集中控制式网络体系架构 ICCN，包括控制转发行为的逻辑的控制层、根据控制层逻辑来转发流量的数据层和拓扑发现；该控制层为控制器以及与控制相关的数据库，所有控制数据包的操作均通过控制器完成，所有与终端和映射相关的信息都存储在注册数据库和映射数据库中；该数据层包括交换机和终端，数据层进行数据包转发。

作为本发明的进一步改进：控制器在网络建立初始获得网络交换机的信息，控制器检查数据包头来验证一个终端是否是合法的或正确的，控制器注册合法终端到注册数据库中；控制器进行路由策略。

作为本发明的进一步改进：控制器根据映射系统来修改数据包包头进行身份与位置分离。

作为本发明的进一步改进：交换机不需要收集邻居交换机的信息，也不需要修改数据包，交换机通过流表的动作来转发包。

作为本发明的进一步改进：拓扑发现中，控制器主动获得网络中交换机信息，网络以域级关系组织，每个控制器维护自己域内拓扑信息，主要域连接所有域，主要域控制器拥有全部域到达交换机信息。

作为本发明的进一步改进：控制器控制传入流量，在主要域中，使用终端地址标识来转发路由，终端的身份标识是公开的。

作为本发明的进一步改进：终端身份标识 HID 是一个 64 位的数字，终端对应的位置标识 LID 为交换机上的 OpenFlow 实例 DPID 的唯一表示；一个终端身份标识 HID 对应至少一个终端对应的位置标识 LID。

作为本发明的进一步改进：控制器注册通信终端信息和保存终端身份标识与位置标识映射信息，控制器通过查询数据库发现目标终端，并

通过最短路径算法建立转发包路径，并向OpenFlow交换机下发转发流表。

作为本发明的进一步改进：终端身份标识 HID 不改变即连接不中断的情况下进行通信；分层机制增大了流表的尺寸，在域内可以部署不同的网络机制。

本发明的有益效果是：本发明减少发现目标并将数据包转发到通信终端的时间，大大提高了通信效率；提高了可扩展性，增强了网络的适应能力；一定程度上增强了网络的安全性。

【附图说明】

图 1 是传统 LISP 协议栈格式及地址转换示意图。

图 2 是本发明 ICCN 结构示意图。

图 3 是本发明命名机制及数据库存储实例图。

图 4 是本发明 ICCN 注册流程图。

图 5 是本发明 ICCN 中终端通信时数据包组成图。

图 6 是本发明 ICCN 中终端通信流程图。

图 7 是本发明 ICCN 中终端移动后通信时数据包组成图。

【具体实施方式】

下面结合附图说明及具体实施方式对本发明进一步说明。

缩略语和关键术语定义

I/LS	Identity/Locator Separation	身份位置分离
SDN	Software Defined Network	软件定义网络
HIP	Host Identity Protocol	主机标识协议
SHIM6	Multihoming Shim Protocol for IPv6	IPv6 多宿协议
LISP	Locator/ID Separation Protocol	位置与身份分离协议
EID	Endpoint Identifier	终端标识
RLOC	Routing Locators	路由标识
ETR	Egress Tunnel Router	发送隧道路由器

ITR Ingress Tunnel Router 接收隧道路由器

DDoS Distributed Denial-of-service 分布式拒绝服务攻击

OpenFlow 新型网络交换模型

ICCN Identity-based Centralized Control Network 基于身份的集中控制式网络体系架构

HID Host Identity 终端身份标识

LID Locator Identity 位置标识

DPID Datapath Identity OpenFlow 交换机实例标识

hx HID Number 身份标识名

lx and dpidx LID Number 位置标识名

cx Controller Number 控制器名

rx Register Database Number 注册数据库名

mx Mapping Database Number 映射数据库名

Dx Domain Number 域名

MD5 Message Digest Algorithm 信息摘要算法第五版

R<> Register Function 注册函数（本发明中均使用 MD5 函数）

C<> Connection Function 连接函数（本发明中均使用 MD5 函数）

一种基于身份的集中控制式网络体系架构 ICCN，包括控制转发行为的逻辑的控制层、根据控制层逻辑来转发流量的数据层和拓扑发现；该控制层为控制器以及与控制相关的数据库，所有控制数据包的操作均通过控制器完成，所有与终端和映射相关的信息都存储在注册数据库和映射数据库中；该数据层包括交换机和终端，数据层进行数据包转发。

控制器在网络建立初始获得网络交换机的信息，控制器检查数据包头来验证一个终端是否是合法的或正确的，控制器注册合法终端到注册

数据库中；控制器进行路由策略。

控制器根据映射系统来修改数据包包头进行身份与位置分离。

交换机不需要收集邻居交换机的信息，也不需要修改数据包，交换机通过流表的动作来转发包。

拓扑发现中，控制器主动获得网络中交换机信息，网络以域级关系组织，每个控制器维护自己域内拓扑信息，主要域连接所有域，主要域控制器拥有全部域到达交换机信息。

控制器控制传入流量，在主要域中，使用终端地址标识来转发路由，终端的身份标识是公开的。

终端身份标识 HID 是一个 64 位的数字，终端对应的位置标识 LID 为交换机上的 OpenFlow 实例 DPID 的唯一表示；一个终端身份标识 HID 对应至少一个终端对应的位置标识 LID。

控制器注册通信终端信息和保存终端身份标识与位置标识映射信息，控制器通过查询数据库发现目标终端，并通过最短路径算法建立转发包路径，并向 OpenFlow 交换机下发转发流表。

终端身份标识 HID 不改变即连接不中断的情况下进行通信；分层机制增大了流表的尺寸，在域内可以部署不同的网络机制。

本发明以一种和谐的方式融合了身份位置分离和 SDN 转发控制分离思想，提出了一种基于身份的集中控制式网络体系架构 ICCN（Identity-based Centralized Control Network），在改进了传统网络中 IP 地址二义性问题的同时，继承并扩展了身份位置分离思想和 SDN 转控分离思想的优点。

本发明实现：控制层各个域控制器集中式管理网络；控制层各个控制器间同步与通信技术；控制层各个域数据库存储终端连接信息，以及终端映射信息；控制层主要域控制器维护域间可达性信息；控制层主要域数据库存储终端映射信息；控制层主要域控制器计算域间通信路径；控制层主要域控制器下达转发流表至交换机；控制层域内控制器主动拓扑发现；控制层域内控制器计算维护网络可达性信息；控制层域内控制器验证终端合法性；控制层域内控制器计算终端注册函数值；控制层域内控制器注册终端到注册数据库；控制层域内控制器计算终端间通信连

接函数值；控制层域内控制器存储终端通信映射连接函数值到映射数据库；控制层域内控制器存储终端身份标识与位置标识映射信息到映射数据库；控制层域内控制器通过查询映射数据库得到通信终端位置标识；控制层域内控制器计算终端通信路径；控制层域内控制器下发转发流表至交换机；控制层域内控制器修改数据包头实现身份与位置分离；控制层域内控制器在终端移动后要更新映射数据库的连接信息与映射信息；控制层域内控制器从数据库中删除从本域移动走的终端的信息；数据层交换机查询转发流表；数据层交换机根据流表转发规则转发数据包；各个域内使用 DPID 转发数据包；域间使用 LID 转发数据包。

图 2 给出了 ICCN 框架的概述，以下详细解释并定义了 ICCN 中的几个重要概念与机制，所有的描述都是基于 SDN 的。

1） 控制层

控制层可以定义为控制转发行为的逻辑，例如路由协议，防火墙负载均衡配置等。在ICCN中，我们简化控制层为控制器以及与控制相关的数据库。所有控制数据包的行为都发生在ICCN的控制器当中。所有与终端和映射相关的信息都存储在ICCN的注册数据库和映射数据库中。

控制器可以在网络建立初始获得网络交换机的信息，控制器还可以检查数据包头来验证一个终端是否是合法的或我们想要的。控制器注册合法终端到注册数据库中。如果一个终端已经在系统中存在，那么控制器就要更新信息。然后在终端请求通信后，控制器还得查询映射系统之后发出决定数据包怎样转发的命令，这一步骤可称为路由策略。此外，控制器根据映射系统来修改数据包包头以实现身份与位置分离。

2） 数据层

数据层可以被解释为根据控制层逻辑来转发流量例如IP转发，2层交换。在ICCN中，数据层包括了交换机和终端。数据包转发是数据层的主

要功能。即，当一个终端发送一个数据包到交换机，接收到控制器命令的交换机会将数据包转发到目的主机。交换机不需要收集邻居交换机的信息，也不需要修改数据包。交换机唯一要做的事情就是根据流表的动作来转发包。

我们将控制层和数据层分开不仅仅是因为软件控制可以独立于硬件开发，也因为更容易调试和检查网络的行为。

3）拓扑发现

在网络建立伊始，控制器主动获得网络中交换机信息，即得知网络中所有节点的可达性信息。ICCN假设网络以域级关系组织。每个控制器维护自己域内拓扑信息。主要域连接所有域，其控制器拥有全部域可达交换机信息，即可以保证终端在全网范围内通信。

4）安全性

在ICCN中，当一个OpenFlow交换机第一次从一个终端接收到数据包时，交换机会因流表无转发动作而将数据包发送到控制器。而控制器将处理数据包头，检查根据终端身份标识而得到的注册函数值，以此来验证此终端是否是合法和想要的终端。因此，控制器可以控制传入流量，尤其拒绝不想要的流量。ICCN在主要域中，使用终端地址标识来转发路由，终端的身份标识是透明的。所以攻击者很难正确的猜测终端的身份标识。因此，攻击者不知道终端在什么位置。因此提高了安全性。

2.2.1 本发明实施例一：

1） 命名机制

与目前的互联网仅使用IP地址不同，ICCN使用2个命名空间，以此来

实现身份位置分离。图3展示了一个ICCN命名机制及数据库存储的实例。

在ICCN中，终端身份标识HID（Host Identity）是一个64位的数字，因此可以使用IPv6地址，在本发明中用hx代表。终端对应的位置标识LID（Locator Identity）有2种情况。1种在域内，每个交换机上的OpenFlow实例都有一个DPID（datapathid）的唯一表示，用来表示终端在域内的地址标识，用dpidx代表，DPID是64位。另外一种是在主要域即域间，也同样用OpenFlow实例的DPID表示地址标识，用lx代表，也是64位。特别的，连接了域与主要域的特殊交换机，拥有2个LID即dpidx和lx，用来保证数据包可以在域内和域间传输。因此我们可以知道在域内使用地址dpidx转发包，而在主要域，即在域间使用lx转发包。由于终端是可以移动的，所以每一个HID都可以对应于许多LID，即一对HID和lx为一对映射，一对HID与dpidx也是一对映射。我们命名每一个域为Dx，主要域命名为MDx。我们用cx来命名控制器，同时我们用rx和mx来命名网络中的数据库。

图3还有2个重要的函数，用来注册终端和存储映射关系。我们表示这2个函数为注册函数R<HID>和连接标识函数C<HID1, HID2, LID1, LID2>。我们假设，控制器和网络中的终端已经相互协商好了R与C函数是什么。在ICCN中，我们使用MD5来简化实现。

表1、2、3给出了数据库中记录的一种格式：

表1 注册数据库中的记录格式

Record of Registration Database	
Host Identity	终端身份标识 hx（64-bit）
Registration	终端注册函数值 MD5<hx>（128-bit）

Value	
Source Switch DPID	终端所接入交换机标识，即终端地址标识 dpidx(64-bit)
Source Access Switch DPID	终端所在域接入主要域的交换机标识，即终端地址标识 dpidx/lx(64-bit)
Domain Name	终端所属域名 Dx

表2 域内映射数据库的记录格式

Record of Mapping Database (Inner Domain)	
Connection Value	一对通信终端连接函数值 MD5<hx, hx', lx, lx'>（128-bit）
Source Host Identity	源终端身份标识 hx（64-bit）
Destination Host Identity	目的终端身份标识 hx'（64-bit）
Source Access Switch DPID	源终端所在域接入主要域的交换机标识，即源终端地址标识 lx(64-bit)
Destination Access Switch DPID	目的终端所在域接入主要域的交换机标识，即目的终端地址标识 lx'（64-bit）

表3 主要域映射数据库的记录格式

Record of Mapping Database (Main Domain)	
Host Identity	终端身份标识 hx（64-bit）

Source Access Switch DPID	终端所在域接入主要域的交换机标识，即终端地址标识 lx(64-bit)
Domain Name	终端所属域名 Dx

2） 注册机制

在ICCN中，当一个终端发送数据包进行注册或和目的终端通信时，我们会检查终端有效性。如果有效则到注册数据库或是与目的终端通信，表4给出了一种终端发送的数据包包头格式，图4是ICCN注册流程。

表4 终端发送的数据包包头格式

Packet (from Host) Header	
Source Host Identity	源终端身份标识 hx（64-bit）
Destination Host Identity	目的终端身份标识 hx’（64-bit）
Registration Value	终端注册函数值 MD5<hx>（128-bit）

终端h1发送数据包，数据包被封装为表1的格式，简写为[h1, h2, R<h1>, Data]，当交换机dpid1首次接收到从终端h1发送来的数据包，交换机在流表中无法查到相匹配的表项，所以流量会被发送至控制器c1处。D1域控制器c1会检查在注册数据库r1中是否有终端h1的记录。如果没有记录，说明终端h1之前没有在此域或者此网络中，那么控制器c1会首先用注册函数MD5<h1>来计算注册函数值；如果有记录，那么就直接取得记录中的注册函数值。c1把计算得来的值或者是从数据库r1中取得的值与

数据包中注册值域的值相比较，如果不相等，那么说明终端不合法，直接丢弃数据包；如果相等，那么就要将在r1中写入或更新记录，同时c0还必须向主要域控制器c0，报告h1的注册信息，c0查询数据库m0，如果没有记录，说明h1此前不在此网络中，那么就要是添加一条，[h1，14，D1]记录；如果m0中有记录，说明h1此前在其他域中，那么c0要向h1的原始域发送删除h1记录的消息，然后c0更新h1在m0中的记录。

3） 通信机制

图5展示了域1中的终端h1请求和域2中的终端2通信过程中的数据包组成。图6详细描述了通信的过程。表5、6分别给出了域内和域间（主要域）存在的一种数据包包头格式。

a) 是否在映射数据库m0中；

b) 如果m0中没有h2的记录，说明h2是非法的终端，转至步骤v；

c) 如果m0中有h2的记录，那么c0返回记录h2的信息[15, h2, D2]给c1；

d) c1接受h2信息后，使用连接函数MD5计算出连接函数值C<h1, h2, 14, 15>；c1将h1与h2通信的一条连接信息[C<h1, h2, 14, 15>, h1, h2, 14, 15]注册到映射数据库m1；c1发送这条记录到h2所在域D2的控制器c2；

e) c2接收到连接信息[C<h1, h2, 14, 15>, h1, h2, 14, 15]，将之注册到映射数据库m2，来保证通信可以成功实现；

f) 如果h1与h2在相同的域中，c1会修改数据包为[dpid1, dpid2, h1, h2, D1, Data]，其中dpid1是h1直连交换机标识，dpid2是h2直连

交换机标识，转至步骤13；

g) 本例中h1和h2不在相同的域，同步骤k一致，先将数据包修改为[dpid1, dpid2, h1, h2, D1, Data]，其中dpid1是h1直连交换机标识，dpid2是域1和主要域直连的交换机标识（我们在域内使用dpidx转发数据包）；

h) c1根据网络拓扑信息使用最短路径Dijkstra算法计算交换机dpid1和dpid2之间最短路径；

i) c1发送相对应的动作到这条路径上的所有交换机；

j) 如果h1和h2不在相同的域，数据包会转发到和主要域直连的交换机dpid2；

k) c1修改数据包为[l4, l5, C<h1,h2,l4,l5>]，其中l4为h1所在域D1和主要域相连的交换机标识，l5是h2所在域D2和主要域相连的交换机标识，C<h1,h2,l4,l5>为连接函数值；

l) c0使用最短路径Dijkstra算法计算l4与l5之间的最短路径（我们在域间使用lx转发数据包）；

m) 转发数据包到目的域D2；

n) c2使用连接函数值C<h1, h2, l4, l5>向m2请求连接信息，如果没有记录，转至步骤v；

o) 如果有连接记录，c2修改数据包为[dpid2, dpid1, h1, h2, D2, Data]，像步骤l一样在D2域内转发数据包；

p) 最终，h2收到数据包；

q) 丢弃数据包。

在终端h1和h2通信的过程中，HID和LID是被分开的，LID实例1即dpidx用于在域内通信，而LID实例2即lx用于在域间通信。

表5 域内存在的数据包包头格式

Packet (Inner Domain) Header	
Source Switch DPID	源终端所接入交换机标识，即源终端地址标识 dpidx(64-bit)
Destination Switch DPID	目的终端所接入交换机标识，即目的终端地址标识 dpidx（64-bit）
Source Host Identity	源终端身份标识 hx（64-bit）
Destination Host Identity	目的终端身份标识 hx’（64-bit）
Domain Name	源终端所属域名 Dx

表6 主要域（即域间）存在的数据包包头格式

Packet (Inter Domain) Header	
Source Access Switch DPID	源终端所在域接入主要域的交换机标识，即源终端地址标识 lx(64-bit)
Destination Access Switch DPID	目的终端所在域接入主要域的交换机标识，即目的终端地址标识 lx’（64-bit）
Connection Value	一对通信终端连接函数值 MD5<hx, hx’, lx, lx’>（128-bit）

2.2.2 本发明实施例二

本节中将介绍当主机移动后，通信双方数据包组成，和通信流程，图7给出了当终端h1从域1移动到域3后，终端h2返回信息到终端h1的过程示意，并且给出了一种数据包组成方式。

首先给出终端h1移动后的重新注册过程以及在主要域中映射更新过程。

a) 域D3控制器c3接收到的h1发送的数据包；

b) 控制器c3没有h1的记录，根据注册流程，c3重新计算注册函数验证h1合法性，合法后将记录写入本域注册数据库r3；

c) 同时c3通知c0检查是否有h1的记录，由于此前h1在域D1中已经被注册过，所以c0中有h1的记录[h1, 14, D1]；

d) c0通知h1原始所在域D1的控制器c1删除h1在r1中的记录；

e) 同时c0需要在m0更新h1的记录为[h1, 16, D3]；

终端h1移动后的注册及映射更新过程已给出，h2返回给h1的数据包的过程有些类似于上一节终端通信过程，因此不再给出具体流程图，只叙述过程如下：

a) 终端h2发送数据包[h2, h1, R<h2>, Data]到h1，在域D2内的过程同h1发送数据包到h2在域D1中的过程类似无论h1移动与否（域内使用dpidx转发包）；

b) 当数据包来到D2域直连主要域的交换机dpid2的时候，数据包将要被修改，因为h1移动后，主要域m0中的h1的记录被更新为[h1, 16,

D3]；

c）控制器c2向c0请求h1的信息，所以c3得到了h1的新地址标识16；

d）c2计算新的连接函数C<h2, h1, l5, l6>然后跟新m2中的记录为[C<h2, h1, l5, l6>, h1, h2, l6, l5]；

e）c2发送记录[C<h2, h1, l5, l6>, h1, h2, l6, l5]到h1当前所属域D3的控制器c3；

f）c3注册记录到m3；

g）c2修改数据包为[l5, l6, C<h2, h1, l5, l6>, Data]；

h）c2转发数据包到主要域；

i）c0通过Dijkstra算法路由数据包到步骤p；

j）c3在m3和r3中找到记录；

k）c3得到目的地身份标识h1所直连交换机的地址标识dpid1；

l）c3修改数据包为[dpid2, dpid1, h2, h1, D3, Data]；

m）c3通过Dijkstra算法转发包到h1；

n）最终，h1收到数据包。

我们给出了 h2 发送数据包到 h1 的过程。h2 持续的发送数据包而无需更改[h2, h1, R<h2>, Data]的任意部分，所以我们说 ICCN 可以支持移动性。

以上内容是结合具体的优选实施方式对本发明所作的进一步详细说明，不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干简单推演或替换，都应当视为属于本发明的保护范围。

权利要求书

1. 一种基于身份的集中控制式网络体系架构 ICCN，其特征在于：包括控制转发行为的逻辑的控制层、根据控制层逻辑来转发流量的数据层和拓扑发现；该控制层为控制器以及与控制相关的数据库，所有控制数据包的操作均通过控制器完成，所有与终端和映射相关的信息都存储在注册数据库和映射数据库中；该数据层包括交换机和终端，数据层进行数据包转发。

2. 根据权利要求 1 所述的基于身份的集中控制式网络体系架构 ICCN，其特征在于：控制器在网络建立初始获得网络交换机的信息，控制器检查数据包头来验证一个终端是否是合法的或正确的，控制器注册合法终端到注册数据库中；控制器进行路由策略。

3. 根据权利要求 1 所述的基于身份的集中控制式网络体系架构 ICCN，其特征在于：控制器根据映射系统来修改数据包包头进行身份与位置分离。

4. 根据权利要求 1 所述的基于身份的集中控制式网络体系架构 ICCN，其特征在于：交换机不需要收集邻居交换机的信息，也不需要修改数据包，交换机通过流表的动作来转发包。

5. 根据权利要求 1 所述的基于身份的集中控制式网络体系架构 ICCN，其特征在于：拓扑发现中，控制器主动获得网络中交换机信息，网络以域级关系组织，每个控制器维护自己域内拓扑信息，主要域连接所有域，主要域控制器拥有全部域到达交换机信息。

6. 根据权利要求 1 所述的基于身份的集中控制式网络体系架构 ICCN，其特征在于：控制器控制传入流量，在主要域中，使用终端地址标识来转发路由，终端的身份标识是公开的。

7. 根据权利要求 6 所述的基于身份的集中控制式网络体系架构 ICCN，其特征在于：终端身份标识 HID 是一个 64 位的数字，终端对应的位置标识 LID 为交换机上的 OpenFlow 实例 DPID 的唯一表示；一个终端身份标识 HID 对应至少一个终端对应的位置标识 LID。

8. 根据权利要求 1 所述的基于身份的集中控制式网络体系架构 ICCN，其

特征在于：控制器注册通信终端信息和保存终端身份标识与位置标识映射信息，控制器通过查询数据库发现目标终端，并通过最短路径算法建立转发包路径，并向 OpenFlow 交换机下发转发流表。

9. 根据权利要求 6 所述的集中式身份网络路由协议 CIN，其特征在于：

终端身份标识 HID 不改变即连接不中断的情况下进行通信；分层机制增大了流表的尺寸，在域内可以部署不同的网络机制。

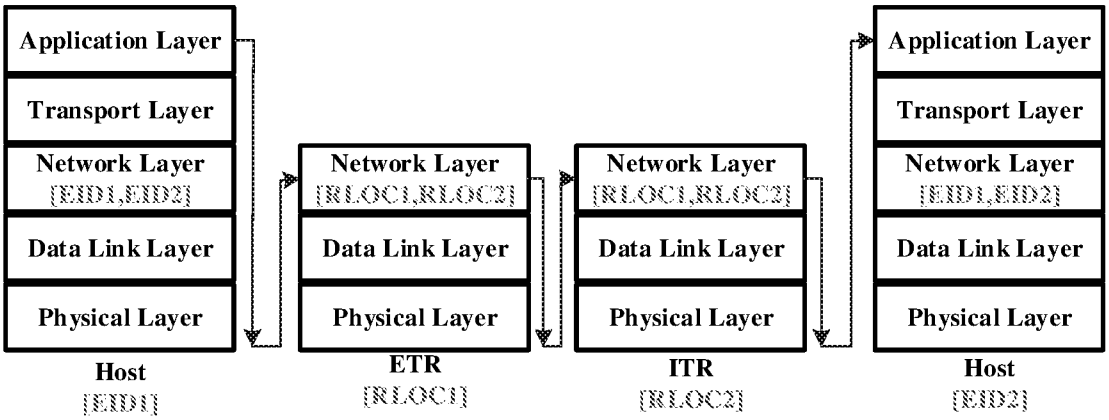
Application Layer
Transport Layer
Network Layer
{EID1,EID2}
Data Link Layer
Physical Layer
Host
{EID1}
Network Layer
{RLOC1,RLOC2}
Data Link Layer
Physical Layer
ETR
{RLOC1}
Network Layer
{RLOC1,RLOC2}
Data Link Layer
Physical Layer
ITR
{RLOC2}
Application Layer
Transport Layer
Network Layer
{EID1,EID2}
Data Link Layer
Physical Layer
Host
{EID2}

图 1

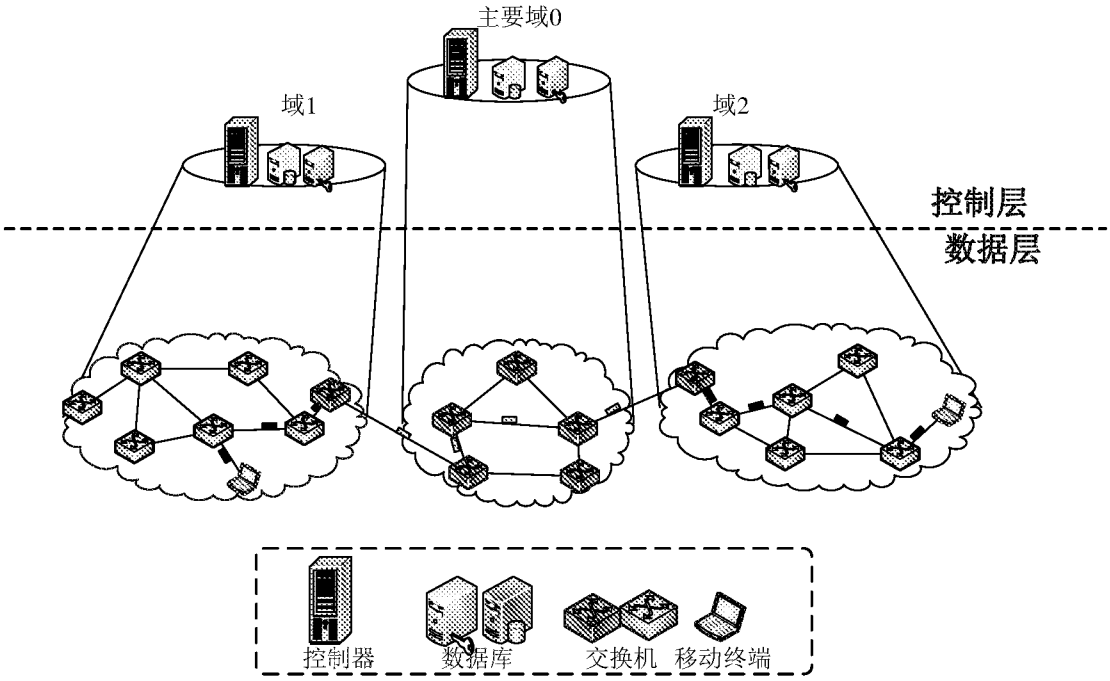
主要域0
域1
域2
控制层
数据层
控制器
数据库
交换机
移动终端

图 2

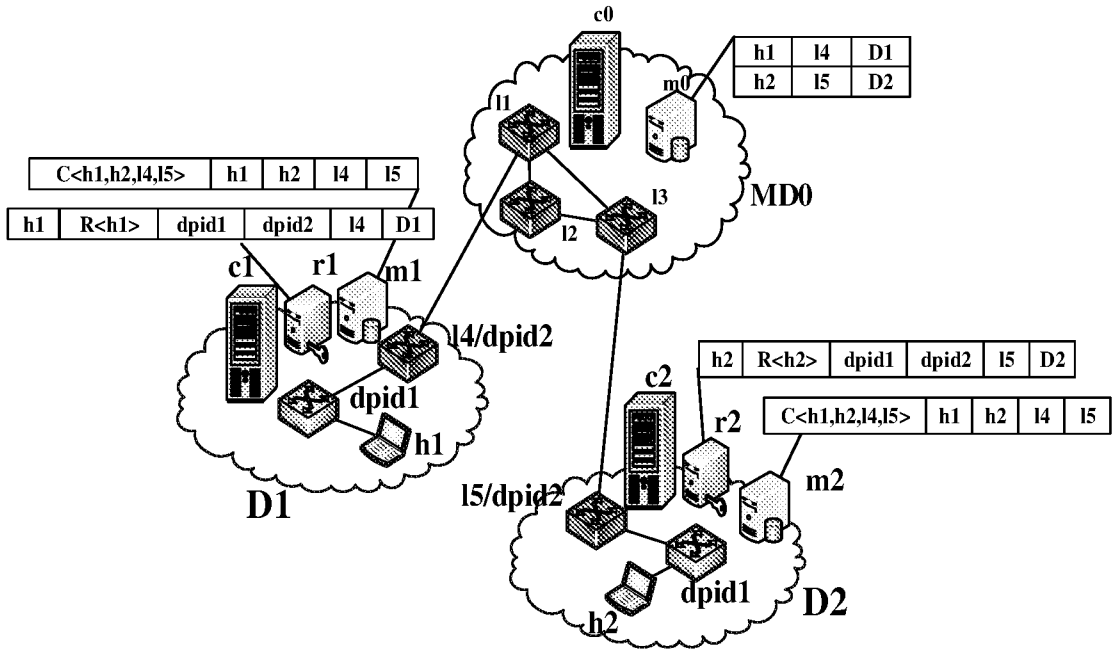
c0
h1 l4 D1
h2 l5 D2
m0
l1
l3
l2
MD0
C<h1,h2,l4,l5> h1 h2 l4 l5
h1 R<h1> dpid1 dpid2 l4 D1
c1
r1
m1
l4/dpid2
dpid1
h1
D1
h2 R<h2> dpid1 dpid2 l5 D2
C<h1,h2,l4,l5> h1 h2 l4 l5
c2
r2
m2
l5/dpid2
dpid1
h2
D2

图 3

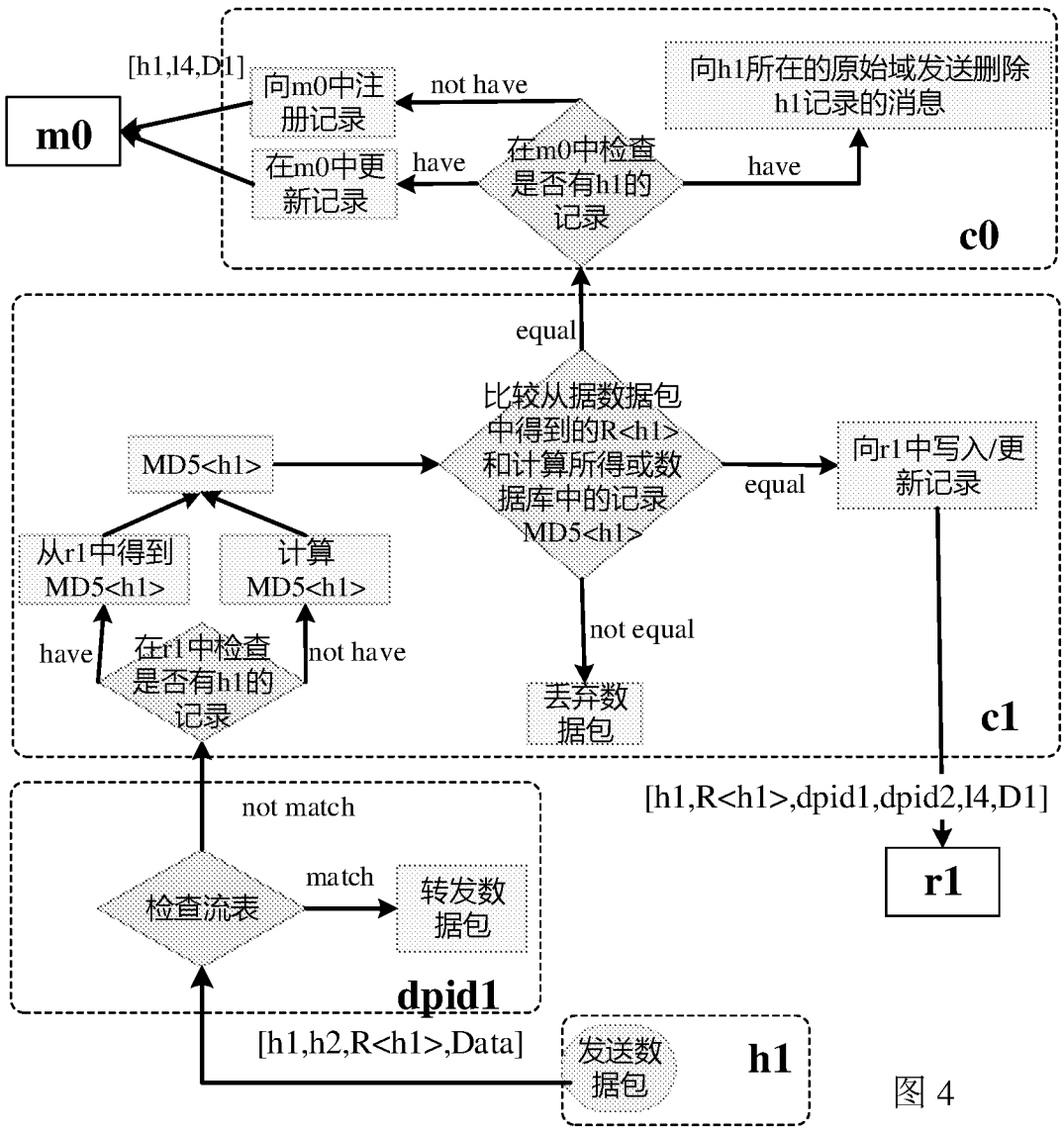
[h1,l4,D1]
m0
向m0中注册记录
not have
向h1所在的原始域发送删除h1记录的消息
在m0中更新记录
have
在m0中检查是否有h1的记录
have
c0
equal
比较从据数据包中得到的R<h1>和计算所得或数据库中的记录MD5<h1>
MD5<h1>
equal
向r1中写入/更新记录
从r1中得到MD5<h1>
计算MD5<h1>
have
在r1中检查是否有h1的记录
not have
not equal
丢弃数据包
c1
[h1,R<h1>,dpid1,dpid2,l4,D1]
r1
not match
match
检查流表
转发数据包
dpid1
[h1,h2,R<h1>,Data]
发送数据包
h1

图 4

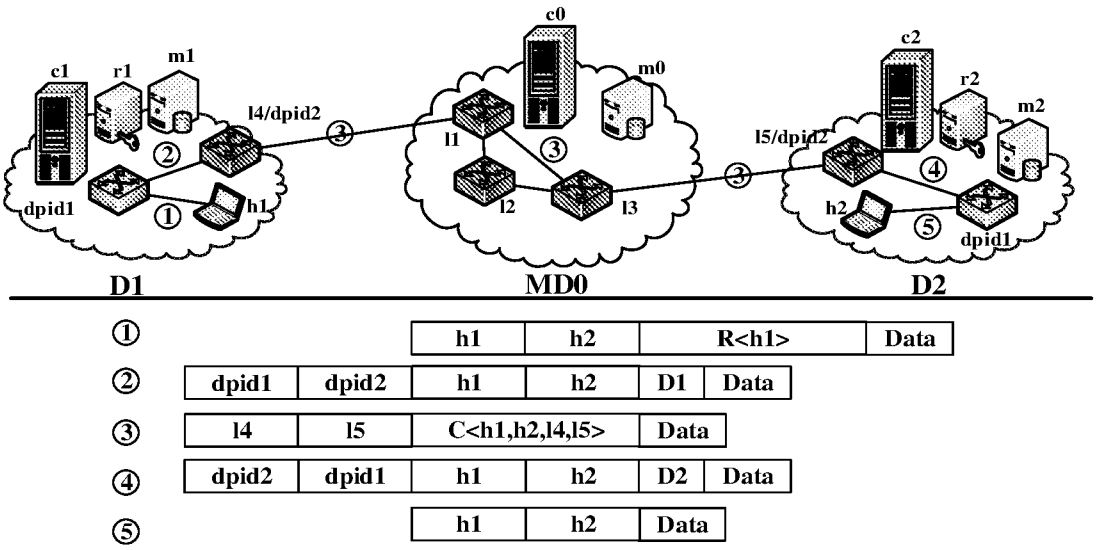
c0
c1
r1
m1
m0
c2
r2
m2
l4/dpid2
l1
l5/dpid2
dpid1
h1
l2
l3
h2
dpid1
D1
MD0
D2
① h1 h2 R<h1> Data
② dpid1 dpid2 h1 h2 D1 Data
③ l4 l5 C<h1,h2,l4,l5> Data
④ dpid2 dpid1 h1 h2 D2 Data
⑤ h1 h2 Data

图 5

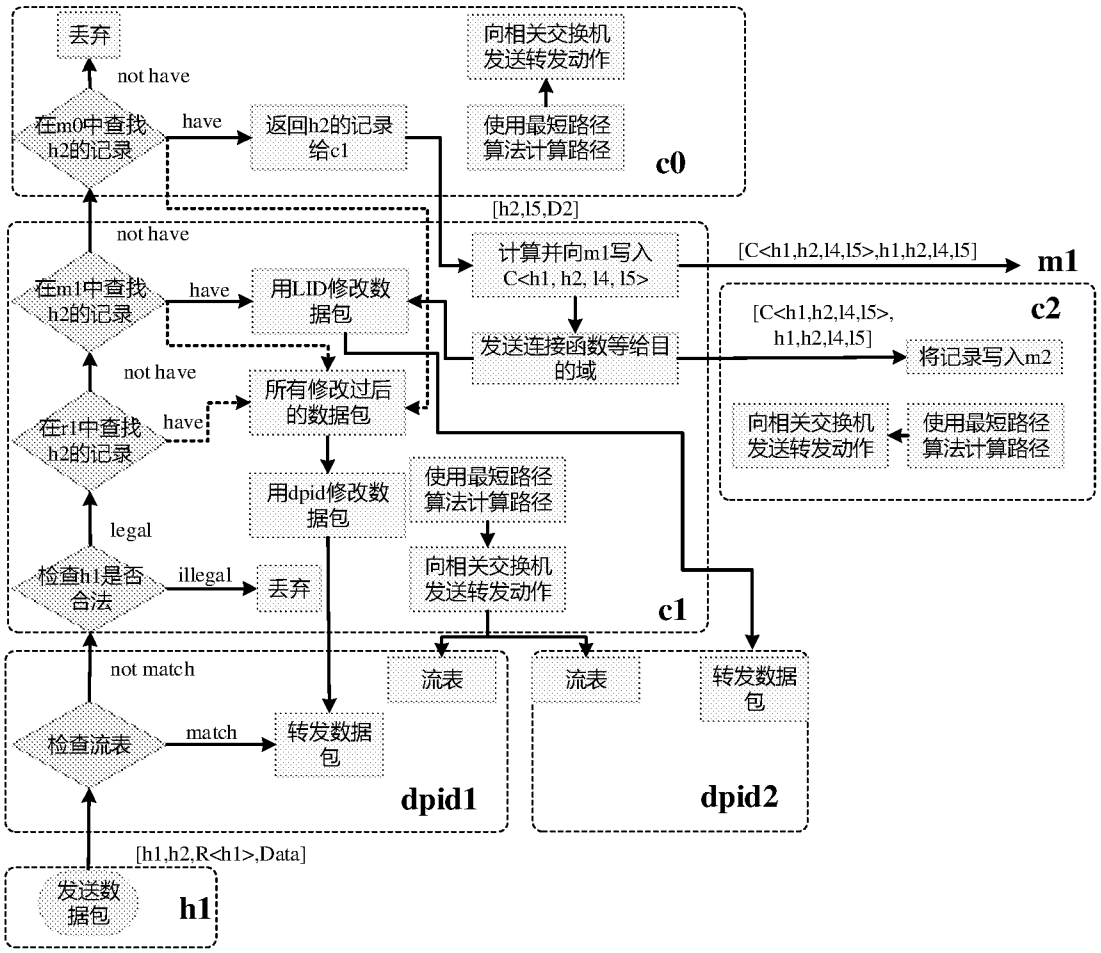
丢弃
not have
在m0中查找h2的记录
have
返回h2的记录给c1
向相关交换机发送转发动作
使用最短路径算法计算路径
c0
[h2,l5,D2]
not have
在m1中查找h2的记录
have
用LID修改数据包
计算并向m1写入C<h1, h2, l4, l5>
[C<h1,h2,l4,l5>,h1,h2,l4,l5]
m1
发送连接函数等给目的域
[C<h1,h2,l4,l5>, h1,h2,l4,l5]
c2
将记录写入m2
not have
在r1中查找h2的记录
have
所有修改过后的数据包
向相关交换机发送转发动作
使用最短路径算法计算路径
用dpid修改数据包
使用最短路径算法计算路径
legal
检查h1是否合法
illegal
丢弃
向相关交换机发送转发动作
c1
not match
检查流表
match
转发数据包
流表
流表
转发数据包
dpid1
dpid2
[h1,h2,R<h1>,Data]
发送数据包
h1

图 6

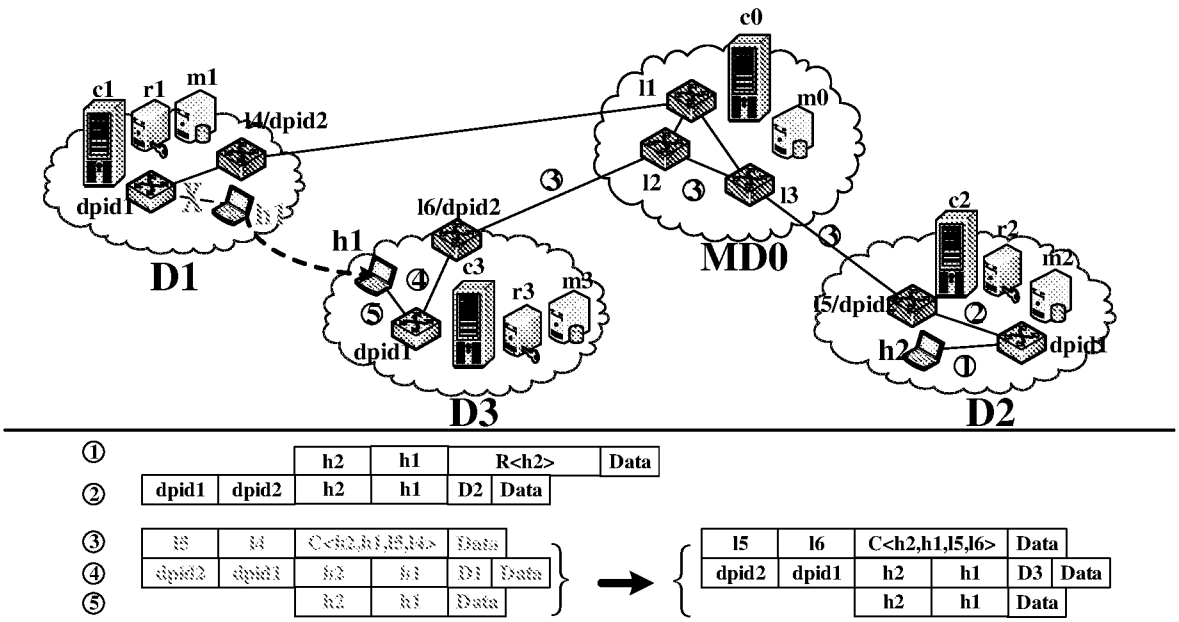
c0
c1
r1
m1
l1
m0
l4/dpid2
l2
l3
dpid1
l6/dpid2
h1
c3
r3
m3
MD0
c2
r2
m2
l5/dpid1
h2
dpid1
D1
D3
D2
①
②
③
④
⑤
h2
h1
R<h2>
Data
dpid1
dpid2
D2
l5
l6
C<h2,h1,l5,l6>
D3

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/098167

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/717 (2013.01) 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

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)

CNPAT, CNKI, WPI, EPODOC: ID HID LID DPID identity location locator separation centralized control network topology data register registration mapping address router domain switch flow table openflow

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LIU, Huiling et al., "ICCN: Identity-based Centralized Control Network", IEEE/CIC ICCC 2015 SYMPOSIUM ON NEXT GENERATION NETWORKING, 04 November 2015 (04.11.2015), sections II-IV	1-9
A	CN 102256236 A (BEIJING JIAOTONG UNIVERSITY), 23 November 2011 (23.11.2011), the whole document	1-9
A	CN 101945034 A (ZTE CORP.), 12 January 2011 (12.01.2011), the whole document	1-9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 September 2016 (10.09.2016)	**27 September 2016 (27.09.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **WANG, Xiaoqian** Telephone No.: (86-10) **62413855**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/098167

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102256236 A	23 November 2011	None	
CN 101945034 A	12 January 2011	None	

国际检索报告

国际申请号
PCT/CN2015/098167

A. 主题的分类

H04L 12/717(2013.01)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. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04W

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）)

CNPAT,CNKI,WPI,EPODOC: 身份 位置 分离 集中 控制 网络 拓扑 数据 注册 映射IP ID 地址 路由 域 交换机 流表 HID LID DPID identity location locator separation centralized control network topology data register registration mapping address router domain switch flow table openflow

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	LIU, Huiling等. "ICCN: Identity-based Centralized Control Network" IEEE/CIC ICCC 2015 Symposium on Next Generation Networking, 2015年 11月 4日 (2015-11-04), 第II-IV节	1-9
A	CN 102256236 A (北京交通大学) 2011年 11月 23日 (2011-11-23) 全文	1-9
A	CN 101945034 A (中兴通讯股份有限公司) 2011年 1月 12日 (2011-01-12) 全文	1-9

☐ 其余文件在C栏的续页中列出。

☑ 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	国际检索报告邮寄日期
2016年 9月 10日	2016年 9月 27日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王小千
传真号 (86-10)62019451	电话号码 (86-10)62413855

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/098167

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 102256236 A	2011年 11月 23日	无	
CN 101945034 A	2011年 1月 12日	无	