第34卷 第15期 计 算 机 工 程 2008年8月
Vol.34 No.15 Computer Engineering August 2008
·网络与通信· 文章编号：1000—3428(2008)15—0126—03 文献标识码：A 中图分类号：N945

基于IPTV的AAA服务器的设计与实现

叶 赛，张洪伟
(四川大学计算机学院，成都 610064)

摘 要：网络电视(IPTV)的设备提供商与运营商拥有各自的用户认证、授权与计费系统，各系统间互不兼容且性能差异大。该文根据AAA的原理与IPTV系统的业务特点，提出一个基于IPTV系统的统一AAA服务器的设计方案。系统采用AAA最新的Diameter协议，优化认证、授权和计费过程，通过引入高速cache，解决大量访问造成的性能瓶颈。实验证明了该方案的可行性。

关键词：AAA服务器；网络电视；Diameter协议；缓存

Design and Implementation of AAA Server Based on IPTV

YE Sai, ZHANG Hong-wei
(College of Computer, Sichuan University, Chengdu 610064)

【Abstract】 Many IPTV companies provide their systems of authentication, authorization, accounting, but the systems are not compatible and their capability are not excellent for IPTV system. According to the theory of AAA and IPTV model, this paper gives a whole solution on AAA server based on IPTV. By using Diameter protocol, it optimizes the processes of authentication, authorization and accounting, and uses cache to resolve the capability bottle-neck of system. Simulation experiment verifies that it is effective.

【Key words】 AAA server; IPTV; Diameter protocol; cache

1 概述

近年来网络服务和网络用户呈爆炸式发展，极大地促进了网络电视(IPTV)的推广和应用。在北美，加拿大电信公司2007年4月的IPTV用户数突破了10万。在欧洲，由于德国和法国的大力推动，2006年全球IPTV的市场份额以欧洲地区所占最大，达到了50%。在亚太，日本的Yahoo BB自2003年初开通就迅速达到了十几万的用户。同时，我国的IPTV市场也在飞速地发展，在2007年初已拥有近60万用户，并且用户数量仍在大量增长。

虽然IPTV发展非常迅速，但是业界对IPTV的标准和规范并没有达成统一，特别是在用户的管理、认证、授权、计费等功能上，IPTV的设备提供商(如中兴、UT、阿尔卡特)都各有一套管理系统，而像中央电视台这样的广电部门同样有着自己的管理系统，再加上电信部门对宽带接入等业务的管理系统，导致系统存在兼容困难和管理冲突问题，因此，亟需设计一个统一的AAA服务器解决上述问题。

2 AAA与Diameter协议

AAA技术是Authentication(认证)、Authorization(授权)、Accounting(计费)的整合。自网络诞生以来，认证、授权以及计费体制(AAA)就成为了运营的基础。网络中各类资源的使用需要由认证、授权和计费进行管理。而AAA的发展与变迁始终吸引着运营商的目光。对于一个商业系统来说，认证很重要，只有确认了用户的身份，才能知道所提供的服务应该向谁收费，同时也能防止非法用户(黑客)对网络进行破坏。在确认用户身份后，系统根据用户开户时所申请的服务类别，授予客户相应的权限。在用户使用系统资源时，需要相应的设备统计用户对资源的占用情况，据此向客户收取相应的费用。

Diameter协议是IETF为下一代AAA服务器提出的一套协议系统[1]，主要由基础协议、传输协议和一系列应用扩展组成。其基本协议定义了在各种应用中相同的功能，为各种认证、授权和计费业务提供安全、可靠、易于扩展的框架，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。应用协议则充分利用了基础协议提供的消息传送机制，定义应用协议的应用标识、参与通信的网络功能实体、相互通信的功能实体间的消息内容以及协议过程，这样就可以完全依赖Diameter基础协议完成特定的挤入和应用业务。

3 IPTV及其层次结构

3.1 IPTV的介绍

IPTV即交互式网络电视，是一种利用宽带有线电视网，集互联网、多媒体、通信等多种技术于一体，向家庭用户提供包括数字电视在内的多种交互式服务的新技术[2]。用户在家中可以有2种方式享受IPTV服务：(1)计算机；(2)网络机顶盒+普通电视机。IPTV既不同于传统的有线电视，也不同于经典的数字电视。有线和数字电视都具有频分制、定时、单向广播等特点，尽管数字电视相对于模拟电视有许多技术革新，但只是信号形式的改变，没有触及媒体内容的传播方式。因此，IPTV能够很好地适应当今网络飞速发展的趋势，从而充分有效地利用网络资源。

3.2 IPTV系统的层次结构

在垂直控制功能方面，一个典型的IPTV系统的层次结构如图1所示，主要包括运营支撑层、业务层、网络承载层和终端层[3]。

作者简介：叶 赛(1982－)，男，硕士研究生，主研方向：数据库，计算机网络；张洪伟，教授、博士后

收稿日期：2007-09-20 **E-mail：**phenix.ye@hotmail.com

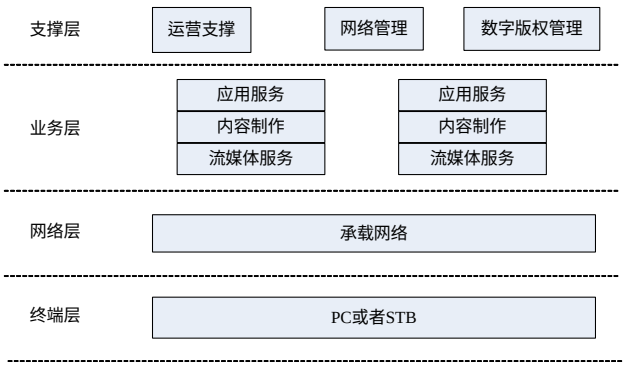

图 1　IPTV 系统的层次结构

(1)支撑层主要完成 IPTV 用户的管理、认证、授权以及系统设备的管理。而 AAA 服务器就是支撑层中运营支撑的一部分，它下接各个不同终端厂商的 STB，上连各个不同的 IPTV 业务平台，在整个 IPTV 系统中起着纽带的作用。

(2)业务层主要是为 IPTV 提供各种多媒体交互业务，如视频点播业务、体育直播业务。

(3)网络承载层主要是 IPTV 的物理介质，要求带宽比较大，最好支持组播，并具有一定的安全保护措施。可以分为接入网、汇聚网和核心网 3 个部分。

(4)最下层的终端层表示 IPTV 的最终用户，他们通过网络承载层进行不同方式的网络接入服务，并通过 PC 或者机顶盒观看电视节目。

4　AAA 服务器的设计

AAA 服务器软件系统按层次结构进行设计。系统包括主程序模块、通信层、应用逻辑处理层和数据访问层。系统的运行平台为 Solaris，在机器启动后利用 shell 拉起主程序。

系统的数据结构分为数据库结构和系统配置文件。数据库主要包括以下的数据表：

(1)mediaprofile 表，存放用户信息，包括用户的 STB 相关信息，用户的能力级以及用户的 SP 提供商等信息；

(2)mediashelfprogram 表，存放媒资信息；

(3)account 表，存放账户信息，包括费率策略、余额等；

(4)cdr 表，用于存放购买 mediashelf 时的计费信息；

(5)其他一些相关的业务逻辑表。

系统配置文件为 XML 格式，其中，install.xml 为系统的安装配置信息；dictionary.xml 提供一个系统所支持的 Diameter 消息和 AVP 的字典；subsystem.xml 包含系统内所有主机的通信信息；cacheindomain.xml 包含服务器中 cache 的配置。

4.1　主程序和通信层

主程序模块主要完成 3 个任务：

(1)读取服务器运行的配置，包括与数据库的连接、从数据库和系统配置文件中加载初始化信息到内存中；

(2)加载日志记录模块；

(3)创建各个子层所需要的线程，包括通信子线程、消息预处理子线程、多个应用处理子线程。程序中采用线程池，以减少线程创建和删除对系统资源的消耗。

通信层要求建立 TCP 的连接，进行消息的接收和发送。机顶盒向 AAA 服务器客户机的 NAS 发送消息，由 NAS 处理后发送到 AAA 服务器的消息接收队列中。当 AAA 服务器处理完这个消息请求后，会把回应消息发给 NAS，再由 NAS 发送给 STB。

4.2　协议层

本层使用 Diameter 协议，主要有组合、解析、校验和处理协议消息等功能。当 NAS 收到 STB 的消息后，会对 STB 发来的用户数据进行处理，然后把这些用户数据封装到 Diameter 消息的 AVP 中发给 AAA 服务器，服务器返回应答给 NAS，由 NAS 解开应答消息并发送给 STB。

4.3　应用逻辑处理层

本层根据业务的需要，对接收到的消息作相应的处理，如用户认证、授权、计费[4]。由于本层对应的应用各不相同，逻辑关系异常复杂，同时各个应用会随着需求的变更不断进行调整，因此为了降低程序的耦合度及日后的维护难度，本层采用模块化设计方式，做到“一个应用一个模块”，一个应用内的业务更改，只对该模块有影响，而不会对其他的模块产生影响。

4.3.1　认证模块的设计

STB 的认证流程如图 2 所示。

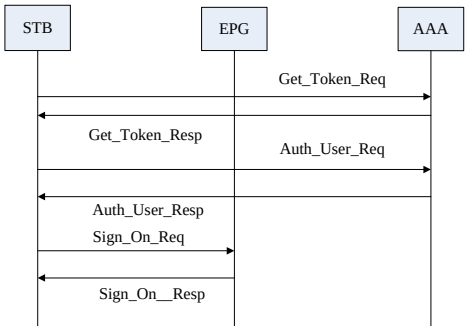

图 2　STB 的认证流程

具体过程如下：

STB 第 1 次向 AAA 服务器发起 Get_Token_Req 请求，请求中包含 STB 的 16 位 SignonID 以及它的 IP 地址，之后 AAA 服务器先判断 STB 的 IP 是否在所管辖的子网内，如果是，继续判断 SignonID 在 AAA 服务器中是否存在(用户到电信运营商申请 IPTV 后，会得到一个 SIM 卡，里面有一个用户标识(SignonID)和对应的用户密码(PASSWORD)[5])，如果存在，AAA 服务器会根据 SignonID 和当前时间戳进行计算，产生一些 168 位的 Token，并通过 Get_Token_Resp 消息把 Token 下发给 STB，否则，AAA 服务器拒绝 STB 的请求。Token 会定期改变，当 STB 发现 AAA 服务器返回的 Token 过期后，会重新向 AAA 发起 Get_Token_Req。

之后，STB 使用这个 Token 作为密钥，将 STBID, MAC, IP, PASSWORD 等消息进行加密(上述消息的定义参照中国电信《IPTV 机顶盒设备技术规范》)，加密算法为 3DES。然后发送 Auth_User_Req 消息发送给 AAA 服务器，AAA 服务器查到这个 STB 对应的 Token 后，以它作为密钥解开消息，并对解开后得到的 PASSWORD 与数据库内 SignonID 对应的 PASSWORD 进行比较，如果两者一致，则通过验证，发送 Auth_User_Resp 消息给 STB，返回码为 0，表示认证成功；如果是用户首次开机，AAA 服务器会将 STBID 等信息与 SignonID 绑定，并且以后发给 STB 的消息都以对应的 Token 进行加密。而 STB 会将自己的 Token 记录在 flash 内，用于以后与 AAA 服务器及 IPTV 其他业务平台的通信。

在 AAA 服务器返回给 STB 认证成功后，STB 会向 IPTV 业务平台的电子节目导航(EPG)发起 SignOn 请求，进行 IPTV 业务的使用。

4.3.2　授权模块的设计

用户可以通过 STB 在 EPG 上选择 IPTV 业务，如直播、点播、回看、即时时移。当用户确定要观看的业务时，EPG 会向 AAA 服务器发起 Set_Entitlement_Req 请求，AAA 服务器会根据该用户的权限判断其是否可以使用这个业务，如果用户的权限符合要求，返回 Set_Entitlement_Resp 消息给 EPG，返回码为 0，表示授权成功，用户可以使用该业务；否则，返回码为-1，EPG 将拒绝用户的请求。

IPTV 的业务鉴权流程如图 3 所示。

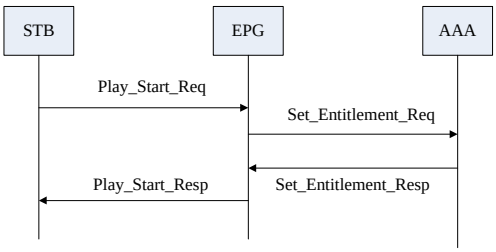

图 3　IPTV 的业务鉴权流程

4.3.3　计费模块的设计

当用户通过 STB 在 EPG 上选择的 IPTV 业务属于付费业务时，EPG 会向 AAA 服务器发起 Account_Req 请求，AAA 服务器根据这个消息的内容知道定购的业务是预付费还是后付费，如果是预付费，先判断用户的账户余额，如果余额大于该业务的费用，返回 Account_Resp 给 EPG，返回码为 0，用户可以使用该业务；否则，返回码为-1，拒绝该用户的行为；如果是后付费，会产生定购的账单 CDR，并返回给用户成功。

IPTV 的计费流程如图 4 所示。

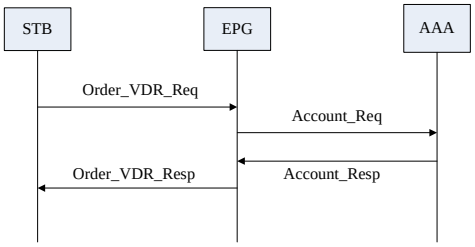

图 4　IPTV 的计费流程

4.4　数据访问层

为了提高数据的访问速度、减少数据库的开销，在数据库与应用之间需要有一个高速缓存区，其模型如图 5 所示。

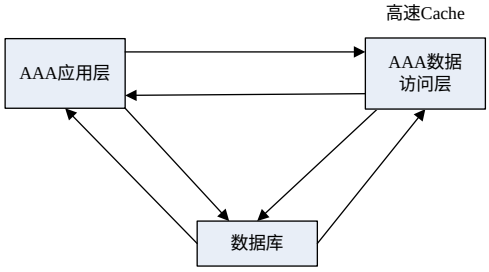

图 5　高速缓存区模型

当 AAA 服务器启动后，高速缓存区会自动加载数据库数据。当应用需要对数据进行查找、删除、修改时，直接在高速缓存区进行操作，之后高速缓存区同步到数据库中。为了处理特殊应用，比如需要实时更新数据库，系统保留了直接访问数据库的接口，但是非特殊情况下，所有的数据操作都在高速缓存区内进行。

5　AAA 服务器的仿真测试

测试环境如下：

(1)1 台 DB Server：操作系统为 Solaris 8，CPU 为 Generic_117000-05 Sun4u Sparc×4，内存 8 GB，数据库为 Oracle9.2.0；

(2)1 台 AAA Server：操作系统为 Solaris 8，CPU 为 Generic_117000-05 Sun4u Sparc×2，内存 4 GB，数据库为 Oracle9.2.0；

(3)1 台 Simulator Server：操作系统为 Solaris 8，CPU 为 Generic_117000-05 Sun4u Sparc×2，内存 4 GB，数据库为 Oracle9.2.0，其中，Simulator 模拟盒子向 AAA Server 发送消息。

AAA 服务器中的用户数大于 100 万，性能测试结果如下：

测试项目描述	测试典型流程	实测指标/(消息数/s)	CPU 使用率/(%)
Get_Token_Req 流程		400	1.5
Auth_User_Req 流程		400	2.0
Set_Entitlement_Req 流程		1 000	2.7
Account_Resp 流程		800	2.9
混合流程(根据统计模型估计 N 个用户的前提下计算 1 s 能产生的每一种类的请求分别有多少)	根据统计模型进行混合测试： (1)Get_Token_Req (15%) (2)Auth_User_Req (15%) (3)Set_Entitlement_Req (30%) (4)Account_Resp (40%)	500	4.9

从模拟测试可以看出，设计的 AAA 服务器可以上接不同平台厂商的 IPTV 业务系统，下接各个终端厂商的 STB，并且能够在百万级用户的情况下，正常承载 IPTV 业务的认证、鉴权和计费工作，从而证明了统一的 AAA 服务器在 IPTV 系统中的可行性。随着 IPTV 的规范和标准的进一步细化，统一 AAA 服务器将逐渐成为市场的主流。

6　结束语

AAA 技术是商用化网络服务的基础，是提高网络服务质量的重要数据来源。本文设计了一种基于 IPTV 的统一 AAA 服务器，随着 IPTV 的发展，这种服务器的功能仍然需要完善，比如现有的标准都是使用专门的 DRM 对节目版权进行认证，以后的 AAA 服务器完全有必要把 DRM 纳入自己的鉴权体系；同时，IPTV 用户量的增加也会对 AAA 服务器的高速缓存带来极大的挑战，所以，未来 AAA 服务器的高速缓存可能会向着分布式、P2P 等领域发展，给用户提供更快更好的服务。

参考文献

[1] IETF AAA Working Group. Diameter Base Protocol[S]. RFC 3588, 2003.

[2] 蔡庆君, 田　辉. IPTV 承载技术探讨[J]. 电信网技术, 2006, (2): 11-14.

[3] 谭淑慧. 中兴通信 IPTV 解决方案[J]. 广西通信技术, 2005, (4): 27-30.

[4] 李　军, 张瀚文, 叶新铭. 面向 WLAN 的移动 IPv6 AAA 系统研究与实现[J]. 计算机应用, 2006, 26(6): 1263-1266.

[5] 中国电信. IPTV 终端设备技术规范[Z]. 2005-08.