

一种虚拟 AAA 服务器实现方法的研究与实现

刘 艳,程景清,朱恒民,丁可柯,孙科学
(南京邮电大学 电子科学与工程学院,江苏 南京 210003)

摘 要:为了解决利用已有的一套 AAA 服务器设备虚拟出多个不同的逻辑 AAA 设备的问题,文中把虚拟设备的概念在 AAA 服务器上应用分析,研究了一种虚拟 AAA 服务器的实现方法,并在介绍原理的基础上给出了具体的虚拟 AAA 服务器的软件设计和结构模块组成。最后,利用文中介绍的方法,在实验室条件下,成功地在一套 AAA 设备上虚拟出了两套逻辑上完全独立的 AAA 服务器,为不同的网络接入提供服务。验证结果表明,文中研究和探讨的实现虚拟 AAA 服务器的方法是完全可行和有效的。

关键词:虚拟设备;虚拟 AAA 服务器;软件设计

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2014)05-0070-04

doi:10.3969/j.issn.1673-629X.2014.05.017

Research and Implementation of a Virtual AAA Server Realization Method

LIU Yan, CHENG Jing-qing, ZHU Heng-min, DING Ke-ke, SUN Ke-xue
(College of Electronic Science and Engineering, Nanjing University of Posts and
Telecommunications, Nanjing 210003, China)

Abstract: In order to solve the problem that uses an existing AAA server equipment to simulate multiple logical AAA servers, studied a kind of implementation method of virtual AAA server based on application and analysis of the concept of virtual device in AAA server, and provided a specific software design and structure modules composition for virtual AAA server on the basis of introducing the principle. Finally, two virtual AAA server were simulated based on an existing AAA equipment under laboratory conditions by the method proposed, providing services to two different access networks at the same time. Experimental results show that the method to implement virtual AAA server is completely feasible and effective.

Key words: virtual device; virtual AAA server; software design

0 引 言

在通讯网络 PS(Packet Service, 分组业务)域系统设备中,AAA 服务器(Authentication、Authorization、Accounting, 鉴权、授权、计费)作为用户进行 PS 业务的认证、授权、计费中心,需要与多种系统设备进行通信交互,是用户进行 PS 相关业务的核心网元。

在现网的 PS 环境中,存在如下应用场景:

1)运行商的 AAA 已经建设完成,现网铺设有多多个 NAS(Network Access Service, 泛指接入网),每个 NAS 上运营的业务不同,需要 AAA 进行独立的营帐、认证、授权以及计费业务处理;

2)运营商建设了不同的 NAS,例如一个是 CDMA 网络,一个是 WiMAX 网络,另外一个为 LTE 网络^[1],同时都需要 AAA 提供独立的营帐、认证、授权以及计费业务处理;

3)同一张接入网,例如 CDMA 网络,但运营商要求,AAA 需要根据用户的不同 IMSI 号段或者归属域名的不同进行独立的营帐、认证、授权以及计费业务处理等;

4)运营商 A 建设了一套 AAA 服务器,同时租用给运营商 B、运营商 C 等运营。需要 AAA 根据不同运营商提供独立的营帐、认证、授权及计费业务处理。

收稿日期:2013-07-06

修回日期:2013-10-12

网络出版时间:2014-02-11

基金项目:国家自然科学基金资助项目(71271120);南京邮电大学教改项目(JG03312JX10, JG03311JX26, JG03313JX17);南京邮电大学通达学院教改项目(TD00211JG32);南京邮电大学青蓝计划(NY210037)

作者简介:刘 艳(1977-),女,硕士,讲师,研究方向为复杂系统与智能控制。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20140211.1450.013.html>

一般的处理方法是,对 AAA 网元进行扩容,增加 AAA 的套数,满足不同场景下独立的营帐、认证、授权以及计费业务处理。这种方法的缺点是,不但增加了客户的成本(需要客户额外增加资金投资,用于购买新设备),同时又延长了工期(设备从发货到工程建设完成,一般周期都比较长),客户一般很难接受,因此迫切需要提供一种有效的技术方法,能够在已有的一套 AAA 设备上虚拟出多个不同的逻辑 AAA(下文简称虚拟 AAA),从而满足不同的独立业务需求。

1 虚拟设备技术与虚拟 AAA 服务器

1.1 虚拟设备技术

通过虚拟技术^[2]将一台独占设备虚拟成多台逻辑

设备,供多个用户进程同时使用,通常把这种经过虚拟的设备称为虚拟设备^[3],比如虚拟机操作系统中会虚拟出各种硬件设备以支持虚拟机操作系统等。目前的虚拟设备技术主要有虚拟存储技术^[4-5]、虚拟仪器/仪表^[6]、虚拟光驱^[7]、虚拟网卡^[8]、虚拟机等。

1.2 虚拟 AAA 简介

虚拟 AAA 是一个逻辑上的概念,即将一套 AAA 系统通过技术方法,在逻辑上划分成多个独立的虚拟 AAA 设备,每个虚拟 AAA 在营帐(业务受理)、认证、授权、计费、OMC 配置、性能统计、告警等各个方面呈现出来的都是相对独立的 AAA 设备。

虚拟 AAA 的效果如图 1 所示(图中 NAS:Network Access Server,网络接入服务器)。

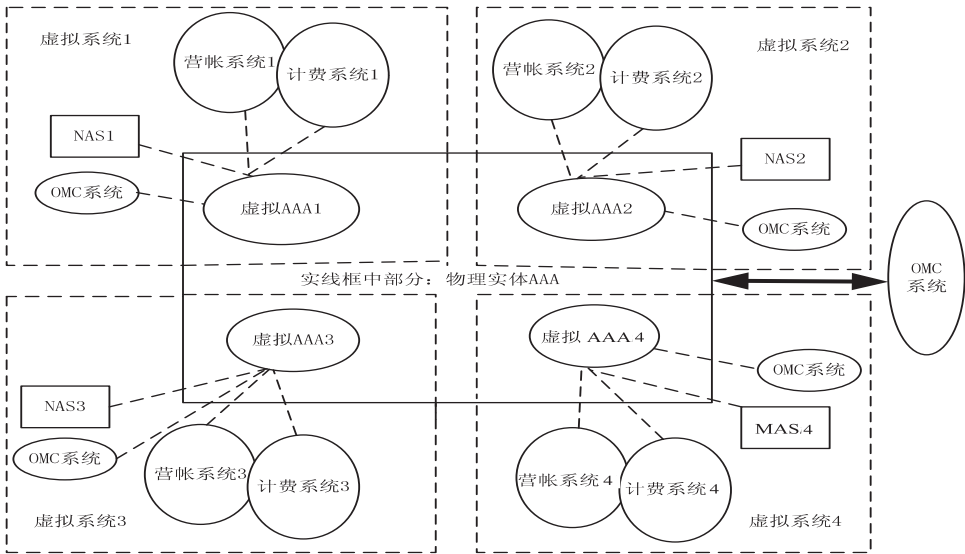


图 1 物理实体 AAA 虚拟为多个 AAA 后对外提供服务的示意图

每个虚拟出来的 AAA 设备,具备的能力至少包含如下部分:

- 1) 虚拟 AAA 提供独立的配置接口;
- 2) 虚拟 AAA 可以开展不同的业务;
- 3) 虚拟 AAA 的营帐接口,支持按照域名方式或者号段方式划分为不同的虚拟 AAA;
- 4) 虚拟 AAA 可以输出话单到不同的位置;
- 5) 虚拟 AAA 提供独立的性能统计项(例如:用户数、接入成功次数、失败次数、无效数据格式等);
- 6) 虚拟 AAA 提供独立的告警、失败观察、信令跟踪、日志维护等操作维护功能;
- 7) 虚拟 AAA 对外提供的业务、营帐接口、计费的 IP 地址信息是独立的。

2 虚拟 AAA 服务器实现原理

虚拟 AAA 服务器的实现原理是根据用户的标识(例如:IMSI 号段或者用户的归属域名)对用户进行区分,归类到不同的虚拟设备中,然后确定每个虚拟设备

自己的 OMC 配置、性能统计、告警、营帐接口、业务接口等信息。

实现原理按步骤说明如下:

步骤 1:首先通过 OMC 系统配置管理域与虚拟 AAA 的对应关系,参考结构如表 1 所示。

表 1 OMC 系统配置管理域与虚拟 AAA 的对应关系表

划分模式	虚拟 AAA 管理域	虚拟 AAA 标识
...

(1)划分模式:IMSI 号段或者域名(在一个配置表中,只能选择一种,要么 IMSI 号段,要么域名,不能混合)。

(2)虚拟 AAA 管理域:

IMSI 号段:此处是号段的范围,例如 46003456 XXX-46003756XXX;

域名:此处是具体的域,例如 cmcc-huadong. com. cn;

(3)虚拟 AAA 标识:数字,从 1 开始,范围 1 ~

255。
举例如表 2 所示。

表 2 OMC 系统配置管理域与虚拟 AAA 的对应关系表数据举例

划分模式	虚拟 AAA 管理域	虚拟 AAA 标识
域名	cmcc-huadong. com. cn	1
域名	cmcc-xibei. com. cn	2

说明,对于用户,如果归属域是 cmcc-huadong. com. cn,则认为归属在虚拟 AAA1;域名为 cmcc-xibei. com. cn 的,归属在虚拟 AAA2。

步骤 2:OMC 系统中,所有有关 AAA 的配置表(具体到每个表和结构,超出文中讨论范围,与实际使用的 AAA 设备相关),增加虚拟 AAA 标识字段,用于标识配置表中的某条配置信息,属于哪个虚拟 AAA。

例如,NAS 配置表结构如表 3 所示。

表 3 NAS 配置表结构

NASIP	NASID	AS	NASTYPE
...

- NASIP:NAS 的 IP 地址;
 - NASID:NAS 的标识,可以是名字;
 - AS:系统设备间安全关联,即密码;
 - NASTYPE:NAS 的类型,例如 AGW、PDSN、LNS、HA 等。
- 增加虚拟 AAA 标识后的表结构如表 4 所示。
- VirAAAID:虚拟 AAA 标识,对应步骤 1 中的“虚

拟 AAA 标识”。

表 4 增加虚拟 AAA 标识后的 NAS 配置表结构

NASIP	NASID	AS	NASTYPE	VirAAAID
...

步骤 3:通过 OMC 系统配置各个虚拟 AAA 需要的配置信息到配置模块。

步骤 4:AAA 业务进程根据用户所属的虚拟 AAA,到对应的 VirAAAID 标识的配置记录中获取配置信息。

步骤 5:不同的 NAS 或者外部系统发起请求(请求可以是用户认证授权、计费话单获取、营帐指令等消息),AAA 业务处理模块根据不同的“虚拟 AAA 管理域”,按不同的配置信息,进行业务逻辑处理。

步骤 6:AAA 业务处理模块根据“虚拟 AAA 管理域”,提供独立的性能统计告警、失败观察、信令跟踪等操作维护功能。

3 虚拟 AAA 服务器软件设计

虚拟 AAA 服务器按层次结构进行设计。软件系统包括(如图 2 所示)主控模块、底层通信以及监听模块、Radius^[9]/Diameter^[10]协议栈处理模块、业务逻辑处理模块、用户数据及计费话单存储中心、AAA 配置模块、OMC 操作维护中心等。系统支持 Windows 和 Linux 操作系统,在开启后自动加载运行。

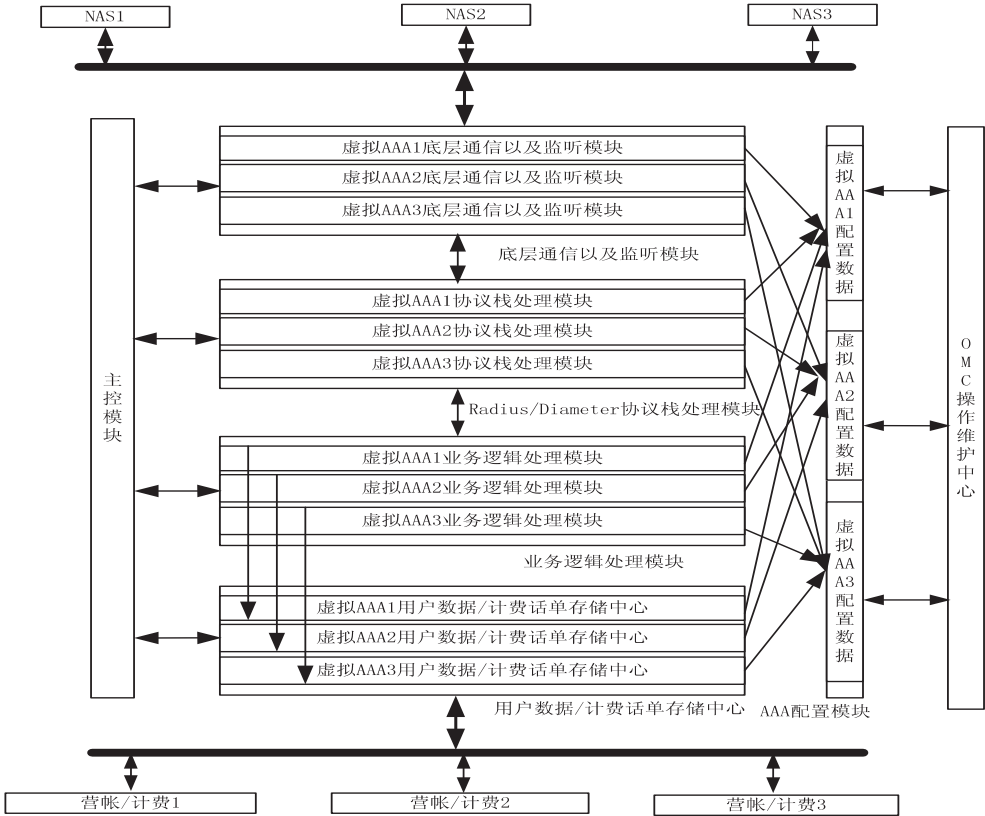


图 2 虚拟 AAA 服务器软件系统结构示意图(以实现 3 个虚拟 AAA 为例)

3.1 主控模块

主控模块是整个软件系统的控制与管理模块,主要负责各个子模块的进程启动以及运行状态监控。在软件系统启动时,主控模块首先启动,然后开始初始化系统所需的系统环境,例如内存检测、硬件存储空间检测等,完成后开始调起各个子模块并监控各子模块的运行。在发现某个子模块无法启动或者运行过程中异常退出时,则重新调起该模块,在某个子模块(除配置维护子模块外)始终无法正常运行时,主控模块负责通过配置维护子模块向外告警,提示操作人员关注。

3.2 底层通讯以及监听模块

底层通讯以及监听模块负责 AAA 与外部系统设备的底层链路连接的建立、监听与运行状态监控,支持基于预置共享密钥的安全连接方式。当外部系统设备有消息到达时,IP 包会首先到达底层通讯以及监控模块,由其解密后,根据消息内容发往不同的处理模块。同时,在 AAA 与外部系统设备链路发生异常时也能够及时检测到,并根据配置信息重新调整链路状态。

3.3 Radius/Diameter 协议栈模块

Radius/Diameter 协议栈模块提供了 Radius/Diameter 协议的信令编解码处理功能,对收到的信令中的报文信息,进行编解码,获取具体的内容提供给业务逻辑处理模块使用。同时支持 Radius/Diameter 协议栈的基于协议层面的链路管理和维护功能,是协议处理的基本模块。

3.4 业务逻辑处理模块

业务逻辑处理模块负责用户具体的业务逻辑处理,例如用户是否是合法用户的认证,认证通过后用户需要授权的信息,包含用户签约的 QoS 参数,用户限制漫游的接入网等信息。业务逻辑处理模块完成用户控制面的业务逻辑控制,是 AAA 的主要功能模块。

3.5 用户数据及计费话单存储中心

用户数据及计费话单存储中心主要实现两大功能:一是存储用户的开户信息,外部营帐系统通过中心对外提供的用户数据接口,对用户信息进行维护,用户信息包含用户名、密码、用户的 IMSI/MSISDN 号码、用户签约的授权信息参数等,是用户的基本信息;另外一个存储用户在进行数据业务时产生的话单信息,信息中包含用户的标识,例如 IMSI/MSISDN、用户名、进行数据业务的开始时间/终止时间、此次数据业务使用的流量等信息,话单信息以文件的形式存储,在外部计费中心需要的时候提供给对应的计费中心,对用户进行计费管理。

3.6 AAA 配置模块

AAA 配置模块负责软件系统运行信息的配置维护、性能数据接收上报、告警数据接收上报等操作维护

功能。

软件系统运行信息的配置维护主要有:底层通信以及监听模块需要的监听外部系统设备的 IP 地址、端口配置、监听频率参数等的配置;Radius/Diameter 协议栈模块需要的对端链路 IP 地址、对端主机名、路由方式等的配置;用户数据及计费话单存储中心需要的外部营帐系统接口机的 IP 地址、加密方式等的配置;用户数据及计费话单存储中心需要的外部计费中心的 IP 地址、FTP 用户名、密码、初始路径等的配置;业务逻辑处理模块需要的业务参数配置,例如管理域与虚拟 AAA 的对应关系配置、允许授权的用户参数列表配置等。

性能数据接收上报主要支持来自各个虚拟 AAA 子模块的性能信息接收并上报给操作维护中心。例如底层通讯以及监听模块的指定 IP 地址收到的报文数、回应的响应数、收到的错误 IP 报文数等;例如业务处理模块指定时段内,成功处理消息数、失败消息数、收到 Radius 消息数、收到 Diameter 消息数、转发的消息数、翻译的消息数等统计信息,是软件系统运行状态的对外接口。

告警数据接收上报模块主要支持来自各个虚拟 AAA 子模块的告警数据接收并上报给操作维护人员。例如某个虚拟 AAA 底层通讯模块的某个 IP 地址链路异常断开、外部营帐接口机断开、外部计费中心话单获取失败告警、主控模块的某个子模块运行状态异常等告警信息,是软件系统故障对外呈现的接口。

3.7 OMC 操作维护中心

OMC 操作维护中心是 AAA 设备的操作维护中心,对操作人员提供人机或者命令接口,配置 AAA 运行所需要的配置信息(例如文中需要的管理域与虚拟 AAA 的对应关系配置信息等),并监控 AAA 设备的运行情况,提供 AAA 设备或者虚拟 AAA 设备的性能统计信息和告警信息,以便监控 AAA 的运行状态。

4 结束语

文中重点研究了一种虚拟 AAA 服务器的实现方法,并在介绍原理的基础上给出了具体的虚拟 AAA 服务器软件设计和结构模块组成。利用文中介绍的方法,在实验室条件下,成功地应用一套 AAA 服务器虚拟出了两套逻辑上完全独立的 AAA 服务器,一个用于 CDMA 网络用户的接入控制,一个用于 WLAN 网络用户的接入控制^[11-12]。验证结果表明,文中研究和探讨的实现虚拟 AAA 服务器的方法,是完全可行和有效的,为虚拟 AAA 服务器的研究与实现提供了思路,具备较高的工程应用价值。

现的更明显。这是因为 LA-ACO 算法能建立多条路径,平衡流量负载;动态更新路径的信息素,并利用信息素的强度作为启发在以后的路由中合理平衡网络流量,提高网络总体吞吐量。

由图 3 可以看出,LA-ACO 和 AODV 的平均端到端的延时随着节点移动性的减弱而减少,同样通过纵向比较,可以发现相同的节点移动频率上,LA-ACO 的平均端到端时延都要小于 AODV,这是因为 LA-ACO 能够依据不同网络状态,自适应地选择轻负载路由,在多条路径间进行负载均衡,并通过路由修复机制缩短了重发延时,然而 AODV 却不具有这种应对路由出现高负载的方法。

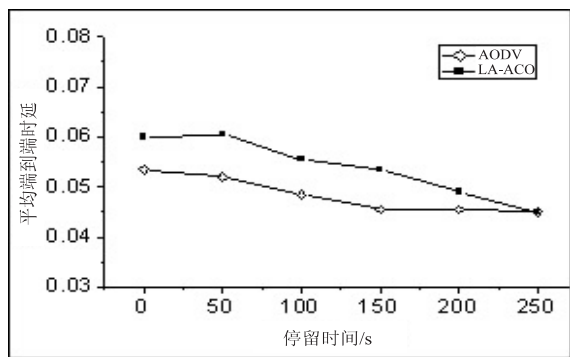


图 3 平均端到端时延比较

4 结束语

文中对 NetAnt 路由协议进行了分析,针对 NetAnt 路由协议没有考虑带宽有限,同时在链路失效时直接进行重新路由这一缺点,对其进行了多路径路由的修改,在链路修复部分引入了链路中断预测机制。利用 NS-2.34 对改进后的协议进行了仿真分析,仿真结果表明,改进后的协议能有效减少端到端平均时延,提高分组投递率,这对改善网络的整体性能具有十分重要

的意义。

参考文献:

- [1] 王 华,薛 涛,崔云平,等. Ad Hoc 网络技术[J]. 硅谷, 2012(17):9-10.
- [2] Ramanathan R,Redi J. A brief overview of Ad Hoc networks: challenges and directions[J]. IEEE Communications Magazine, 2002,40(5):20-22.
- [3] 石丛军,任清华,郑 博,等. MANET 节点移动模型仿真研究[J]. 计算机工程,2009,35(14):101-103.
- [4] 王浩波,黄 伟,刘存才. 无线信道干扰概率对网络性能影响分析[J]. 通信系统与网络技术,2012,38(1):10-11.
- [5] 田旺兰. 无线传感器网络中影响能源消耗的因素的研究[J]. 电脑知识与技术,2008,4(3):742-744.
- [6] Perkins C,Belding-Royer E, Das S. Ad hoc On-demand Distance Vector (AODV) routing[EB/OL]. [2008-12-13]. <http://www.ietf.org/rfc/rfc3561.txt>.
- [7] Johnson D, Hu Y, Maltz D. The Dynamic Source Routing (DSR) protocol for mobile ad hoc networks for IPV4[EB/OL]. [2008-12-13]. <http://www.ietf.org/rfc/rfc4728.txt>.
- [8] 常慧君,单 洪. Ad Hoc 路由协议 LAR 的性能分析与研究[J]. 微计算机应用,2009,30(3):20-24.
- [9] 安辉耀,卢锡城. 移动自主网络多路径路由技术研究进展[J]. 计算机工程与科学,2006,28(2):4-9.
- [10] 秦 军,付珍珍,王小丽. 基于蚁群的 Ad Hoc 网络分簇路由算法[J]. 计算机技术与发展,2012,22(1):72-75.
- [11] Chandra S,Shrivastava U,Vaish R, et al. Improved-AntNet: ACO routing algorithm in practice[C]//Proc of 11th international conference on computer modelling and simulation. Cambridge:[s. n.], 2009:25-29.
- [12] 周少琼,徐 祎,姜 丽,等. 蚁群优化算法在 Ad Hoc 网络路由中的应用[J]. 计算机应用,2011,31(2):332-334.
- [13] 方路平,刘世华,陈 盼,等. NS-2 网络模拟基础与应用[M]. 北京:国防工业出版社,2008:89-104.


(上接第 73 页)

参考文献:

- [1] 3GPP TS29.273. Evolved Packet System (EPS);3GPP EPS AAA interfaces[S]. 2010.
- [2] 王志新,张 华,黎永明. 虚拟技术及其应用[J]. 上海理工大学学报,1998,20(1):49-55.
- [3] 刘保华,黄考利,杨锁昌. 虚拟仪器的软件实现方法[J]. 自动化博览,2002(1):34-36.
- [4] 李子臣,王文静. 网络时代经济高效的数据存储方式:虚拟存储[J]. 现代情报,2002(6):119-121.
- [5] 郭御风,李 琼,刘光明,等. 虚拟存储技术研究[J]. 计算机应用研究,2004,21(2):56-60.
- [6] 乔维德. 虚拟仪器技术及其展望[J]. 电气时代,2005(12):18-20.

- [7] 杨 达,高 欣. 浅谈虚拟光驱及应用[J]. 工业技术与职业教育,2001,9(4):15-16.
- [8] 肖 凌,李之棠,梅 松. 一种基于虚拟网卡的 Windows-VPN 体系结构研究[J]. 小型微型计算机系统,2007,28(9):1586-1590.
- [9] Rigney C,Rubens A C,Simpson W A, et al. Remote Authentication Dial In User Service (RADIUS)[S]. RFC 2865,2000.
- [10] Fajardo V,Arkko J,Loughney J, et al. Diameter base protocol[S]. RFC 6733,2012.
- [11] 3GPP TS23.402. Architecture enhancements for non-3GPP accesses version10.0.0[S]. 2010.
- [12] 3GPP TS23.234. 3GPP system to Wireless Local Area Network version10.0.0 (WLAN) interworking; System description[S]. 2010.

一种虚拟AAA服务器实现方法的研究与实现

作者：[刘艳](#)，[程景清](#)，[朱恒民](#)，[丁可柯](#)，[孙科学](#)，[LIU Yan](#)，[CHENG Jing-qing](#)，[ZHU Heng-min](#)，[DING Ke-ke](#)，[SUN Ke-xue](#)
作者单位：[南京邮电大学 电子科学与工程学院, 江苏 南京, 210003](#)
刊名：[计算机技术与发展](#) 
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2014(5)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjtz201405017.aspx