基于双栈架构的下一代 AAA 服务器设计与实现

刘 艳,程景清,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:针对下一代通讯网络 EPC(Evolved Packet Corenetwork)系统中 AAA 服务器通信协议的特点:同时支持 Radius 协议和 Diameter 协议,为了解决 AAA 对不同协议的兼容和自动翻译问题,文中设计和实现了一种基于 Radius/Diameter 双协议栈的用于下一代通讯网络 EPC 系统中的 AAA 服务器。通过采用协议适配与转换模块、Radius 协议栈模块、Diameter 协议栈模块等,经过简单的配置,AAA 服务器即可自动完成不同协议的翻译和转换。实验结果表明,这种支持双栈架构的下一代 AAA 服务器,能够很好地兼容不同的协议,并有效降低了工程维护成本。

关键词:EPC;下一代网络;AAA;Radius;Diameter;双协议栈
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2014)03-0242-04
doi:10.3969/j.issn.1673-629X.2014.03.060

Design and Implementation of Next-generation AAA Server Based on Dual-stack Architecture

LIU Yan, CHENG Jing-qing, SUN Ke-xue
(College of Electronic Sci. and Eng., Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: For the characteristics of the communication protocol of the AAA server in the next-generation communications networks EPC system: To support Radius protocol and Diameter protocol simultaneously, in order to solve problem of compatibility and automatic translation between different protocols, designed and implemented a AAA server based on Radius/ Diameter dual-stack for next-generation communications networks EPC system. By using protocol adaptation and conversion module, Radius protocol stack modules, Diameter protocol stack module etc., through simple configuration, AAA server can automatically complete the translation and conversion of different protocols. Experimental results show that this support dual-stack architecture of the next generation of AAA server can be well compatible with different protocols, and effectively reduce engineering and maintenance costs.

Key words: EPC; next-generation; AAA; Radius; Diameter; dual-stack

0 引 言

在通讯网络 PS(Packet Service:分组)域系统设备中,AAA 服务器(Authentication:鉴权,Authorization:授权,Accounting: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。例如在 CDMA 移动通讯网络中,需要与接入网设备 PDSN、HA 等通信;在 GPRS/WCDMA 移动网络中,需要与 GGSN 通信;在 WiMAX 网络中,需要与 AGW 通信;在宽带接入网络中,需要与 BAS/BRAS 等进行通信。

AAA 与这些系统设备的通信协议,在 PS 域初期发展阶段采用的是 Radius 协议[1]。但是,随着 PS 域的迅速发展,在其上开展的新业务越来越多,也越来越丰富。这些新业务要求通信各方处于对等地位,并且许多新业务对移动性有较大依赖,要求 AAA 协议支持 Mobile IP 和漫游,而 Radius 协议在这方面的支持是很薄弱的[2];同时在其他需求上,如纠错、安全性能、传输的可靠性、代理的支持、审计功能、能力协商等方面,Radius 协议也显得不足。因此,2001 年 6 月,IETF 的 AAA 工作组同意,将 Diameter 协议作为下一代的 AAA 协议标准,从而丰富了 AAA 的协议支持。

收稿日期:2013-05-12 **修回日期**:2013-08-20 **网络出版时间**:2014-01-07
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);南京邮电大学通达学院教改项目(TD00211JG32);南京邮电大学科研项目(xc212024)
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.20140107.1726.049.html

Diameter 协议[3]可以认为是 Radius 协议进一步的完善和发展[4-5]。

这样,下一代通讯网络中的 AAA 服务器(文中简称下一代 AAA 服务器),需要同时支持 Radius 和 Diameter 协议,以便在与系统设备互联互通的时候,自动完成协议的转换与翻译。

1　Radius/Diameter 协议简介

1.1　Radius 协议简介

Radius 是目前最常用的认证计费协议之一,第一个 Radius 的 RFC 是在 1997 年出版的[6]。Radius 是一种 C/S 结构的协议,任何运行 Radius 客户端软件的计算机都可以成为 Radius 的客户端。Radius 协议认证机制灵活,可以采用 PAP(Password Authentication Protocol)、CHAP(Challenge/Handshake Authentication Protocol,质询/握手认证协议)或者 Unix 登录认证等多种方式。Radius 也是一种可扩展的协议,它基于其管理的 Attribute-Length-Value 信息实现认证、授权与计费功能[7]。

1.2　Diameter 协议简介

Diameter 协议不是一个单一的协议,而是一个协议簇,它包括基本协议(Diameter Base Protocol)和各种由基本协议扩展而来的应用协议,如 NASREQ、Mobile IP、CMS Security 等。Diameter 基本协议为各种认证、授权和计费业务提供了安全、可靠、易于扩展的框架。其主要涉及性能协商、消息如何被发送、对等双方最终如何结束通信等方面。还定义了某些规则,以应用于 Diameter 节点之间的消息交换上。另外,基本协议还说明了消息格式、传输方式、错误报告等。Diameter 消息分为头部和由以属性值对 AVP 的形式逐个头尾相接组成的消息体两部分。虽然 Diameter 基本协议要求必须被所有的协议支持,但它一般不会单独使用,需要应用扩展它提供具体的服务。目前,IETF 的 AAA 工作组已经完成了 Diameter NASREQ 应用[8]、Diameter Mobile Ipv4/ Ipv6 应用等应用协议的制定,以便满足当前的网络访问的需要。

2　下一代网络中 AAA 的位置及系统组成结构

下一代网络 EPC 中 AAA 的位置以及系统组成结构,参考 3GPP TS23.402 的定义如图 1 所示[9]。

从图 1 中可以看出,在下一代网络中,AAA 通过 Sta 接口[10]、S6b 接口[10],对终端或者用户通过授信的非 3GPP 网络接入 EPC 进行控制面的信令控制,并通过 SWx 接口与 HSS 进行交互,完成用户的认证、授权过程,完成对用户的接入进行控制;同时 AAA 通过 SWa[10]、SWm[10]接口以及 S6b 接口,对终端或者用户通过非授信的非 3GPP 网络接入 EPC 进行控制面的信令控制,并通过 SWx[9]接口与 HSS 进行交互,完成用户的认证、授权过程,完成对用户的接入进行控制。同时在下一代网络中,3GPP 组织也在 3GPP TS23.234 中独立定义了宽带接入网络 WLAN 接入时 EPC 的系统架构以及 AAA 在其中的位置,具体请参考文献[11]。

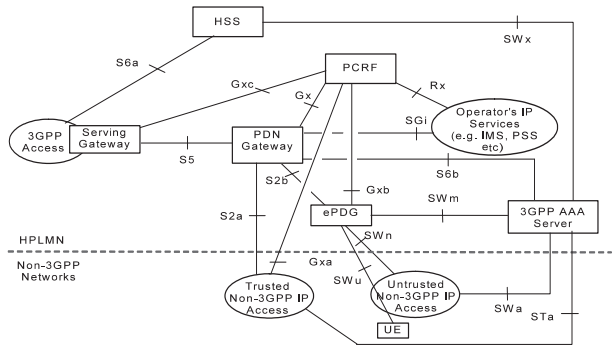

图 1　(授信/非授信)非 3GPP 网络接入 EPC 中 AAA 的位置以及系统组成结构示意图

3　基于双栈的下一代 AAA 服务器设计

下一代 AAA 服务器按层次结构进行设计[12]。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、数据访问控制模块、协议适配与转换模块、Radius 协议栈模块、Diameter 协议栈模块、业务逻辑处理模块、配置维护模块以及数据存储模块等。系统支持 Windows 和 Linux 操作系统,在开启后自动加载运行。

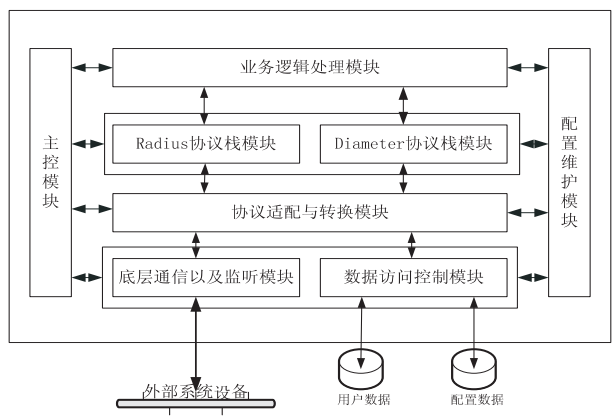

图 2　基于双栈的下一代 AAA 服务器软件系统结构示意图

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 配置维护模块

配制维护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;数据访问控制模块需要访问的数据库 IP 地址、用户名、密码配置,数据库连接管理参数配置;协议适配转换模块需要的 Radius 与 Diameter 转换的策略配置,例如哪条 Radius 属性翻译为应该为哪条 Diameter 属性、来自哪个 IP 地址的外部系统设备是 Radius 的还是 Diameter 的,翻译中存在不可识别的属性应该怎么翻译等;Radius/Diameter 协议栈模块需要的本地域名配置,路由信息配置,号段或者 NAI(Network Access Identifier)分析配置,各自支持的 AVP(Attribute Value Pairs)列表配置等;业务逻辑处理模块需要的业务参数配置,例如漫游区配置、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子模块的性能信息接收并上报给操作维护人员。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子模块的告警数据接收并上报给操作维护人员。例如底层通讯模块的某个 IP 地址链路异常断开,数据访问控制模块的数据库连接异常,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。

3.3 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。

3.4 数据访问控制模块

数据访问控制模块主要完成数据库的访问,例如用户数据的增删查改、配置数据的增删查改等。为了软件系统的可靠性以及高移植性,数据访问控制模块封装了一系列数据操作的命令,提供给上层模块使用。不管底层是 Oracle 数据库还是 Sqlserver 数据库或者是 MySql 数据库,均由该模块统一封装基本的数据操作指令。在底层数据库发生变化时,对外提供的接口指令不变,上层模块也不需要进行任何修改。保证了代码在数据库层面的高移植性和安全性。

3.5 协议适配与转换模块

协议适配与转换模块根据底层通讯以及监听模块转发上来的消息(Radius 或者 Diameter),选择合适的 Radius/Diameter 协议栈模块,首先进行编解码,获取消息中携带的内容。然后,在业务逻辑处理模块完成处理后,根据消息需要发往的系统设备支持的协议类型是 Radius 或者 Diameter,决定是否进行协议转换,如果需要转换则根据从配置模块获取的转换策略,对不同的协议消息进行翻译,然后交给底层通讯以及监听模块转发出去。

3.6 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。

3.7 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,例如用户需要授权的 QoS 参数信息、能够使用的带宽信息、用户限制漫游的接入网等。业务逻辑处理模块完成用户层面的业务逻辑控制。

3.8 流程简要说明

根据上述模块,基于双栈架构的下一代 AAA 服务器实现的业务处理步骤如下:

步骤 1. AAA 服务器上通过配置维护模块配置协议处理策略和转换规则,如下:

1)对来自不同系统设备的消息配置不同的协议处理策略;

例如:对来自 PDSN 系统设备的消息,配置根据其标识,NAS-IP/NAS-ID 或者 IP,配置使用的协议栈为 Radius;而对来自 AGW 网元消息,配置根据其标识,NAS-IP/NAS-ID 或者 IP,配置使用的协议栈为 Diameter 等。

2)配置 Radius/Diameter 协议相互转换的转换规则。

例如:对 Radius 向 Diameter 的消息转换,配置规则如表 1(该表格仅是示例,列出了部分 AVP 的转换,具体需要根据实际业务进行配置)。

步骤 2. 底层通信以及监听模块监听到系统设备

消息到达 AAA(为了便于描述假设消息是基于 Radius 协议的码流);

表 1　Radius 向 Diameter 的消息转换配置

Radius AVP	Diameter AVP	说明
User-Name	[User-Name]	NAI
无	[Origin-State-Id]	AAA 主动生成
Event-Timestamp	[Event-Timestamp]	Event-Timestamp
Calling-Station-ID	*[Subscription-Id] {Subscription-Id-Type} {Subscription-Id-Data}	Calling-Station-ID = MDN
Release-Indicator	[Termination-Cause]	AAA 转换
PPAQ	*[Used-Service-Unit]	
QuotaId	无	Diameter 中无对应参数,不需要转换
Update-Reason	[Reporting-Reason]	
无	[Tariff-Change-Usage]	Diameter 中无对应参数,不需要转换
DurationQuota	[CC-Time]	
VolumeQuota	[CC-Total-Octets]	

步骤 3. AAA 协议适配与转换模块根据静态的配置数据,选择适用的协议栈进行消息码流处理;或者如果没有静态数据配置策略,协议适配与转换模块根据消息码流的格式,自动选择 Radius 或者 Diameter 协议进行处理;

步骤 4. Radius 协议栈处理模块对码流进行编解码等处理,处理后的码流送达业务处理模块;

步骤 5. 业务处理模块按照一定的业务逻辑,完成对消息的业务层处理,并判断消息下一步到达的系统设备所支持的协议类型是否也是基于 Radius 协议的?

如果支持,则不需要进行协议转换与翻译,业务处理后的消息经协议栈模块重新编解码后,通过协议适配与转发模块发送回去,流程结束;

如果下一步到达的系统设备所支持的协议类型为 Diameter,则流程转步骤 6,消息码流送达协议适配与转换模块;

步骤 6. 协议适配与转换模块对消息按照配置模块的转换规则进行转换,完成后,消息经协议栈模块重新编解码后,流程转步骤 7;

步骤 7. 转换为基于 Diameter 协议的消息码流送达协议适配与转发模块,流程转步骤 8;

步骤 8. 协议适配与转发模块经底层通讯以及监听模块发出转换后的 Diameter 消息,流程结束。

4　结束语

文中设计和实现的基于双栈方式的下一代 AAA 服务器,同时支持 Radius/Diameter 协议的处理,且可配置地支持不同协议系统设备间的消息转换,具备很高的应用性和灵活性,在实际应用部署中,能够带来显著的经济价值,是下一代网络中 AAA 服务器应用的一个发展方向。但由于篇幅所限,文中并没有探讨下一代 AAA 服务器的容灾方式,安全特性,高性能架构以及基于云服务模式的业务处理等内容,这些可以作为进一步研究和应用的方向。

参考文献:

[1] Rigney C, Rubens A C, Simpson W A, et al. Remote Authentication Dial In User Service (Radius)[S]. RFC 2865, 2000.

[2] 朱海龙,张国清. 基于 DIAMETER 的 AAA 技术及其在 Mobile IP 中的应用[J]. 计算机工程与应用,2003(21):159-163.

[3] Fajardo V, Arkko J, Loughney J, et al. Diameter base protocol [S]. RFC 6733, 2012.

[4] 李斌祥. 采用 Radius 协议的 AAA 系统的研究[J]. 重庆邮电学院学报(自然科学版),2006(Sup):193-196.

[5] 蔡　磊,陈　越,王　娜,等. DIAMETER 协议和 Radius 协议的比较[J]. 微计算机信息,2006,22(5-3):244-246.

[6] 李　倩. AAA 认证协议的分析[J]. 北京工商大学学报(自然科学版),2006,24(4):45-47.

[7] 张　琪,喻占武,李　锐,等. 基于 AAA 服务的协议分析与比较[J]. 计算机应用研究,2007(2):296-298.

[8] 黄永锋,王　滨,许晓东. RADIUS 在 802.1x 中的应用[J]. 计算机工程与设计,2006,27(5):798-801.

[9] 3GPP TS23.402. Architecture enhancements for non-3GPP accesses Version10.0.0[S]. 2010.

[10] 3GPP TS29.273. Evolved Packet System (EPS);3GPP EPS AAA interfaces[S]. 2010.

[11] 3GPP TS23.234. 3GPP system to Wireless Local Area Network Version10.0.0 (WLAN) interworking;System description[S]. 2010.

[12] 陈能干,裘姝平. 基于 Diameter 的 AAA 服务器的设计与实现[J]. 计算机工程与设计,2004,25(12):2274-2276.

(上接第 241 页)

[8] 王明兰,叶东升. 测试用例描述语言研究[J]. 计算机工程与设计,2006,27(22):4281-4284.

[9] Aurum A, Peterson H, William C. State-of-the art: Software inspectiors after 25 years[J]. Software testing, verification and reliability, 2002, 12(3):133-154.

[10] Myers G J. The art of software testing[M]. New Jersey: John Wiley & Sors, Inc., 2004.

[11] Patton R. Software testing[M]. 2nd Revised ed. [s. l.]: Sams Publishing, 2005.

[12] Dustin E, Garrett T, Gauf B. Implementing automated software testing—How to save time and lower while raising quality [M]. Beijing: Publishing House of Electronic Industry, 2011: 98-100.

基于双栈架构的下一代AAA服务器设计与实现

作者： 刘艳， 程景清， 孙科学， LIU Yan， CHENG Jing-qing， 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
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(3)