

基于可编程平台的标识网络移动性管理机制

柳依岸*, 郜 帅, 侯心迪, 刘宁春

(北京交通大学 电子信息工程学院 移动专用网络国家工程研究中心, 北京 100044)

摘 要: 标识网络的提出解决了传统 TCP/IP 网络中 IP 地址“二义性”带来的移动性问题, 然而标识网络的颠覆式创新在现网中部署存在困难。随着协议无关的可编程平台技术不断发展, 为解决标识网络部署困难带来可能, 为标识网络的大规模推广带来便利条件。该文提出一种基于可编程平台的标识网络移动性管理机制, 结合可编程平台数据与控制分离的特点, 在数据平面设计一套报文处理与转发逻辑实现数据报的解析与转发, 在控制平面设计包含四个模块的控制系统实现设备身份认证与映射注册、跨接入域通信的映射查询、移动终端跨接入域移动切换等网络功能。基于可编程平台搭建了标识网络原型实验系统, 对基于可编程平台的标识网络移动性管理机制的功能和性能进行实验测试评估。结果表明, 该机制能够支持标识分离映射、标识发布与查询、设备移动切换等功能, 性能满足大部分实时应用需求。

关键词: 标识网络; 可编程平台; 标识分离映射机制; 移动管理; 映射关系更新

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2023)10-0059-07

doi: 10.3969/j.issn.1673-629X.2023.10.010

Mobility Management Mechanism of Smart Identifier Network Based on Programmable Data Plane

LIU Yi-an*, GAO Shuai, HOU Xin-di, LIU Ning-chun

(National Engineering Research Center of Advanced Network Technologies, School of Electronic Information and Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The proposal of Smart Identifier Network solves the mobility problem caused by the "ambiguity" of IP address in traditional TCP/IP network, but the subversive innovation of Smart Identifier Network is difficult to deploy in the existing network. With the continuous development of protocol-independent programmable data plane technology, it is possible to solve the difficulties of Smart Identifier Network deployment and bring convenient conditions for the large-scale promotion of Smart Identifier Network. We propose a Smart Identifier Network mobility management mechanism based on programmable data plane, which combines the characteristics of data and control separation of programmable data plane, designs a set of message processing and forwarding logic in the data plane to realize the parsing and forwarding of packet, and realizes network functions such as device identity authentication and mapping registration, mapping query of cross access domain communication, and cross access domain mobile switching of mobile terminals in the control plane design with four modules. In this paper, a prototype experimental system of Smart Identifier Network is built based on the programmable data plane, and the functions and performance of the identity network mobility management mechanism based on the programmable data plane are experimentally tested and evaluated. The results show that the mechanism can support functions such as identity separation mapping, identity publishing and query, and device mobile switching access, and the performance meets the requirements of most real-time applications.

Key words: smart identifier network; programmable data plane; identifiers separating and mapping scheme; mobility management; mapping relationship updating

0 引 言

在传统互联网 TCP/IP 结构体系创造之初, 终端设备大多采用以“固定、有线”为主的连通方式, 网络

结构固定, 使得 IP 具有身份和位置双重属性^[1], 这种在当时简单有效的设计在如今却直接或间接带来了现网中移动性^[2]、路由可扩展性^[3]、网络安全^[4]等问题。

收稿日期: 2022-12-29

修回日期: 2023-04-28

基金项目: 中央高校基本科研业务费专项资金资助(2022JBGP005)

作者简介: 柳依岸(1998-), 男, 硕士, 通讯作者, 研究方向为新型网络、SDN 等; 郜 帅, 博士, 教授, 研究方向为未来网络架构、移动互联网、无线传感网络等。

针对上述问题,国内外许多团队提出从根本上重新设计的网络原理、机制、体系结构,部分采取颠覆性的演进设计,以避免传统互联网 TCP/IP 体系中的根源性问题。具有代表性的包括位置身份分离协议 LISP^[5]、主机标识协议 HIP^[6]、面向数据分发的网络 NDN^[7]、移动性网络 MobilityFirst^[8]、面向云计算的网络 NEBULA^[9]、不同主体灵活通信的 XIA^[10]。国内张宏科院士团队的标识网络(Smart Identifier Network, SINET)^[11-12],提出了全新网络体系结构的“网通层”和“服务层”两层总体模型与理论。标识网络将网络结构划分为核心网与接入网两个部分,为了解决 IP 地址的二义性,定义了接入标识与路由标识,在接入网中使用接入标识传输,核心网中使用路由标识传输,并提出接入标识与路由标识分离映射理论,建立接入标识与路由标识的映射机制,完成身份位置的解绑。标识网络的接入标识与路由标识分离映射理论解决了传统互联网 TCP/IP 体系的设计性问题,为传统网络移动支持性差、安全性差、路由可聚合性差等问题提供了可行的替代方案,对未来网络发展有积极意义,是具有影响力的下一代互联网代表架构^[13]。

目前在部分专用网络中标识网络的部署应用已经取得了良好效果,然而标识网络很难在现有的网络中使用,现有的 TCP/IP 网络体系的应用非常成熟,更具体地说 IP 协议深深地嵌入到主机网络和应用软件中以及路由器硬件和软件中,架构更替面临极高的部署障碍。

近年可编程交换平台^[14]依托软件定义网络(Software Defined Networking, SDN)^[15]的快速发展,为打破当前网络设备封闭的局限性带来希望。可编程网络平台架构中,采用转发与控制分离的思想,将网络中的路由交换解耦为数据面与控制面,数据面负责网络的转发逻辑,控制面负责网络的控制逻辑。转发逻辑由可编程的数据平面实现,能够灵活地设计并实现不同的报文解析处理流程与转发逻辑,控制平面负责从数据平面收集信息,实现网络的复杂控制计算逻辑,指挥数据平面的转发,同样具有可编程的灵活性。可编程交换平台的发展降低了网络创新开发和部署运维的成本,采用可编程平台使得标识网络的推广与应用成为可能。

该文在标识网络移动性管理机制的研究基础上,提出采用可编程网络平台架构实现基于可编程平台的标识网络移动性管理机制。首先根据可编程平台特点设计总体架构,在数据平面设计报文处理与转发逻辑,在控制平面设计网络功能对应的处理模块。然后实现搭建一套原型系统进行功能测试与性能测试。

1 相关工作

近年针对标识网络移动性管理机制的研究主要集中在基于 Linux 系统的网络转发平台上。在文献[16]中提出了标识网络的网络层移动管理基础,标识分离映射机制。在文献[17]中针对标识网络移动管理方案提出改进的层次移动管理机制、位置管理机制、寻呼机制。在文献[18]中引入移动管理域优化了映射关系处理。在上述文献中大多根据 Linux 系统网络转发平台特点设计标识网络移动切换管理机制。在传统网络结构中由于网络的控制能力分散在各个网元设备中,所以需要将定制软件安装进网络拓扑中大部分网元设备与终端中,例如在文献[18]中,需要将定制软件部署至标识映射服务器(Identity Map Server, IDMS)、接入交换路由器(Access Switch Router, ASR)、移动终端(Mobile Node, MN)中。当移动终端发生移动切换,新的映射关系由新的本地 ASR 生成并发布至 IDMS,并由 IDMS 通知原 ASR 更新旧的映射关系。当发生三角路由时主要由 ASR 处理失效的映射关系。在传统平台中网络控制能力分散在各个网元设备中,大部分的逻辑处理工作由各网元设备处理并在网元设备之间通过信令交互与交换信息。逻辑处理在一定程度上占用了 ASR 的部分计算能力,同时部分信令的开销也占用了一定的设备转发能力,这种情况下可能会更快地产生 ASR 单点失效的问题。由于网络拓扑中各个网元均需要定制化的开发,网络系统在开发、部署、运维、推广上可能会存在障碍。

该文提出基于可编程网络平台架构实现标识网络移性管理机制,由于转发与控制分离的特点,控制面集中网络的管控能力,部分需要 ASR 处理的逻辑与信令交互集中至控制器处理,相较于传统的基于 Linux 系统的网络转发平台省去了部分 ASR 之间信令交互的资源开销与时间开销。可编程平台易于开发部署推广的特点一定程度上也便于标识网络的推广与应用。

2 基于可编程平台的标识网络移动性管理机制

2.1 可编程平台下标识网络总体架构设计与原理

基于可编程平台的控制与转发分离的理念,标识网络架构总体分为数据平面和控制平面两部分设计。数据平面负责根据可编程设计的数据面解析处理逻辑处理报文,并按照控制面下发的流表进行转发。控制平面负责网络整体的管控能力,同时对数据面下发流表指导转发,配合数据平面实现网络基础通信功能,包括标识网络中设备注册、认证、映射发布与查询。以及在此之上提供标识网络的移动性管理机制。可编程平台下标识网络整体架构如图 1 所示。

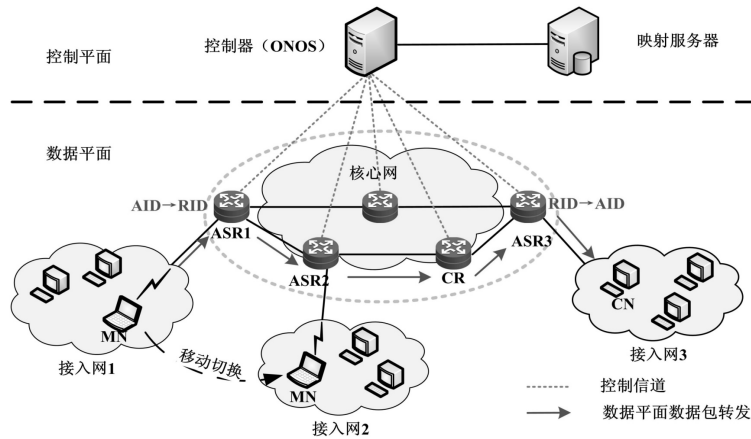


图 1 基于可编程平台的标识网络架构

标识网络逻辑上将网络拓扑划分为接入网与核心网。接入网中的终端采用 128 位全局唯一的接入标识 AID (Access Identifier, AID) 表示身份信息, 并且在移动切换过程中不会改变。当终端接入网络完成认证, 控制面会给终端分配代表接入位置信息的 RID (Route Identifier, RID), RID 用于报文在核心网中路由。接入交换路由器 (Access Switch Router, ASR) 负责接入网内的通信以及跨域通信时身份标识与路由标识的转换, 从而实现身份与位置分离, ASR 的流表中包含了当前域内所有的终端的 AID 与 RID 映射关系。核心路由器 (Core Router, CR) 负责核心网的报文转发。

2.1.1 数据平面设计

数据平面依靠可编程交换设备实现对报文解析、报文处理、报文转发的功能, 通过数据平面的设计实现标识网络数据包转发、设备认证、映射查询、移动切换等网络功能。数据平面的报文处理逻辑如图 2 所示。

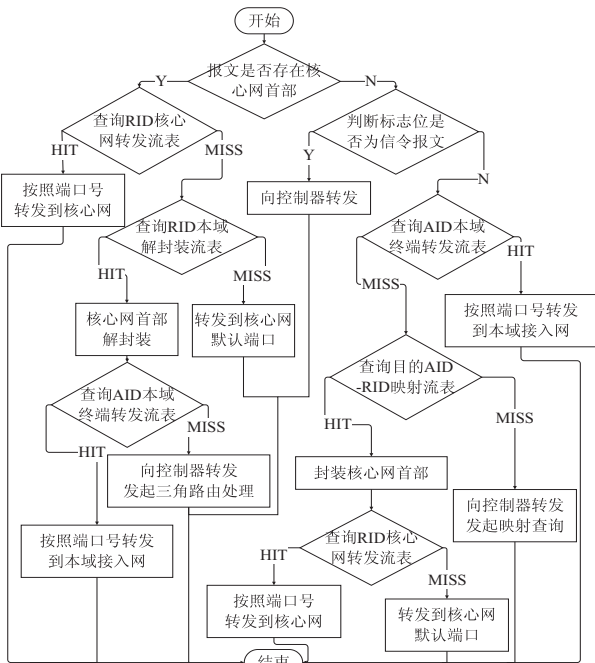


图 2 基于可编程平台的标识网络数据平面转发逻辑

(1) 当数据平面可编程交换设备收到一个数据报, 首先按照标识网络解析报文首部, 判断报文是否存在核心网首部, 若存在执行(2); 若不存在则执行(3);

(2) 对具有核心网首部的报文, 根据核心网首部中的目的 RID, 在 RID 核心网转发流表中查询是否有对应的流表能够转发, 若存在流表执行按照对应的端口号转发到核心网, 流程结束; 若不存在流表执行(4);

(3) 对无核心网首部的报文即接入网报文, 判断接入网首部中的标志位是否标记为信令报文, 若是执行向控制器转发并结束流程; 若不是执行(5);

(4) 对核心网报文, 根据核心网首部中的目的 RID, 在 RID 本域解封封装流表中查询是否有对应的流表, 若存在流表将核心网报文解封封装, 去掉核心网首部, 执行(6); 若不存在流表转发到核心网默认端口, 流程结束;

(5) 对接入网报文, 根据接入网首部中的目的 AID, 在 AID 本域终端转发流表中查询是否有对应的流表能够转发, 若存在流表执行按照对应端口号转发到本域接入网, 流程结束; 若不存在流表执行(7);

(6) 对核心网报文解封封装后的接入网报文, 根据接入网首部中的目的 AID, 在 AID 本域终端转发流表中查询是否有对应的流表能够转发, 若存在流表执行按照对应端口号转发到本域接入网, 流程结束; 若不存在流表向控制器转发, 发起三角路由处理流程;

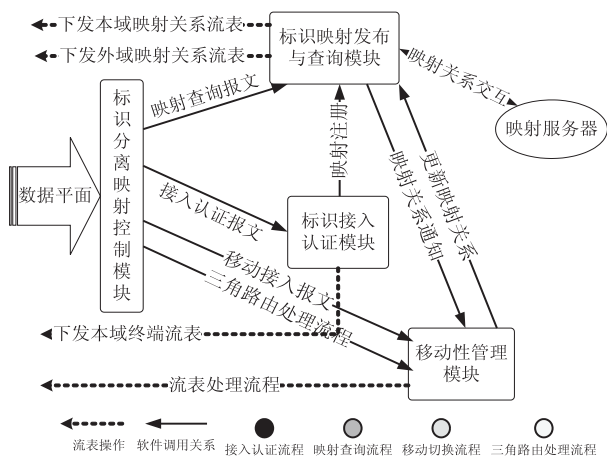
(7) 对目的 AID 不在本域的接入网报文, 根据接入网首部中的目的 AID, 在目的 AID-RID 映射流表中查询是否有目的 AID 映射的 RID, 若存在流表执行封装核心网首部, 将源、目的 AID 映射成源、目的 RID, 执行(8); 若不存在, 向控制器转发报文, 发起映射查询, 结束流程;

(8) 对接入网报文封装成核心网报文, 根据核心网首部的目的 RID, 在 RID 核心网转发流表中查询是

否有对应的流表能够转发,若存在流表执行按照对应的端口号转发到核心网,流程结束;若不存在流表,转发到核心网默认端口,流程结束。

2.1.2 控制平面设计

在可编程网络平台中,控制平面负责网络整体的功能实现,从基本的端到端通信到复杂的网络管控都依赖于控制平面。在可编程平台下的标识网络移动性管理机制中,控制平面也是系统运行的核心。控制平面通过接收数据平面转交的报文获取数据平面的信息,进而发起不同的网络流程进入不同的处理逻辑。在控制平面处理流程中通过向数据平面下发不同的流表完成对数据平面的转发工作的指挥。控制平面总体架构设计如图 3 所示,控制平面系统包括四个模块,负责不同的功能。



映射服务器负责存储全局设备的映射关系,并将存储的数据对外提供查询、更新、注册等功能。

标识分离映射控制模块负责处理从数据平面转交的报文,解析报文意图并从报文中提取报文信息,例如源目的 AID、标志位、报文负载等,并根据报文意图开启不同的逻辑流程,向后续模块传递信息。设计如下:

(1) 当标识分离映射控制模块收到数据平面转交的接入认证报文时,会提取出报文中的源 AID、报文负载密文、报文来源的数据平面交换机以及交换机端口号,将信息转交给标识接入认证模块,开启接入认证流程。

(2) 当收到数据平面转交的映射查询报文时,会提取出报文中的目的 AID、报文来源的数据平面交换机,将信息转交给标识映射发布与查询模块,开启映射查询流程。

(3) 当收到数据平面转交的移动接入报文,会提取出报文中的源 AID、报文来源的数据平面交换机以及交换机端口号,将信息转交给移动性管理模块,开启移动切换流程。

(4) 当收到数据平面转交的三角路由报文,会提取出报文中的源 AID、报文来源的数据平面交换机,将信息转交给移动性管理模块,开启三角路由处理流程。

标识接入认证模块负责对设备进行接入认证,并处理设备所在接入域的交换机的流表逻辑。当标识接入认证模块收到标识分离映射控制模块的接入认证请求,会根据传递过来的信息:设备源 AID、接入认证报文负载密文、报文来源交换机、报文来源交换机端口号,解密报文密文,认证设备身份。完成身份认证后会向设备所在接入域的交换机下发 AID 本域终端转发流表,最后将信息转交给标识映射发布与查询模块,开启映射注册流程。

标识映射发布与查询模块负责处理设备的映射关系以及处理数据平面中映射关系对应的流表,并将处理结果与映射服务器同步,包括映射注册、映射查询、映射更新。设计如下:

(1) 当标识映射发布与查询模块收到映射注册请求,会根据请求中的信息为终端分配与接入域相关的 RID,并将映射关系写入映射服务器以同步到全局。新的 RID 本域解封装流表下发到接入认证设备所在接入域的交换机,使得数据平面会解封装该 RID 对应的报文。最后会将该设备的 AID、RID 映射关系、所在接入域交换机、交换机端口号等信息转交给移动性管理模块存储。

(2) 当收到标识分离映射控制模块发送的映射查询请求,会根据请求中的目的 AID 向映射服务器查询 AID 对应的 RID 映射关系,并将查询到的映射关系下发到发起映射查询的设备所在接入域的数据平面交换机中,指挥发往该目的 AID 的报文的网首部封装。

(3) 当收到移动性管理模块的映射更新请求,会根据请求中的信息为终端重新分配与接入域相关的 RID,并将更新后的映射关系写入映射服务器,同时向设备所在的接入域交换机下发新的本域 RID 解封装流表,最后将更新后的映射关系通知给移动性管理模块。

移动性管理模块负责根据移动切换报文判断移动切换的信息,管理移动前后的映射关系同步以及数据平面的流表逻辑。

(1) 当移动性管理模块收到标识分离映射控制模块发送的移动切换请求,首先根据源 AID 在存储的信息中查询 AID 接入的交换机并与移动接入报文的来源交换机对比:(a) 如果是在同一台交换机不同的端口之间移动,则向来源交换机下发新的 AID 本域终端转发流表,更新数据平面中记录的接入交换机端口信息,因为仍在同一接入域内,故映射关系无需处理。

(b)如果是设备在不同的接入域交换机间移动,首先根据模块内存储的先前接入交换机的信息,将先前接入交换机内本设备的 AID 本域终端转发流表清除,向新接入的接入域交换机下发 AID 本域终端转发流表,再将信息发送给标识映射发布与查询模块开启映射更新流程,为设备重新注册新的接入域相关的 RID 并处理对应的流表。

(2)三角路由是由于设备移动切换后新的 AID-RID 映射关系无法直接同步到先前与设备通信的接入域,先前的通信对端依然按照旧的映射关系将报文错误的发送到设备移动切换前的接入域交换机中,数据平面感知到三角路由报文时会将报文转交给控制面处理,最终到达移动性管理模块。当收到三角路由报文,会根据报文源 AID 在存储中找到发送此报文的对端接入域交换机,将信息转交给标识映射发布与查询模块,将对端交换机中过期的目的 AID-RID 映射流表通过映射查询流程更新,从而解决三角路由问题。

2.2 基于可编程平台的标识网络工作流程

在可编程平台架构下的标识网络划分为数据平面与控制平面,数据平面负责对报文进行处理并按照控制平面的指导转发,控制平面负责实现网络中的负责逻辑功能,维护标识网络的映射关系,通过数据平面转交的报文获取数据平面的信息,并且通过下发流表实现对数据平面的控制。以图 1 为例介绍基于可编程平台的标识网络工作流程。标识网络将网络划分为接入网与核心网,接入网中的设备通过接入交换路由器(ASR)接入网络,图 1 中展示了三个接入网通过核心网联通。其中移动终端 MN 位于接入网 1,对应的通信对端是位于接入网 3 的有线固定终端 CN, MN 与 CN 位于不同的接入网,需要通过核心网路由通信。MN 会因为移动从不同的接入网接入网络。

2.2.1 基础通信工作流程

以图 1 中的拓扑结构下移动终端 MN 与有线终端 CN 的通信为例,介绍基于可编程平台的标识网络通信的具体工作流程。如图 4 所示,流程中移动终端 MN 与有线终端 CN 已经完成设备注册,映射服务器中包含了这两台终端的 AID-RID 映射关系。当移动终端 MN 首次与有线终端 CN 通信时,通信报文到达移动终端 MN 所在接入网 1 的接入交换路由器 ASR1 时,由于此时数据平面还没有目的 AID-RID 映射流表,数据平面将报文转交给控制平面,发起标识映射查询流程。控制器收到数据平面转交的报文,由标识映射分离控制模块提取报文中的信息,解析报文的意图,转交给标识映射发布与查询模块向映射服务器发起映射查询。控制器从映射服务器查询到通信对端 CN 的 AID-RID 映射关系,完成映射查询流程,将映射关系

以目的 AID-RID 映射流表的形式下发至 ASR1。

当移动终端 MN 后续的通信报文到达 ASR1 时,击中目的 AID-RID 映射流表,报文被封装上核心网首部向核心网内转发,在核心网通过 RID 路由到有线终端 CN 所在接入网 3 的接入交换路由器 ASR3。报文击中数据平面 RID 本域解封装流表,解封装核心网首部,根据目的 AID 路由到接入网 3 中的有线终端 CN。

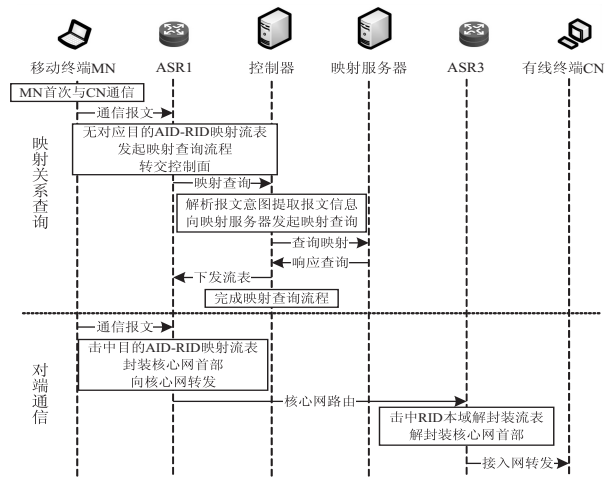


图 4 基于可编程平台的标识网络基础通信流程

2.2.2 移动切换工作流程

仍以图 1 中拓扑结构为例,介绍基于可编程平台的标识网络移动切换工作流程以及三角路由的产生与处理流程。如图 5 所示,当移动终端移动切换后接入到接入域 2 的无线 AP, AP 感知到终端接入向 ASR2 发送移动切换报文, ASR2 收到并解析移动切换报文发起移动切换流程转交给控制面处理。控制器收到数据平面移动切换报文,解析报文意图,提取报文中的信息,转交给移动性管理模块进入移动切换流程。移动性管理模块首先根据终端新的接入位置信息分配新的 RID,并将新的映射关系通过标识映射发布与查询模块更新给映射服务器。收到映射服务器的更新响应后,向移动终端新接入的 ASR2 下发移动终端 MN 的 RID 本域解封装流表和 AID 本域终端转发流表,此时移动终端 MN 的通信恢复。同时由于移动终端 MN 已经离开接入域 1,所以还要将 ASR1 中移动终端 MN 的 AID 本域终端转发流表删除,移动切换流程结束。

在移动终端 MN 离开接入域 1 后,通信对端 CN 如果继续与 MN 通信,由于 ASR3 中的目的 AID-RID 映射流表对应的映射关系是 MN 移动之前的映射关系,此时报文击中过期的目的 AID-RID 映射流表,经过封装核心网首部后在核心网中路由到 ASR1, ASR1 将报文解封装后无法击中对应的 AID 本域终端转发流表,此时产生了三角路由, ASR1 会将报文转交给控制器处理。控制器收到三角路由的报文后,解析报文意图,提取报文中的信息,转交给移动性管理模块,进

入三角路由处理流程。移动性管理模块会根据报文中的信息找到具有过期流表的 ASR3,并向它更新目的 AID-RID 映射流表,后续的通信报文就会根据最新的映射关系路由到移动终端 MN 所在的 ASR2,三角路由处理流程结束。

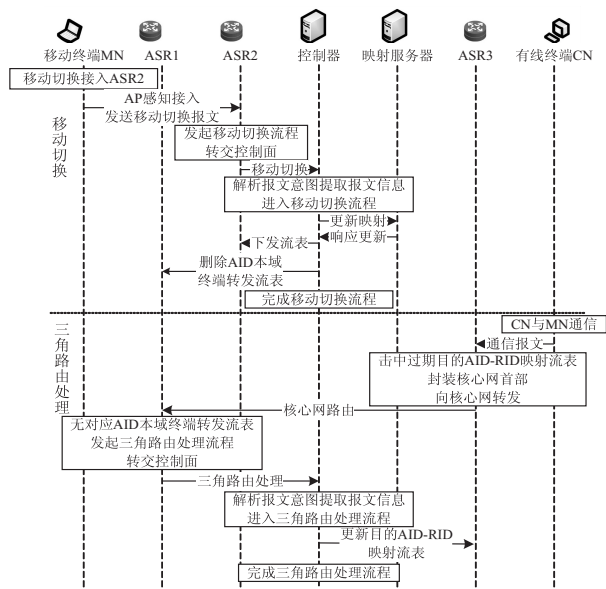


图5 移动切换流程与三角路由处理

3 原型系统搭建与测试

3.1 实验环境

基于可编程平台的标识网络原型系统网络拓扑如图6所示。数据平面由四台可编程P4交换机构成,型号均为Barefoot Networks Wedge100BF-32X。其中三台ASR1、ASR2、ASR3作为接入网接入交换路由器,代表三个接入网。一台作为核心网交换路由器CR。两个无线接入点AP1和AP2分别与ASR1和ASR2连接。控制平面由两台高性能服务器构成,一台作为控制器使用,另一台作为映射服务器使用,配置为Intel® Xeon® Silver 4212 CPU @ 2.20 GHz * 48,搭载62.6GiB内存。数据平面ASR1、ASR2、ASR3分别与CR相连,数据平面四台可编程P4交换机通过P4Runtime协议与控制面进行通信。移动终端MN通过无线接入点AP1接入ASR1,也可以移动切换到AP2接入ASR2。有线终端CN与ASR3相连。

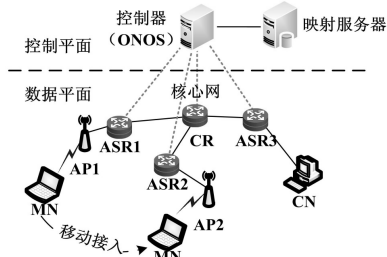


图6 基于可编程平台的标识网络原型系统网络拓扑

3.2 功能测试

首先对设备注册与通信功能进行测试。移动终端MN与有线终端CN在接入网络后首先向ASR1和ASR3发送接入认证报文,交换机收到接入认证报文后转发至控制平面的控制器处理。控制器解析接入认证报文中的信息以及负载密文,通过后为终端设备分配RID并将映射关系发布至映射服务器。并将对应的流表下发至ASR1与ASR3。图7(a)展示了控制器中终端注册的日志,其中包括报文解析、身份认证、映射注册、流表下发的过程。

在移动终端MN与有线终端CN均完成设备注册后,便可开始通信。当MN首次与CN通信时,会触发映射查询,报文从ASR1转交到控制器进行映射查询,映射查询的结果将以流表的形式下发到ASR1。当映射查询结束后,MN的通信报文将经过ASR1核心网首部封装,经核心网路由器CR的转发到达ASR3,解封装后到达CN。通过上述流程,当CN也完成映射查询后,MN与CN能够进行双向端到端通信,在CN上部署视频服务,MN能够访问播放,实现了网络功能的正常运行。

再对移动切换功能进行测试。在移动终端MN与有线终端CN完成设备注册并通信后,MN发起移动切换,从ASR1的AP1接入点切换至ASR2的AP2接入点,AP2感知到无线终端接入,向ASR2发送移动切换报文,ASR2将移动切换报文转交给控制器进行移动切换流程。图7(b)展示了控制器中移动切换日志,其中包括报文解析、流表删除、映射关系更新、流表下发。移动切换流程结束后,CN与MN的通信恢复。

```

| sinetforward | —ManageApp: 收到packet in 报文—— 正在解析SINET报文
| sinetforward | AID = ff:120 DeviceId= device:sinet206 Port= 164 sinet.Type = 2
| sinetforward | 报文类型解析为: 认证报文 已向认证软件转发
| sinet-auth | 载入publicParameter,a.properties文件
| sinet-auth | 开始为 ff:120 验证身份
| sinet-auth | verify succeed!
| sinet-auth | 开始向ASR分发AID转发流表
| sinet-auth | Inserting rule on switch device:sinet206: table=Ingress.aid_fwd
| sinet-auth | 流表分发结束 向注册软件转发
| sinet-map | connected to database: com.mysql.cj.jdbc.ConnectionImpl@6c713975
| sinet-map | 注册成功! RID = 5493 开始为此ASR分发change_src流表项
| sinet-map | Inserting rule on switch device:sinet206: table=Ingress.enable_srcrid
| sinet-map | Inserting rule on switch device:sinet206: table=Ingress.aid_disable
| sinet-map | 向移动性软件转发(写入AIDMAP) 与数据库交互结束
| sinet-mobility | 移动性收到从sinet-mapAPP转发的内容(map) 新增MAP项
  
```

(a) 终端注册控制器日志

```

| sinetforward | —authManageApp: 收到packet in 报文—— 正在解析SINET报文
| sinetforward | AID = ff:120 DeviceId= device:sinet208 Port= 56 sinet.Type = 7
| sinetforward | 报文类型解析为: 移动报文 已向移动性软件转发(收到移动性切换报文)
| sinet-mobility | 不同ASR切换, 进入域间切换流程, 处理流表
| sinet-mobility | Removing rule on switch device:sinet206: table=Ingress.aid_fwd
| sinet-mobility | Removing rule on switch device:sinet206: table=Ingress.enable_srcrid
| sinet-mobility | Inserting rule on switch device:sinet208: table=Ingress.aid_fwd
| sinet-mobility | 向映射模块发起映射更新
| sinet-map | connected to database: com.mysql.cj.jdbc.ConnectionImpl@7e5c4c5e
| sinet-map | 更新映射关系, 分配新的 RID=5495
| sinet-map | 开始为此ASR分发change_src流表项
| sinet-map | Inserting rule on switch device:sinet208: table=Ingress.enable_srcrid
| sinet-map | Inserting rule on switch device:sinet208: table=Ingress.aid_disable
| sinet-map | 向移动性转发(更新AIDMAP) 与数据库交互结束
| sinet-mobility | 移动性收到从sinet-mapAPP转发的内容(map) 更新MAP项
  
```

(b) 移动切换控制器日志

图7 功能测试结果

3.3 性能测试

首先根据移动切换流程分析移动切换时延组成,

时延组成如图 8 所示。从 AP 感知到终端移动接入发出移动切换报文开始,网络层切换时延分为三部分,从数据平面 Packet_in 转交至控制平面的时延、控制平面处理的时延、控制平面流表下发至数据平面生效的时延。Packet_in 时延和流表生效时延受数据平面到控制平面网络实体端到端时延和控制平面与数据平面通信协议解析时延的影响,经多次测试均值在 4.8 ms 左右。控制平面处理流程时延由报文信息解析时延、映射关系更新时延、流表处理流程时延三部分构成。每部分时延受控制器系统运行状态影响,且在控制系统不同模块之间数据传输时延经多次测试为 5.2 ms 左右。实验环境中不同网络实体之间往返时延 RTT 多次测试结果见表 1。

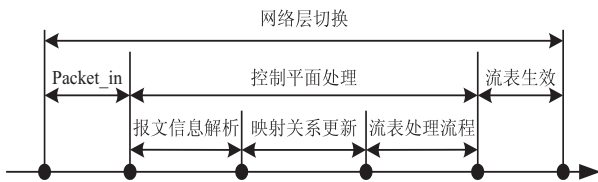


图 8 网络层切换时延组成

表 1 实验环境中不同网络实体之间的往返时间 ms

对端实体	RTT 最小值	RTT 最大值	RTT 平均值
MN-AP1	1.584	27.343	5.787
MN-AP2	1.437	33.562	6.221
ASR-控制器	0.283	0.452	0.303
控制器-映射服务器	0.172	0.382	0.261

下面对移动性管理机制进行多次重复性能测试,在移动终端 MN 与有线终端 CN 完成设备注册与映射查询,能够正常通信时,在 CN 上以每秒 1 000 次的速率向 MN 发送数据包,同时使 MN 在 AP1 与 AP2 之间反复切换,利用抓包软件测量 AP 接入点处从 AP 发出移动切换报文到收到 CN 发送的数据包之间的时间间隔,该时间间隔即为切换时延。

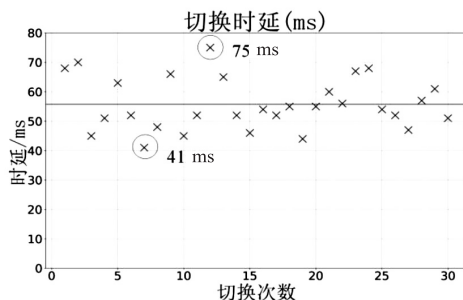


图 9 移动切换性能测试结果

图 9 为 MN 移动切换 30 次获取的实验结果。其中切换时延最大值为 75 ms,最小值为 41 ms,图中横线为平均值 55 ms。从实验结果来看,该移动性管理机制能够满足大部分实时应用需求。基于可编程平台

中集中化管控的控制平面系统减少了在传统交换设备平台中原本不同 ASR 之间传递信息的流程,将原本 ASR 之间交互的信息统一到控制器中处理,省去了不同 ASR 之间通信与处理时延,性能测试结果也显示相对于文献[18]中基于传统交换设备平台的标识网络移动切换性能更快。

4 结束语

针对标识网络在现网中的部署障碍,结合标识网络优势与可编程网络平台特性,该文提出一种基于可编程平台下的标识网络移动性管理机制。基于可编程平台控制与转发分离的理念,数据平面设计一套报文解析与处理流程,实现对标识网络报文的处理转发以及对标识网络设备注册、移动切换的支持。控制平面通过设计控制平面系统与映射服务器,实现设备身份认证与映射关系注册、映射关系查询、设备移动切换等网络功能。同时对应设计,搭建了一套对应的原型系统,并进行了功能测试和性能测试,测试结果表明该机制能够支持标识网络的运行以及对设备移动切换具有良好支持,切换性能满足大部分实时应用需求。

参考文献:

- [1] 郭锐,冯志杰,高宗宁.一种新型网络通信协议的设计与研究[J].计算机技术与发展,2017,27(1):75-79.
- [2] AL-SURMI I, OTHMAN M, ALI B M. Mobility management for IP-based next generation mobile networks: review, challenge and perspective[J]. Journal of Network & Computer Applications, 2012, 35(1): 295-315.
- [3] ZHAO X, PACELLA D J, SCHILLER J. Routing scalability: an operator's view[J]. IEEE Journal on Selected Areas in Communications, 2010, 28(8): 1262-1270.
- [4] 姚琳元.智慧协同网络中安全防御关键技术研究[D].北京:北京交通大学,2018.
- [5] IANNONE L, SAUCEZ D, BONAVENTURE O. Implementing the locator/id separation protocol: design and experience[J]. Computer Networks, 2011, 55(4): 948-958.
- [6] NIKANDER P, GURTOV A, HENDERSON T R. Host identity protocol (HIP): connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks[J]. IEEE Communications Surveys & Tutorials, 2010, 12(2): 186-204.
- [7] ZHANG L, AFANASYEV A, BURKE J, et al. Named data networking[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.
- [8] VENKATARAMANI A, KUROSE J F, RAYCHAUDHURI D, et al. Mobilityfirst: a mobility-centric and trustworthy internet architecture[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 74-80.

(下转第 114 页)