论文分类号 TP393　　单 位 代 码 10183
密　　级　　研究生学号 2002532174

吉 林 大 学

硕 士 学 位 论 文

基于Diameter协议的移动IPv6应用扩展的研究与实现

Research and Implementation of Mobile IPv6 Application Extension Based on Diameter protocol

作者姓名　　李晓东
学科专业　　计算机应用技术
导师姓名　　魏达
及 职 称　　副教授

学位类别　　工学硕士
论文起止年月： 2004 年 3 月至 2005 年 3 月

吉林大学硕士学位论文原创性声明

本人郑重声明：所呈交学位论文，是本人在指导教师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：李晓东

日期：　2005 年 3 月 15 日

作者姓名	李晓东	论文分类号	TP393
保密级别		研究生学号	2002532174
学位类别	工学硕士	授予学位单位	吉 林 大 学
专业名称	计算机应用技术	培养单位（院、所、中心）	计算机科学与技术学院
研究方向	计算机网络通信与安全	学习时间	2002 年 9 月至 2005 年 7 月
论文中文题目	基于 Diameter 协议的移动 IPv6 应用扩展的研究与实现		
论文英文题目	**Research and Implementation of Mobile IPv6 Application Extension Based on Diameter protocol**		
关键词(3-8个)	**AAA Diameter 移动 IPv6 PANA OpenDiameter**		

导师情况	姓名	魏达	职称	副教授
	学历学位	硕士	工作单位	吉林大学计算机科学与技术学院

论文提交日期	2005年4月25日	答辩日期	2005 年 6 月 日
是否基金资助项目	否	基金类别及编号	

如已经出版，请填写以下内容

出版地（城市名、省名）		出版者（机构）名称	
出版日期		出版者地址（包括邮编）	

提　要

自网络诞生以来，认证（Authentication）、授权（Authorization）以及计费（Accounting）体制（AAA）就成为其运营的基础。网络中各类资源的使用，需要由认证、授权和计费进行管理。

本文首先分析了由于以全 IP 网络为基础的下一代网络 NGN 的发展以及 ‘三网’融合的演进过程中，作为 NGN 业务和应用层协议组成部分的 AAA 协议的发展。然后介绍移动 IP 技术的发展，并重点讨论移动 IPv6 环境下的面临的认证、授权、记费问题。

其次，介绍 Diameter 基础协议及其应用协议扩展如 NASREQ、MIPv4 应用扩展，并在此基础上结合 PANA 协议提出移动 IPv6 应用扩展框架模型及协议细节。

第三，在 OpenDiameter 开源软件包的基础上完成移动 IPv6 应用扩展的概要设计和详细设计，并根据设计写出一组 API，做为 OpenDiameter 开源软件包类库的组成部分。

最后，利用已经完成的 API，分别模拟实现 AAA 服务器端、AAA 客户端、移动节点上 AAA 软件，组建网络测试移动 IPv6 节点在移动过程中的 AAA 过程，并给出实验过程。

关键词：AAA , Diameter 移动 IPv6, PANA EAP, OpenDiameter

目　录

第一章　引言

1.1 研究背景

随着网络的发展以及业务的要求，电话网、计算机网、有线电视网也趋于融合，网络面临的负荷在不断增大，业务需求也趋于多样化，信息产业面临着巨大的挑战。因此，在客观上要求提供内容更加丰富高效的信息网络、提供多种多样的网络接入技术、提供种类繁多的应用业务，促使各种网络互联互通，从而逐渐融合成为一种前所未有的网络系统——下一代网络 NGN。

下一代网络 NGN 应该是一种可以提供数据、语音、多媒体等各种业务的综合开放的网络架构，它应该具有三大特征：1、采用开放的网络架构；2、以业务为驱动，业务与呼叫控制分离，呼叫与承载分离；3、应该是基于统一协议的分组网络[1]。以 IP 技术为核心的 IP 网络，以其灵活多样的接入方式和低成本的易于扩展的应用业务，成为网络融合的主导力量。但是各种接入业务和各类应用业务，在各自的发展过程中形成了不同的业务认证、授权以及计费体制。如何整合各类业务的 AAA（Authentication、Authorization、Accounting）过程是所有运营商在部署或升级网络前需要面对的现实问题。互联网最早的几种 AAA 技术，如 TACACS(Terminal Access Controller Access Control System) 、RADIUS(Remote Authentication Dial In User Service)等已被广泛使用，但网络融合过程以及各种新业务生产，使得基于原有 AAA 技术的路由器和网络接入服务器难以应对。

因此，基于 IP 技术的 AAA 的新框架结构便应运而生。1998 年 12 月，IETF（国际互联网工程特别工作组）在第 43 次会议上成立了 AAA 工作组，着手 AAA 相关标准的研究。到目前，经过多年的发展，AAA 的新框架结构 Diameter 技术已经成型，AAA 向 Diameter 演进的号角已经吹响。

由于人类生活节奏的加快以及信息化技术的发展，人们需要在任何时间、任何地点都可以接入网络，这使得提供移动性接入成为当前的技术研究热点。移动 IP 是在原有的 IP 协议基础上提出的移动性支持方案，它提供了在漫游环境下的网络无缝接入并对上层协议是透明的。与此同时，由于 IPv4(Internet Protocol version 4)设计上的缺陷，在 Internet 迅猛发展的今天，IPv4 的地址资源不足、路由性能不佳、安全机制匮乏、网络配置困难等问题难以适应网络发展的要求。虽然有 NAT 等替代方案，

但都不能完整解决 IPv4 本身所具有的痼疾。20 世纪 90 年代初，IETF 就已经开始探讨下一代网络协议，最终 IPv6(Internet Protocol version 6)得到广泛认同，被 IETF 选为下一代互联网络协议。IPv6 不但提供了长达 128 位的地址空间，也提供相对完整安全机制。由于 IPv6 的分组报头是固定的 40 个字节，所以大大减少了路由器处理的负担。同时，IPv6 的有状态自动配置和无状态自动配置也简化和加速了网络的配置过程。因此，移动 IPv6 的研究得到广泛的关注，很多国际标准正在逐步形成。

2003 年 11 月，信息产业部在第 2 次中国互联网大会上宣布，将着手实施名为“中国下一代互联网示范工程”(CNGI：China Next Generation Internet)的新一代互联网计划。按计划，中国将在 2005 年底以前投资 14 亿元构建连接中国各主要城市的 IPv6 商用骨干网，2006 年正式开始 IPv6 商用服务，届时将形成全球最大规模的 IPv6 商用网。同时 3G 网络正逐步向全 IP 网络演进，不仅在核心网络使用支持 IP 的网络实体，在接入网络也使用基于 IP 的技术，而且移动终端也成为可激活的 IP 客户端。基于 IP 的无线接入网络可以集合众多的无线接入网技术，包括 2G、3G、WLAN 等，为各种网络的融合提供了一条途径；由于 IP 技术更开放，全 IP 网络就提供了一个开放的应用平台，能更快地创建和支持新业务。

在这样的网络中，移动 IP 将被广泛使用。支持移动 IP 的终端可以在注册的家乡网络中移动，或漫游到其他运营商的网络。当终端要接入到网络，并使用运营商提供的各项业务时，就需要严格的 AAA 过程。AAA 服务器要对移动终端进行认证，授权允许用户使用的业务，并收集用户使用资源的情况，以产生计费信息。

由于未来的全 IP 网络中将采用 IPv6 协议，所以 Diameter 移动 IP v6 应用将会广泛地使用到需要对移动终端进行认证、授权和计费的场合。因此，针对下一代 AAA 协议中 IETF 的标准协议 Diameter 协议的移动 IPv6 扩展的研究有一定的实用价值和理论价值，拥有广阔的应用前景。

1.2 研究现状

目前，国际上 IPv6 标准日趋成熟，中国作为一个互联网和移动通信技术及市场快速发展的国家，在标准制定上与国际接轨已经是一项十分迫切的任务。IETF 是 IPv6 标准的制定工作的主体，在近期这种状况不会改变，但是鉴于 IPv6 的重要性和对下一代网络的巨大影响，越来越多的国际标准化组织加入 IPv6 标准的制定工作。特别是 3GPP，从传统意义上来说，互联网和移动通信是两个不同的行业。但随着 IP 技术的发展，这两个行业的共同点越来越多，尤其是第三代移动通信‘全 IP’

解决方案的提出，IPv6 成为互联网和移动通信网的公用基本协议。尽管 IPv6 标准发源于互联网行业，而从商业意义上来说移动通信行业可能是最早和最大的受益方之一。国际标准化组织，除了 IETF 继续完善于 IPv6 有关的标准以外，3GPP 和 ITU-T 也成立了相应的工作组来制定与 IPv6 相关的标准。最近 IETF 和 3GPP 联合组成了一个工作组来协调 IPv6 标准在第三代通信系统中的应用。ITU-T 是政府间的国际标准组织，也是传统国际电信标准的归口单位。目前 ITU-T 与 IETF 已经在 IP 标准领域开展合作。ITU-T 专门设有一个 IP 标准计划，IPv6 有关的标准也列在其中。

到目前为止，移动 IPv6 的标准仍在制订的过程中，并经历了多次版本更新。最新的标准文档《Mobility Support in IPv6 （RFC3775）》和《Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents（RFC3776）》中详细的说明了对移动 IPv6 的支持以及相关安全措施。世界上有很多组织或者机构在对移动 IPv6 进行研究，并且已有了一些在不同操作系统上开发出来的实验系统。例如 Windows 下的 Microsoft MIPv6 Project (MIPv6) 实验系统，Free BSD 下的 CMU Monarch Project，KAME Project 实验系统，以及 Linux 下的 Lancaster 移动 IPv6，USAGI ，MIPL 移动 IPv6 实验系统等等。

IETF 在 1998 年 12 月成立了 AAA 工作组，着手下一代 AAA 协议的研究开发，很快 4 个协议方案 SNMP(Simple Network Management Protocol)、RADIUS+、DIAMETER 和 COPS(Common Open Policy Service) 被提出。2001 年 6 月，IETF 的 AAA 工作组同意将 Diameter 协议为下一代的 AAA 协议标准。

Diameter 协议首先经 Sun 公司提出后，受到了业界的广泛支持。它在设计过程中，不仅保持了与广为使用的 RADIUS 协议的兼容，更克服了 RADIUS 协议的许多不足，而且它不仅仅被互联网采用，更被下一代移动通信网（3G）采用[2]。该协议族包括 Diameter 基础协议和应用协议。目前已经提出了《Diameter Base Protocol (RFC 3588)》标准文档，作为 Diameter 基础协议的应用协议扩展，目前 IETF 已经制定了 NASREQ（Network Access Server Requirements 网络访问服务要求）应用扩展、移动 IPv4 应用扩展等辅助协议，但还没有制定基于 Diameter 的移动 IPv6 扩展协议。

目前对 Diameter 协议族的实现做的较完善的开发计划是 OpenDiameter 开源软件包，目前最高版本是 1.0.7e 版，其中实现了基础协议及 EAP（Extensible Authentication Protocol）和 PANA（Protocol for carrying Authentication for Network Access）协议。由 Andrei Pelinescu、Cristian Constantin 等人开发的 DISC（Diameter Server Client）软件包，

也提供了最基础的 Diameter API 函数调用。华南理工大学与诺基亚互联网联合实验室在“MIPv6 Service Management System”中对 Diameter 协议的应用做出了有益的尝试，在该项目中借鉴了 SUN 公司提供的 Diameter API 函数和 Intel 公司的 COPS Client API 函数将 Diameter 和 COPS 协议结合起来，完成了移动 IPv6 节点的认证过程的基本消息传送。该协议族还没有大规模的商用，目前 AAA 服务器的主流还是基于 RADIUS 协议的，但随着网络业务类型的日益多样化，基于 Diameter 协议的 AAA 服务器必然取代 RADIUS 协议的统治地位，成为对各种网络服务提供认证、授权、记费的基础。

1.3 本文的主要工作

本文的主要工作是给出基于 Diameter 协议的移动 IPv6 应用扩展的设计与实现。因此结合 PANA 协议完成移动节点同 AAA Client 之间的通信。

本文将首先讨论 AAA 协议和移动 IPv6，然后详细分析 Diameter 基础协议，并给出 Diameter 协议 MIPv6 应用扩展的协议细节，包括本地 AAA 服务器和外地 AAA 服务器之间的通信、AAA 服务器与 AAA Client 之间的通信、移动节点同 AAA Client 之间的通信等。最后，根据该协议并结合 OpenDiameter 开源软件包，完整的给出移动节点在漫游过程中的认证、授权、记费功能模块及实验结果。

1.4 本文的组织结构

第二章介绍 AAA 协议的相关内容。主要包括 AAA 协议的评估准则、传输要求、URI 框架以及几种常见的 AAA 协议的基本情况。

第三章介绍移动 IPv6 相关内容。深入探讨了 IPv6、移动 IPv6 的报文、寻址与安全等内容。同时与 IPv4、移动 IPv4 做了比较。

第四章深入研究 Diameter 协议族，对 Diameter 基础协议进行透彻分析，同时介绍 NASREQ 应用扩展、EAP 应用扩展，最后重点讨论 PANA 协议在 Diameter 中的应用。

第五章结合上述讨论给出 Diameter MIPv6 应用扩展框架设计。详细的给出消息定义、传输过程、以及各网络实体的基本操作，并在此基础上进一步给出增强功能设计。

第六章根据给出的 Diameter MIPv6 应用扩展框架设计，结合 OpenDiameter 开源软件包，设计 MIPv6 应用扩展模块并给出 API。

第七章利用第六章给出的 API，在 WINDOWS 环境下，实现一个

基本的移动 IPv6 节点的移动过程，以测试所给出 API 的正确性并给出结果。最后总结经验与不足，并展望 Diameter 协议的未来。

第二章　AAA 协议

2.1　AAA 协议的概念

自网络诞生以来，认证（Authentication）、授权（Authorization）以及计费（Accounting）体制（AAA）就成为其运营的基础。网络中各类资源的使用，需要由认证、授权和计费进行管理。

认证要解决的不但是用户身份问题，而且需要对网络进行认证，这是一个双向的认证过程。对用户所宣称的身份进行验证，并且记录该用户的一些属性，比如角色、安全标识、组成员信息等。用户可以用“用户名/密码”、数字证书来宣称身份。

授权解决的是用户可以执行哪些操作和获得哪些服务，根据认证的结果，用户请求的服务以及当前系统的状态决定可以为用户提供的特定权限的服务。

记账用于记录用户进行的操作、使用的资源，以便进行分析、审计和计费[3]。记账管理要求对资源使用情况进行度量、定价，并且通告给使用者。典型的记账信息包括用户标识、服务类型、服务起始和结束时间。

认证、授权和记费简称为 AAA。

2.2　AAA 协议评估准则

2001 年六月，IETF 的 AAA 工作组在 2000 制定的标准文档《Network Access AAA Evaluation Criteria (RFC2988）》的基础上进一步制定了标准文档《Authentication, Authorization, and Accounting Protocol Evaluation(RFC3127)》,该文档从一般需求、认证需求、授权需求、记费需求、移动 IP 需求五个方面对 SNMP、Radius++、Diameter、COPS 这些 AAA 协议进行了全面的评估，并最终认为 Diameter 协议更加符合 AAA 要求，成为支撑 AAA 协议的最佳选择[4]。

2.2.1　一般需求

1、AAA 协议应能支持百万数量级的用户和上万的并发请求。AAA 框架和协议必需有能力支持数量上万的设备、AAA 服务器、代理。

2、当同一个给定服务器的通信发生错误的时候，协议需提供一种机制可以将服务从一台服务器切换到做备份用的另一台服务器上。

3、AAA 的相互认证：要求支持 AAA 客户和服务器之间相互认证。即不但 AAA 服务器可以认证 AAA 客户身份是否合法，AAA 客户也可以认证 AAA 服务器的合法性。

4、AAA 协议需认证、完整性保护和传输层的机密性，安全模式指的是逐跳的安全和两个通信对等端建立的任何安全。当 AAA 消息由一个可以接收的 AAA 实体处理时，这些安全机制可以不使用。同样，当下层应用了其它安全服务协议（如：IPSec），AAA 协议本身的安全机制可以不需要。

5、当数据对象由一个或多个属性组成的时候，这就意味着只有数据最终到达的 AAA 目标实体可以对数据解密，而不管实际上数据会穿越一个或多个 AAA 中间实体。

6、对象级认证应能稳定穿越一个或多个 AAA 中间实体，在一个代理链上任何 AAA 实体可以校验认证。就是说由对象层次的安全所隐蔽的数据不能被中间服务器修改。

7、AAA 协议必须能够传递证书，这种要求是做为一种优化手段来考虑，用以替代过去习惯使用的带外(out-of-band)协议取得证书。

8、可靠的 AAA 传输机制：指的是对丢失包的恢复机制，它包括逐跳重传和失败恢复；由 AAA 控制的重传机制；由一个成功发送的传输来承认，有别于语义学和语法的评价；AAA 消息中的贪心回退的确认；AAA 相应的即使传送。

9、支持代理和路由 broker：Broker 可以在向前的路径之上做为传输代理，也可以做为外路上的中间认证人。

10、审核能力：当报文从家乡 HA 到网络服务之后返回这个过程中，审核的处理能对 AAA 报文执行行为进行决策处理。

11、特别服务属性：AAA 协议可由第三方扩展（其它 IETF 工作组），简单的需求可以允许类似 AAA WG 这样的其它组织按照特定要求对标准属性进行扩展定义。

2.2.2 认证需求

1、AAA 协议必须允许使用 NAI（Network Access Identifier）来标识用户或设备。

2、AAA 协议必须支持 CHAP（Challenge-Handshake Authentication Protocol）信息的传输，CHAP 信息主要是在网络访问服务器上用来对远程拨入的 PPP（Peer-Peer Protocol）用户进行认证。

3、AAA 协议必须支持 EAP（Extensible Authentication Protocol）扩展认证数据负载的传输，EAP 协议在认证过程中可能进行多次信息传

输， AAA 协议必须有相关机制完成这些信息的传输。

4、虽然 PAP 密钥认证协议由于密钥的明文传送已经被建议不要使用，但它仍然在很大范围里得到应用。因此，AAA 协议必须提供对明文密钥的安全传输能力，这种安全传输能力包括：线上安全和在传输路径网络中对代理保密。

5、AAA 协议必须提供重新认证机制，并且这些认证可以由任意一方发起，也就是说可以由 AAA 客户端发起也可以由家乡或被访问网络的 AAA 服务器发起。

2.2.3 授权需求

1、当用户或设备接入的时候，AAA 协议必须支持动态或静态的 IP 地址分配，并且应该对 IPv4 和 IPv6 提供全面的支持。所谓静态是指，AAA 客户端和服务器端都知道一个提前配置的地址。

2、做为一个新的 AAA 协议，应该具有同原有已经广泛部署的 AAA 协议（如：RADIUS）的向下兼容性，两种协议之间应该能够进行会话或通过某种机制相互翻译。同时，根据对代理的能力要求，要求 AAA 协议也具有相似的功能。

3、根据 AAA Client 和 AAA Server 的要求，应该具有重新授权功能。这种授权也可以规定一个时间段，例如，AAA 服务器可以在最初的时候授权用户使用某种服务，但一段时间后也可决定不再提供相应服务。重新授权并不要求必须重新认证。同时要求 NAS（Network Access Server）有能力根据授权策略断开某个会话。

4、AAA 协议的授权要求应该具有某种访问操作的限制性行为，如会话终止、空闲超时设定、包过滤、静态路由、QOS（Quality Of Service）参数等。同时 AAA 服务器还应该具有某些资源管理功能，用以辅助完成用户并发登录时的控制、端口的使用限制或 IP 地址池等功能。

5、AAA 协议要求设计相应的机制来恢复丢失或受损的数据，如 AAA 服务器或 NAS 重启、NAS/AAA 之间通信时的损耗，但必须同记费流分离。

6、授权决定可能对上下文敏感，AAA 协议必须允许这种决定。AAA 协议需要支持那种依赖于（甚至可能仅仅依赖于）系统现有状态的授权。例如，只允许七个会话，那么第七个决定依赖于现存的六个会话。因为上下文可能包括多个服务，AAA 协议很可能必须提供某些支持。AAA 协议应当既支持事务授权，也支持会话连续授权。这说明 AAA 实体必须保留状态和行为，状态指示出发生了什么情况[5]。

2.2.4 记费需求

一个新的 AAA 协议应该满足如下记费方面的需求[3]：

1、实时记费的要求。2、强制性的压缩编码。3、记费记录的可扩展性。4、允许记费过程成批处理。5、保证传输的完成。6、应该支持记费时间戳，用来记录登录、登出、认证、授权、临时记费信息等内容。7、支持动态记费，提供动态的认证、授权过程。

2.2.5 移动 IP 的特殊需求

新的 AAA 协议应该提供对移动 IP 的支持，移动 IP 的 AAA 过程除了满足上述要求之外，还应该满足下列需求：

1、必须支持移动 IP 注册消息的编码、译码过程。移动 IP 是建立在 IP 协议基础之上，并对报文进行修改得到的。AAA 协议必须能够认识这些报文，并根据报文内容进行相应的处理。

2、AAA 协议必须是防火墙友好的[6]。所谓防火墙友好的协议，是指将防火墙作为一个代理处理，AAA 协议的正常报文可以自由穿透防火墙。例如，一个家乡代理 AAA 服务器可以位于防火墙之后并能够协同移动 IP 的外地代理提供 AAA 服务。

3、本地家乡代理的分配。由于移动节点在移动的过程中，家乡网络的配置有可能发生变化，如家乡代理的地址的改变，因此，要求 AAA 协议能够提供家乡代理的动态分配过程。

2.3 AAA 协议传输框架要求

由于 AAA 协议关系到服务商提供服务的方方面面，因此，AAA 消息的传输也有着特殊的要求。IETF 的 AAA 工作组已经制定出了 RFC3539，提出了关于 AAA 协议消息传输方面的经验性建议和相关讨论。

1、传输协议要求。AAA 服务器和 AAA 代理要求必须支持 TCP 协议和 SCTP（Stream Control Transmission Protocol）协议。AAA 客户端应该支持 SCTP，但必须支持 TCP，随着网络的发展，对 SCTP 支持的要求会越来越高。

2、AAA 协议的传输要求通常都是业务驱动而不是网络驱动的。这就意味着 AAA 消息的发送的速率更多的应该是按业务发生的速率来决定而不是由网络拥塞窗口的大小来决定的[7]。虽然如此，在某些情况下也会根据网络的情况决定，例如，当 NAS 重启的时候，大量的先前缓存的记费数据会连续的快速的发送给记费服务器。相似的，当 NAS 从

某种严重的错误中恢复之后，将有大量的用户同时发出登录请求。在这两种情况下，消息的产生速率都有可能超过网络能够传送的速率，因此，需要有队列机制来保证消息的完整传送。

3、拥塞控制。由于拥塞的存在，当 AAA 协议运行在 TCP 协议基础上的时候一定要允许 Nagle 算法的使用，而基于 SCTP 协议的时候则不需要使用。Nagle 算法通过暂缓发送的方法，解决了小包发送问题[8]，从而控制网络的拥塞。同时，一些其他拥塞控制方面的手段也应该被应用在内，如利用拥塞窗口确认、RTO（Retransmission Timeout）重传超时确认等手段。

4、多重连接。在 AAA 客户端和 AAA 代理、服务器之间应该只用一条永久连接，并且应该能提供流水线操作以处理多条请求。同时，AAA 客户端、代理也可能同其他 AAA 代理、服务保护多重连接，这种连接可以被作为备份连接使用或者用作负载平衡。在移动环境中，为了最小化连接的使用，AAA 实体可以中断在一定时间间隔不使用的连接。

5、应用层的监控。为了使 AAA 协议更快的检测到传输和应用错误，AAA 协议应该支持应用层的监控消息。这种机制可以提供一种应用层的错误发现和错误恢复功能。这种监控功能工作在所有打开的连接上，可以允许 AAA 客户端和代理自己决定何时重发数据或使用其他连接，同时，也可以决定一个连接的状态。如遇到错误的时候挂起或关闭、恢复功能时间打开等。

6、主、从式错误恢复和连接的负载平衡。应用层的监控将与主、从式错误恢复机制共同提供一种更可靠的传输和基本的负载平衡。

7、重复检测。应该有多种机制进行重复检测，如会话 ID、端到端和逐跳消息标识符。这三种方法相互配合，完成对消息的重复检测，以防止有相同的消息被服务器多次处理。

2.4 当前的 AAA 协议

认证、授权和计费是通信网络的基本功能之一，因此，AAA 服务器在电信行业有着广泛的应用，例如窄带 IP 网、宽带网、固网短信息、移动短信息等。随着电信业务集中化趋势的发展，电信行业出现了百万用户级以至千万用户级的系统，这对 AAA 系统的性能提出了很高的要求。AAA 做为一个已经成形的认证、授权和计费协议，在目前已有多种 AAA 的应用协议，RADIUS 和 TACACS+是目前应用最为广泛的主流 AAA 协议。COPS 和 DIAMETER 协议则是针对新的业务层要求提出的下一代 AAA 协议的代表，下面将对这些应用加以简单介绍。

2.4.1 RADIUS 协议概况

RADIUS 协议是 IETF 通过的 AAA 协议标准（RFC2865），它采用了基本的客户/服务器模式。网络接人服务器 NAS（Network Access Server）作为 Client 向 RADIUS 服务器提出认证请求，以实现对连接到 NAS 并请求接人服务的用户进行认证、授权和计费。用户的 AAA 消息由 Client 提供给 RADIUS 服务器，并且根据服务器的授权为用户提供相应权限的服务。RADIUS 服务器主要实现对用户的认证并向 Client 返回必要的配置信息。

User 与 RADIUS 服务器之间可以协商采用多种认证方法，当用户提供了用户名和原始密码后，RADIUS 服务器可以支持点对点的 PAP 认证（PPP PAP），点对点的 CHAP 认证（PPP CHAP），UNIX 的登录操作（UNIX Login）和其他认证，RADIUS 协议的可扩展性保证了这些认证方法的实现。RADIUS 协议通过属性（Attribute）域携带认证、授权以及详细的配置信息可以方便地扩展新的认证方法。RADIUS 协议通过代理服务器（Proxy）功能实现漫游。

RADIUS 服务器性能指标是与运行环境密切相关的。下面是从用户角度描述的 RADIUS 服务器性能指标[9]。

1、最大吞吐量。即系统每秒能接人的最大用户数量，或者说是每秒钟最多能够成功处理的有效服务请求包的数目。

2、平均响应时间。即从网络访问服务器 NAS 发出服务请求到服务器应答包的返回时延。

3、系统稳定性。即在服务请求繁忙时系统的稳定性

4、系统可靠性。测试系统能否对各种服务请求和异常做出正确的处理，包括计费的准确性。

5、系统可扩展性。因为 RADIUS 协议是一个开放的协议，在不与标准协议冲突的前提下，允许增强服务器服务功能和提高处理性能。

RADIUS 协议采取了如下措施以保证信息的安全传输[10]。

1、在 RADIUS Client 和 RADIUS Server 之间通过共享密钥(Shared Secret)建立信任，而此共享密钥从不在网上进行传播。

2、通过请求鉴别码(Request Authenticator)和应答鉴别码(Response Authenticator)字段，支持每个报文的完整性和认证。

3、对用户密码的加密。密码的传输过程中使用流加密机制。

2.4.2 TACACS 协议概况

TACACS 协议是 Cisco 公司的安全控制协议，对认证和授权处理提

供详细的记帐信息和灵活的管理控制。

TACACS 协议以 Client/Server 模式工作，它主要用于拨号入网用户的授权控制，在 Cisco 系列路由器中得到广泛应用。由于该协议中的认证功能及 Client/Server 模式，也用作分布式认证系统[11]。路由器作为 TACACS 客户，通过拨号线路接收到用户名和口令之后，发送请求到 TACACS 认证服务器，服务器根据保存的用户数据决定是否接受该请求并发送应答信息。

TACACS 对数据并不加密，因此它的安全性要差一些，针对这种情况，又设计了 TACACS+协议。它不仅为用户获得对 Router 或 NAS 的访问提供集中化认证，而且还采用 MD5 加密算法实现 NAS 和 TACACS 安全服务器之间的加密通信。

TACACS 协议提供了同 RADIUS 相似的功能，但两则也有所不同：

1、传输：RADIUS 采用 UDP 协议，而 TACACS+采用 TCP 协议。

2、加密：RADIUS 仅仅对用户口令部分进行加密传输，而其它部分是明文传输的，TACACS+对整个消息包进行加密。

3、认证和授权：在 RADIUS 中，认证和授权是结合在一起的，也就是说，在对用户进行认证的同时也就同时完成了授权，而在 TACACS+中认证和授权是两个分离的过程。

2.4.3 COPS 协议概况

COPS 协议是由 IETF 设计的，用来在策略服务器与策略客户之间交换策略信息。与以往的网络管理协议相比，COPS 协议可以对网络进行超前的、全局的管理。COPS 是一种通信机制，IETF 的特意将 COPS 协议设计成为可扩展的、通用性强的协议标准，不但可以有效地简化策略服务器与客户间的策略规则传输，而且可以很容易的扩展到其他领域的应用。基本的 COPS 协议具有以下特点：

1、COPS 协议工作在 C/S 模式。在此模式下，策略客户与策略服务器之间的策略交互以请求－决策－报告－修改－删除的方式进行。

2、COPS 使用可靠的 TCP 通信协议交互服务器与客户之间策略报文，因此不需要为 COPS 制定其他的通信机制。

3、COPS 协议被设计成具有良好的扩展性，它可以传输各种其他协议自定义对象，可以传输多种的客户特定信息，而无须改变协议本身。

4、COPS 协议提供了报文级的安全认证，可以进行安全认证、重发保护和维护报文的完整性。它也能使用像 IPSEC 或 TLS 等已有的安全机制来保证 PEP 和 PDP 间的认证和信道安全。

5、COPS 协议具有状态性。请求、决定状态被策略客户与服务器共

享，PEP 发出的策略请求被远端 PDP 存储，直到被 PEP 请求删除此状态。同时，对于已在 PDP 存储的请求状态，PDP 可以在任何时间异步地产生策略决定，修改原决定。

6、COPS 协议允许策略服务器对客户进行策略配置，而当原配置不再可用时，还可以将其从客户中删除，重新配置。

自 COPS 协议制定以来，COPS 协议及其应用处于不断发展之中，一方面表现为自身的完善，包括安全方面的增强，另一方面表现为与其它协议(如 RSVP,TLS 等)的配合。可以认为，COPS 协议及其应用是网络管理与高性能网络技术的结合部之一[12]。

2.4.4 Diameter 协议概况

Diameter 基础协议为各种认证、授权和计费业务提供了安全、可靠、易于扩展的框架。以此为基础定义 Diameter 应用，只需要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，就可以完全依赖 Diameter 基础协议完成特定的接入和应用业务。看来，Diameter 应用协议拥有广阔的发展空间[13]。

目前，IETF 的 AAA 工作组已经完成 Diameter NASREQ 应用、Diameter 移动 IP v4 应用、Diameter 多媒体应用等应用协议的制定。而在定义一个新的 Diameter 应用时，IETF 建议新协议里尽可能地重用已有的 AVP 和已有的命令代码。

创建新的应用包括定义新的命令代码或者在已有的命令代码的定义中增加几个必须的 AVP。命令代码 0-255 用于与 RADIUS 的后向兼容；0xffffffe 到 0xffffff 是实验码，只用于测试，使用实验码的两个 Diameter 对等实体间并不能保证互通。这些命令必须包含供应商特定的应用标识。其他命令代码是由 IANA(Internet Assigned Numbers Authority)分配的，是标准化的命令。

第三章　移动 IPv6

由于 Internet 的快速发展，TCP/IP 协议得到广泛的应用并成为事实上的工业标准。无线设备和新业务的进一步发展以及随之而来的大量地址需求，大量的设备或移动终端要求相互独立的 IP 地址并接入互联网。在这种情况下，很快会超出现在互联网协议的能力，使得在未来的网络发展中面临着 IP 地址不足的困境。同时由于 IPv4 本身的设计缺陷，使得代替协议的提出迫在眉睫。IPv6 协议被认为是现有 IPv4 协议最可能的替代者，许多著名的通信公司都积极推进 IPv6 的研发和产品开发工作，许多国家也投入巨额资金进行 IPv6 骨干网的构建以及相关技术的研究。

随着下一代高速移动无线网的建设、无线游戏、音乐点播、视频会议等业务正在成为现实，因此，未来的网络协议必须要支持移动性，允许主机节点在不同的 IP 网络中无缝漫游。IPv6 协议拥有巨大的地址空间，不但能够满足网络的飞速发展，也是集成移动性、安全性和质量为一体的最佳技术选择[14]。

3.1　IPv6 协议

IPv6 最早出现在 1992 年初，经过多次修改完善，在 1998 年 IETF 完成了新的 IPv6 规范，即 RFC2460。目前，IPv6 的主要协议已经成熟并形成了 RFC 文本，包括 IPv6 基本协议、邻居发现协议、互联网控制信息协议、OSPFv3, RIPng 等等。经过多年的工作，已经有超过 100 多个关于 IPv6 的 RFC 发布。现将 IPv6 协议相关内容介绍如下：

3.1.1　IPv6 的报文

IPv6 同 IPv4 一样被包括在一个物理帧中，但为了满足新的网络需求，在分组报头上作出了较大的改进。IPv6 的分组头设计为固定的 40 个字节，并且不再包含校验和字段，分段字段移到了扩展报头中，简化了路由器的处理。IPv6 分组头之后可以跟若干个扩展报头，这些扩展报头提供了某些选项，一般来讲，中间路由器则可以忽略。

如图 3-1 所示，IPv6 协议的分组头由 8 个字段共 40 个字节组成[15]，各字段的含义如下所述。

1、版本号：长度 4 位，对于 IPv6，该字段必须为 6。

2、业务流类型：长度为 8 位，该字段用于源节点或者中间路由器

标识和区分不同的类型和优先级的 IPv6 分组，支持差分服务（DiffServ,Differentiated Service）。

3、流标签：长度为 20 位，用于标识属于同一业务流的包。一个节点可以同时作为多个业务流的发送源。流标签和源节点地址惟一标识了一个业务流。

4、下一个头：长度为 8 位，这个字段指出了 IPv6 头后所跟的扩展报头类型或者高层协议净荷。

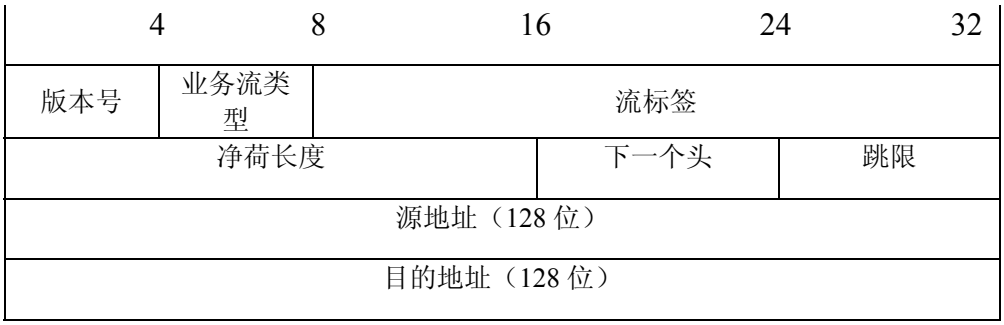


图 3-1　IPv6 的报头结构

Fig3-1 Structure of message head of IPv6

5、跳限：长度为 8 位。每当一个节点对包进行一次转发之后，这个字段就会减 1。如果该字段达到 0，这个包就将丢弃。IPv4 中与此字段对应的是生存期字段（TTL）。

6、源地址：长度为 128 位，IPv6 分组的发送方地址。

7、目的地址：长度为 128 位，IPv6 分组的接收方地址。这个地址可以是单播、组播或泛播地址。如果使用了路由头，那么其目的地址也可以是其中某一个中间节点的地址，而不是必是最终地址。

IPv6 中将 IP 头搬到净荷中，使得路由器可以像转发无选项的分组一样来转发包含有选项的分组。转发路由器除了必须处理逐跳选项之外，对其他类型的选项不做任何处理。IPv6 主要定义了如下几种选项：

（1）逐跳选项头（Hop by Hop Options Headers）：紧跟在 IPv6 头后，包含分组所经路径上每个节点都必须检查的选项数据。

（2）路由头（Routing Header）：指明分组在到达目的地的途中将经过哪些节点，包含各节点的地址列表。

（3）分段头（Fragment Header）：此扩展报头包含一个分段偏移值、一个“更多段”标志和一个标识符字段，源节点使用它对长度超出源、目的间路径最大传输单元（MTU）限制的分组进行分段。

（4）目的地址选项头（Destination Option）：此扩展报头用来携带由目的地节点检查的信息。在 IPv6 规范里，只包括一些填充选项，用于把选项填充为 64 位的整数倍。此外，移动 IPv6 中对此选项做了更多

的定义，以支持节点的移动。

（5）认证头（Authentication Header）：此扩展报头提供了一种机制，对 IPv6 头、扩展报头和净荷的某些部分进行加密。

（6）封装安全净荷头（ESP Header）：这是最后一个扩展报头，不进行加密。它指明剩余的净荷已经加密，并为已获得授权的目的节点提供足够的解密信息。

3.1.2 IPv6 的寻址

IPv6 协议实现支持 ICMPv6(Internet Control Message Protocol version 6)，ICMPv6 除了支持基本的报文控制的功能，还包含了组播收听者发现协议和邻居发现协议。所有类型的IPv6 地址都被分配到接口，而不是节点。一个IPv6 单播地址属于单个接口。因为每个接口属于单个节点，多个接口的节点，其单播地址中的任何一个可以用作该节点的标识符。所有接口至少需要有一个链路本地单播地址。一个单接口可以指定任何类型的多个IPv6 地址(单播、任意点播、组播)或范围。IPv6 地址可以分为以下三种类型：

1、单播地址（Unicast Address）：点对点通信时使用的地址。该地址仅标识一个接口，网络负责把送往单播地址的分组传送至该接口上。IPv6 的单播地址有多种类型，常用的有以下几种：

①链路局部地址（Link-Local Address）：仅在单一链路内才有意义，它仅适用在主机连接到单个链路或一个 LAN 内的场合。设计链路局部地址的目的是为了在单个链路上寻址。

②区域局部地址（Site-Local Address）：其设计目的是为了在区域内进行寻址，而无需全球网络前缀。因此，只在区域内保证它的惟一性，路由器同样也不能将其转发到本区域之外。

③可聚类全球单播地址（Aggregatable Global Unicast Address）：该地址的网络前缀由多个聚类等级标识符组成。设计这样的地址格式为了既支持基于当前供应商的集聚，又支持被称为交换局的新的集聚类型。其组合使高效的选路集聚可用于直接连接到供应商和连接到交换局两者的站点上。站点可以选择连接到两种类型中的任何一种集聚点。IPv6

3	13	8	24	16	64
格式前缀(FP)	顶级集聚标识符(TLA)	保留域(RES)	下一级集聚标识符(NLA)	站点级集聚标识符(SLA)	网络接口标识

图 3-2　可聚类全球单播地址的格式

Fig 3-2 Unicast address format

可聚类全球单播地址的格式[16]如上图 3-2 所示：

2、组播地址（Multicast Address）：表示主机组，或者说它标识一组接口。送往一个组播地址的分组将传送至有该地址标识的所有接口上。组播地址在 IPv6 包中不能用作源地址或出现在任何选路头中。对于那些不属于目的组播地址中范围字段标明了的任何组播包，路由器都不会转发。如果组播地址中的范围字段是保留值 0，则节点不能发起到此组播地址的包，即使这样的包被接收到也会被丢弃；节点也不能发起到范围保留字段是 F 的组播地址的包，如果这样的包被发送或接收，则必须将此组播地址当成全球范围组播地址（范围值 E）[17]。

3、泛播地址（Anycast Address）：标识一组接口，它与组播的区别在于分组的发送方法。送往泛播地址的分组并不被发送到组内的所有成员，而是被发送至该地址标识的“最近的”一个接口。

3.1.3 IPv6 的安全

安全问题始终是与 Internet 相关的一个重要话题。由于在 IPv4 协议设计之初没有充分考虑其安全性，因而在早期的 Internet 上时常发生网络遭到攻击、机密数据被窃取等事件。为了加强 Internet 的安全性，从 1995 年开始，IETF 着手研究制定了一套用于保护 IP 通信的安全协议(IPSec IP Security)。IPv6 协议内置的安全机制同 IPSec 的机制和服务一致，要求 IPv6 协议强制实现，以提供端到端的安全保证。

IPSec 主要有三个协议，即认证协议(AH Authentication Head)、封装安全负载(ESP Encapsulation Security Payload)和密钥交换协议(IKE Internet Key Exchange)，用于提供数据认证、数据完整性和加密性三种保护形式。在实际进行 IP 通信时，可似根据安全需求同时使用两种协议或选择一种协议。AH 和 ESP 都可以提供认证服务，但 AH 提供的认证服务要强于 ESP[18]。而 IKE 主要是对密钥进行交换管理，以及对算法、协议和密钥三个方面进行协商。

1、认证协议（AH）：AH 设计目的是为保证无连接的完整性，对 IP 数据包提供原始认证，以及对应答信息提供保护。AH 能对 1P 报头和高层协议数据进行认证，且所提供的保护机制是逐段的。AH 利用传输中不改变的数据报头计算出认证信息，为 IP 数据报保持认证信息。

2、封装安全负载（ESP）：ESP 设计的目标是为 IPv6 数据报信息的完整性和机密性提供保证。ESP 能根据所使用的算法，对 IP 数据报提供数据来源认证和无连接的完整验证。ESP 提供的服务包括：使用公共密钥加密，对数据来源进行身份验证；按 AH 提供的序列号机制提供对抗重放的服务；使用安全网关有限地提高业务的机密性；通过加密提

高数据报的机密性；采用数机密性；通过加密提高数据报的机密性；采用数据加密标准中的密码块链技术对 IP 数据报提供数据源认证和无连接的完整性的认证。

3、密钥交换协议（IKE）：IKE 是一套密钥交换规范，它为 IPsec 中的数据验证(AH)、数据加密(ESP)提供安全的密钥交换手段。IKE 的密钥协商分为两个阶段：在第一阶段，双方建立起一条安全的、提供身份认证的数据通道，这个数据通道被称之为 ISAKMP（Internet Security Architecture and Key Management Protocol）SA（Security Association）。第二阶段在第一阶段建立的数据通道保护下，协商生成用于特定应用的安全通道，对于 IPSec 而言，该安全通道被称之为 IPSec SA。这种设计在确保安全性的同时，提高了协议的性能[19]。

3.2 移动 IPv6 协议

移动通信网络将在未来的网络中起着相当重要的角色，而 IPv6 协议将首先在移动通信网络中得到应用，因此 IPv6 协议对移动性的支持显得特别重要。

所谓移动 IP，也就是允许节点在网络中从一个链路移动另一个链路而不需要改变移动节点的 IP 地址。无论节点连接到 Internet 的任何地方，目的地址是移动节家家乡地址的包都能够路由到移动节点，而且漫游中的移动节点还能保持与通信对端的通信。也就是说，移动节点的移动对于传输层以及更高层协议和应用是透明的。

IPv6 协议对移动性的支持主要体现在以下两点：

1、自动配置功能：IPv6 的节点自动配置功能使得节点在改变网络接入点之后能够保持网络连接。

2、扩展报头机制：IPv6 的移动选项可以放在扩展报头中。

3.2.1 移动 IPv6 的基本操作及报文

无论移动节点在家乡链路还是离开家乡链路，都可以通过它的家乡地址与其通信。当移动节点在家乡网络时，其工作方式同固定主机是一样的，移动节点家乡地址的子网前缀是移动节点家乡链路的子网前缀或子网前缀之一，发送给移动节点的分组被转发到它的家乡链路。

移动 IP 中定义了如下功能实体：

1、移动节点（Mobile Node）：是指从一个网络或子网链路上切换到另一个网络或子网的主机或者路由器。移动节点可以改变它的网络接入点，但不需要改变 IP 地址，并且用原来的 IP 地址能够保持与其他节

点的通信。

2、家乡代理（Home Agent）：是指位于移动节点家乡链路（home link）上的路由器。当移动节点离开家乡网络时，它负责把发往移动节点的分组通过隧道转发给移动节点，并且维护移动节点当前位置的信息。

3、外地代理 FA（Foreign Agent）：位于移动节点所访问的网络上的路由器，为注册的移动节点提供路由服务。它接收移动节点的家乡代理通过隧道发来的报文，进行拆封后发给移动节点；对于移动节点发出的报文，外地代理提供类似默认路由器的服务。

家乡代理和外地代理可以统称为“移动代理”。

典型的移动 IP 网络中功能实体及相互关系如下图 3-3 所示：

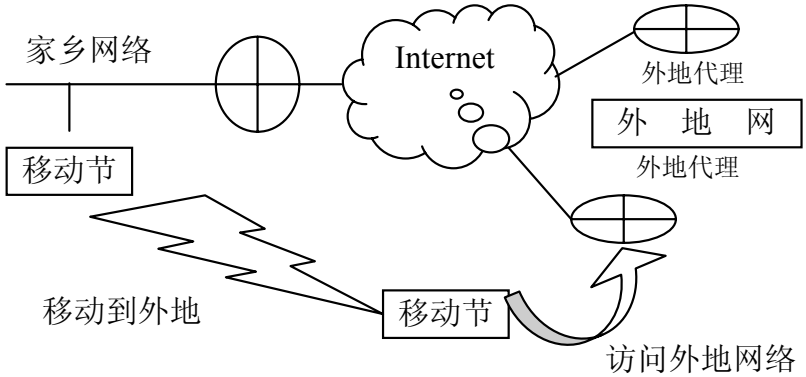


图 3-3 移动 IP 功能实体及相互关系

Fig. 3-3 Function entity and relationship of mobile IP

在移动 IPv6 中，由于移动节点可以通过 IPv6 的邻居发现机制，采用无状态的地址自动配置的方式获得转交地址，因此没有了外地代理的概念，而由处在外地的接入路由器承担对移动节点的绑定请求等的转发任务。移动 IPv6 基本操作过程有如下几个方面[20]：

1、移动绑定。当移动节点移动到外地链路上时，要通过 IPv6 邻居发现机制，通常是以无状态的地址自动配置方式获得一个或多个转交地址，转交地址的子网前缀是移动节点访问的外地链路的子网前缀。移动节点在获得转交地址后，需要把一个转交地址注册到它的家乡代理上，通过向家乡代理发送“绑定更新”消息，以及家乡代理应答“绑定确认”消息完成注册。

2、分组路由。家乡代理在获得移动节点的转交地址并完成绑定后，在移动节点的家乡链路上使用代理邻居发现机制，在家乡链路上截获目的地址是移动节点的家乡地址的 IPv6 分组，然后通过隧道将它们转发到移动节点的主转交地址。家乡代理对分组使用 IPv6 封装，外层 IPv6 报头中目的地址是移动节点的主转交地址。

3、返回路径可达过程。移动节点和家乡代理通过建立安全关联，

使用 AH 和 ESP，实现到家乡代理绑定更新的保护。到通信对端的绑定更新可以使用绑定管理密钥来保护，通过返回路径可达过程建立绑定绑定管理密钥。

返回路径可达过程由 4 条消息组成。移动节点先同时送 HoTI（Home Test Init）消息和 CoTI(Care-of Test Init)消息，通信对端很快处理这两个消息后，返回 HoT（Home Test）消息和 CoT（Care-of Test）消息。该过程如 3-4 图所示。

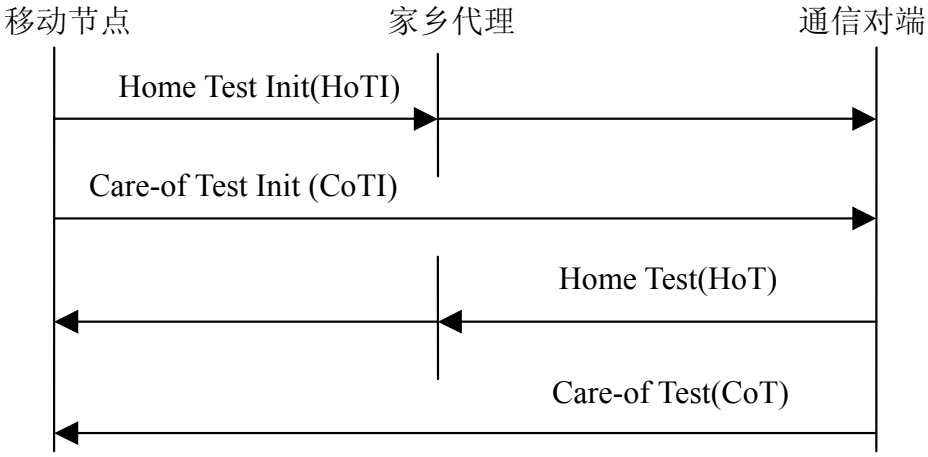


图 3-4　返回路径可达过程
Fig. 3-4 Return Routability Procedure

HoTI 消息用于请求获得家乡密钥令牌，传送移动节点的家乡地址给通信对端，也携带通信对端必须随后回传的 HoT，该消息经过隧道到家乡代理后，再到达通信对端。

CoTI 消息用于请求获得转交密钥令牌，传送移动节点的转交地睛给通信对端，也携带通信对端必须随后回传的 CoT，该消息直接被发送到通信对端。

HoT 消息是通信对端对 HoTI 消息的响应，还有家乡密钥令牌等信息，该消息经过家乡网络转发给移动节点。

CoT 消息是通信对端对 CoTI 消息的响应，携带转交密钥令牌等信息，该消息直接发送到移动节点。当移动节点接收到 CoT 消息和 HoT 消息后，返回路径可达过程结束。这样，移动节点根据收到的信息计算绑定管理密钥，获得向通信对端发送绑定更新的授权。在该过程中假如有攻击者能对远端结点到家乡代理的消息进行监听，那么它可容易地得到 HoT，从而形成重定向攻击[21]。这是返回路径可达过程安全方面的不足。

4、动态家乡代理地址发现。当移动节点离开家乡时，家乡链路上的部分节点可能进行了重新配置，原来的家乡代理被其他的路由器代替。在这种情况下，在需要给家乡代理发送绑定更新注册它的主转交地

址时，移动节点可能不知道自己家乡代理。在这种情况下可以能过发送ICMPv6“家乡代理地址发现请求”消息，目的地址为其家乡子网前缀的“移动 IPv6 家乡代理”泛播地址，源地址是移动节点的转交地址。家乡链路上收到这个请求消息的家乡代理会回答一个 ICMP“家乡代理地址发现应答”消息，给出自己的全球单播 IP 地址，以及包含家乡链路上所有家乡代理的全球单播 IP 地址的列表。

3.2.2 移动 IPv6 的安全

移动 IP 在网络层实现了移动互联，但是，也带来了潜在的安全问题，主要来源于移动环境和移动 IP 协议两个方面。移动主机在许多情况下通过无线链路接入到网络，因此更加容易遭受被动窃听、重放攻击和其他主动攻击。在移动 IP 协议中，移动主机不断切换到不同的外地风络，通过这些外地网络与家乡网络和通信对端通信，外地网络的安全性和可信度都影响通信的安全性。

移动 IPv6 协议中提供了相关的安全机制，包括对移动节点发往家乡代理或者通信对端的绑定更新保护机制，以及对隧道、家乡地址信息、数据分组中的路由指令等保护机制。

1、保护发往家乡代理的绑定更新。移动节点的和家乡代理之间的信令必须是完整的，满足一定的排序规则，并且提供对重放攻击的保护，因此，在它们之间需要维护一种安全关联。例如，使用认证头（AH）或者封装安全净荷（ESP）报头进行完整性保护，使用顺序号字段保证绑定更新和绑定确认消息相匹配，满足它们的有序性。

2、保护发往通信对端的绑定更新。通过使用绑定管理密钥，可以保护发往通信对端的绑定更新。可以使用返回路径可达过程在通信对端和移动节点间交换的数据创建绑定管理密钥，这个过程需要使用节点密钥、临时随机数、令牌和一些加密函数。

3、对载荷数据分组的保护。对于同移动节点交互的数据分组，可以采用与静止节点类似的方法进行保护。

3.2.3 移动 IPv6 与 IPv4 的比较

相对移动 IPv4 而言，移动 IPv6 协议继承了移动 IPv4 协议的许多特性，并借用了移动 IPv4 中的许多概念，包括移动节点、家乡代理、家乡地址和转交地址，但是移动 IPv6 的设计吸取了移动 IPv4 协议的开发经验，产生了许多新特性，在移动 IPv4 的基础上有了许多显著的改进。

1、转交地址。移动 IPv4 的转交地址是外地代理转交地址，是外地

网络上外地代理的一个 IP 地址。由于 IPv6 具有巨大的地址空间，每个移动节点在任何访问的网络上都能获得一个全球唯一的 IP 地址，所以移动 IPv6 协议没有外地代理转交地址的概念，也不存在外地代理。

2、优化路由。前文所述的对三角路由的改进问题。移动 IPv6 中允许移动节点在通信对端上绑定移动节点的当前转交地址和家乡地址。这样，可以实现通信对端和移动节点的直接通信，不再将分组发往家乡地址，由家乡代理截获后通过隧道发往移动节点，而是由通信对端检查响应的绑定更新消息，将分组直接发往移动节点的转交地址，避免了移动 IPv4 协议中的三角路由问题，实现路由的优化。

3、移动检测。移动 IPv6 提供了移动节点与当前位置默认路由器之间通信能力的双向确认，移动节点接收默认路由器发送的分组，以及发送分组到默认路由器，这种双向确认能力可以提供位置检测能力。在移动 IPv4 中，只有从路由器到移动节点的转方向需要确认，这就是可能产生无法检测到位置。

第四章　Diameter 协议研究

Diameter 协议在设计时，克服了现有 AAA 技术的许多不足，并保持了与广为使用的 Radius 协议的兼容,而且它被设计得非常灵活，容易进行新应用的扩展,以满足新的需求，所以它不仅被互联网采用，更被下一代移动通信网(3G)采用。

Diameter 协议包括基础协议和各种扩展而来的应用协议如 NASREQ、Mobile IP、CMS Security 等,其协议层次结构如图 4-1 所示。

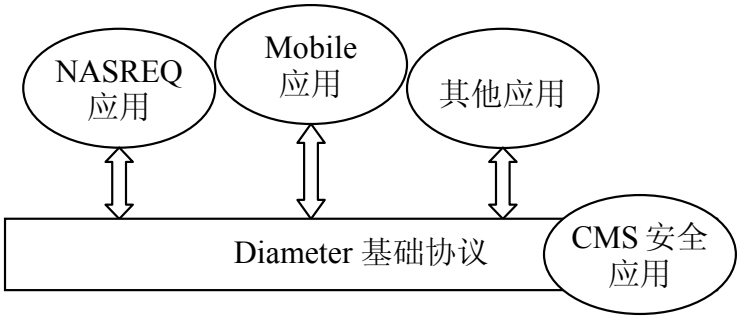


图 4-1 Diameter 协议族
Fig.4-1 Diameter protocol family

Diameter 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各个方面。还定义了某些规则，以应用于 Diameter 节点之间的消息交换上。

NASREQ 应用能提供与 RADIUS 提供的类似的网络接入功能，而且考虑了与 RADIUS 的兼容，NASREQ 主要应用于 PPP/ SLIP 拨号、宽带/ DSL、VOIP 等接入环境中。

Mobile IP 应用于移动 IP 业务中。Diameter 基本协议的目标是为网络接入、移动 IP 等应用提供 AAA 框架。它定义了所有 Diameter 基本应用所需的消息格式、传输、错误报告、计费和安全服务。

Diameter CMS(Cryptographic Message Syntax ——密码消息语法)协议实现了协议数据的 Peer-to-Peer(端到端)加密。由于 Diameter 网络中存在不可信的 Relay(中继)和 Proxy(代理)，而 IPSec 和 TLS 又只能实现逐跳的安全，所以 IETF 定义了 Diameter CMS 应用协议来保证数据安全[22]。

4.1　Diameter 基础协议

Diameter 协议是为了给应用程序提供 AAA 框架，如网络访问或 IP

移动性。Diameter 协议不但要提供给本地的 AAA 服务，也要适用于漫游状态。其中 Diameter 基础协议[23]指定了消息格式，传送，错误报告，记费和安全服务用于 Diameter 应用程序。所有的 Diameter 协议应用程序都需要支持 Diameter 基础协议。基于 Diameter 协议的 AAA 服务器提供接入服务的基本框架如下图 4-2 所示。

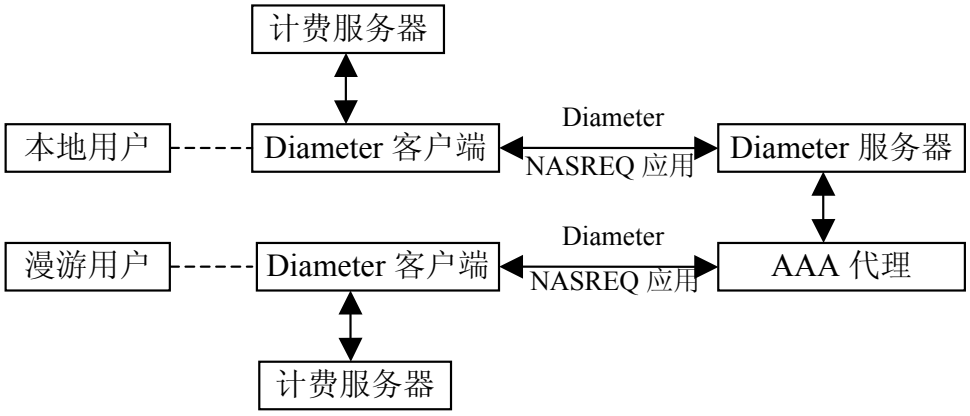


图 4-2 Diameter 协议基本框架
Fig.4-2 Basic framework of Diameter protocol

另外，基本协议还说明了消息格式、传输方式、错误报告等。基本协议一般不会单独使用，需要扩展成某个应用以提供具体的服务[24]。应用协议则利用基础协议提供的消息传送机制，以此为基础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，这样就可以完成特定的接入和应用业务。

4.1.1 Diameter 网络节点

在 Diameter 协议中，包括多种类型的 Diameter 节点。除了 Diameter 客户端和 Diameter 服务器外，还有 Diameter 中继、Diameter 代理、Diameter 重定向器和 Diameter 协议转换器。

1、Diameter 中继。中继代理一种 Diameter 代理，他接收请求并基于在消息中发现的信息将消息中继给其他 Diameter 节点。该路由决定是利用支持域列表和已知的对等节点。

中继可以用来会聚从在共同地理区域的多个网络访问服务器来的请求。中继服务的使用是有利的，他是减少了配置由于要同其他领域的 Diameter 服务器通信所必须的安全信息的需要。同样的，也减少了 Diameter 服务器在 NAS 节点增加或减少时候的配置负载。如图 4-3 的例子描述了一个从 NAS 的访问设备，用户是 bob@example.com。在发送请求之前，NAS 先做一个 Diameter 路由查询，用“example.com”做为主键，并决定将消息转发给 DRL（Diameter Relay 转发服务器）。DRL

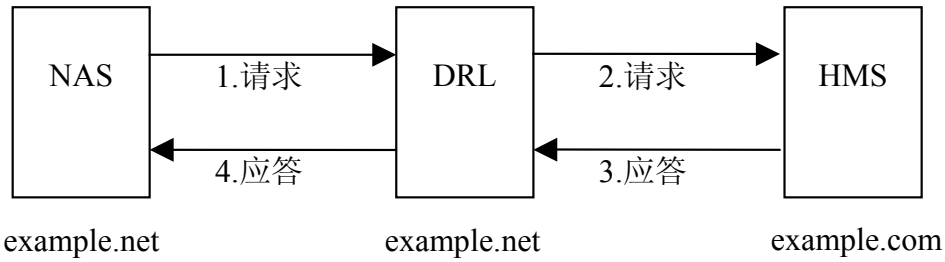


图 4-3 Diameter 消息的中继

Fig.4-3 Relaying of Diameter messages

执行同 NAS 同样的查询，并将消息转发给 HMS（example.com 是家乡 Diameter 服务器）。HMS 识别出该请是可以被本地支持的（通过域），处理认证和授权请求并做出一个应答，然后根据保存的传输状态传回给 NAS。

中继通过插入或移去路由信息改变 Diameter 消息，而不是转发消息的其他部分。中继不应该保持会话状态，但一定要保持转输状态。

2、Diameter 代理。同转发相似，代理通过 Diameter 路由表路由 Diameter 消息。然后不同的是，它改变消息以执行强制的策略。在这种要求下它必须保持下行流对端的状态（例如：访问设备）以执行资源的使用，提供准入控制和预留。

代理可能用在呼叫控制中心或者访问提供外部资源联接的 ISP 们，他们可以监视使用的端口数和类型，并且可以进行分配并根据配置做出准入控制。希望限制资源的代理必须保持状态，所有的代理都必须保持传输状态。增强性策略要求提供可理解的服务，代理必须通告他们所支持的应用。

3、Diameter 重定向器。重新定向代理在 Diameter 路由服务需要集中的情况下非常有用。一个给所有的协定成员提供服务的重新定向代理就是一个例子，它并不希望负担域间的所有消息。当它成员的框架结构改变而不要求协定提供路由更新的情况下，是十分有利的。

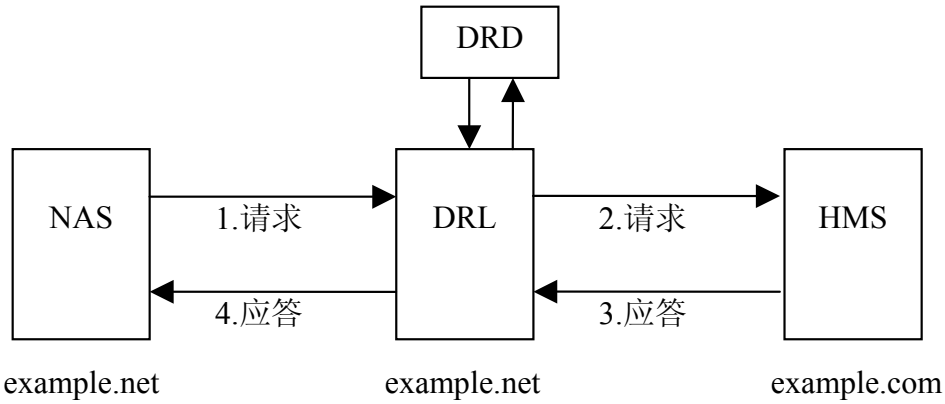


图 4-4 Diameter 消息的重定向

Fig.4-4 Redirecting Diameter Message

重新定向代理并不转发消息，并且只返回一个带有对于 Diameter 代理直接通信必须信息的应答，他们并不改变消息，他们也不能保持会话状态。此外，虽然它不改发消息，也就不要求保持传输状态。

图 4-4 提供了一个例子，描述了从一个服务设备、NAS 发送家乡服务器的消息重新定向的过程，为了用户 bob@example.com。该消息被发送转发服务器 DRL，该 DRL 并没有关于 example.com 的路由消息。DRL 有一个默认的路由配置 DRD(Diameter Redirect 重新定向代理)，它将返回一个重新定向通告给 DRL，也是 HMS 的联系信息。根据收到的重定向通告，DRL 同 HMS 建立一个传输连接，并发送消息给它。

4、Diameter 协议转换代理。一个转换代理是一个提供协议之间转换的服务设备。主要用于实现 RADIUS 与 Diameter，或者 TACACS+与 Diameter 之间的协议转换。转换代理很适用作同 Diameter 架构通信的聚合服务，允许嵌入式系统在一个较低的层次下移植。

给定的 Diameter 协议引入了长期授权会话的理念，转换代理必须有会话状态并且必须保持转换状态。

4.1.2 Diameter 的消息格式

一个 Diameter 协议的报头格式被按下图 4-5 形式表达出来，该报文在网络里以字节顺序传输。

0 7	31
版本	消息长度(Message Length)
命令标识	命令代码(Command Code)
应用 ID（Application ID）	
逐跳标识（Hop-by-Hop Identifier）	
端到端标识（End-to-End Identifier）	
AVPs……	

图 4-5 Diameter 消息报头
Fig.4-5 Diameter Header

1、版本 (Version)：该版本域应该被设为 1。

2、消息长度 (Message Length)：消息长度域由三个八位组表明了 Diameter 消息的长度（包括头域）。

3、命令标识 (Command Flags)：该命令标识域是八个比特。各比特的分配如下图 4-6 所示：

R（请求）：如果置 1，消息是一个请求。如果置 0，消息是一个应答。

图 4-6 命令标识
Fig.4-6 Command Flages

P（代理）：如果置 1，消息可能被代理、转发或都重新定向。如果没有置 1，消息必须被本地处理。

E（错误）：如果置 1，消息包括一个协议错误，并且消息遵照这个命令里的 ABNF（Augmented Backus-Naur Form 扩展巴科斯范式）的描述。消息带有‘E’比特置位的通常是一个错误消息。该比特在请求消息中一定不能置 1。

T（潜在的重传消息）：在一个连接失败程序之后被置 1，以帮助支持完全相同的请求。当由于连接失败而要求重发，由此可能有重复请求的时候该位置 1。它只在当无法收到一个请求的回答并且重发该消息的时候被置 1。回答消息中从不置 1。

r(保留) －被保留来将来用。都为 0

4、命令代码 (Command-Code)：命令代码域是有三个八位组，被用来沟通同消息有关的命令。24 比特的地址空间是由 IANA 来管理的。命令代码的值 16,777,214 和 16,777,215（十六进制值 FFFFFE-FFFFFF）被保留给实验用。目前已经定义的命令代码如下表 4-1 所示。

命令名	缩写	代码
中断会话请求	ASR	274
中断会话回应	ASA	274
记费请求	ACR	271
记费应答	ACA	271
能力交换请求	CER	257
能力交换应答	CEA	257
设备监视请求	DWR	280
设备监视应答	DWA	280
断开连接请求	DPR	282
断开连接应答	DPA	282
重新授权请求	RAR	258
重新授权应答	RAA	258
会话终止请求	STR	275
会话终止应答	STA	275

表 4-1 已经定义代码
Diagram4-1 Defined Code

5、应用 ID（Application-ID）：应用 ID 是四个八位组，并被用来

标识消息是哪种应用协议可用的。该应用可以是一个认证应用，也可以是一个记费应用或者一个厂商特定标识应用。可以看到可用的应用 ID 值。报文头里的应用 ID 必须同任何包含在消息中的相关 AVPS(Attribution Value Pair)相同。

6、逐跳标识（Hop-by-Hop Identifier）：逐跳标识是一个无符号的 32 比特整数域并且匹配请求和应答。发送者必须保证一个请求的逐跳标识在一个给定的连接和任何给定的时间是唯一的，并可能尝试通过重启以保证唯一。回答消息的发送必须保证逐条标识域包含同相应请求相同的逐跳标识。逐跳标识通常是一个单调递增的数字，它的初始值是随机产生的。收到的应答消息如果有一个不可知的逐跳标识，则必须被抛弃。

7、端到端的标识（End-to-End Identifier）：端到端的标识是一个无符号 32 比特整数域（按网络字节顺序），用来检查重复消息。在重新启动之上，可设置高十二比特容纳当前时候的低位十二比特，低位的 20 是一个随机值。请求消息的发送者必须给每一个消息插入一个独一无二的标识。在一时期内，标识必须保持本地唯一性（即使经过重启）最少四分钟。

AVP 是一种同 Diameter 消息相关的封装信息的方法。DiameterAVP 携带特定的认证、授权、记费、路由和安全消息，还有请求和应答的配置细节。每个类型的 AVP 八位组字符串必须以一个 32 比特为边界的填充排列，同时其他的 AVP 类型自然排列。许多 0 值的比特被增加到 AVP 数据域的尾部，直到字长边界。填充的长度并不反应在 AVP 的长度域里。

AVP 报头里的内容必须被以网络字节顺序发送。AVP 报头的格式如图 4-7 所示：

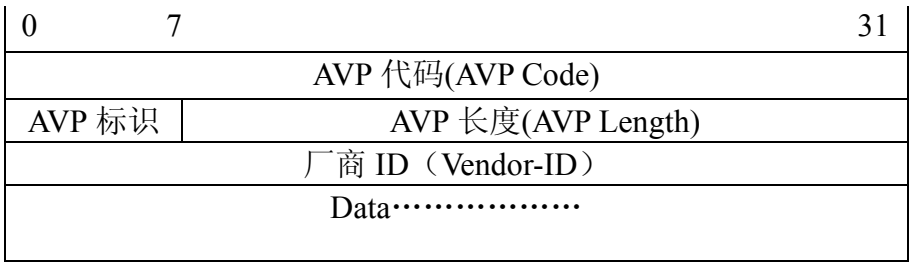


图 4-7 AVP 报头
Fig.4-7 AVP Header

1、AVP 代码 (AVP Code)：AVP 代码，由厂商 ID 域、唯一属性的标识组合而成。AVP 代码值 1-255 已经被保留为向后兼容 RADIUS，不带有厂商 ID 域。AVP 数 256 和以上的数字用于 Diameter 协议，由 IANA 来分配。

2、AVP 标识 (AVP Flag)：AVP 标记域通知接收者如何处理每一个属性必须被处理。该命令标识域是八个比特。各比特的分配如下图 4-8 所示：

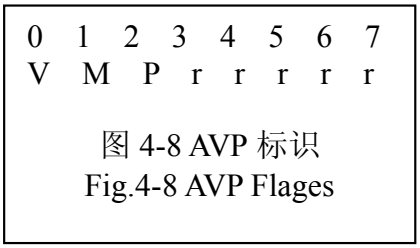


图 4-8 AVP 标识
Fig.4-8 AVP Flages

①V 比特，被认作厂商指定的比特。表明厂商 ID 域选项是不是在该 AVP 头里出现。设置的 AVP 代码属于特定的厂商代码地址空间。

除非另外说明，AVPS 将有以下默认的 AVP 标记：M 比特必须被置 1。V 比特一定不能置 1。

②M 比特是强制比特，表明是否支持 AVP 的请求。如果一个 Diameter 客户、服务、代理、协议转换代理收到的 AVP 带有 M 比特置 1，并且 AVP 和他的值都不可认的，该消息应该被拒绝。Diameter 中继和重新定向一定不能拒绝一个带有不可认别 AVP 的消息。M 比特置 0 的 AVP 可以直接忽略。

③P 比特表明了是否需要端到端的安全。

④r 比特是没有使用的并应该被设为 0。未来的 Diameter 应用可能定义在 AVP 报头里附加比特，一个不可识别的比特应该被认为是一个错误。P 比特表明了需要端到端的安全。

3、AVP Length (AVP 长度):AVP 长度域是三个八位组，并且表明了 AVP 的八位组数量，包括 AVP 代码，AVP 长度，AVP 标记，厂商 ID 域和 AVP 数据。如果一个消息带有不合法的属性长度，该消息应该被拒绝。

4、Vendor-ID：厂商 ID 只有当 V 比物被置 1 的时候才可以引入。四个八位组的厂商 ID 域包含 IANA 分配的“SMI 网络管理私有企业代码”值，按网络比特顺序编码。任何厂商希望执行一个厂商特定的 Diameter AVP 都必须用他们自己的厂商 ID 连同他们的私有管理 AVP 地址空间，保证不能同任何其他厂商的厂商指定 AVPS 或未来 IETF 应用中的 AVPS 重复。

AVP 值是 Diameter 协议业务实现的基本单位，AVP 有多种值类型并通过不同的 AVP 代码值来表示不同的应用，包括授权、记费、路由信息、错误恢复、安全传输等重要信息都是通过不同的 AVP 值来负载并提供保证的。

4.1.3 Diameter 网络节点间的对等连接

Diameter 基础协议通过有穷自动机的形式详细描述和定义了功能节点的连接状态及对应操作[25]。同时，对用户会话状态的维护和控制也给出具体的定义。基础 Diameter 协议运行在 TCP 和 SCTP 协议的端口 3868 之上。Diameter 客户必须支持 TCP 或 SCTP，同时代理和服务器也必须两种协议。而未来的 Diameter 版本将要求客户支持 SCTP。

一个 Diameter 节点可能同与已经宣布接受连接的端口不同的其他源端口初始化连接，并且必须准备接受 3868 端口上的连接。当没有同对端的传输连接的时候，连接的尝试应该是周期性的。这种行为通过定时期来操作，推荐值是 30 秒。这些规则也有例外，例如当一个对端终止了传输连接并且不想进行通信。

1、Diameter 对端的发现。允许动态 Diameter 代理发现，使 Diameter 服务的简单并且强壮的发展提供可能。为了提高 Diameter 对端动态操作中的互操作性，描述了下列机制。它们是基于 IETF 标准的。

有两情况下，对等端点可能完成节点发现过程。第一，当 Diameter 客户端需要发现 Diameter 代理的第一跳。第二，当 Diameter 代理需要发现另一个代理以处理 Diameter 操作。推荐使用下面的搜索过程：

①Diameter 节点同他的静态配置的 Diameter 代理列表里的端点协商。如果它们存在并回应的时候可以用。

②Diameter 程序用 SLP [26]（Service Location Protocol）来发现 Diameter 服务。这种服务定位协议提供了一种可扩展的框架，用来发现和选择网络服务。当使用这个协议的时候，Internet 上的计算机只需要很少的或非静态的网络服务的配置。这种应用对于计算机的移动性更为重要。

③Diameter 程序在一个特定的域里完成一个请求服务。Diameter 程序必须更进一步知道在哪个域里找 Diameter 代理。这种要求可以使用某种机制推导出来，例如，从 Diameter 节点在 Diameter 操作里必须实现的 NAI 域。

2、能力交换。当两个 Diameter 对等节点建立了一个传输连接，他们必须交换他们在对等状态机中指定的能力交换消息。该消息允许一个对等端点身份和能力的发现机制。

一个收到不带任何发送者公有应用的能力交换消息的接受者必须返回一个能力交换应答，并且应该将结果代码 AVP 的值设为 DIAMTER-NO-COMMON-APPICATION，同时应该断开与传输层连接。

当收到不带有任何安全机制的能力交换消息的接收者也必须返回一个能力交换消息应答，并且将结果代码 AVP 的值设为

DIAMETER-NO- COMMON-SECURITY，将应该断开传输层连接。

状态	事件	动作	下一状态
Closed	Start	I-Snd-Conn-Req	Wait-Conn-Ack
	R-Conn-CER	R-Accept/Process-CER/ R-Snd-CEA	R-Open
Wait-Conn-Ack	I-Rcv-Conn-Ack	I-Snd-CER	Wait-I-CEA
	I-Rcv-Conn-Nack	Cleanup	Closed
	R-Conn-CER	R-Accept/Process-CER	Wait-Conn-Ack/Elect
	Timeout	Error	Closed
Wait-I-CEA	I-Rcv-CEA	Process-CEA	I-Open
	R-Conn-CER	R-Accept/Wait-Returns/ Process-CER	Elect
	I-Peer-Disc	I-Disc	Closed
	I-Rcv-Non-CEA	Error	Closed
	Timeout	Error	Closed
Wait-Conn-Ack/ Elect	I-Rcv-Conn-Ack	I-Snd-CER/Elect	Wait-Returns
	I-Rcv-Conn-Nack	R-Snd-CEA	R-Open
	R-Peer-Disc	R-Disc	Wait-Conn-Ack
	R-Conn-CER	R-Reject	Wait-Conn-Ack/ Elect
	Timeout	Error	Closed
R-Open	Send-Message	R-Snd-Message	R-Open
	R-Rcv-Message	Process	R-Open
	R-Rcv-DWR	Process-DWR/R-Open	R-Snd-DWA
	R-Rcv-DWA	Process-DWA	R-Open
	R-Conn-CER	R-Reject	R-Open
	Stop	R-Snd-DPR	Closing
	R-Rcv-DPR	R-Snd-DPA/Closed	R-Disc
	R-Peer-Disc	R-Disc	Closed
	R-Rcv-CER	R-Snd-CEA	R-Open
	R-Rcv-CEA	Process-CEA	R-Open
I-Open	Send-Message	I-Snd-Message	I-Open
	I-Rcv-Message	Process	I-Open
	I-Rcv-DWR	Process-DWR/I-Open	I-Snd-DWA
	I-Rcv-DWA	Process-DWA	I-Open
	R-Conn-CER	R-Reject	I-Open
	Stop	I-Snd-DPR	Closing
	I-Rcv-DPR	I-Snd-DPA/Closed	I-Disc
	I-Peer-Disc	I-Disc	Closed
	I-Rcv-CER	I-Snd-CEA	I-Open
	I-Rcv-CEA	Process-CEA	I-Open
Closing	I-Rcv-DPA	I-Disc	Closed
	R-Rcv-DPA	R-Disc	Closed
	Timeout	Error	Closed
	I-Peer-Disc	I-Disc	Closed
	R-Peer-Disc	R-Disc	Closed

表 4-2 对等连接的有限状态机

Diagram 4-2 Finite state mechine of peer connection

从未知对端收到的 CER 可能会直接的丢弃，或者返回一个结果代码设为 DIAMETER_NUKNOWN_PEER 的 CEA 消息。这上两种情况下传输连接会被关闭。

3、对等连接的状态机。当从一个 Diameter 对端收到一个连接请求时，通常情况下不可能知道对端的标识除非收到 CER 消息。这是因为主机和端口决定 Diameter 对等节点的身份；并且请求连接的源端口是任意的。收到 CER 消息后，连接对端的标识可以通过初始主机域唯一得到。

因此，一个 Diameter 对等节点必须同收到连接请求状态机逻辑分离，接受他们，并等待 CER。一旦一个 CER 在一个新连接的基础上到达，标识对等端点的初始主机用来定义同那个对端之间的状态机，并且新的连接和 CER 做为一个 R-conn-CER 事件通过该状态机。

上表 4-2 包括了一个必须被所有 Diameter 执行遵守的有限状态机。当每一个对端通信的时候，每一个 Diameter 节点必须遵守该状态机的描述。多个动作被用逗号分割，并且作为空间要求在后继线上继续。同样，状态和下一状态可能也跨多条线，做为空间请求。

该状态机接近于 AAA 传输框架协议(RFC3539)里描述的状态机，用于打开，关闭，错误恢复，探测和重新打开传输连接。特别注意，AAA 传输框架协议要求用监视消息来探测连接。对于 Diameter，DWR 和 DWA 消息用于这个目的。

I- 用来表示发起者连接，而 R-用来表示接收者连接(监听)。缺少前缀表示该事件或动作也同样与连接无关。

该状态机可能存在的稳定状态是关闭，I-OPEN，R-OPEN；所有其他状态都是中间的。

4.1.4 Diameter 消息的安全传输

Diameter 基础协议假定消息是使用 IPSEC 或 TLS 安全保护的。这个安全机制在没有第三方不可信任的代理存在的环境里是可以接受的。在其他情况下，必须实现端到端的安全机制。

Diameter 客户，如网络访问服务器(NAS)和移动代理必须支持 IP 安全并可能支持 TLS。Diameter 服务器必须支持 TLS 和 IPSEC。Diameter 程序必须在每个连接上使用某种传输层安全机制(IPSE 或 TLS)。

如果一个 Diameter 连接没有被 IPSEC 保护，那么 CER/CEA 交换必须包括一个带内安全 ID AVP，并带有一个 TLS 的值。对于 TLS 应用，当完成 CER/CEA 交换之后，如果两个端点都在开放状态的时候 TLS 握手将开始进行。如果 TLS 握手成功，所有更进一步的消息都是通过 TLS

进行发送。如果握手失败，两端都转到关闭状态。

在外部域交换的边缘进行交换的时候建议使用 IPSEC。对于不支持证书的 NAS 设备，可以在 NAS 和本地 AAA 代理之间使用提前共享密钥。

对于内部域交换的保护，推荐使用 TLS。

1、IPSEC 的使用。所有的 Diameter 程序必须在传输模式里支持带有非零加密的 IPSEC ESP 和认证算法以提供每个包的认证，完整性保护和机密性，并必须支持 IPSEC 的重放保护机制。IPSEC 协议集根据 IKE 协议协商成功的安全关联来确认通信实体使用的协议、加密算法、密钥等，对于不同的安全级别，通信实体还可以确认不同强度的加密算法和密钥长度等安全要素[27]。

Diameter 实现必须支持对每个认证对端的 IKE，安全关联的协商和密钥管理。Diameter 程序必须支持对端使用提前共享密钥认证，并可以支持基于数字签名的证书的认证方式。

构造 Diameter 程序时必须支持 IKE 的主要模式和野蛮模式[28]。当提前共享密钥使用在认证中时，应该使用 IKE 的野蛮模式，不应该使用 IKE 的主要模式。当用数字签名来认证的时候，主模式和野蛮模式都可以被使用。

第二阶段的快速模式交换用来协商对 Diameter 连接的保护，必须明确的携带负载标识域。既然 IPSEC 加速硬件可能只能处理一个有限数量的活动 IKE 第二阶段的 SA，作为保持第二阶段的活动 SA 到最小的数量的一种方法。收到一个被删除的 IKE 第二阶段的消息，不应该立即中断 Diameter 连接。而应该让连接保持，并且当有另外的通过它的发送的通信时候，则提出另一个 IKE 第二阶段 SA 以保护他。这样避免了潜在的可以连续关闭打开连接的可能性。

2、TLS[29]使用。一个 Diameter 节点发起同别一个 Diameter 节点的连接的时候是担当一个 TLS 客户端，而一个 Diameter 节点接受了 TLS 连接时是担当一个 TLS 服务器。Diameter 节点为了安全而实现了 TLS，他们必须在在 TLS 会话建立的时候相互进行认证。为了确定如何相互认证，这个 Diameter 节点担当 TLS 服务器的节点必须要求提当客户端的节点提供一个证书，并 TLS 客户端必须准备在被要求的时候提供该证书。

Diameter 节点必须能够同下列密码组件进行协商：

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

Diameter 节点应该能够同下列 TLS 密钥套件进行协商

TLS_RSA_WITH_AES_128_CBC_SHA

Diameter 节点可能同其他 TLS 密钥套件进行协商。

3、端到端的安全机制。作为任何带有端到端的协议，一个 Diameter 对端的信任模型的正确的配置是本质上安全的。当使用证书的时候，配置被 Diameter 对端信任的根证书授权。这个根 CA 很可能是唯一在 Diameter 程序里的，而同其他目的的证书不同(如 WEB)。通常，我们希望配置这种根 CA，以反映各不同组织的主机之间的商业关系。结果，一个 Diameter 对端将不会被配置成允许同任意连接都可以进行连接。当证书认证的 Diameter 对端可能是不能预先知道的话，则要求部署一种对端发现机制。

IPSEC 同 TLS 相比缺乏灵活性，当它需要配置根 CA 的时候。既然 IKE 第一阶段使用端口标识是被禁止的，在 IPSEC 里便不可能被唯一的给每一个应用单独配置可信任的根 CA；同样的策略必须被为所有的应用来使用。例如，在 Diameter 协议里被任何的根 CA 也被信任用来保护 SNMP。这种限制是非常笨拙的。TLS 支持证书策略的应用层粒度的使用，可能被用来在管理域里保护 Diameter 连接。IPSEC 更合适当一个提前共享密钥被做为安全机制的时候被用来域间使用。

当提前共享密钥认证被用在 IPSEC 以保护 Diameter 协议，唯一的提前共享密钥被在 Diameter 对端之间配置，他们通过他们的 IP 地址或也有可能是他们的 FQDN(Fully Qualified Domain Name)。结果，对于一组 Diameter 对端是必须是预先知道的。因此，对端机制发现通常不需要。

推荐 Diameter 对端实现相同的安全机制(IPSEC 或 TLS)在所有的端到端连接。不一致的安全机制的使用可能会导致多余的安全机制的使用或错误，以衣潜在安全漏洞。当 IPSEC 被用在 Diameter 协议里，典型安全策略是同外部通信“发起 IPSEC，从我到任何终端 Diameter 端口”。对内部通信，其策略是“要求 IPSEC，从任何端口到我，目的端口 Diameter”。

如果 IPSEC 被用来保护 Diameter 的端到端连接，IPSEC 策略将被设为要求 IPSEC 为内部连接提供保护，并被发起 IPSEC 保护外部连接。这种方式可以通过内部或外部过滤策略来实现。

4.2 Diameter NASREQ 应用扩展

Diameter NASREQ 应用，是用于网络接入服务的 AAA，可以满足拨号（PPP）、宽带/DSL、无线电话（如 3GPP/CDMA2000）和无线数据（IEEE 802.11a/b）等接入服务器进行认证、授权和计费的需要。Diameter NASREQ 应用能提供与 RADIUS 提供的网络接入类似的功能，

而且已经考虑了与 RADIUS 的兼容。Diameter NASREQ 协议通过 CER、AAR(AA-Request)、AAA (AA-Answer)消息中 Auth-Application-Id AVP 的值置 1 来通告对 Diameter NASREQ 应用的支持[30]。

1、Diameter NASREQ 应用扩展命令代码。该应用扩展中定义了新的消息命令代码和 AVP 值，扩展 Diameter 基础协议并提供接入服务过程。这些新的消息命令如下表 4-3 所示。

命令名	缩写	代码
AA-Request	AAR	265
AA-Answer	AAA	265
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271

表 4-3 Diameter NASREQ 命令代码
Diagram 4-3 Command code of Diameter NASREQ

2、协议过程。当网络接入服务器收到新的呼叫或连接请求时，就开始 NASREQ 消息的交换。有关呼叫的信息、用户的标识、认证信息等被封装到 AA 请求（AA-Request，简称 AAR）消息的 AVP 内，可以通过多个中继、代理发送到 AAA 服务器。服务器处理请求后，会发送 AA 应答（AA-Answer，简称 AAA）消息。应答消息中包含的处理结果代码（Result-Code）AVP 除了指示成功或失败外，还有要求多次认证的 DIAMETER_MULTI_ROUND_AUTH，这时就需要客户端和服务器之间进行多次的 AAR 和 AAA 交互，直到结果指示成功或失败。

跟 RADIUS 不一样，Diameter 支持认证和授权分开进行，也就是说可以先进行认证，然后再发送授权请求。

3、安全协议。Diameter NASREQ 应用中讨论了如何在 Diameter 协议中承载 PPP 认证协议。由于 PAP 存在安全漏洞，所以不鼓励使用 PAP，除非用在一次性密码（One-Time Password）认证的场合[31]。在 Diameter NASREQ 应用中使用 CHAP，主要也是为了和 RADIUS 的兼容。而 EAP（Extensible Authentication Protocol）较之 PAP 和 CHAP 有很多优越性：EAP 可以支持多种认证方案，如智能卡认证、公共密钥、一次性密码等；由于认证是在 EAP 客户端和家乡 AAA 服务器之间进行，EAP 可以实现端到端的认证；端到端的认证也提供了双向认证，而 PAP 和 CHAP 在

漫游环境下是无法实现这一点的。Diameter NAS 应用和 Diameter EAP 应用一起使用，就能很好地满足来自网络接入服务器、漫游操作等对网络接入的安全要求。

4.3 Diameter EAP 应用扩展

EAP(Extensible Authentication Protocol)是一种支持多种认证机制的框架协议。它不但可以支持使用 PPP 拨号接入方式和有线、无线链路接入方式，也可以支持 IKEv2 中的 IPSEC 的远程访问[32]。Diameter EAP 应用扩展可以用在 NAS 和后端认证服务器之间用作 EAP 认证。该应用扩展是基于 Diameter NASREQ 应用扩展基础上发展起来的，并可以应用在 NASREQ 相似的网络中。

1、Diameter EAP 应用扩展命令代码。本应用扩展中定义了两个新的命令代码以用来完成 EAP 认证扩展过程。命令代码为 268 的 DER (Diameter-EAP-Request Diameter EAP 请求)和 DEA (Diameter-EAP-Answer Diameter EAP 请求)，请求和应答消息的不同之处在于命令标识域的 R 比特置 1 或置 0 来判定。

2、Diameter EAP 应用扩展协议过程。当认证的对端或者访问设备通过链路层进行认证的时候，一旦 EAP 认证过程开始启动，访问设备首先就发送一个带有空 EAP-Payload AVP 值的 DER 消息表明认证过程开始。服务器则根据认证过程返回带有不同 EAP-Payload 和 Result-Code AVP 值的 DEA 消息，并根据初始化过程交换的认证信息进行多次往返，并最终完成认证过程。该过程如下图 4-9 所示。

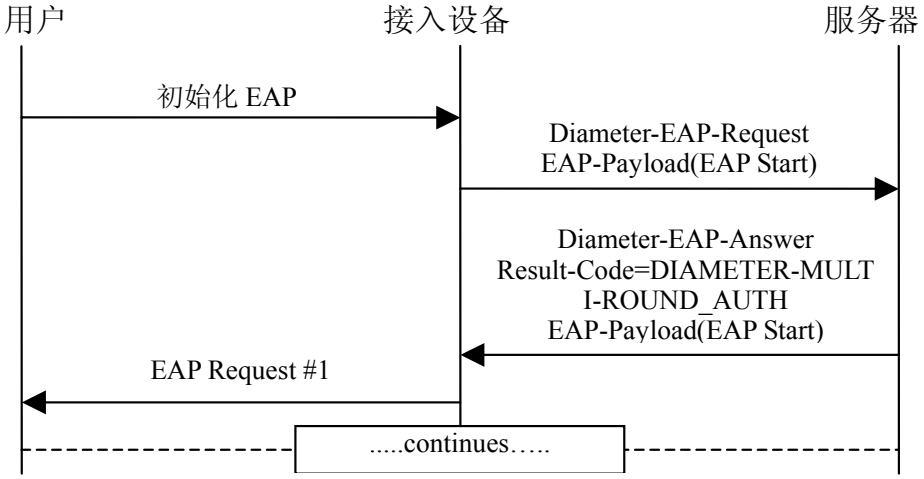


图 4-9 Diameter EAP 基本认证过程

Fig.4-9 Basic pocudure of Diameter EAP

具体来讲，EAP 在链路建立阶段并没有选定某一种特定的认证机制只需说明要使用 EAP 认证即可，而把具体认证过程推迟到后面个独立

的认证阶段。在这一阶段进行认证方式的协商和具体认证过程，并由认证成功与失败的结果来决定是否进入网络层，以使网络层数据能够在链路上进行传输[33]。

4.4 PANA 协议

在某些网络应用之中，一些基于 IP 的设备需要在得到授权访问网络之前进行认证过程。这种认证协议要求多种不同的认证方式、动态的服务、节点的移动性支持。如果没有这种认证协议的存在，则需要在数据链路层加入其他不充分的认证方式以完成这种认证过程。例如，为了满足客户认证的需求而在数据链路层和网络层的增加一个额外的层(如 PPPoE PPP over Ethernet)、或者修改网络层协议(如带有注册请求标识的 Mobile IPv4)甚至通过定义应用层协议来完成这种认证过程(如, 通过基于 WEB 登录的 http 转发)。在这种情况下，IETF 建立了 PANA(Protocol for carrying Authentication for Network Access)工作组，定义 PANA 协议[34]用以完成这种基于 IP 协议的认证过程，并允许客户端同后端 AAA 服务框架进行交互而不需要了解 AAA 协议的细节。

PANA 协议运行在客户端(PAC)和服务器端(PAA)之间以完成网络访问服务过程。该协议是基于 UDP 协议之上的，但拥有完善的重传机制以可靠的传送消息。在该中协议里包含了一系列请求和应答消息，这些请求和应答消息的内容被用在端到端的认证过程，每一个消息都是由零个或多个 AVP 负载来实现的。PANA 的主要负载都是 EAP 消息，用于 PAC 和 PAA 之间建立 EAP 会话。PAC 和 PAA 之间应该是直接连接的，并且两者之间不能有 IP 路由器[35]。

PANA 协议的报头格式如下图 4-10 所示：

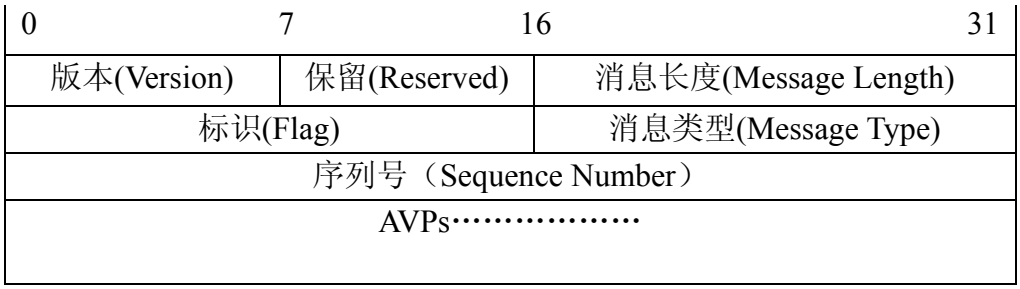


图 4-10 PANA 报头
Fig.4-10 PANA Header

1、版本(Version)：版本号必须被设为 1，以表明该 PANA 消息为第一版。

2、保留(Reserved)：该八位组被保留将来使用，并设为 0。

3、消息长度(Message Length)：该域被用来表明包括报头在内的消

息长度。

4、标识(Flag)：该标识域是两个八位组，其内部比特标识如下图 4-11 所示。

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
R	S	N	r	r	r	r	r	r	r	r	r	r	r	r	r

图 4-11 PANA 报头标识域
Fig.4-11 Flag field in PANA Header

①R 比特：如果该位为 1，则表明是请求。否则该消息为应答。

②S 比特：当该比特在 PANA-Start-Request 消息里置 1，则表明 PAC 要求 NAP(Network Access Provider 网络访问提供者)或 ISP(Internet Service Provider Internet 服务提供者)的认证。当该比特在 PANA-Start-Answer 消息里置 1 的时候，表明接受一个 NAP 或 ISP 的认证过程。

③N 比特：当该比特在 PANA-Auth-Request 消息里置 1，则表明当前 EAP 认证是用于 NAP 认证，否则表明当前 EAP 认证用于 ISP 认证。

④r 比特：该比特是保留域，通常设为 0，并被消息处理机制忽略。

5、消息类型(Message Type)：该域被用来表明通信消息的类型。

6、序列号（Sequence Number）：该域包含一个 32 比特的值。

PANA 协议会话过程包括如下几个阶段：

1、发现和握手阶段。该阶段始化一个新的会话，PAC 通过明确的发送请求通告或接收到通告，PAC 通过应答通告开始会话建立。

2、认证和授权阶段。发现和握手阶段之后开始 PAC 和 PAA 之间的 EAP 过程，EAP 负载用来完成认证过程。在认证完的结束阶段，PAA 向 PAC 传输认证和授权的结果。该阶段可能包括两个过程，分别用来 NAP 和 ISP 之间的认证过程。

3、访问阶段。成功的认证和授权之后，主机便可以通过 EP(Enforcement Provider 执行点)进行基于 IP 包的通信。该阶段的任何时间，PAC 和 PAA 之间都可以相互通过 ping 来验证会话的有效性。

4、重新认证阶段。当会话时间用完而终止的时候可以由 PAC 和 PAA 任何一端发起重新认证。

5、终止阶段。PAC 和 PAA 可以在任何时刻决定终止该过程。也可以由任何一方发送终止消息。但这种终止不一定要求 PCA 和 PAA 的参于，会话时间终止和会话可用性测试的失败，都可会导致终止阶段的发生。

第五章 Diameter MIPv6 应用扩展框架设计

移动 IP 定义一种允许移动节点改变其在 INTERNET 上接入点并具有最小服务中断的方法。移动 IP 本身并不对跨管理域移动性提供任何特定支持，因此限制了移动 IP 在大规模商业部署的可用性。

AAA 协议的 Diameter 协议正好允许移动用户可以在不同的服务提代商之间漫游并得到服务，而不是被限定在家乡服务提供商。对于部署在商业网络中的移动 IP，都应该支持 AAA 认证协议。Diameter 协议的 MIPv4 扩展已经说明允许移动 IPv4 节点从（家乡或外地）服务提供商那里接收服务并且允许 Diameter 服务器提供认证、授权和从 MIPv4 节点收集计费信息。

虽然从较高层次上看 MIPv4 和 MIPv6 是相似的，但事实上在考虑到内部域部署的时候有很大的不同。例如 MIPv6 没有等价于 MIPv4 的外地代理，并由此无法定义任何机制通过外地代理访问网络以及认证、授权访问网络资源。此外，扩展 Diameter MIPv4 协议用来支持 MIPv6 将减弱灵活性并导致一些 AAA 能力交换的问题：很难区分哪个 AAA 节点只支持 MIPv4，哪个节点仅支持 MIPv6 以及哪个节点支持两者[36]。因此，本章为移动 IPv6 和 AAA 的交互作用提供了一个解决方案，支持一个 IPv6 节点在不同的管理域之间漫游。

5.1 模型和假定

移动 IPv6 在 Diameter 协议中基本 AAA 过程如下图 5-1 所示。

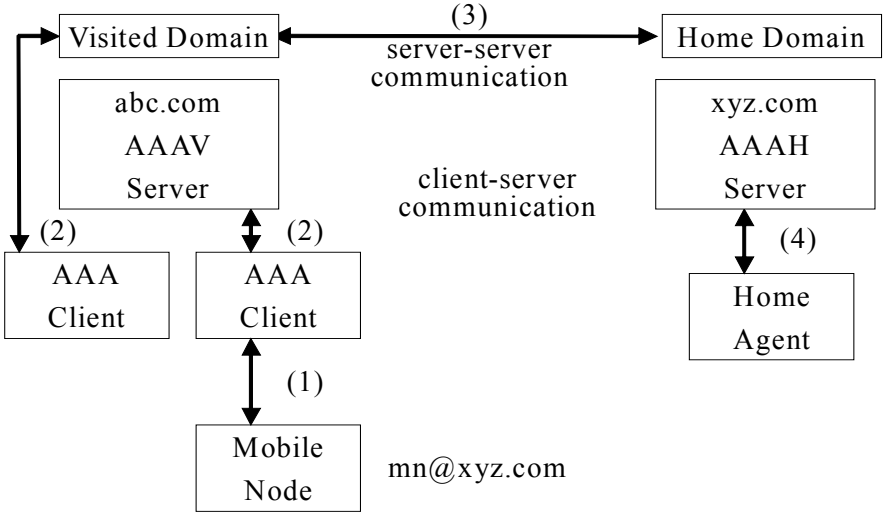


图 5-1 Diameter MIPV6 应用体系结构

Fig.5-1 Dimaeter MIPV6 application infrastructure

1、AAA 客户端：它的功能是允许 MN(Mobile Node)注册并被网络服务提供商所认证，通过提供标识和授权信息给本地网络，本地网络用 AAA 机制去验证用户，为网络的使用产生记费数据并授权资源的使用。除了认证和授权，MN 可能提供 AAA 客户端同移动性管理信息（如内含的绑定更新）以完成移动 IP 过程。AAA 客户端可以成为一个服务员，如存在于一个访问路由器里或 UNAP 中的 AA 代理（认证或授权代理）的标识。

2、AAAV：是一个被访问网络的 AAA 服务器

3、AAAH：是 MN 家乡网络的 AAA 服务器

4、HA：是一个家乡代理

本文提出的框架结构及实现中基于如下三个基本假定：

1、各网络节点都是使用 NAI 进行标识的，NAI 是形如 user@realm 用于 Diameter 协议析取一个用户的标识和域。该标识 user 可以在认证、授权的时候用来标识用户，在 NAI 字符串中紧跟在‘@’字符后的部分的 realm 域用于消息的路由目的。NAI 域的名字要求是唯一的，并且是在 DNS 名字空间里被管理的[37]。当移动节点没有 NAI 但只有一个家乡地址，移动节点也可以使用 IPv6 家乡地址从 AAA 基础设施处得到认证和授权。

2、移动节点和一个 AAA 家乡服务器共享一个长时间的密钥。这个长期密钥提供网络认证和用户认证，它可能也被用来引申出会话密钥或本地安全关联。

3、在被访问的 AAA 服务器和家乡 AAA 服务器之间的通信是安全的。这个内部 AAA 安全关系允许家乡和被访问域相互信任，并且在认证和保护的方式交互。这种内部的安全关系可以通过 TLS 的证书双向身份认证过程保证。

5.2 Diameter MIPv6 应用扩展的消息设计

Diameter 协议的应用扩展是通过定义新的消息和新的 AVP 负载值来完成的，在 MIPv6 环境下，现定义四个新的 Diamter 消息是用于 MIPv6 的 AAA 过程：(AA-Registration-Request, AA-Registration- Answer ,Home-Agent-MIPv6-Request,Home-Agent-MIPv6-Answer)和 AVPs (MIP-Binding-Update AVP,MIP-Binding-acknowledgement AVP, MIPv6-Mobile-Node-Address AVP, MIPv6- Home-Agent-Address AVP, MIPv6-Feature-Vector AVP, Key-Request AVP, MN-Key-Distribution AVP,Key-Distribu -tion AVP)以完成先前所确定的功能

1、命令代码：按照 RFC3588 定义的命令代码的定义规范，这些命

令代码（24 比特的地址空间）的标准化工作是由 IANA 进行分配的，因此在本文中参照 Diameter MIPv4 应用中的命令代码 AMR/AMA（260），HAR/HAA（262）[38]给本文定义的 ARR/ARA 和 HOR/HOA 消息对分别指派命令代码值用于实验。

* AA-Registration-Request Command (ARR) (Code 660)
* AA-Registration-Answer Command (ARA) (Code 660)
* Home-Agent-MIPv6-Request Command (HOR) (Code 662)
* Home-Agent-MIPv6-Answer Command (HOA) (Code 662)

2、AVPs。AVP 的代码值也是由 IANA 进行分配的，在本文中直接指派命令代码用于实验的目的。这些代码值并未得到 IANA 的认可，因此我们选用较大的值以免同现有的 AVP 值冲突。

①MIP-Binding-Update AVP：MIP-Binding-Update AVP (AVP Code 6001)是一个八位组字符串类型并且包含了移动 IP 的绑定更新消息。

② MIP-Binding-acknowledgement AVP ： MIP-Binding-acknowledgement AVP (AVP Code 6002)是一种八位组字符串类型并且包含了由家乡代理发送给移动节点的移动 IP 绑定确认消息。

③ MIPv6-Mobile-Node-Address AVP ： Mobile-Node-Address AVP (AVP Code 6003)是一个 IP 地址类型并且包含了移动节点的家乡地址。

④ MIPv6-Home-Agent-Address AVP ： Home-Agent-Address AVP (AVP Code 6004)是一个 IP 地址类型并且包含了移动节点的家乡代理地址。

⑤MIPv6-Feature-Vector AVP：MIPv6-Feature-Vector AVP (AVP Code 6005)是一个无符号 32 类型并且允许家乡域的动态家乡代理分配。

⑥Security Key AVPs：通过该 AVPs 的建立，AAA 服务器能扮演一个密钥分发的角色并且能利用他自身的属性和特征使用很多加密解密方式。

5.3 移动节点和 AAA Client 之间的信息交换

移动节点和 AAA Client 之间的信息交换不是 Diameter 协议内定义。在本文中，将 PANA 协议与 Diameter 协议结合起来，完成移动节点 MN 与 AAA Client 之间信息交换过程。PANA 协议提供了一种完整的基于 IP 的安全认证数据传输过程，移动节点 MN 和 AAA Client 分别作为 PANA 协议体系中的网络实体 PAC 和 PAA，同时，AAA Client 还作为 Diameter 协议体系结构中 AAA 客户端同 AAA 服务器端进行通讯，如下图 5-2 如示。

在该图中可以看出，AAA Client 网络实体应该兼具有一个网络接入

服务器形式存在的，并可以处理路由功能，因此，它或它管理的路由功能部分必须不断的发送路由通告，以告知所接入的节点本网络域的网络前缀。近一步说，路由通告部分功能应该由移动 IPv6 协议栈完成。

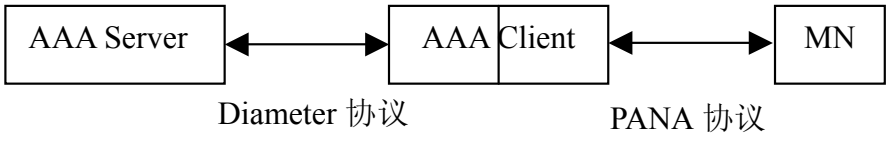
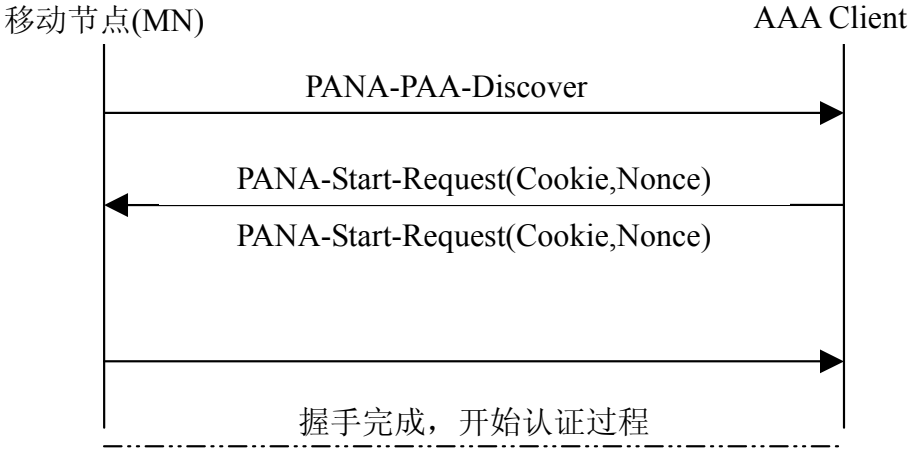


图 5-2 AAA Client 功能结构
Fig.5-2 AAA Client function structure

移动节点不断的监听路由通告，当移动节点移动到外地域的时候，通过外地 AAA Client 的路由通告发现自己是否已经改变了位置，如果发现移动到外地网络的路由通告，则开始初始化 PANA 认证过程。该过程首先应该完成 PANA 的发现过程，移动节点通过向一个多播地址的特定端口(自定义)或者特定 IP 地址的 UDP 端口(自定义)发送 PANA-PAA-Discover 消息完成发现过程。当完成发现过程之后，可以由移动节点或者 AAA Client 首先发起握手和认证、授权过程。

在移动节点和 AAA Client 之间进行握手的过程中，在交互的消息中包含了 Cookie 值 ，该值中包含了移动节点 MN 的基本信息和产生的随机数以确保安全。两端进行认证、授权过程中，使用 EAP 加密机制保证交互过程的安全。由移动节点发起的握手和认证过程的消息交互过程如上图 5-3 所示。



1.Cookie=<secret-version>|HMAC_SHA1(<Device-Id of PaC>,<secret>)
2.Nonce 随机数：用来建立 MN 和 AAA Client 之间的安全并联

图 5-3 移动节点与 AAA 客户端握手过程
Fig.5-3 The procedure of handshake between MN and AAA Client

当 AAA Client 通过基本握手过程之后，AAA Client 通过安全的方

式已经得到 MN 的基本认证数，则将 AAA Client 将这些数据通过 Diameter 所定义的认证请求/应答消息与 AAA Server 进行通讯，由 AAA Server 根据认证数据进行认证，并根据得到的认证结果决定是否允许移动节点 MN 的接入。

在该过程中的包含的主要数据类型值有如下几种：

1、MIP 特征数据。同移动 IPv4 相反，IPv4 在家乡或被访问网络里移动节点发送一个带有特定 IP 地址值的注册请求以请求分配一个动态的家乡代理。IPv6 移动节点应该使用一些 MIP 的特征数据，其内容包括 MIPv6 特征向量（MIPv6 Feature Vector）AVP 的信息：IPv6 移动节点将不使用特殊的 IPv6 地址值，而使用标识（FLAG），并且这将有效的减少访问的数据链路上数据发送量。此外，服务员程序只需要封装相应的 MIPv6-Feature-Vector AVP 里的数据即可。

2、EAP 数据。IPv6 移动节点应该能够使用不同的认证方式，如不同的 EAP 类型。EAP 数据使用由 PANA 协议进行传输。

3、安全密钥数据。移动节点需要使用密钥请求来表明需要的密钥及产生这些密钥的方式。这些安全密钥数据应该包括相关信息以让 AAA 客户端创建相应的安全密钥 AVPs.(Security Keys AVPs)。

4、内嵌数据。内嵌数据使移动节点能够在得到网络的认证和授权的时候发送一个绑定更新（例如：通过 PANA 协议所提供的能力），因而节省了在家乡和被访问域的多次往返。

5.4 协议的基本功能设计

在访问网络前，被访问网络希望认证该用户，IPv6 移动节点将也想对网络进行认证，以避免进入非法网络，以造成 false BTS 攻击。IPv6 移动节点应该有能力使用许多不同的认证方式，IPv6 移动节点能够使用如 EAP 这样的第三层认证。因此，除了最基本的为了给一个移动节点访问网络资源能力而提供的对移动节点进行的认证和授权过程，还有如下基本功能需要在扩展协议中实现。

1、动态家乡代理分配。当移动节点需要向家乡代理发送一个绑定更新注册新的主转交地址的时候，移动节点可能不知道它的家乡链路里可以作为家乡代理的任何路由器的地址。因此，必须有一些不同的路由器来代替以前的移动节点完成动态家乡代理分配特性。本文中，取代以前那种发送特定的 IP 地址给请求家乡地址/家乡代理的请求的方案，在家乡（被访问）域，是基于标识进行处理的。因此只需要通过访问链路发送最少的数据，并且在指派家乡代理的时候由 AAAH（AAAV）来创建绑定更新消息。

2、安全关联的动态建立。在移动节点和家乡代理之间的安全关联，用来认证绑定更新和确认消息。在动态家乡代理地址发现完成之后，移动节点发送一个绑定更新给选定的家乡代理，以在路由表里建立一个为家乡地址同 MN 相关联的转发条目。

3、密钥分发过程。该项功能不是必须在存的，但是在认证和授权的步骤完成之后，AAA 服务可以扮演一个密钥生成和（或）密钥分发的角色。Diameter MIPv4 应用定义了一个密钥分发机制，对于 MIPv6，也同样可能用多种方案可供选择。

4、绑定更新的最优化。除了认证、授权和密钥分发功能，AAA 服务还能完成移动性过程，如动态的家乡代理分配。万一 IPv6 移动节点已经有一个前提配置的家乡代理，一些优化过程也可以通过移动节点在 AAA 请求消息里封装绑定更新给它的家乡代理的过程中处理。

5.4.1 协议信息流及各实体的基本操作

在本文中，移动节点 MN 同 AAA Client 之间的通信过程是由采用 PANA 协议完成的，两者之间的通信过程已经在 5.3 节定义。本节介绍 AAAV Server、AAAH Server、Home Agent 等网络实体的基本信息流和操作。移动节点 MN 移动到外地域时进行的消息流过程如下图 5-4 所示。

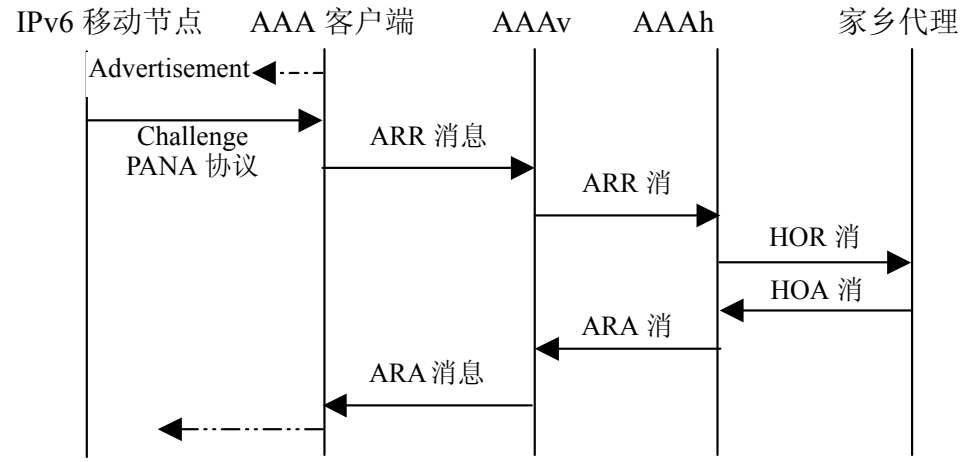


图 5-4 基本认证过程的消息流

Fig.5-4 The message stream of basic authentication procudure

1、被访问服务器(AAAV)的操作。当 AAAV 收到一个 ARR 消息时，首先被访问 AAA 服务器核实消息是否来自一个合法的 AAA 客房端，然后检查 MIPv6 特征向量 AVP，然后将它发送给 MN 的家乡 AAA 服务器。

当从家乡 AAA 服务器收到一个 ARA 消息时，被访问服务器可能

有选择的根据特定 EAP 所说明的行为规范或其他机构定义的机制将包含在从家乡 AAA 服务器发送的消息里的 AVP 内含的本地信息（举例来说：会话密钥等）发送该消息给 AAA 客房端。

2、家乡服务器(AAAH)的操作。当从 AAAV 收到一个 ARR 消息后，AAAH 首先核实消息是否来自一个合法的 AAAV。在 AAA 服务器之间的安全由 IPSec 和 TLS 来保护，AAAV 和 AAAH 之间的相互认证是通过 X.509 证书完成，证书的分发应该由权威的 CA 认证机制来完成，并保护证书的合法性与完整性。AAAH 接下来使用 NAI 认证用户，该 NAI 是由 MN 提供用来做为 MN 标识的。如果移动节点被成功认证则：

①AAAH 也基于主机挑战和根据部署的认证算法信息计算一些网络认证数据。根据认证方法需求，AAAH 可能经过 AAAV 同 MN 进行多次消息交换（如对于一个用户认证机制，要求更多的往返过程）：AAAH 可以发送一个 ARA 命令并带有合适的认证信息和指令。它可以被 AAA 客户端转变为 EAP 数据并且通过 PANA 协议传送给 MN。消息往返的次数依赖与认证机制的使用。

②如果 MN 请求一些安全密钥，AAAH 完成适当的步骤并最终发送相应的消息并完成密钥分发。

③如果一个 MIPv6-Home-Agent-Address AVP 存在：AAAH 检查该地址和可用家乡代理，并确定移动节点被允许请求 AAAH，然后发送 MIP-Home-Binding-Update AVP 给家乡代理，该 AVP 被包含在（Home-Agent-MIP-Request）消息。

④如果不存在 MIPv6-Home-Agent-Address AVP，AAAH 考虑是否存在 MIPv6-Feature-Vector AVP，如果存在，AAAH 在家乡网络完成动态的家乡代理分配

⑤如果 MN 发送了一个内嵌的绑定更新或一个 HA 请求，AAAH 接下来将发送一个 ARA 消息给 AAAV，该消息里包括了 MIP-binding-Acknowledgement AVP。

3、家乡代理的操作。当收到一个 HOR 消息的时候，HA 首先处理 Diameter 消息。如果 HOR 是非法的，那么将返回一个带有结果代码 AVP 的值设为 DIAMETER_ERROR_BAD_HOR 的 HOA 消息。否则，家乡代理处理 MIP-Binding-update AVP 并建立绑定确认，并使用 MIP-Binding-Acknowledgement AVP 封闭它。HA 也建立绑定缓存并根据收到的数据计算用于 MN 之间的安全关联的密钥。

5.5 协议的增强功能设计

除了前面描述的基本功能，AAA 框架可以支持更多的特征以支持

IPv6 的移动节点的域内漫游，因此提供了更具灵活性并允许新的选项以提供开发商业模型服务。

一个 IPv6 移动节点可以有一个提前配置的家乡地址，也可能提前配置家乡代理或自动请求地址。移动 IPv6 Diameter 应用的基本特征允许认证和绑定更新的优化，在家乡域的可选择的家乡代理分配和密钥分配过程。

协议的增强特征主要包括如下两种：

1、被访问域的动态家乡代理/家乡地址分配。

2、家乡域的动态家乡地址分配。

5.5.1 增强特性

1、被访问域的动态家乡代理/家乡地址分配。被访问域的动态家乡代理分配允许更灵活的机制并允许新的商业场景。例如，服务提供者可能仅仅属于一个以计费为目的的 AAA 服务器，并且由于存在漫游协议，它可能要求给它的用户提供移动 IP 服务。在这种情况下，当 CN 需要联系 MN 时，将使用一个应用层的标识（如 MN、SIP、URL），并且 CN 并不需要知道 MN 的家乡地址。它可以支持在初始化联接点（也就是当 MN 节点在外地址重启时）和外地域的联接点之间支持移动性。

2、家乡域的动态家乡地址分配。移动节点可能不总有一个提前配置的 IPv6 地址，并且可能需要有一个动态分配过程。此外，家乡代理和移动节点家乡地址需要在相同的链路上，以支持被访问域的动态的家乡代理分配和被访问域的动态家乡地址分配。最终，这个动态家乡地址特征提供了更多的灵活性，即使当家乡代理是在家乡网络中被分配的，既然家乡代理和家乡地址应该是在同一子网的。

3、增强 AVPs MIPv6-Feature-Vector AVP。除了在前面 5.2 节所描述的新的命令代码和 AVPS，还需要定义新的 AVP 以支持增强的特征。在这个扩展模式下，在被访问网络中的动态家乡代理分配是可行，因此定义了附加的标识 MIPv6-Feature-Vector AVP。

下列标识允许 AAAV 通告它的能力。如果家乡代理是被分配在被访问网络，家乡地址必然也被分配在被访问网络。

AAA 客房端在 ARR 消息里封装一个 MIPv6-Feature-Vector AVP，如果 MN 发送一些 MIP 特征数据的时候，并直接发送给 AAAV。

标识值定义如下：

1 Home-Agent-Requested（家乡代理请求）:当移动节点请求分配一个动态家乡代理时，该标识被设为 1。当该标识被设为 1 的时候，MN 和 HA 之间共享一个动态会话密钥，以用来认证从 MN 到 HA 之间的绑

定更新。MN 通过一些安全密钥请求表明他支持什么样的计算方法；或一个 MN 和 AAAH 之间都知道的已经存在的默认的方法。（如在 MN 和服务提供商签约时提前设定的）

2　Mobile-Node-Home-Address-Requested flag:如果移动节点没有任何家乡地址和请求，则该标识被设为 1。默认值为 0。

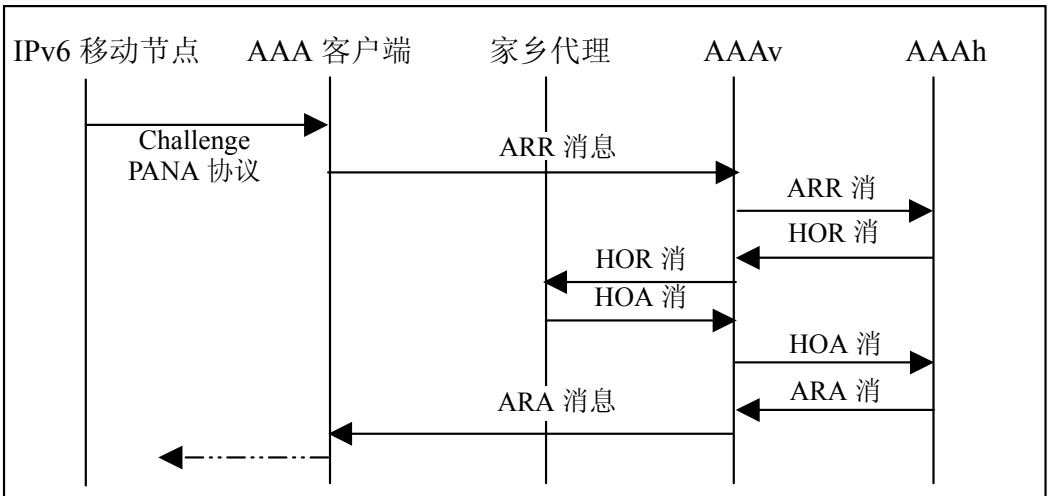
4　Home-Address-Allocatable-Only-in-Home-Domain flag（仅在家乡域分配家乡地址标识）:如果移动节点请求一个家乡地址并且希望由他的家乡网络进行分配。默认值是 0，并且表示不指定 MN 对于在家乡域或被访问域分配家乡地址。

8　Home-Agent-in-Visited-Domain flag（被访问域的家乡代理标识）:该标识被设为 1 的时候表明移动节点希望在被访问域得到它的家乡代理。

16　Visited-Home-Agent-Available flag（被访问家乡代理可用标识）:如果 MN 请求一个被访问域的动态家乡代理分配并且被访问域也同意分配一个给 MN，则该标识设为 1。

5.5.2　在被访问网络域分配家乡代理

在被访问网络域分配家乡代理。如果 AAAH 接受被访问域的分配的 HA，将发生如下图 5-5 所示的消息交换过程：



注：AAAH 服务器在发送给 AAAV 服务器 HOR 消息的时候，不能带有任何 Mipv6-Moblie-Node-Address AVP 和 Mipv6-Home-Agent-Address AVP。

图 5-5 被访问网络域分配家乡代理的消息流

Fig.5-5 The message stream of distributing home agent in visited network field

①AAAV 可能为 HA 发送一些安全密钥原料用来从中引申出来密钥，以建立在 MN 和家乡代理之间的安全关联，并依赖密钥分配机制来

认证未来的绑定更新。

②AAAH 可能也可能根据 MN 的请求发送其他密钥原料。AAAV 分配一个家乡代理、建立并发送一个最新创建的绑定并封闭在 HOR 消息里。

AAAV 可能为 MN 分配家乡 IP 地址并通过在 HOR 消息里增加 MIPv6-Mobile-Node-Address AVP 通知家乡代理；或者让家乡代理分配家乡地址并不在 HOR 消息里提供 MIPv6-Mobile-Node- Address AVP。

AAAV 可能根据采纳的密钥分发机制建立在 MN 和家乡代理之间的安全关联，并发送给家乡代理一些密钥原料。

③如果为 MN 请求并建立一个绑定缓存，家乡代理分配一个家乡 IP 地址

家乡代理根据可用的机制建立安全关联

家乡代理建立绑定确认并封装发送给 MN。

家乡代理发送回一个 HOA 给 AAAV 以通知状态：它包括移动节点的家乡地址（如果家乡代理分配了）；它也包括由家乡代理建立的绑定确认并封装发送给 MN。

④AAAH 通告家乡 IP 地址（包含在 MIPv6-Mobile-Node- Address AVP 中）和家乡代理地址（包含在 MIPv6-Home-Agent- Address AVP），并包含在 HOA 消息里从 AAAV 发送。

⑤AAAH 发送给 AAAV 一个 ARA 消息，携带家乡 IP 地址、家乡代理 IP 地址和带有上这信息的密钥原料

5.5.3 密钥分配

根据以前章节里的定义，很多安全密钥需要建立。并且在 IPv6 移动节点和其他网络实之间共享，例如：

在移动节点和他的家乡之间的密钥，用来认证绑定更新和绑定确认消息。

在移动节点和访问路由器之间的密钥用来保护（例如机密性和完整性保护）访问链路上的数据安全。

AAA 实体可以在计算中完成一个主要角色并分配这些安全密钥。基于 AAA 框架并允许认证密钥分配已经提出了两种密钥分配方法。

1、基于随机数的密钥分配。家乡 AAA 服务器给每一个请求密钥者生产一个随机数。然后做为一个同移动节点共享的密钥算法输入数据，连同这个随机数、同移动节点之间长期密钥共享和非强制性的其他数据，家乡 AAA 服务产生出希望得到的安全密钥。

这个密钥被安全的传输给移动节点希望共享密钥的网络实体。并且

随机数被发送给移动节点，移动节点可以根据它与家乡网络共享的长期密钥和密钥生成算法产生安全会话密钥。

这种基于随机数的密钥分配当前被用在蜂窝网络和 DIAMETER MIPv4 应用中。

2、基于 Diffie-Hellman 密钥分配。Diffie-hellman 算法[39]是第一个公开密钥算法，其安全性源于在有限域上计算离散对数比计算指数更为困难。该算法可以使两个用户之间安全的交换一个密钥，但不能用于加密或解密信息[40]。首先，通信双方 *A* 和 *B* 协商一个大的素数 *n* 和 *g*，*g* 是模 *n* 的本原元，这两个数不必是秘密的。故 *A* 和 *B* 可以通过不安全的途径协商它们，它们也可以在一组用户中公用。作为另一种选择，密钥分配也可以基于 Diffie-Hellman 机制。Diffie-Hellman 允许两个节点在一个安全的方式建立共享密钥。虽然它有一个主要的弱点，它不允许一个节点计算出同它正在建立的安全密钥。为了克服这个弱点，两个节点的公共密钥值必须被认证。

AAA 框架和许多安全关联，如移动节点和他的家乡网络（AAAH）之间、AAAV 和 AAAH 之间的安全关联都可以提供认证。

如果移动节点希望同一个在访问域的实现建立一个安全关联（例如：在被访问域分配的家乡代理），移动节点首先发送他的公共 Diffie-Hellman 值 DH_MN，并由他的家乡代理根据长期共享关联鉴别。如果 MN 希望建立一个安全关联的网络实体是在被访问域的，AAAV 恢复实体的 Diffie-Hellman 公共值并发送给，该公共值是使用外部域安全机制并根据 AAAV 同 AAAH 之间共享的安全关联来鉴别的，该值将连同从 MN 发向家乡网络的其他消息一起发送。

AAAH 认证实体和 MN 的 Diffie-Hellman 公共值。它可以使用安全关联发送 MN 的 Diffie-Hellman 公共值给 AAAV，并发送实体的 Diffie-Hellman 公共值给 MN，并通过同 MN 之间共享的安全关联鉴别。

在这种方法下，AAAH 被用来鉴别 Diffie-Hellman 公共值，但作为与以前方法不同的地方，AAAH 本身没有密钥值的相关知识，他不能产生会话密钥的值。这种方法允许安全的分配安全密钥，而不需要 AAA 服务这些密钥的值。AAA 服务器可以提供证书鉴别机制。

第六章　Diameter MIPv6 应用扩展的实现

Diameter MIPv6 应用扩展的实现是基于 Diameter 基础协议实现的基础之上，根据 Diameter MIPv6 应用扩展协议设计的消息流及扩展的 Diameter 消息完成 IPv6 移动节点接入外地网络域的认证和授权过程。当移动节点已经完成外地网络域的接入过程之后，AAA Client 收集接入网络节点接入网络使用资源的情况，并定时向被访问网络域 AAA 服务器发送计费信息。

本文的 Diameter 基础协议的实现是采用 OpenDiameter 开源软件包，该软件包采用了 C++编写，并充分利用了已经有的标准 C++类库，如 ACE(Adaptive Communication Environment)、BOOST、OPENSSL 等，借用了这些类库的成熟经验，提高了 OpenDiameter 开源软件包的开发速度与可靠性、稳定性。

我们在本章首先介绍 OpenDiameter 软件包的体系结构及相关类库，然后给出 Diameter MIPv6 应用扩展的 API 的详细设计。

6.1　OpenDiameter 软件体系结构

该 OpenDiameter 的软件架构实现借鉴了很多由 ACE 开发的设计模式。特别是，SOCKET 接受者，连接者和线程池模式都得到了应用。除了基于模式的 ACE，由 ACE 库提供的 OS 抽象层也被大量利用在该实现中。该软件已经注意尽力使实现是独立于平台的。所有的系统调用都是通过利用 ACE 提供的抽象来使用的。另外，所有的系统调用并没有被基于 ACE OS 的抽象层所掩盖，而尽可能的使之与 POSIX(Portable Operation System Interface for Computing System)适应。由于 ACE 的全面使用，OPEN DIAMETER 库的支持平台同 ACE 的支持平台是相同的[41]。

6.1.1　模块和库

当前的 OpenDiameter 软件被分为四个逻辑模块。一个应用核心，一个会话管理模块，一个传输管理模块和一个消息解析模块。前三个模块组成了 Diameter 基础协议的引擎并被包含在一个独立的库里(libdiameter)。消息解析模块则被作为一个单立的库来实现的(libdiamparser)，以致于它可以被应用程序用来利用 AAA 服务来同使用 Diameter 消息模式的 OpenDiameter 程序进行通信。这两个库是用 C++

写的，并提供 Diameter C++ API 以提供实现 Diameter 基础协议的功能。

如图 6-1 所示，Diameter 消息解析库(libdiamparser)被作为一个独立的库来实现的，并没有混同在 Diameter 基础协议引擎库(libdiameter)里。这两个库对所有使用它们的客户和服务器的认证应用都公用的。

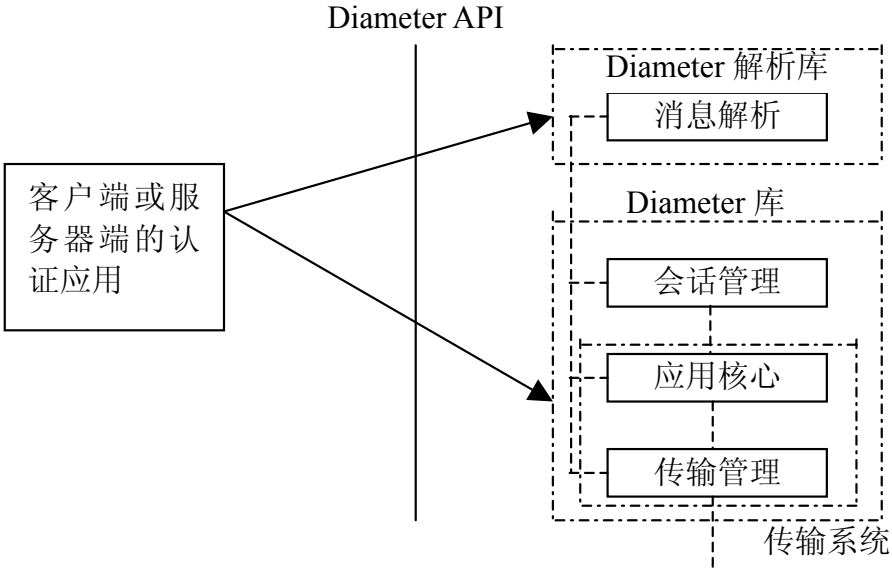


图 6-1 Diameter 类库模块
Fig.6-1 The modules of Diameter Library

1、应用核心。应用核心对所有的全局数据和整个 Diameter 库服务的初始化和终止起到一个中心存储的功能。对于每一个希望使用这些库的应用来说，必须创建一个应用实例。这是来自于 Diameter API 草案的设计。一个应用核心是一个基于内存的‘堆’，那么就存在当特定情况下在一个程序里建多个应用核心的可能性。然而，根据 OpenDiameter 软件开发组织的建议给每个软件程序只建立一个应用核心，因为它们有可能会在传输层争用每个应用核心都需要监听的端口。

2、传输管理。传输管理是应用核心的一个完整的伙伴。它的功能是用来保持同其他 Diameter 对端的连接状态(包括发现)以及路由和传送 Diameter 消息、本地 Diameter 消息的传送，也就是那些本地会话，传输管理模块传送消息给它的会话管理模块。

由于 ACE 通信接收器/连接器模式的引入，传输管理的实现围绕着 ACE 服务处理类来考虑。应用核心里存在一个工厂，并且因此 ACE 的接收器和连接器实际上是在该工厂里进行服务的。一个单独的类作为软件管理模块的初始者和终止者。如图 6-1 所示，在使用 Diameter 库的时候，应用核心要求传输管理模块的存在，无论什么类型的应用使用该库都是如此。

3、会话管理。会话管理模块的主要功能是为使用 Diameter 库的客户/服务认证应用存储和保持 Diameter 会话。使用红黑树做为一个通过会话 ID 存储会话键值的数据库。每一个会话存储当状会话状态，会话时间和其他会话的相关信息。既然一个应用是同 Diameter 库通过会话相关联的，Diameter API 草案指出了处理会话 时候必须的功能。它也通过一个已经存在的会话，从一个应用传送的消息相关，因此应用每产生一个消息都将同会话是相关的。

4、消息解析。消息解析模块是用来解析包括头和栽荷的消息，栽荷部分包括 Diameter AVP。在消息解析模块里，在初始阶段所有已知的 AVP 和命令代码都被装载到内存里，方法是通过字典文件构造一个运行时字典数据库。这些字典文件，就象配置文件，都是基于 XML 的。Apache 的 Xerces C++ XML 库是用来解析字典文件的。它是一个开放源代码的库，并在 Apache 的 WEB 服务环境里得到广泛使用。字典的可扩展性将由 XML 的使用来提供。不管是不是服务于一个线程环境，运行时字典数据的互斥的保护并不是必须的，因此所有对运行时字典数据库进行访问的时候都是只读的。

6.1.2 体系结构的线程视图

整个 OPEN DIAMETER 实现的体系结构的线程图如下图 6-2 所示。

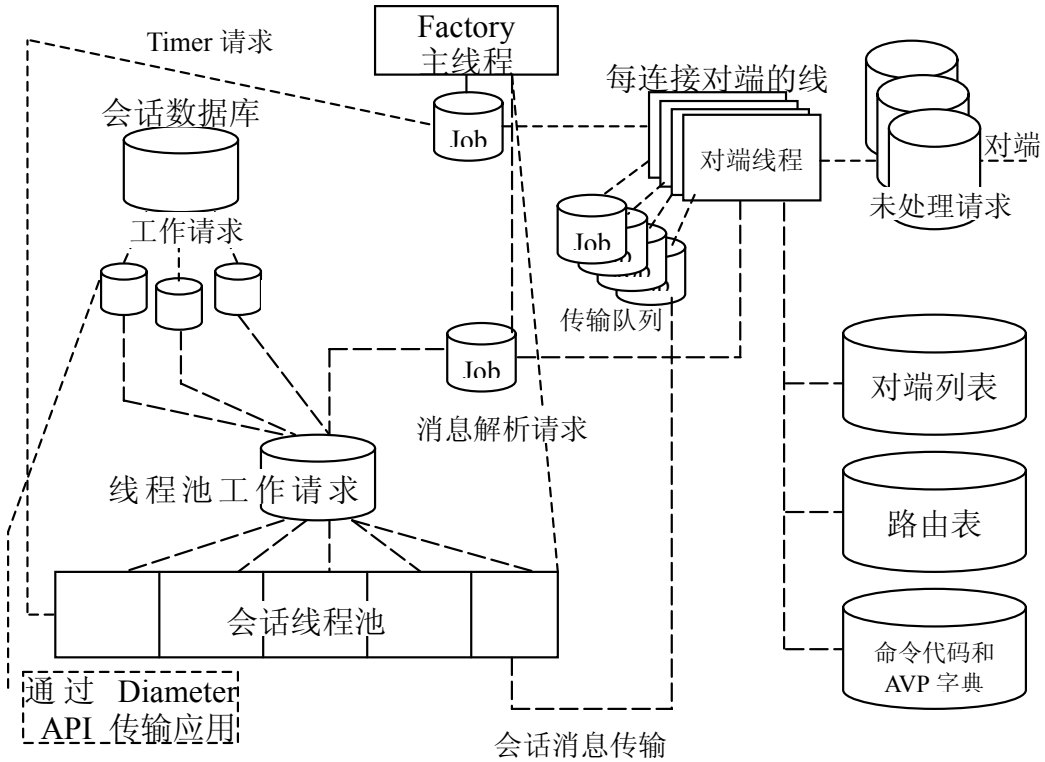


图 6-2 Open Diameter 体系结构的线程

Fig.6-2 Thread of system structure of Open Diameter

如图 6-2 所示，Diameter 协议函数的执行是通过多线程来提供的。线程的处理是基于 ACE 线程实现的。实现中的组件之间的内容和序列的发生是通过使用被保护的队列来实现的。线程里的队列和锁(提供保护)也是基于 ACE 的。

从图 6-2 可知，Diameter 程序里存在线程，每一个这些线程都是基于 ACE 线程/任务类的，它不但提供了平台抽象的线程并且是一个严格定义了实现模块边界的设计模式。在每一个线程里，一个保护消息队列允许线程相互传送预先形成的消息。为了实现 Diameter 协议，队列被称为工作队列。

1、主线程。一个主线程的存在是为了协调程序里的其他线程，主线程，也被看作工厂，其责任是为每一个活动的对端连接产生一个线程(为连接或接受通信请求)。它负责发起并监视一个本地异步连接请求，也接受远程连接请求。当这些请求中任何一个成功的话，主线程而为最新建立的连接产生一个线程并将连接的所有者传送给新线程。为这些特定通信模式使用 ACE 的一个好处是下层的通信传输是是独立于模式的。线程产生的行为都是基于成功的连接之后的，而确保了无论底层传输是使用 TCP 还是 SCTP 都是一致的。

工厂也还有一个维持已经存的线程池的责任，这个线程池是用来执行会话管理中的负载平衡的。此外，工厂也给所有需要内部时钟的提供了全局的记时服务。所有的记时器请求都是基于该服务回应的，并且这些全局的记时器在主线程的上下文里的运行。

2、对端连接线程。工厂产生一个线程来处理每一个成功的对端连接。对端线程的处理是依赖与对端状态机，以发送或接受 Diameter 消息去往其他对端(传送)或者本地处理(会话管理)，维护对端表和其他为建立 Diameter 对端连接所必需的功能。

在 libdiameter 里，使用一个单独的类(AAAPeerService)是服务于传输管理是中的发起和终止的需求。在这个独立的类里，对端表是用来检查看是否一个连接到本地配置的对端并尝试启动。一旦有这种操作，则由主线程来发起一个异步连接到对端。这些未处理的连接由主线程来监视他的成功或失败。如果成功，一个对端线程被产生并且该最新建的连接的所有者也被传送给该线程。此外，该独立的类也包含对于每一个线程请求都是全局的易访问的被保护的数据库，例如路由表和对端表。

对于接入的连接，主线程一直监听众所周知的 Diameter 端口以等待连接请求。一旦收到一个连接请求，则立即产生一个对端线程。不管怎么样，连接或接受，对端线程的设计模式都是相同的。一个已经建立的连接需要在该线程里进行服务。Diameter 对端状态机，独立于设计模式，指示了执行线程根据是否连接或接受请求所做出的行为。例如，如果接

受了请求，状态要求等待一个完全的 CER 消息的到达，然再决定是否接受对端。如果接受了，则对端线程将该新的对端做为一个动态条目加入到对端表里。对于连接的对端，则在状态机开始的时候需要发送一个 CER 消息。

3、线程池。线程池设计模式的存是为了给会话管理中负载平衡提供便利的。Diameter 协议行为在对端任务之上的所有要求都在该池中通过线程来完成。该线程池是一些线程集合而成的用以持续监视一个工作请求队列。工作请求队列是有互斥锁保护的，同一时间只能有一个线程的一个条目出队。该条目里包括了特定的工作指令以及数据，也就是解析过的消息，查找一个会话并切换状态机，呼叫用户同意等。发送一个指令并携带与之相关的数据的能力通过这个队列分配一个待处理工作给下一个可用的空闲线程运行的机会。并行负载平衡是公平的，先到先服务的并且是基于互斥锁来完成的。

6.1.3 基本消息处理

本节描述了进入和输出的消息是如何被传输管理和会话管理进行处理以及消息解析的，并提供更细节的 OpenDiameter 软件体系结构。

1、消息的传输和会话的处理。一个从远程对端接入的消息最初收到和处理是通过传输管理里的一个为远程对端服务的对端线程进行的。一旦完全收到，传输管理可以部分的解析消息头和部分消息体，以决定是否需要转发。如果消息是发给其他远程主机的，消息被加入到工作队列里为终点对端服务的对端线程里。消息是本地处理的，传输管理则传送消息给会话管理。

在这个处理过程中，一个应用可能需要使用消息来查询会话数据库。这个查询将返回一个与该消息相关的适当的会话对象。这个会话对象可以被用来更新会话状态机或发送一个应答给收到的消息。如果这个消息只是一个基础协议的消息并只用在 Diameter 库(ASR，ASA，STR，STA)，则这些消息的处理是内部的，也就是说库的本身签署处理这些基础协议消息。

对于一个由应用产生的输出消息，应用现实一个 Diameter API 传输类将消息同一个会话关联起来。这包括将一个消息加入到那个会话的工作队列里。每一次，一个新的线程池工作请求被建立起来并被注入到线程池工作请求队列。一旦有下一个可用的线程出队，则根据该输出消息完成所有的会话状态机的更新，如果必要的话，将消息入队到要发送到的对端线程的工作队列里。对端线程的工作队列，也被看作传输队列。

在内部，每一个对端线程除了一个传输队列之外都有一个内部的未

处理消息队列。一旦发生记时事件，由工厂去尝试连接，一旦同对端的连接重新建立起来，工厂激活一个新的对端线程同完程对端进行新的通信。如果重新连接失败，别一个在时间表内的进行下一个连接过程。

2、消息解析。直径消息的解析可能最少发生以下事件：

①当一个直径消息从对端接收到，传输管理需要解析消息以决定消息是不是需要加入到消息解析队列里由会话管理进行进一步的处理或者将他转发给其他对端。在这种情况下，只有特定的 AVP 如终点主机 AVP 和终点域 AVP 需要被解析，而不是根据命令字典解析所有的。

②当收到一个直径消息由会话管理来进行处理，消息根据字典被会话管理器完全解析并传送给适当的应用消息签署为特定的应用指定处理。

③当一个直径消息通过一个应用处理句柄或被传输管理器为特定的应用而产生，这个消息需要被消息解析模块构建。在这种情况下，消息是完全被根据字典解析并传送给传输模块。

④当一个直径消息由某应用产生并发送给对端，消息需要被传输管理器进行解析以决定向哪个对端发送消息。在这种情况下，只有一些特定的 AVP 如目的主机 AVP 和目的域 AVP 需要被解析。

对于所有的上面的情况，不管对为了信息的重组和分解而进行的解析是否完成，都使用相同的日期格式。用于信息解析的数据结构是容器列表(AAAAvpContainerList)，容器(AAAAvpContainer)和容器条目(AAAAvp ContainerEntry)。

容器和容器条目的分配和释放是通过容器管理者(AAAAvpContainerManager)和容器条目管理者(AAAAvpContainerEntry Manager)分别完成的，所有的管理者类型都被定义为一个单独的类。容器和容器条目的资源管理是基于提前分配而不是按要求分配，其目的是为了避免频繁的内存分配和释放。

在组类型 AVP 里的 AVP 数据是被存储在一个独特的容器列表里，并为这个组 AVP 在容器条目里存放一个指针。换句话说，一个直径消息负载和一个组类型 AVP 是按同样的方式进行处理的。这种方式也一样可以处理嵌套的组 AVP，这种嵌套组 AVP 也就是一个组 AVP 包含了另一个组 AVP 作为他一个 AVP 元素。

OpenDiameter 定义了解析者类，可以提供一个解析任何数据结构统一的方法。一个解析者类对象包含下列成员：

- 自然数据：较少结构化的数据，如字符串缓存
- 应用数据：自然数据表示法的组织结构。如 AVP 容器列表
- 字典数据：描述自然数据和应用数据之间的数据转化规则的数据。
- 数据 set/get 函数：一组用来 set/get 自然数据的函数，应用数

据和字典数据 to/from 解析者类。

• 转换函数：一对函数，用于自然数据和应用数据之间的转换。

6.1.4 OpenDiameter 开源软件包相关类库

OpenDiameter 是用 C++语言开发的，因此最大程度的利用了现有的成熟的 C++类库，以最少的代码完成最优秀的工作。该项目中广泛的使用 XML 作为配置文件类型，并采用 Xerces XML Parser 类库所提供的 API 进行解析。

1、ACE 类库。

Adaptive Communication Environment (ACE) 是一种免费开放原代码的面向对象框架结构，该结构实现了许多并行通信软件的核心设计模式[42]。ACE 提供丰富的 C++ wrapper facades, 以及可跨平台执行通信软件的基本任务的框架对象。ACE 提供的基本任务包括事件分离与事件处理的分发, 信号量处理，服务初始化，进程间通信, 共享内存管理, 消息路由, 分布式服务的动态配置，并发执行与同步。

ACE 的使用对象是面向开发高性能与实时通信服务应用的开发人员。它可以简化实现进程间通信，直接动态链接，以及并发处理功能的面向对象网络应用与服务的开发过程。同时，ACE 通过在运行过程中动态将服务连接到应用中并在一个或多个进程或线程中执行这些服务这种方式实现了系统的自动配置与重新配置。

ACE 仍在不断的发展，它的应用前景非常光明。ACE 的商业用途的支持由 Riverace 公司使用公开原代码方式进行。同时，许多 ACE 开发小组的成员正在进行 ACE ORB (TAO)的开发工作。

2、BOOST 类库。

BOOST 是一个准标准库，相当于 STL 的延续和扩充，它的设计理念和 STL 比较接近，都是利用泛型让复用达到最大化[43]。不过对比 STL，BOOST 更加实用。STL 集中在算法部分，而 BOOST 包含了不少工具类，可以完成比较具体的工作。

BOOST 主要包含一下几个大类：字符串及文本处理、容器、迭代子(Iterator)、算法、函数对象和高阶编程、泛型编程、模板元编程、预处理元编程、并发编程、数学相关、纠错和测试、数据结构、输入/输出、跨语言支持、内存相关、语法分析、杂项。有一些库是跨类别包含的，就是既属于这个类别又属于那个类别。

在文本处理部分，conversion/lexcial_cast 类用于“用 C++”的方法实现数字类型和字符串之间的转换。 主要是替代 C 标准库中的 atoi、itoa 之类的函数。当然其中一个最大的好处就是支持泛型了。

并发编程里有 thread 库，提供了一个可移植的线程库，不过在 Windows 平台上用处不大。因为它是基于 Posix 线程的，在 Windows 里对 Posix 的支持不是很好。 这里面除了 regex(正规表达式)、python 和 test 需要编译出库才能用，其他的大部分都可以直接源代码应用，比较方便。这些库的使用需要有相关的背景知识，比如元编程、STL、泛型编程等等。

3、OpenSSL 类库

Eric A. Young 和 Tim J. Hudson，自 1995 年开始编写后来具有巨大影响的 OpenSSL 软件包，这是一个没有太多限制的开放源代码的软件包，这使得我们可以利用这个软件包做很多事情。1998 年，OpenSSL 项目组接管了 OpenSSL 的开发工作，并推出了 OpenSSL 的 0.9.1 版，到目前为止，OpenSSL 的算法已经非常完善，对 SSL2.0、SSL3.0 以及 TLS1.0 都支持。OpenSSL 目前最新的版本是 0.9.7e 版。

OpenSSL 采用 C 语言作为开发语言，这使得 OpenSSL 具有优秀的跨平台性能，可以在不同的平台使用同样熟悉的东西。OpenSSL 支持 Linux、Windows、BSD、Mac、VMS 等平台，这使得 OpenSSL 具有广泛的适用性。虽然 OpenSSL 使用 SSL 作为其名字的重要组成部分，但其实现的功能确远远超出了 SSL 协议本身。OpenSSL 事实上包括了三部分：SSL 协议、密码算法库和应用程序[44]。

①SSL 协议部分完全实现和封装了 SSL 协议的三个版本和 TLS 协议，SSL 协议库的实现是在密码算法库的基础上实现的。使用该库，你完全可以建立一个 SSL 服务器和 SSL 客户端。该部分在 Linux 下编译会形成一个明文 libssl.a 的库，在 Windows 下则是名为 ssleay32.lib 的库。

②密码算法库是一个强大完整的密码算法库，它是 OpenSSL 的基础部分，也是很值得一般密码安全技术人员研究的部分，它实现了目前大部分主流的密码算法和标准。主要包括公开密钥算法、对称加密算法、散列函数算法、X509 数字证书标准、PKCS12、PKCS7 等标准。事实上，OpenSSL 的 SSL 协议部分和应用程序部分都是基于这个库开发的。目前，这个库除了可以使用本身的缺省算法外，在 0.9.6 版本之后，还提供了 Engine 机制，用于将如加密卡这样外部的加密算法实现集成到 OpenSSL 中。密码算法库在 Linux 编译后其库文件名称为 libcrypto.a，在 Windows 下编译后其库文件为 libeay32.lib。

③应用程序部分是 OpenSSL 使用入门部分。该部分基于上述的密码算法库和 SSL 协议库实现了很多实用和范例性的应用程序，覆盖了众多的密码学应用。主要包括了各种算法的加密程序和各种类型密钥的产生程序(如 RSA、Md5、Enc 等等)、证书签发和验证程序（如 Ca、X509、Crl 等）、SSL 连接测试程序（如 S_client 和 S_server 等）以及其它的

标准应用程序（如 Pkcs12 和 Smime 等）。

6.2 Diameter MIPv6 模块体系结构

Diameter MIPv6 应用扩展协议的实现从功能的角度划分应该包括如下三个模块，分别为：AAA Server 端模块、AAA Client 端模块、移动节点 MN 端模块。

AAA Server 端模块：该模块的主要功能是提供消息的解析、建立与 AAA 实体的安全连接、消息的安全传输、同后台存储用户数据的数据库连接并认证用户信息、记录用户使用资源的情况并将有关数据记录在后台数据中。该模块是核心模块，它可以根据从 AAA Client 传送来的消息不同自动的充当本地 AAA 服务器或外地 AAA 服务器。例如，如果 AAA Client 传送来的消息是本地消息，则 AAA Server 端软件自动充当本地 AAA 服务器软件。相反，如果传送来的消息是外地消息（根据 NAI 进行判断），则 AAA Server 端软件自动同外地 AAA 服务器端软件通过已知端口（3868）建立连接并完成信息交互过程。

AAA Client 端模块：位于移动节点 MN 端软件模块同 AAA Server 软件模块之间，其主要功能是提供移动节点 MN 的接入、与 AAA Server 端软件模块交互以及认证信息数据的发送接收、定期发送路由通告以告知本系统支持的服务。事实上，AAA Client 端软件模块应该位于 NAS（网络访问服务器）或支持接入功能的路由器之上，不但能够完成接入功能，还能在完成认证之后配置路由器等设备转发移动节点发送的数据包。同时，AAA Client 还应该完成对移动节点使用网络资源数据的收集功能定时向 AAA 服务器发送计费信息。

移动节点 MN 端模块：该软件模块的主要提供同 AAA Client 端软件连接并提交认证信息的功能，同时，该模块不断的监听网络上的路由

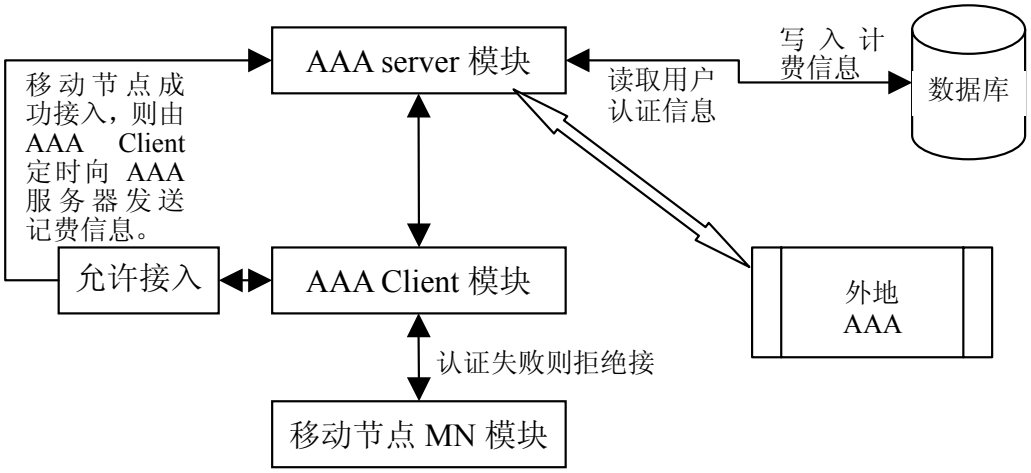


图 6-3 Diameter MIPv6 软件体系结构
Fig.6-3 Software structure of Diameter MIPv6 Application

通告，根据路由通告内容判断移动节点的位置信息并作出相应的处理。Diameter 协议的 MIPv6 应用扩展协议的软件模块体系结构图如上 6-3 所示。

6.3 AAA Server 端模块的设计及实现

AAA Server 端模块是建立在 OpenDiameter 类库之上的，该模块直接调用 OpenDiameter 库提供四个逻辑模块：应用核心模块、会话管理模块、传输管理模块和消息解析模块完成基本的会话、传输、消息解析等工作。为了完成移动 IPv6 的特定功能，本文设计了与外地 AAA 服务器建立连接并交互信息的子模块（libAAAServerCore），以用来处理当 AAA 服务器软件收到外地消息的时候，与外地 AAA 服务器软件建立连接并进行消息交互的过程。同样，为了处理在外地域分配家乡代理的功能，设计了分配家乡代理子模块（libAllocateHomeAgent）。更进一步，为了在增强协议中提供密钥分配功能，设计了密钥分配子模块（libKeyDistribute）。因此，AAA Server 端模块的功能结构图如下图 6-4 所示。

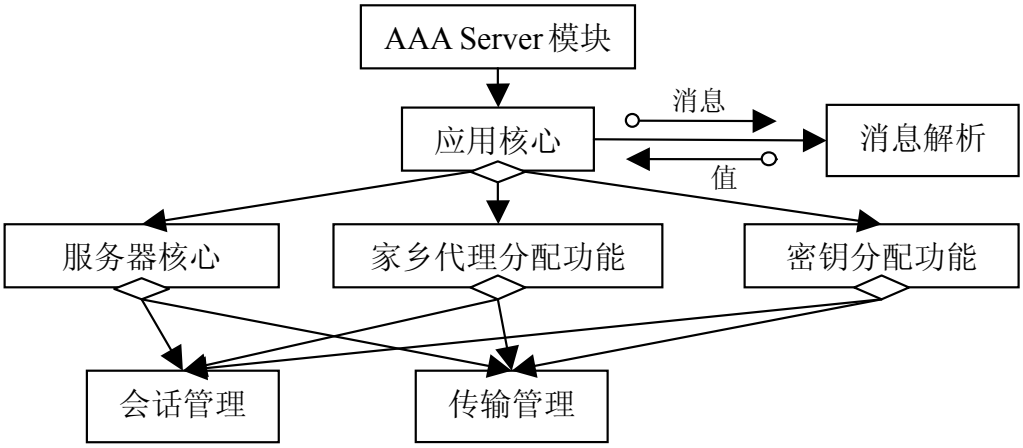


图 6-4 AAA Server 端功能结构图
Fig.6-4 Software model structure of AAA server software

AAA Server 模块是多线程的、实时的。该模块的工作流程如下图 6-5 所示。在该工作流程中所使用的线程池与 OpenDiameter 基础协议实现中使用的基于 ACE 的线程池是相同的。该线程池维护一个合适的大小，并可以在短时间有大量并发连接请求的时候自动扩展线程池的容量。

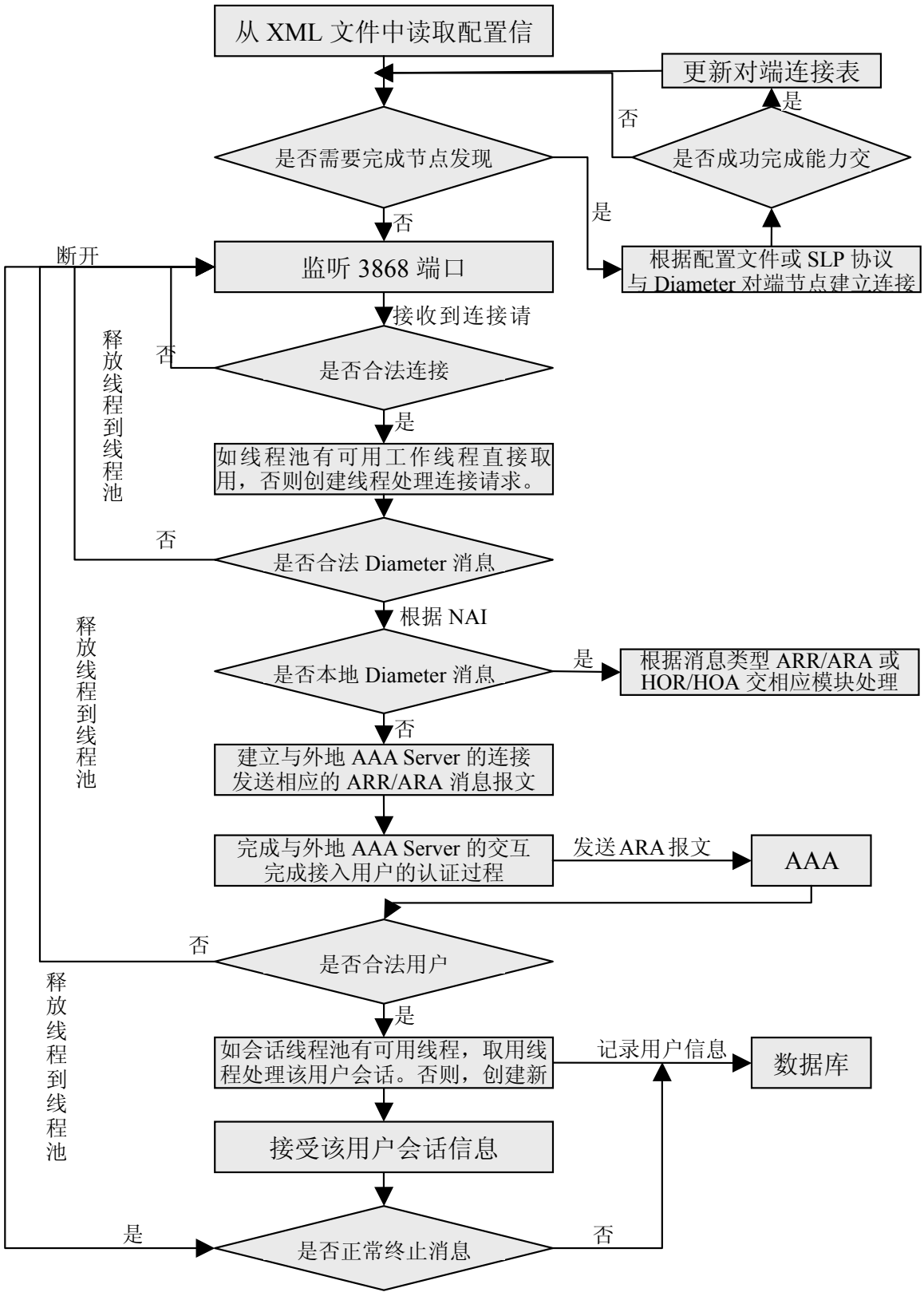


图 6-5 AAA Server 端软件工作流程图

Fig.6-5 Work flaw chart of AAA server software

6.3.1 服务器核心

当 AAA Server 端软件收到的 Diameter 消息非本地消息的时候，则由应用核心模块调用服务器核心子模块处理相关消息，并同外地 AAA 服务器软件进行通讯、交互相关信息。该模块的基本静态类图如下图 6-6 所示。

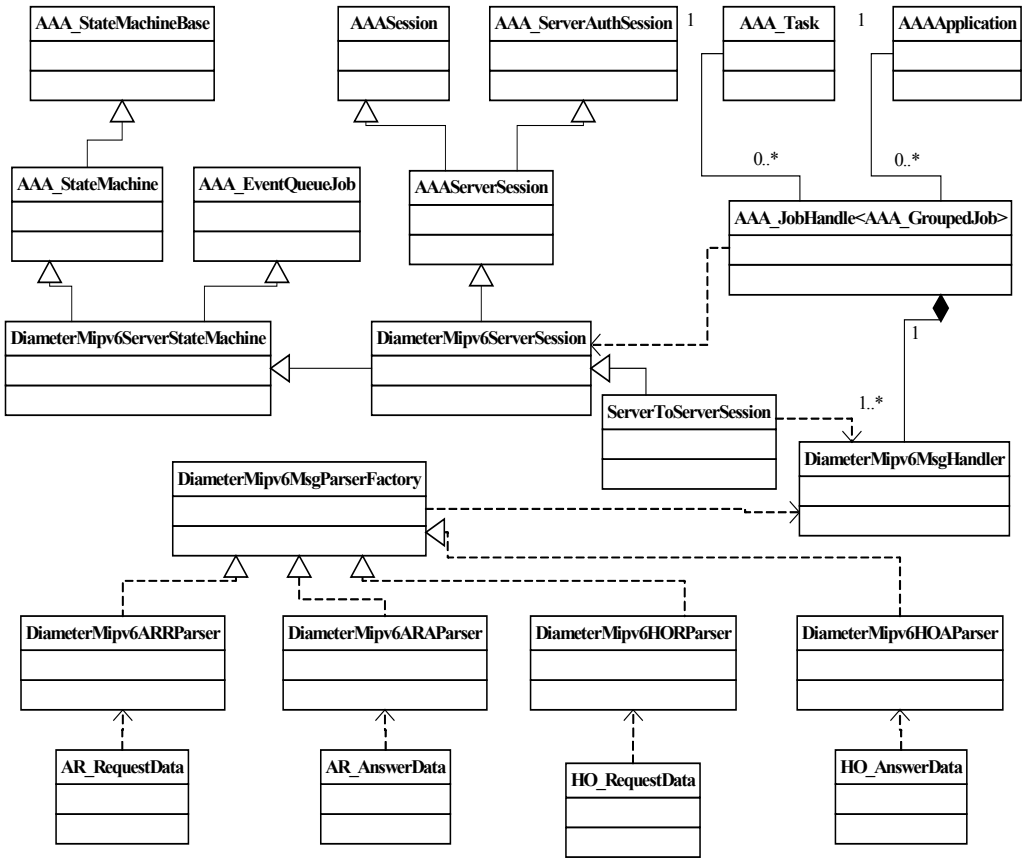


图 6-6 Diameter Mipv6 服务器核心模块类图
Fig.6-6 Class diagram of Diameter Mipv6 server core module

在该模块的设计实现中，尽可能的利用了OpenDiameter中提供的Diameter基础协议类库中类。根据OpenDiameter开源软件开发规范，并在这些基类的基础之上扩展出了DiameterMipv6ServerStateMachine，DiameterMipv6ServerSession，DiameterMipv6JobHandler，DiameterMipv6-ParserFactory以及由AAAMessage扩展而来的四个消息类分别处理ARR/ARA、HOR/HOA消息对。同时，在头文件Diameter_Mipv6_parser.h中增加为了处理MIPv6消息而增加的消息对的命令代码以及相关AVP的值和命令代码值。

在这些类中的消息发送和接受以及多线程操作都是基于ACE类库实现的，Diameter对等节点连接后的能力交换传输过程已经在

AAA_PeerStateMachine得到完善的处理。

※ 类 DiameterMipv6ServerStateMachine

Diameter Mipv6 服务器状态机类从 AAA_StateMachine、AAA_EventQueueJob 两个类多继承得来的，它定义了 Diameter Mipv6 应用服务器扩展协议中的状态机，包含了 Diameter Mipv6 服务器端软件处理工作流程过程中的各种函数，该类中的大部分函数是虚函数，Diameter Mipv6 服务器端核心模块中的大部分类都是继承该类并重载其相关函数。构造函数[45]中以 DiameterMipv6ServerSession 和 AAA_JobHandle<AAA_GroupedJob>类的实例为参数，分别处理 Diameter 会话与具体工作流程中的 Job。

属性：session。该属性是 DiameterMipv6ServerSession 类实例的引用，用于处理具体的会话。

属性：handle。该属性是 AAA_JobHandle<AAA_GroupedJob>类的实例，用以处理具体的工作进程。

属性：ar_requestData。该属性是 AR_RequestData 类的实例，该类定义了 ARR 请求消息的数据结构。

属性：ar_answerData。该属性是 AR_AnswerData 类的实例，该类定义了 ARA 请求消息的数据结构。

属性：ho_requestData。该属性是 HO_RequestData 类的实例，该类定义了 HOR 请求消息的数据结构。

属性：ho_answerData。该属性是 HO_AnswerData 类的实例，该类定义了 HOA 请求消息的数据结构。

属性：authenticationDone。该属性是 bool 型，如果认证成功则该值为真，否则为假。

属性：authorizationDone。该属性是 bool 型，如果授权成功则该值为真，否则为假。

※ 类 DiameterMipv6ServerSession

Diameter Mipv6 服务器会话类是处理 Diameter 对端节点之间会话的基类，该类从 AAAServerSession 和 DiameterMipv6ServerStateMachine 多重继承得来。该类重载 AAAServerSession 类中的虚函数以处理对端节点的连接、断开连接、消息处理等功能，其中消息的处理是由 DiameterMipv6MsgHandler 类的实例来进行的。与该类相关的类和数据类型主要有 AAAApplicationCore 类、AAAMessage 类、AAAReturn Code

枚举类型。

其中，AAAApplicaionCore 类是 OpenDiameter 基础协议类库中的核心类，该类通过读取指定的 XML 配置文件得到具体应用的配置信息，同时使用 AAA_Task 类根据优先级和权重启动线程调度过程并使用计时器安排管理线程。AAA_Task 类是从 ACE_Task<ACE_MT_SYNCH> 类继承得来，通过继承得到对多线程的同步处理。

AAAMessage 定义了 Diameter 消息的基本数据结构，包括 AAADiameter-Header 类和 AAAAvpContainerList 类等，分别定义 Diameter 消息头格式和 AVP 容器。

AAAReturnCode 枚举类型定义为 Diameter 协议中定义的 API 返回代码，主要包括成功、失败、协议错误、安全错误、AVP 丢失、传输错误等等。

DiameterMipv6ServerSession
-msgHandler : DiameterMipv6MsgHandler
+DiameterMipv6ServerSession(in &appCore : AAAApplication, in appId : diameter_unsigned32_t = 4) +Self() : DiameterMipv6ServerSession +HandleMessage(in &msg : AAAMessage) : AAAReturnCode +HandleDisconnect() : AAAReturnCode +HandleSessionTimeout() : AAAReturnCode +HandleAuthLifetimeTimeout() : AAAReturnCode +HandleAuthGracePeriodTimeout() : AAAReturnCode +HandleAbort() : AAAReturnCode +HandleTimeout() : AAAReturnCode

图 6-7 DiameterMipv6ServreSession 类

Fig.6-7 Class DiameterMipv6ServreSession

该类的定义如上图 6-7 所示。该类构造函数的参数为 AAAApplicationCore 类的实例引用&appCore，用来初始化 Diameter 会话类，并启动相关处理线程。另一个参数为 unsigned32 类型 appID，默认初始值为 4，用来表明该 Diameter 应用为 Diameter MIPv6 应用扩展。

属性：DiameterMipv5MsgHandler 类的实例 msgHandler。该类用来具体解析 Diameter MIPv6 应用扩展中定义的消息。

类中方法的实现完成具体会话全过程，包括消息处理、会话终止、会话超时、认证超时等会话处理过程，并返回 AAAReturnCode 值以表明处理结果。

※ 类 DiameterMipv6MsgHandler

Diameter Mipv6 消息处理类用来设计具体处理 Diameter Mipv6 应用扩展协议中定义的消息，并由 AAA_JobHandle<AAA_GroupedJob>类进行管理。AAA_JobHandle 是一个模板类，定义 template <class JOB> class

AAA_JobHandle : public boost::shared_ptr<JOB>。在该类的定义中应用了 Boost 类库中的智能指针 shared_ptr<T>来封装模板类，该智能指针中有一个指针计数器，允许多个指针指向同一个对象，并且可能当没有指针指出该对象的时候释放该对象资源，同时，使用该智能指针封装是线程安全的[46]。AAA_GroupedJob 类维护了一个工作队列，并按优先级、权重进行作业调度，任何一项消息处理工作都在该队列中进行调度，以实现负载平衡。

该类继承了 AAASessionMessageHandler 类以处理会话的消息，并根据 DiameterMipv6ServerSession 类传来的 AAAApplication 类的实例，得到会话消息的命令代码。然后，根据不同的命令代码使用 DiameterMipv6ParserFactory 类构造不同的消息解析类，对 AAAMessage 的 AVP 值进行解析，并最终将解析结果返回给相应的会话处理线程。

同时，当该类得到 AAAMessage 的解析结果的时候，如果该会话消息是外地消息，则启动一个新的会话处理 Diameter 服务器之间的连接以及消息交换过程，该过程在实现的时候重载 DiameterMipv6ServerSession 类创建内部类 ServerToServerSession，并使用 AAAServerSessionClassFactory<class T>模板类封装后以 AAAApplicationCore 类的方法 RegisterServerSessionFactory (AAAServer SessionClassFactory * fac)注册该会话，完成 AAA 服务器之间的会话处理过程。该类的定义如下图 6-8 所示。

DiameterMipv6MsgHandler
-&parserFac : DiameterMipv6MsgParserFactory -m_cmdCode : AAACommandCode -m_AAAmsg : AAAMessage
+DiameterMipv6MsgHandler(in *s : DiameterMipv6ServerSession) +~DiameterMipv6MsgHandler() +GetCommandCode() : AAACommandCode +IsLocalMessage(in &msg : AAAMessage, in auto_ptr<DiameterMipv6ParserFactory> *fac) : bool +InitServerToServerSession(in &msg : AAAMessage) : ServerToServerSession

图 6-7 DiameterMipv6MsgHandler 类
Fig.6-7 Class DiameterMipv6MsgHandler

在该类的实现中，定义了 AAACommandCode 数据类型，该类型是从 ACE 类库中直接引用的 ACE_UINT32 以提供数据类型的跨平台性。

※ 类 DiameterMipv6ParserFactory

Diameter Mipv6 消息解析工厂类采用了简单工厂设计模式，该类为工厂模式中的核心类，它根据不同的参数产生不同的产品类

DiameterMipv6ARRParser、DiameterMipv6ARAParser、DiameterMipv6-HORParser、DiameterMipv6HOAParser 四个 MIPv6 应用扩展中应用的消息解析类。这个具体消息的解析类都是从 AAAParser<AAAMessage*, MessageData*>类直接扩展得到，其中 MessageData 类是 ARR/ARA、HOR/HOA 消息的数据结构定义类。其类图如上图 6-8 所示。

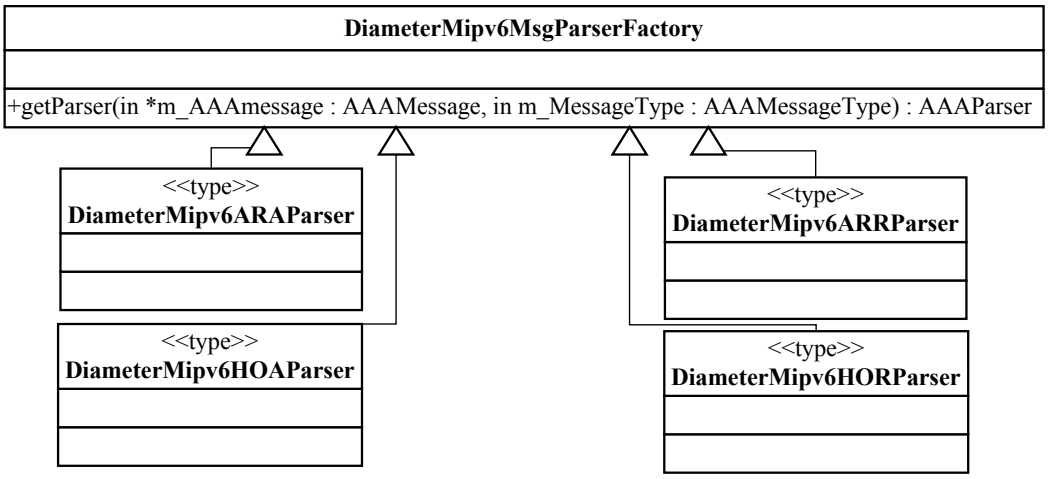


图 6-8 DiameterMipv6ParserFactory 类图
Fig.6-8 Class diagram of DiameterMipv6ParserFactory

在该类中，定义了 AAAMessageType 枚举类型，其定义如下：

```
typedef  enum{
    ARR_Message,
    ARA_Message,
    HOR_Message,
    HOA_Message
}AAAMessageType;
```

根据该枚举类型的不同值，DiameterMipv6ParserFactory 类分别产生不同的消息类型数据结构类作为 AAAParser 类的参数，并定义不同的消息解析类。

※ Diameter MIPv6 相关消息类定义

Diameter MIPv6 应用扩展协议中为了完成对外地移动 IPv6 节点的认证和授权过程以及在外地域分配家乡代理的过程，定义了两个消息对 ARR/ARA、HOR/ HOA 消息对，以及扩展的 AVP 值。这些消息的数据结构及方法分别定义在类 AR_RequestData、AR_AnswerData、HO_RequestData、HO_AnswerData 四个类中，扩展的 AVP 类型数据结构也包含在各自的消息类中。AR_RequestData 消息类的结构图如下 6-9

所示。其他三个类与该类的结构相似。

AR_RequestData
-MIP-Binding-Update : AAA_ScholarAttribute<diameter_octetstring_t> -MIP-Binding-acknowledgement : AAA_ScholarAttribute<diameter_octetstring_t> -MIPv6-Mobile-Node-Address : AAA_VectorAttribute<diameter_octetstring_t> -MIPv6-Home-Agent-Address : AAA_VectorAttribute<diameter_octetstring_t> -MIPv6-Feature-Vector : AAA_ScholarAttribute<diameter_unsigned32_t> -Key-Request : AAA_ScholarAttribute<diameter_unsigned32_t> -MN-Key-Distribution : AAA_VectorAttribute<diameter_octetstring_t> -Key-Distribution : AAA_VectorAttribute<diameter_octetstring_t>
+AR_RequestData() +Clear() +*Self() : AR_AnswerData

图 6-9 AR_RequestData 类
Fig.6-9 Class AR_RequestData

在这些类的定义与 AVP 相关的模板类为 AAA_ScholarAttribute <typename T>和 AAA_VectorAttribute <typename T>，这两个类定义对了不同 AVP 类型的定义及基本操作，以完成从 Diameter 消息中将 AVP 值拷贝入 AAAAvpContainer AVP 容器类中提供给消息解析类处理。

属性：MIP_Binding_Update。该 AVP 为八位组字符串类型，包含了移动 IP 的绑定更新消息。AVP 代码值为 6001。

属性：MIP_Bingding_acknowledgement。该 AVP 也为八位组字符串类型，包含了由家乡代理发送给移动节点的移动 IP 绑定确认消息。AVP 代码值为 6002。

属性：MIP_Mobile_Node_Address。该 AVP 是 IPv6 地址类型，由 diameter_octetstring_t 类型的八位组进行封装、包含了移动节点的家乡地址。AVP 代码值为 6003。

属性：MIP_Home_Agent_Address。该 AVP 是 IPv6 地址类型，同样由 diameter_octetstring_t 类型的八位组进行封装、包含了移动节点的家乡代理地址。AVP 代码值为 6004。

属性：MIP_Feature_Vector。该 AVP 是一个无符号 32 位 INT 类型，根据其不同的值代表不同的意义。

当该值的二进制数第一位标识 Home-Agent-Requested 为 1 的时候，表明移动节点请求分配一个动态的家乡代理；

第二位标识 Mobile- Node-Home-Address-Requested 为 1 的时候，表明移动节点没有任何家乡地址和请求，默认值为 0；

第三位标识 Home-Address-Allocatable-Only-in-Home-Domain 为 1 的时候，表明如果移动节点请求一个家乡地址并且希望由它的家乡网络进行分配，默认值是 0；

第四位标识 Home-Agent-in-Visited-Domain 为 1 的时候，表明移动

节点希望在被访问域得到它的家乡代理；

第五位标识 Visited-Home-Agent-Available 为 1 的时候，表明 MN 请求在被访问域动态家乡代理分配并且被访问域也可以分配给 MN。AVP 代码值为 6005。

属性：Key_Request。该 AVP 是一个无符号 32 位 INT 类型，当该值 的二进制数的第一位标识 Is_Request 值为 1，则表明需要密钥分配过程；当该值的第二位标识 Key_Exchange_Method 的值为 0，表明密钥分配过程使用随机数方法，值为 1，表明密钥分配过程使用 Diffie-Hellman 算法。AVP 代码值为 6006。

属性：MN-Key-Distribution。该 AVP 为八位组字符串类型，如果是使用随机数密钥分配过程，该值为空。如果是使用 Diffie-Hellman 算法进行密钥分配过程，则包含密钥交换过程中所需要的 MN 的 Diffie-Hellman 公共值。

属性：Key-Distribution。该 AVP 为八位组字符串类型，如果使用随机数方法，其值为根据随机数计算的密钥；如果使用 Diffie-Hellman 算法进行密钥分配过程，则其值为 MN 的 Diffie-Hellman 公共值。

6.3.2 家乡代理分配

当 Diameter MIPv6 应用服务器端解析移动节点发送的 Diameter 消息的时候，如果 MIP_Feature_Vector AVP 的二进制值的第一位被设为 1，则启动家乡代理分配过程。在该过程中，AAA 服务器需要同家乡代理服务器进行通信，交换 HOR/HOA 消息，以获取家乡代理的地址信息并填充 ARR/ARA 消息的内容发送给移动节点。

家乡代理的分配可以由家乡 AAA 服务器完成，也可以由外地 AAA 服务器完成。这两种情况下，都是 AAA 服务器同 HA 之间的消息交换。根据 MIP_Feature_Vector AVP 中的不同标识决定家乡代理在外地域或者在家乡域进行。

类 DiameterMipv6HomeAgentDistribution 完成 AAA 服务器与家乡代理 HA 之间的通信、HOR/HOA 消息的产生的解析以及 ARR/ARA 消息的填充。该类的结构定义如下图 6-10 所示。

在该类的实现中，属性*peerEntry 是指向 AAA_PeerEntry 类的实例的指针。有 AAA_PeerEntry 类的构造函数的参数中可以指定对端节点的连接端口和连接方式，连接方式可以使用 TLS 方式连接或普通方式。对端连接的实现使用了 ACE 类库中的 Acceptor/Connector 设计模式，并且重用 ACE_SOCK_Acceptor/ACE_SOCK_Connector 或 ACE_SSL_SOCK_Acceptor/ACE_SSL_SOCK_Connector 类。

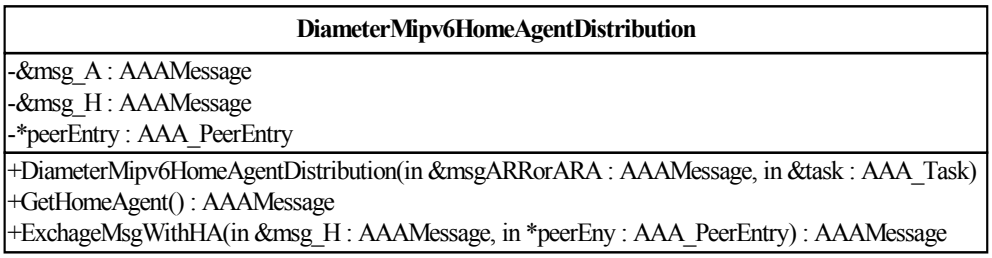


图 6-10 DiameterMipv6HomeAgentDistribution 类
Fig.6-10 Class DiameterMipv6HomeAgentDistribution

6.3.3 密钥分配

AAA 服务器的密钥分配过程是 Diameter MIPv6 应用扩展协议中的增强扩展部分，也就是 Diameter 协议可以作为一个密钥分发中心。密钥分配请求和分配过程通过 ARR/ARA 消息中包含 Key_Request、MN-Key-Distribution 、Key-Distribution 三个 AVP 来完成。在消息过程中，根据 Key_Request AVP 的不同值决定是否需要进行密钥分配以及如何进行密钥分配，如果需要进行密钥分配，则启动密钥分配过程。

类 DiameterMipv6KeyDisInterface 被设计用来生成密钥并填充生成新的 ARR 或 ARA 消息框架，类 KeyDis_DiffieHellman 和类 KeyDis_RandomNum 分别实现该接口以完成密钥分配过程，移动节点可以根据 AAA 服务器分配得来的密钥生成安全关联，建立与 Diameter 网络实体的安全传输过程。该类支持基于随机数的密钥分配和基于 Diffie-Hellman 密钥交换算法的密钥分配。密钥分配功能的相关类的设计如下图 6-11 所示。

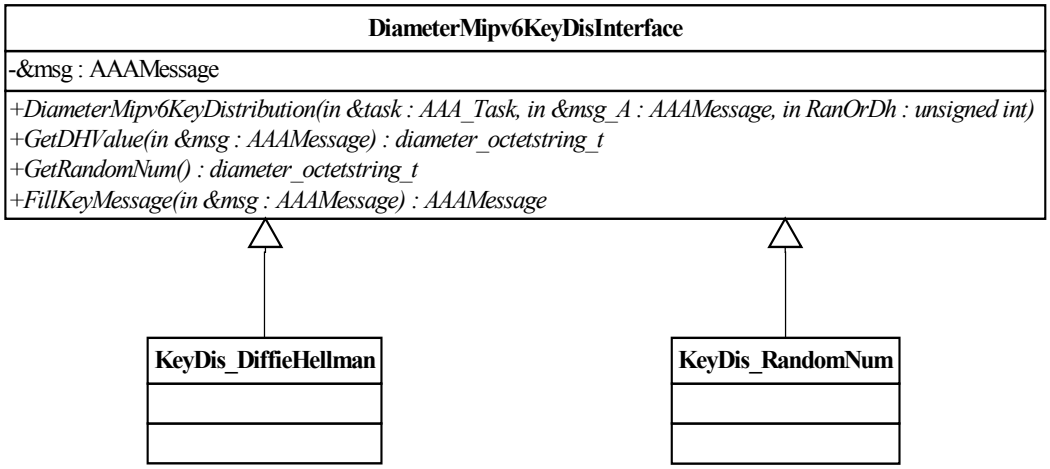


图 6-11 密钥分配功能类图
Fig.6-11 Class diagram of key distribution function

在该功能模块中，AAA 服务器本身作为一个密钥分发中心，为移动节点和其通讯对端安全的建立公共密钥。

6.4 AAA Client 端模块的设计及实现

AAA Client 端软件主要完成两方面的工作，一方面处理移动节点或本地节点的连接认证请求并根据认证结果完成认证和授权过程，另一方面同 Diameter 服务器连接并完成认证消息的交换。由于 AAA Client 是作为一个接入路由器存在于网络之上，所以该软件模块还应该包括定时发送路由通告的功能，以使得移动节点能够根据路由通告确认自己所接入的网络信息。

AAA Client 端软件同移动节点之间的连接认证过程是使用 PANA 协议，以确保外地节点在没有得到授权之前不能接入网络，并完成基于 IP 的认证过程。因此，在该过程中 AAA Client 端软件实际上是实现了 PANA 协议中定义的网络实体 PAA。

AAA Client 端软件同 AAA 服务器之间的连接过程是基于 Diameter 协议，AAA Client 端软件是作为一个 Diameter 对端节点存在的，两者之间的 Diameter 消息是 ARR/ARA 消息对。AAA Client 端软件收到移动节点发送来的认证信息并根据该信息封装到 Diameter 消息中，发送给 AAA 服务器，并接受 AAA 服务器发送回的 ARA 消息并根据该消息完成授权过程。该过程的功能结构图如下图 6-12 所示。

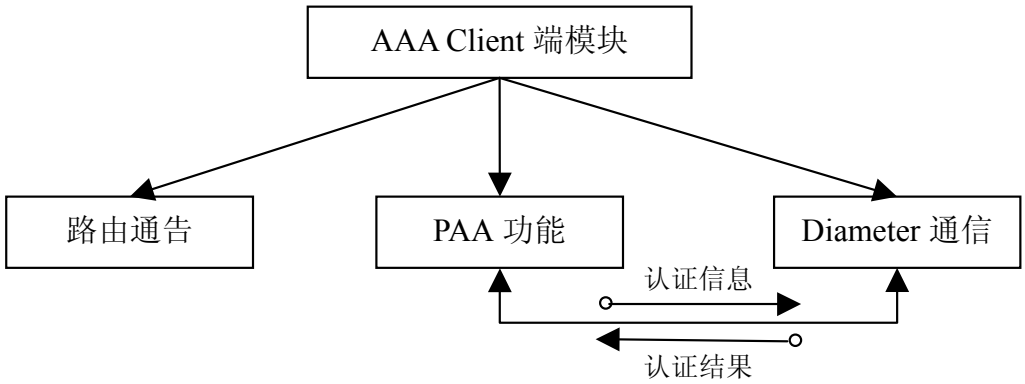


图 6-12 AAA Client 端功能结构图
Fig.6-12 Function model structure of AAA client software

路由通告是一个相对独立的过程，当 AAA Client 端软件启动的时候，首先初始化该功能并发送 ICMPV6 路由通告报文。然后，初始化 Diameter 通信功能模块，建立与 AAA 服务器之间的连接，连接过程需要解析 XML 配置文件并读取相关内容。该过程是利用 Xerces XML C++ 库中提供的 API 实现，Xerces XML 类库提供 SAX(Simple API for XML)、DOM(Document Object Model)两种 XML 分析器的标准接口[47]，在本文的实现中采用 DOM 程序接口。当 AAA Client 端软件完成初始化过程之后，则启动 PAA 功能模块，监听固定端口 1001 以处理 PAC 的接入。

AAA Client 端软件工作流程图如下图 6-13 所示。

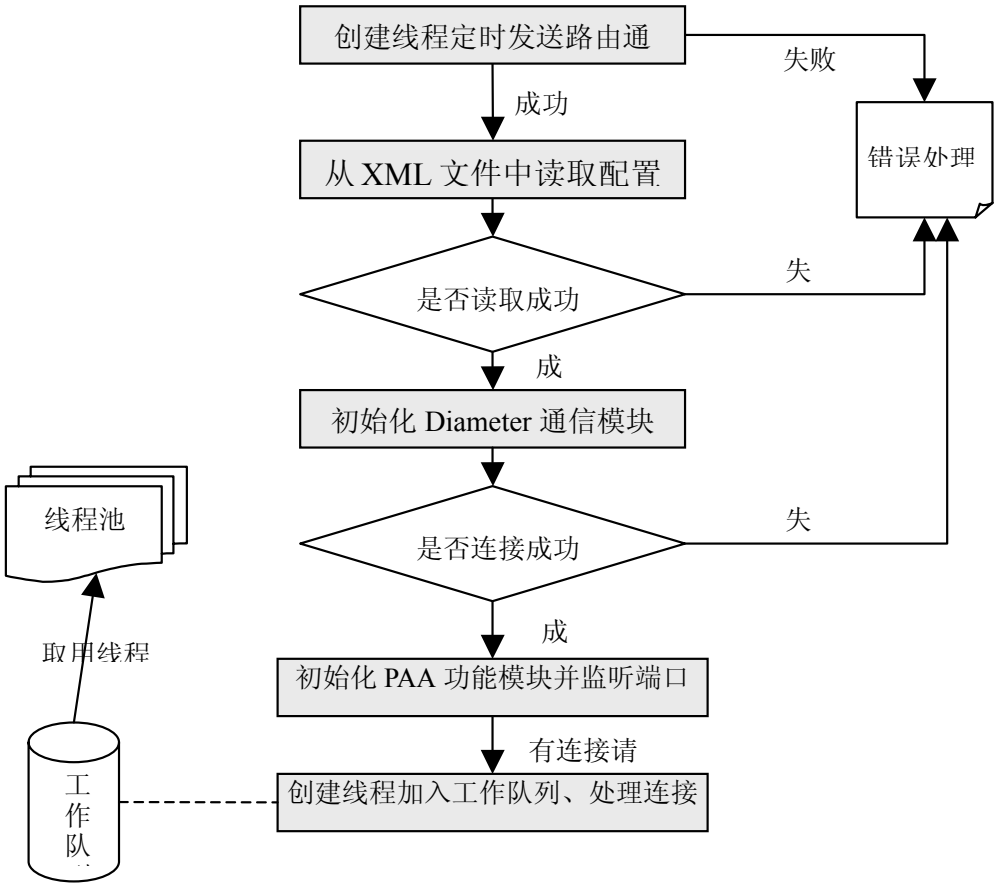


图 6-13 AAA Client 端软件工作流程图

Fig.6-13 Work flaw chart of AAA Client software

由于本文主要是完成 Diameter 协议在移动 IPv6 下的应用，而不是移动 IPv6 的实现，因此简化了 AAA Client 端和 MN 端软件之间邻居发现机制、移动检测过程以及与 HA 之间的交互过程等具体的实现细节，仅由 AAA Client 端的路由通告进程和 NM 端软件的移动检测进行共同完成基本的移动检测过程。

6.4.1 路由通告

路由通告消息是 ICMPV6 消息，由路由器以组播方式向所在链路发送，宣告其可用性及其可到达的链路和 Internet 参数，包括网络地址前缀、建议的最大跳数及本地 MTU，也包括指明节点应使用的自动配置类型的标志。本文所提及的路由通告是指非请求的路由通告，由路由器周期性的发出。

根据 MIPv6 邻居发现协议标准中的从任何给定网络接口发送非请求组播路由的周期应该庆参数 MinRtrAdvInterval 和 MaxRtrAcvInterval

值之间，推荐的限制值为：MinRtrAdvInterval=0.05 秒、MaxRtrAcvInterval=1.5 秒。在本文的实现中以 1 秒为周期发送路由通告。

ICMPV6 的报头数据结构如下所示[48]：

```
struct icmp6_hdr {
        uint8_t         icmp6_type;
        uint8_t         icmp6_code;
        uint16_t        icmp6_cksum;
        union {
           uint32_t     icmp6_un_data32[1];
           uint16_t     icmp6_un_data16[2];
           uint8_t      icmp6_un_data8[4];
        } icmp6_dataun;
    };
```

移动 IPv6 中的邻居发现机制的网络路由前缀通告消息格式数据结构如下所示[49]：

```
struct AdvPrefix {
        struct in6_addr          Prefix;
        int                   PrefixLen;
        int                   AdvOnLinkFlag;
        int                   AdvAutonomousFlag;
        uint32_t              AdvValidLifetime;
        uint32_t              AdvPreferredLifetime;
         int                   AdvRouterAddr;
        struct AdvPrefix  *next;
};
```

该路由通告消息的发送使用 ACE 类库中的 ACE_SOCK_Dgram_Bcast 类向本网段的节点发送报文。

6.4.2 PAA 功能模块

在该模块中，利用 OpentDiameter 软件包中的 PANA 库提供的 API 实现 PANA 代理模块。PANA 消息的传输是基于无连接的 UDP 传输协议，PAA 功能模块有一个进程负责侦听固定的 UDP 端口以处理进入的消息。当有消息进入的时候，该进程读取该消息、对该消息进行必要的检验，如果该消息合法则进入消息处理工作队列进行进一步的解析。该模块的软件体系结构如下图 6-14 所示。

PANA 消息的处理也是基于会话的，当消息被解析为合法的消息则将认证信息传送给 Diameter 通信模块，并等待由 Diameter 通信模块完成 AAA Client 模块与 AAA Server 模块认证结果，根据认证结果交相应的会话状态机处理工作队列，如发现、授权、终止。该模块同时维护一个会话数据库存储会话状态、EAP 负荷等数据，并且可以根据用户的设备 ID 查询该会话数据库。

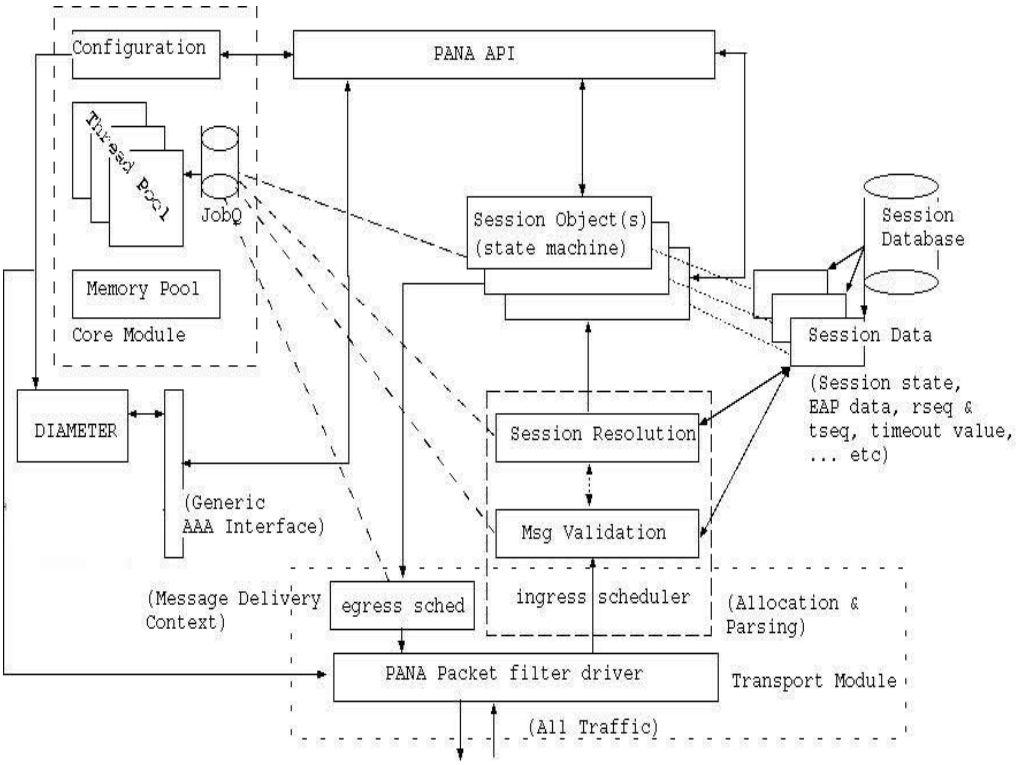


图 6-14 PAA 软件模块体系结构

Fig.6-14 Infrastructure of software module of PAA

PANA 消息类及消息头类的定义如下图 6-15 所示：

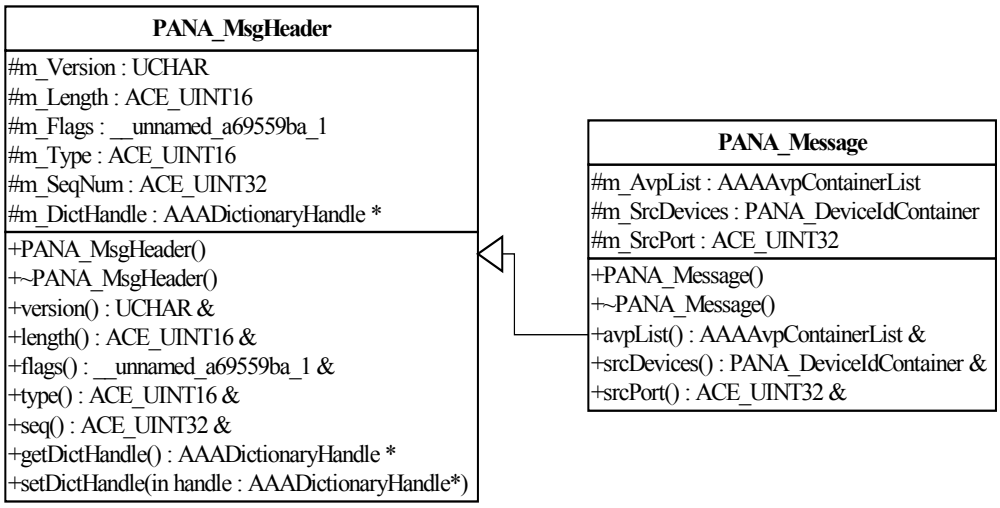


图 6-15 PANA 消息类图

Fig.6-15 Diagram PANA Message Class

在 PANA_MsgHeader 类中。属性 m_Version：该值为无符号字符类型，表明该 PANA 消息头的版本。并通过方法 UCHAR &version()函数获取该值的引用，可以在封装消息的时候进行设置。

属性 m_Length：该值为 ACE_UINT16 类型，表明该报头的长度。设置或得到该值的方法同上。

属性 m_Flag：该值为结构类型，其定义如下

```
typedef struct {
        ACE_UINT16 request     : 1;   // 请求标识
        ACE_UINT16 separate    : 1;   // 独立标识，表明完成独立的
EAP过程
        ACE_UINT16 nap         : 1;   // Nap标识，表明完成NAP认
证过程
        ACE_UINT16 reserved    : 13;  //保留
    } Flags;
```

在 PANA_Message 类中的 AVP 值相关类重用 Diameter 协议 AVP 容器类以及 AVP 解析类。而属性 m_SrcDevices 的类型是 PANA_DeviceIdContainer 设备 ID 容器类，通过函数 srcDevices()进行设置或获取。

PAA 端会话的实现基于工厂设计模式和 Adapter 设计模式[50]，其静态类图如下图 6-16 所示。

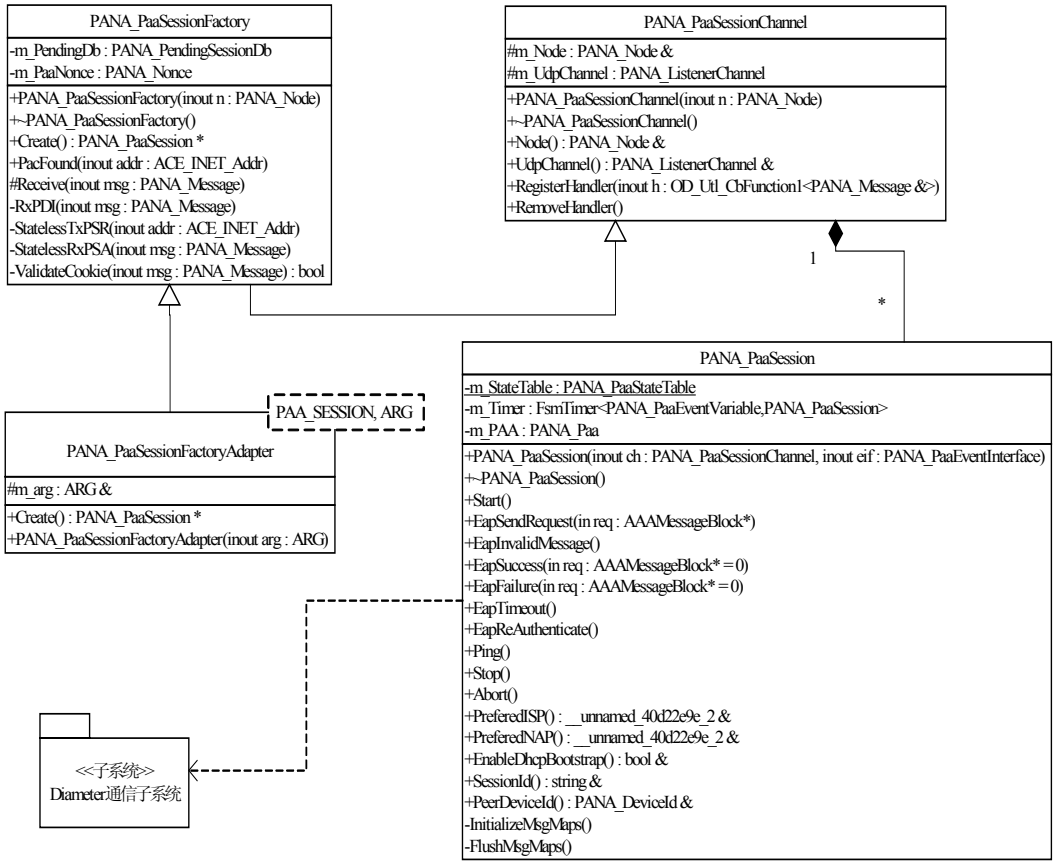


图 6-16 PAA 会话静态类图

Fig.6-16 Static Class Diagram of PAA Session

PANA_PaaSessionChannel 类的方法 PANA_ListenerChannel

&UdpChannel()初始化一个 PANA_UdpIPv6 类实例侦听固定端口。并且在收到 PANA 发现消息后，需要认证消息的合法性的时候调用 Diameter 通信子系统相关类。当认证成功之后，重新维护本地的路由表，将该节点的相关信息加入路由条目，并设置相关的 IP 过滤规则。

6.4.3 Diameter 通信模块

该通信模块的主要功能是完成 AAA Client 和 AAA Server 之间的通信过程，完成认证和授权过程。当授权成功移动节点接入之后，直接使用已经完成的记费 API 封装记费数据并定时向 AAA Server 发送。AAA Client 和 AAA Server 之间的通信过程使用 ACE 连接者与接受者模式，根据 XML 配置文件中的服务器对端的网络信息进行连接并传输。AAA Client 端的认证过程的类是从 AAA_Client AuthSession 和 AAA_SessionMsgMux<class T>多重继承得来，该类管理 AAA Client 端完成认证过程的会话并处理会话状态机。处理每一个具体的会话的类是从 AAA_SessionMsgMuxHandler<class T>继承实现，以具体处理 ARR/ARA 消息的封装、发送以及接收、解析的全过程，并将解析的结

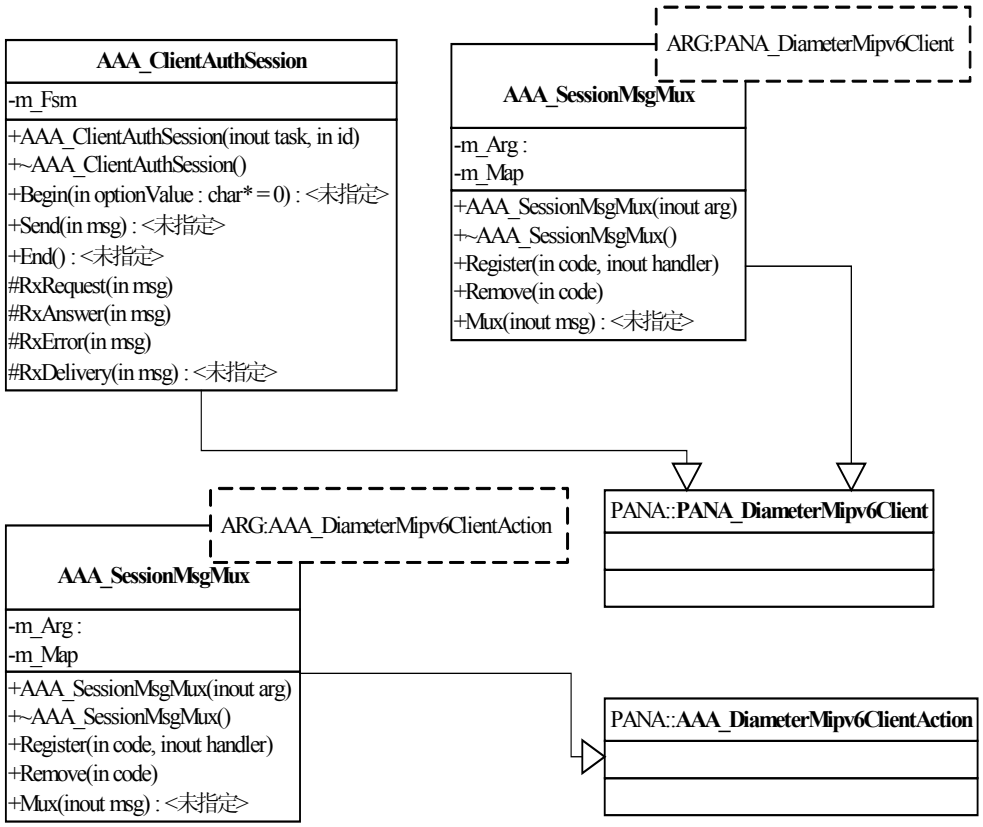


图 6-17 Diameter 通讯模块类图
Fig.6-17 Diameter Communication Module Class Diagram

果作为参数传递并存储在本地维护的会话数据库中供 PAA 模块查询，以完成对移动节点的管理。其中 ARR/ARA 消息对的数据结构类以及消息的解析类已经在 Diameter 移动 IPv6 Server 端模块 API 定义并实现。该通讯模块相关的类静态结构图如上 6-17 所示。

6.5 移动节点 MN 端模块的设计及实现

在移动 IP 中，移动节点需要有相应的机制来处理移动 IP 报头，完成绑定更新等过程。在本文中，只完成移动检测过程以及认证注册过程，当认证注册过程成功之后转交移动 IPv6 相应模块进行正常通信。移动节点的注册认证过程使用 PANA 协议，移动节点本身作为 PAC 网络实体使用 EAP 扩展认证协议的相关安全要求进行 PAA 发现、握手、认证信息加密传输过程。

该模块的基本功能模块如下图 6-18 所示：

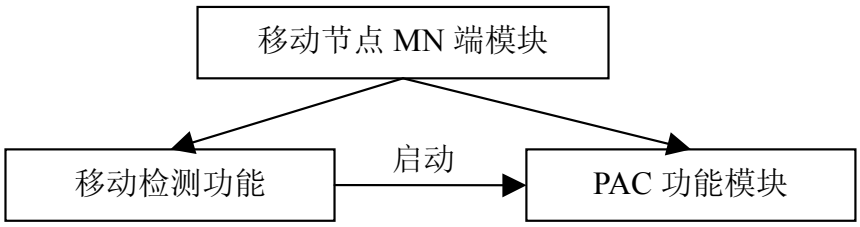


图 6-18 移动节点 MN 端模块功能结构图
Fig.6-18 Function model structure of Mobile Node software

该部分软件开始的时候，从配置文件中读取该节点的本地 AAA 服务器相关配置信息或者使用 PANA 协议的 PAA 发现机制自动发现 PANA 协议的代理节点，发起认证过程接入过程。一旦成功认证，则启动移动 IPv6 的通信模块进行正常通信。同时，不断的时间移动性检测过程，如果发现收到外地 AAA 服务器的路由通告，则启动 PAC 功能模块，与外地 AAA Client 的网络接入功能部分 PAA 功能模块进行通信完成认证过程，然后转到移动 IPv6 模块进行正常通信。该模块的工作流程图如下 6-19 所示

6.5.1 移动检测功能

当移动节点正常接入到网络上之后，启动线程侦听固定端口上的数据包。当移动到外地链路时，并接收到外地链路上的路由通告消息时，经过 IP 层进行相应处理后，根据路由通告消息的网络前缀判定本节点所处的网络。如果是外地网络，则启动 PAC 功能模块发起与 AAA Client 端软件 PAA 模块的认证过程。

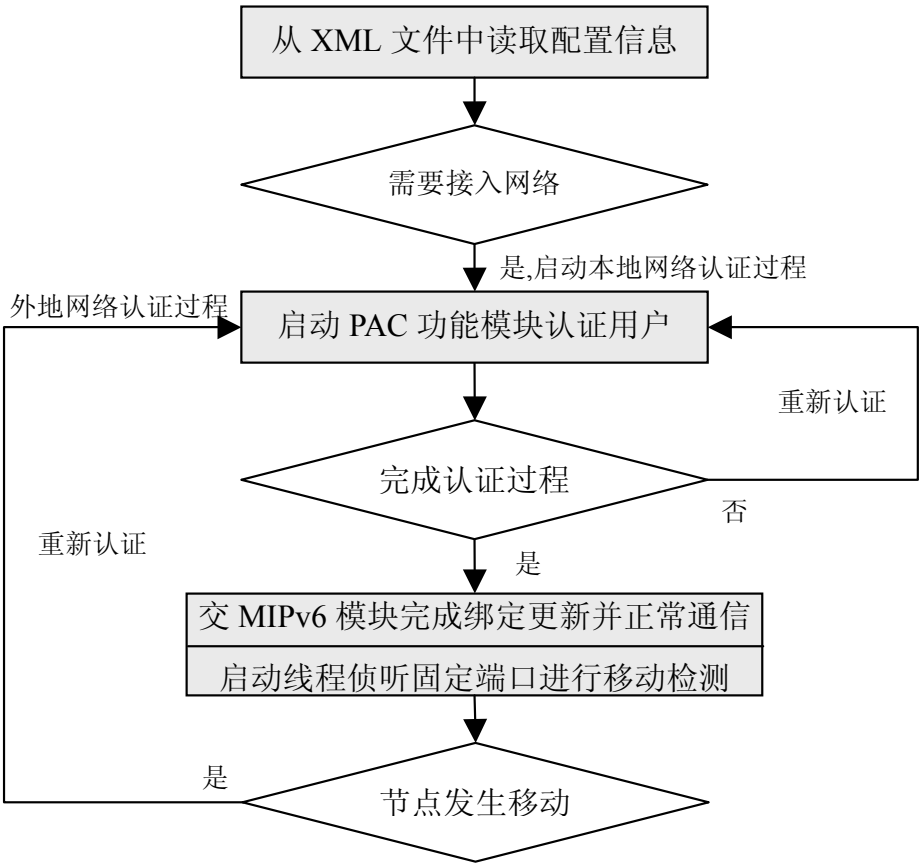


图 6-19 MN 端软件工作流程图

Fig.6-19 Work flow chart of Mobile Node software

6.5.1 PAC 功能模块

PAC 功能模块的初始化过程与 PAA 模块比较相似，PAC 的功能函数也是基于线程的，其附助功能如内存、线程池的管理维护都是相同的。两者最大的不同是 PAC 功能模块中不再需要同 Diameter 通信过程的接口和网络接入控制点模块的接口。PAC 的通过发送请求完成 PANA 协议的发现握手过程并初始化一个 PANA 会话，PAC 实体在任何时候只有一个活动会话，因此不需要会话数据库之类的存储结构。

PAC 发送 PANA-Start-Request 消息请求的时候，根据本地的设备 ID 计算封装一个 Cookie AVP 包含在消息之中。该 Cookie 的计算可以使用 MD5 或 SHA1 等单向散列算法。该 Cookie 的结构如下所示：

Cookie =<secret-version> | HMAC_SHA1(<Device-Id of PaC> , <secret>)

随机产生的序列数<secret>由 PAA 产生，包含在回应的 PANA-Start-Answer 消息中作为一种安全机制防范 DOS 攻击。

PAC 模块的功能结构图如下 6-20 所示。

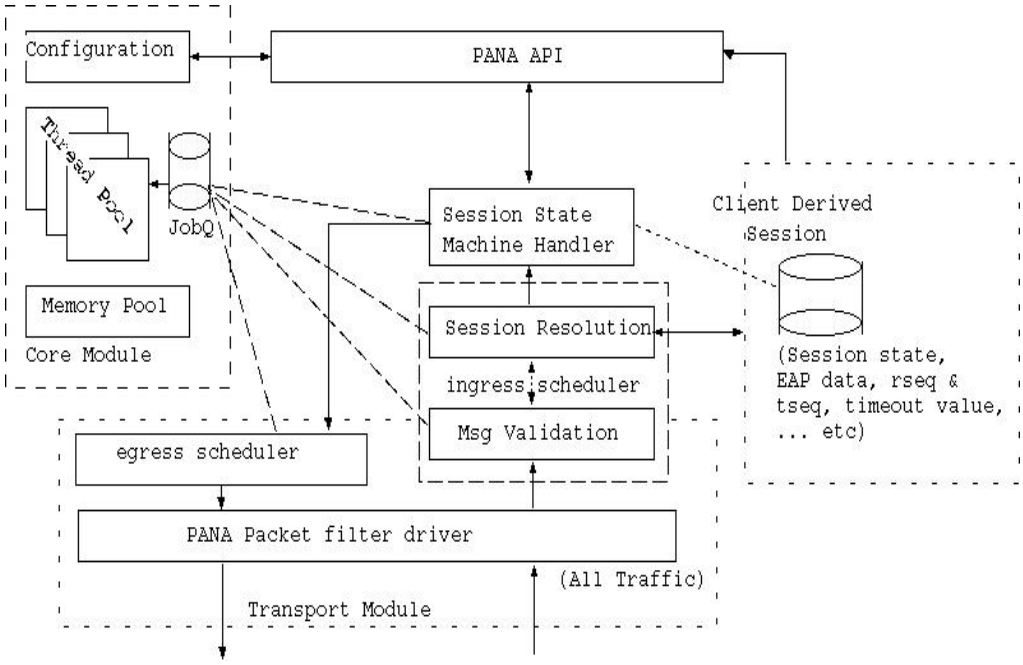


图 6-20 PAC 软件模块体系结构

Fig.6-20 Infrastructure of software module of PAC

第七章　实例测试及总结

7.1　实例测试环境

本实例的目的在于建立一个移动 IPv6 的实验环境，并分别根据上文提供的 API 类库分别构造 Server 端、Client 端和 MN 端软件，完成基本的认证和授权过程。由于 Diameter 协议的记费过程与移动 IPv6 应用扩展中的记费过程没有质的差别，因此不对记费过程进行完整测试。

7.1.1　软件环境

对于操作系统的选择，考虑到 WINDOWS 操作系统被广泛使用的可视化界面，主要的编程和测试工作将在 WINDOWS XP 工作站上进行。由于 API 的开发广泛的采用了 ACE 这种跨平台的 C++类库，开发平台的选择不影响程序的正确性。为了与 OpenDiameter 类库保持一致，编程语言使用 C++。编程开发环境采用微软的 Microsoft Visual Studio .NET 2003，该集成开发环境较好的支持了标准 C++。

7.1.2　硬件环境

本实例测试过程中使用的网络拓扑结构如下图 7-1 所示。在该网络拓扑图中，AAA Server、Client 和接入路由器分为三个部分。在实际测

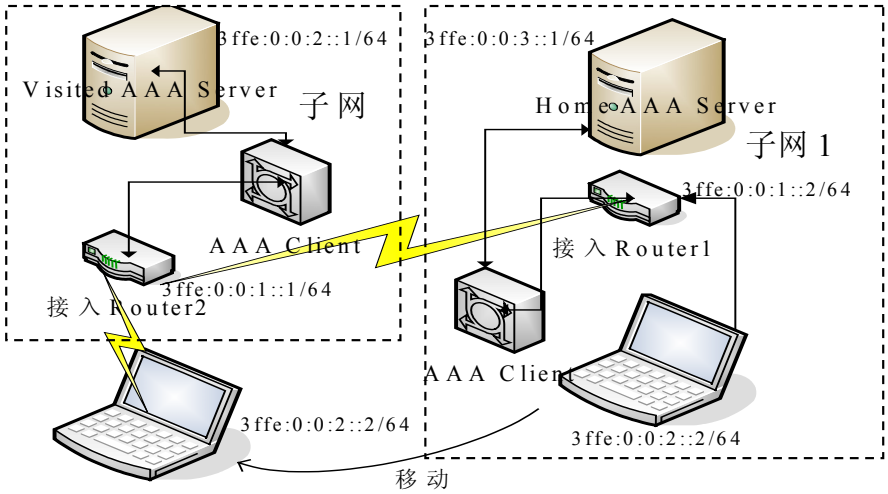


图 7-1　实例测试的网络拓扑结构图

Fig.7-1 Topology structure of network of example

试过程中，由于实验条件的限制，该三部分功能的软件都安装在同一个服务器之上。同样，由于没有无线接入设备，移动节点的移动过程使用

不同的网络接口来模拟位置移动。

7.2 实例测试过程

本实现的测试实例构建的实验环境的配置如下所示：

1、接入 Router1 和本地 AAA 服务器：Router1 的 IPv6 地址为 3ffe:0:0:1::1/64，提供基本的网络接入功能。模拟该路由功能的计算机由 AAA 服务器的 NAS(网络访问接入服务器)模块完成。同时该接入 Router1 连接网络前缀为 3ffe:0:0:1 的子网和网络前缀为 3ffe:0:0:2 的子网。由于实验环境的限制，本实例测试过程中使用装有双网卡的计算机来模拟路由功能。本地 AAA 服务器的 IPv6 地址为 3ffe:0:0:1::2/64，管理域后缀为 lxd.com。由于实验条件的限制，在该服务器上直接安装 Diameter Mipv6 应用扩展服务器软件和客户端软件，简化了 Server 和 Client 之间的通讯过程。配置过程使用命令行模式，直接使用 IPv6 命令给不同的网卡分配 IPv6 地址。

C:\>ipv6 adu 4/3ffe:0:0:1::1

C:\>ipv6 adu 4/3ffe:0:0:2::1

2、接入 Router2 和外地 AAA 服务器： Router1 的 IPv6 地址为 3ffe:0:0:1::2/64，提供基本的网络接入功能。模拟该路由功能的计算机由 AAA 服务器的 NAS(网络访问接入服务器)模块完成。同时该接入

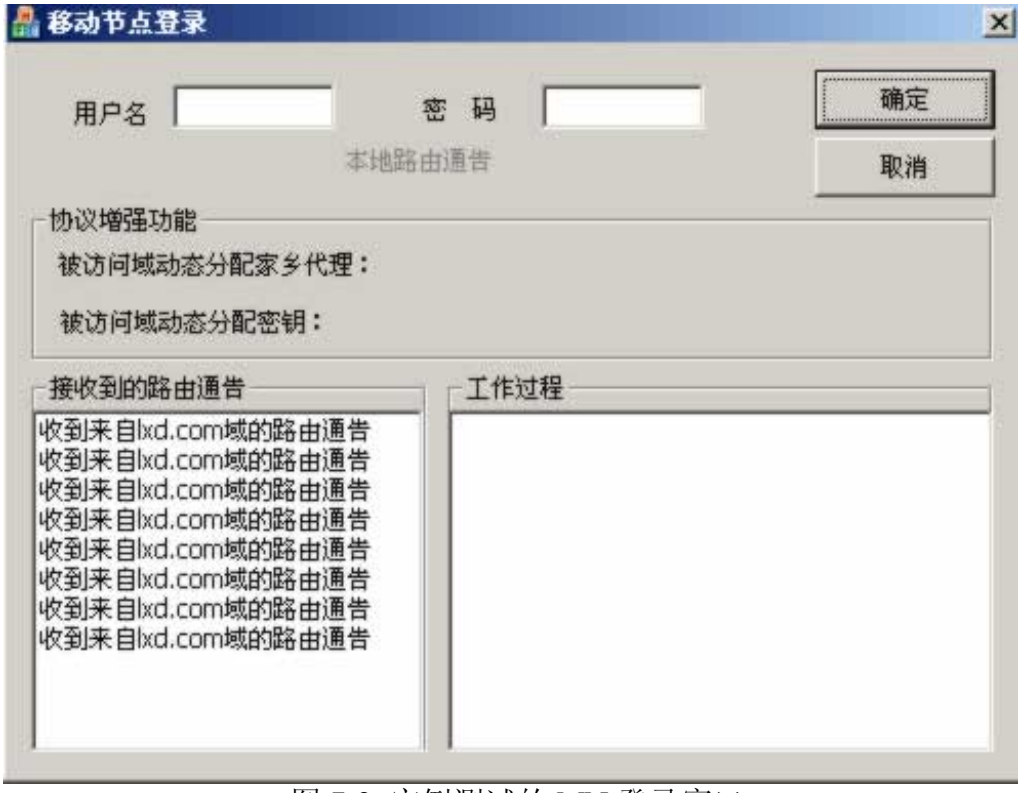


图 7-2 实例测试的 MN 登录窗口

Fig.7-2 Login window of Mobile Node of the test example

Router2 连接网络前缀为 3ffe:0:0:1 的子网和网络前缀为 3ffe:0:0:2 的子网。外地 AAA 服务器的 IPv6 地址为 3ffe:0:0:3::1/64，管理域后缀为 li.com。该服务器上的软件配置过程与本地 AAA 服务器相同。

3、MN：安装 Diameter Mipv6 应用扩展 MN 端软件。初始状态接入子网 1,由本地 AAA 服务器认证。该节点的 IPv6 地址为 3ffe:0:0:2::2/64，NAI 为用户名@lxd.com。

在两台 AAA 服务器上启动 AAA 服务器和 AAA 客户端软件（集成在同一个软件内），同时，AAA 服务器软件启动一个线程发送本管理域的路由通告。在移动节点启动客户端登录软件。如上图 7-2 所示，登录软件启动的时候收到来自本地 AAA 服务器发送的路由通告，通告本管理域的 NAI 后缀。

7.2.1 可漫游用户登录测试过程

1、登录到本地 AAA 服务器。在 MN 登录软件窗口中输入登录的

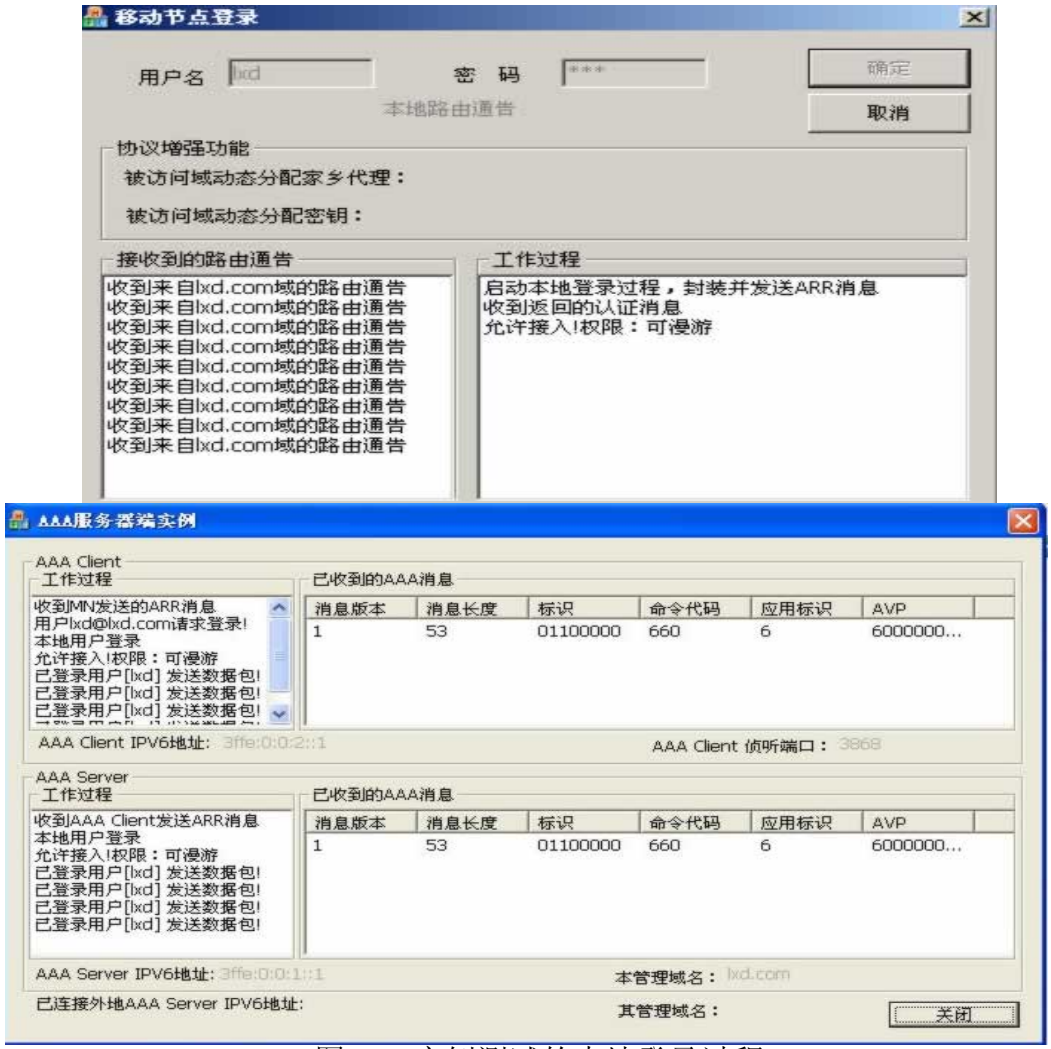


图 7-3 实例测试的本地登录过程

Fig.7-3 The procedure of local login of the test example

用户名和密码，并点击确定。则登录软件根据 PANA 规范向本地 AAA 服务器发送登录信息，AAA 服务器根据本地的配置文件作出认证、授权的决策，并回送 MN 端登录软件。如果认证成功，MN 端登录软件启动一个线程，定时向 AAA 服务器发送数据包。AAA 服务器则捕获该数据包，完成计费过程的模拟。该过程测试过程的登录窗口如上图 7-3 所示。

2、移动节点漫游过程。本实验过程由于没有无线移动实验环境，因此采用了网线插拔来模拟节点的移动过程。当 MN 移动到另一个网络中，根据外地 AAA 服务器发送的路由通告判断已经接入到外地 AAA 服务器。于是开始初始化外地 AAA 服务器的注册过程，外地 AAA 服务器收到异地用户的注册消息后，向 MN 节点的本地 AAA 服务器发送客户的认证信息，在收到 MN 节点的本地 AAA 服务器认证、授权结果后，将认证、授权结果回送给 MN。并根据认证的结果决定是否允许接入，如果允许接入，则由模拟路由器转发该节点发送的数据包；否则，

图 7-4 可漫游用户实例测试的异地漫游登录过程

Fig.7-4 The procedure of foreign login of mobile enable user in the test

拒绝接入，模拟路由器过滤该节点发送的所有数据包。该实验的外地 AAA 服务器认证、授权过程如上图 7-4 所示。

7.2.2 不可漫游用户登录测试过程

不可漫游用户在本地登录过程同可漫游用户在本地登录过程相同。当不可漫游用户漫游到外地网络的时候，外地 AAA 服务器同样向移动

图 7-5 不可漫游用户实例测试的异地漫游登录过程

Fig.7-5 The procedure of foreign login of mobile unenable user in the test example

节点 MN 的本地 AAA 服务器发送认证请求信息，本地 AAA 服务器根据认证信息作出认证、授权决策并回送外地 AAA 服务器。外地 AAA 服务器根据认证、授权结果决定是否允许动节点接入。该过程 AAA 服务器之间的信息交换过程如上图 7-5 所示。

由于此次登录的用户的权限为不可漫游用户，因此，当移动节点移动到外地网络管理域时，外地 AAA 服务器通过与移动节点 MN 的本地 AAA 服务器之间的通信得到该节点的认证、授权信息。并拒绝该用户的接入，同时配置模拟路由器拒绝转发任何该节点发送的数据包。

7.3 全文总结

当今 Internet 发展日新月异，新的技术应用不断涌现，网络用户也急剧增加，对网络接入过程的管理和控制日益重要。同时，作为未来的移动网络服务方案，移动 IPv6 是一个十分活跃的研究热点之一。本文主要讨论了 IETF 提出的下一代 AAA 服务器协议 Diameter 协议和移动 IPv6 相关技术，然后在此基础上提出了基于 Diameter 协议的移动 IPv6 应用扩展协议的细节。在此协议的基础上，讨论了 OpenDiameter 开源类库的实现，并结合该类库给出 Diameter 协议移动 IPv6 应用扩展协议的实现类库设计。最后，使用此类库实现一个 Diameter MIPv6 应用的 Server、Client、MN 三个软件实例，并在模拟的移动 IPv6 环境中测试了库的正确性。

由于时间和条件的限制，在实验测试的时候作了部分简化，仅完成节点的基本认证、授权过程和模拟计费功能的数据包捕获。同时，EP 的功能没有具体的实现，仅是简单使用 IP 过滤手段控制接入节点的数据包发送。另一方面，由于本文限于 AAA 协议的研究与实现，所以没有完成对移动 IPv6 的实现。只是简单的实现了路由通告和移动测试部分功能，没有完整实现家乡代理的功能。因此，本文还可以作如下几点的改进：

1、完善 PAA 功能模块与 EP 之间的接口。使用 SNMPV3 对 EP 进行设置，控制用户接入。

2、完善 Diameter 协议与移动 IPv6 协议栈实现模块的无缝结合。实现家乡代理 HA 对 Diameter 消息的解析以及绑定更新过程的优化。

参 考 文 献

[1] 赵慧玲、叶华等。以软交换为核心的下一代网络技术，人民邮电出版社，第 1 版，第 3 页，2002.8
[2] 刘清、乐燕群。AAA—维系运营商与用户联系的命脉, 计算机世界报，第 02 期 B4、B5 版，2003
[3] B.Aboba，”Criteria for Evaluating AAA Protocols for Network Access，RFC2989”，November 2000
[4] D.Mitton， M.St.Johns，”Authentication Authorization and Accounting Protocol Evaluation”，RFC3127，June 2001
[5] S.Farrell，J.Vollbrecht，”AAA Authorization Requirements”，RFC2906，August 2000
[6] 黄岚兰、王能。Internet 中 AAA 协议的概述及比较，微型电脑应用，第 6 期，第 7 页，2003
[7] B.Aboba，J.Wood，”Authentication, Authorization and Accounting (AAA) Transport Profile”，RFC3539，June 2003
[8] John Nagle，”Congestion Control in IP/TCP Internetworks”，RFC896，January 1984
[9] 孟小华。RADIUS 服务器性能测试软件的设计与实现，微型机与应用，第 6 期，第 12 页，2004
[10] 张海峰、姜建国。RADIUS 协议安全性分析，计算机工程，第 7 期，第 122 页，2004.5
[11] 邓微波、张雄。基于 LDAP 的 TACACS 服务器，计算机应用，第 24 卷，第 120 页，2004.6
[12] 陆正福、杨洋。COPS 协议的分析及其 Petri 网建模，计算机工程，第 30 卷第七期，第 82 页，2004.4
[13]乐燕群、刘清。Diameter 就是“万金油”－Diameter 的两种应用，计算机世界报，第 02 期 B7、B8 版，2003
[14] IPv6 支撑移动互联网的基石 http://www.cnii.com.cn/20020808/ca88960.htm
[15] S. Deering，R. Hinden，”Internet Protocol Version6(IPv6) Specifica -tion”，RFC2460，December 1998
[16] R. Hinden，S. Deering，” IP Version 6 Addressing Architecture”，RFC 2373，April 2001
[17] 杨映红、陈志。IPv6 地址结构解析，重庆大学学报，第 26 卷 10

期，2001.10
[18] 刘水生、张永明。新一代的网络安全协议－IPv6，天津通信技术，第 4 期，2003.12
[19] 董晓虎、徐明伟等。密钥交换协议 IKE 实现的可扩展设计，小型微型计算机系统，第 25 卷 6 期，2004.6
[20] 孙利民、阚志刚等。移动 IP 技术，电子工业出版社，第 1 版，2003.8
[21] 胡旭栋、于建华等。对移动 IPv6 中重定向攻击的防御，计算机工程，第 30 卷 11 期，2004.6
[22] 赵源超、陈健等。新一代的 AAA 协议—Diameter，中国数据通信，第 11 期，2004.11.16
[23] P. Calhoun，J. Loughney,etc.，”Diameter Base Protocol”，RFC3588，September 2003
[24] 裘姝平、陈能干。基于 Diameter 协议的 AAA 的研究，计算机应用，第 23 卷 10 期，2003.10
[25] 邱锡鹏、刘海鹏。Diameter 协议研究，计算机科学，第 30 卷 2 期，2003.2
[26] E. Guttman，C. Perkins,etc.，”Service Location Protocol, Version 2”，RFC2608，June 1999
[27] 王焕宝，张佑生等。IPSEC 下安全关联协商的实现环境，安徽机电学院学报，第 17 卷第 2 期，2002.6
[28] 孔凡玉，李大兴。IPSEC 中 IKE 协议的安全性分析与改进，计算机应用研究，第 3 期，2003.7
[29] T. Dierks，C. Allen，” The TLS Protocol Version 1.0”，RFC3588，January 1999
[30] R. Calhoun，Glen Zorn，”Diameter Network Access Server Application”，draft-ietf-aaa-diameter-nasreq-17.txt，July 2004
[31] 徐霖洲，丘海明 等。PPPoE 原理、应用及改进建议，中山大学学报(自然科学版)，第 41 卷 6 期，2002.11
[32] P. Eronen，T. Hiller etc.，”Diameter Extensible Authentication Protocol (EAP) Application”，draft-ietf-aaa-eap-10.txt，November 2004
[33] 熊海泉，滑雪增等。PPP 上的 EAP 可认证扩展协议，计算机工程，第 29 卷 13 期，2003.8
[34] D.Forsberg，Y.Ohba，” Protocol for Carrying Authentication for Network Access”，draft-ietf-pana-pana-07.txt，December 2004
[35] A.Yegin，Y.Ohba，” Protocol for Carrying Authentication for Network Access (PANA) Requirements”，draft-ietf-pana-requirements-09.txt，August 2004

[36] M.Faccin，E.Perkins，”Diameter Mobile IPv6 Application”，draft-le-aaa–diameter-mobileipv6-03.txt，August 2004
[37] B.Aboba，M.Beadles，”The Network Access Identifier”，RFC2468，January 1999
[38] R.Calhoun，E.Perk etc.，” Diameter Mobile IPv4 Application”，draft-ietf-aaa-diameter-mobileip-20.txt，August 2004
[39] Diffie W, Hellman M. New directions in cryptography [J] .IEEE Transaction on Information Theory, 1976, IT-22(6): 644-654.
[40] 孔晖, 郑志华, 徐秋亮。几种典型的认证 Diffei-Hellman 型密码共识协议的分析与比较,计算机工程与应用，2001.18
[41] Open Diameter Software Architecture, http://diameter.sourceforge.net/diameter-architecture/index.html
[42] Stephen D.Huston,James CE Johnson 著,马维达译。ACE 程序员指南——网络与系统编程的实用设计模式,中国电子出版社,2004.11
[43] BOOST C++ Libraries, http://sourceforge.net/projects/boost/
[44] 王志海。OpenSSL 与网络信息安全-基础、结构、指令, 中国 OpenSSL 专业论坛 http://openssl.cn/file/openssl-1-gaishu-1.pdf
[45] Stanley Lippman, Josée Lajoie 著,潘爱民、张丽译。C++ Primer 中文版，中国电力出版社,第二版,第 362 页
[46] Peterchen，”Smart Points to Boost Your Code”，http://www.codeproject.com/ vcpp/stl/boostsmartptr.asp
[47] 马红华、灯芯工作室编著，用 XML 轻松开发 WEB 网站,北京希望电子出版社,2001.2,第二版,211
[48] W. Stevens，M. Thomas,etc.，” Advanced Sockets Application Program Interface (API) for IPv6”，RFC3542，May 2003
[49] Samita Chakrabarti，Erik Nordmark，” Extension to Sockets API for Mobile IPv6”，draft-ietf-mip6-mipext-advapi-03.txt，September 2004
[50] Victor I. Fajardo，” PANA Functional Architecture”，http://diameter.sourceforge.net/pana/index.html，Feb 6, 2004

摘要

由于网络的发展以及业务的要求，电话网、计算机网、有线电视网三网融合的需求日益迫切，下一代网络 NGN、移动 IP 以及 IPv6 技术得以迅速发展。以 IP 技术为核心的 IP 网络，因其灵活多样的接入方式和低成本的易于扩展的应用业务，成为网络融合的主导力量。虽然原有的互联网最早的几种 AAA 技术，如 TACACS、RADIUS 已经得到广泛的应用，但是由于协议设计的固有缺陷使得它们在新的业务认证、授权以及计费体系中已经力不从心，面对移动 IPv6 环境下的 AAA 过程更是束手无策。因此，在 IETF 的推动下，AAA 的新框架结构 Diameter 技术已经成型，Diameter 协议已经成为支持新业务的 AAA 过程的协议标准。

Diameter 协议是一个协议族，它包括了一个基础协议和若干个应用协议扩展组成。基础协议中定义了 Diameter 协议的报头规范、AVP 报文规范、各种 Diameter 网络实体的体系结构和安全方面的要求等。在此基础协议之上，可以灵活的扩展出很多针对不同业力类型的 Diameter 应用协议，如提供网络服务的 NASREQ 应用协议扩展、针对移动 IPv4 的应用协议扩展、针对 SIP 协议的应用协议扩展等。虽然从较高层次上看 MIPv4 和 MIPv6 是相似的，但事实上在考虑到内部域部署的时候有很大的不同。例如 MIPv6 没有等价于 MIPv4 的外地代理，并由此无法定义任何机制通过外地代理访问网络以及认证、授权访问网络资源。

本文在深入研究 Diameter 相关协议族的基础上结合 PANA 协议给出了移动 IPv6 认证、授权、计费基本过程的框架以及移动 IPv6 相关的一些特殊需求过程(如，在被访问网络域动态分配家乡代理、密钥分配等)的基本框架，并在根据此扩展协议在 OpenDameter 开源代码的基础上设计了 Diameter 协议移动 IPv6 应用扩展的类库。最后，在开发实现的类库基础之上，构建了一个模拟的移动 IPv6 网络实验环境，并在该实验环境上测试了类库设计开发的正确性。

Diameter 协议的应用扩展是通过定义新的消息和新的 AVP 负载值来完成的，在 MIPv6 环境下，现定义四个新的 Diamter 消息是用于 MIPv6 的 AAA 过程：(AA-Registration-Request, AA-Registration- Answer,Home-Agent-MIPv6-Request,Home-Agent-MIPv6-Answer)和 AVPs(MIP-Binding-Update AVP , MIP-Binding-acknowledgement AVP, MIPv6-Mobile-Node-Address AVP, MIPv6- Home-Agent-Address AVP, MIPv6- Feature-Vector AVP, Key-Request AVP, MN-Key-Distribution AVP, Key-Distribution AVP)以完成 AAA 过程、被访问网络域动态分配家乡代理地址、密钥再分配

过程。同时最大程度的重用了 Diameter 基础协议中已经定义的消息及 AVP 负载，如完成 Diameter 节点间能力交换的 CER/CEA 消息对、EAP 认证扩展中的 DER/DEA 消息对。

PANA 协议运行在客户端(PAC)和服务器端(PAA)之间以完成网络访问服务过程。该协议是基于 UDP 协议之上的，但拥有完善的重传机制以可靠的传送消息。在该中协议里包含了一系列请求和应答消息，这些请求和应答消息的内容被用在端到端的认证过程，每一个消息都是由零个或多个 AVP 负载来实现的。PANA 的主要负载都是 EAP 消息，用于 PAC 和 PAA 之间建立 EAP 会话。在本文中，将 PANA 协议与 Diameter 协议结合起来，完成移动节点 MN 与 AAA Client 之间信息交换过程。移动节点 MN 和 AAA Client 分别作为 PANA 协议体系中的网络实体 PAC 和 PAA，同时，AAA Client 还作为 Diameter 协议体系结构中 AAA 客户端同 AAA 服务器端进行通讯。AAA Server 在启动之时，就发起同其他管理域的 AAA Server 的通讯，并通过能力交换得知对端节点支持的 Diameter 服务。

移动节点可能不总有一个提前配置的 IPv6 地址，并且可能需要有一个动态分配过程。此外，家乡代理和移动节点家乡地址需要在相同的链路上，以支持被访问域的动态的家乡代理分配和被访问域的动态家乡地址分配。即使当家乡代理是在家乡网络中被分配的，这种动态家乡地址分配的特征也提供了更多的灵活性。这个针对移动 IPv6 的应用扩展了 Diameter 消息，使用 HOR/HOA 来封装相关 AVP 值，实现该功能。

移动 IPv6 节点在漫游过程中需要建立很多安全密钥在 IPv6 移动节点和其他网络实之间共享，例如：在移动节点和他的家乡之间的密钥，用来认证绑定更新和绑定确认消息；在移动节点和访问路由器之间的密钥用来保护（例如机密性和完整性保护）访问链路上的数据安全。因此，当 AAA 服务器可以充当一个密钥分配中心的角色，在移动节点漫游过程中完成密钥的分配。在该过程当中可以使用基于随机数的密钥分配或 Diffie-Hellman 密钥交换的分配方式。

在协议的实现方面，本文学习借鉴了 OpenDiameter 开源软件包代码，并重用了其中已经实现的 Dimaeter 基础协议的类库、EAP 认证扩展的类库、PANA 认证过程的类库。选择 OpenDiameter 开源软件包是原因是，该软件是目前开发最完善的 Diameter 协议开源软件包。其软件架构实现大量使用了 ACE 开发的设计模式，如 SOCKET 接受者，连接者和线程池模式都得到了应用。除了基于模式的 ACE，由 ACE 库提供的 OS 抽象层也被大量利用在该实现中。该软件已经注意尽力使实现是独立于平台的。所有的系统调用都是通过利用 ACE 提供的抽象来使用的。由于 ACE 的全面使用，OPEN DIAMETER 库的支持平台同 ACE

类库一样拥有良好的跨平台特性。

Diameter MIPv6 应用扩展协议的实现从功能的角度划分应该包括如下三个模块，分别为：AAA Server 端模块、AAA Client 端模块、移动节点 MN 端模块。AAA Server 端模块：其主要功能是提供消息的解析、安全传输、建立与 AAA 实体的安全连接、会话管理等功能，该模块是核心模块。AAA Client 端模块：位于移动节点 MN 端软件模块同 AAA Server 软件模块之间，其主要功能是作为 PAA 节点完成移动节点 MN 的接入认证过程、与 AAA Server 端软件模块交互以及认证信息数据的发送接收、定期发送路由通告等。事实上，AAA Client 端软件模块应该位于 NAS（网络访问服务器）或支持接入功能的路由器上，不但能够完成接入功能，还能在完成认证之后根据认证结果转发或过滤移动节点发送的数据包。同时，AAA Client 还应该完成对移动节点使用网络资源数据的收集功能定时向 AAA 服务器发送计费信息。移动节点 MN 端模块：该模块不断的监听网络上的路由通告，根据路由通告内容判断移动节点的位置信息并充当 PAC 节点与 AAA Client 的 PAA 模块完成登录认证过程。

对于系统开发环境的选择，考虑到 WINDOWS 操作系统被广泛使用以及良好的可视化界面，主要的编程和测试工作将在 WINDOWS XP 工作站上进行。同时，由于 WINDOWS XP 上已经提供了对 IPv6 相对完善的支持，只需要在命令行下输入 IPv6 Install 就可以启动并配置，为程序的开发调试带来便利。为了重用 OpenDiameter 已经实现的类库，编程语言采用了与之一致的 C++。

由于实验环境的限制，在对已经完成的 API 进行实例测试的过程中，将 AAA Server 与 AAA Client 集成到同一个服务端软件内部。由于针对移动 IPv6 的应用协议扩展中的 AAA 过程主要改动主要是 Diameter 消息和 AVP 值。以及本地 AAA Server 和外地 AAA Server 之间的通讯、AAA Client 和 MN 之间的 PANA 认证过程，而 AAA Client 与 Server 端之间消息发送和解析过程与 Diameter 基础协议没有差别。因此，这种实例的简化不会影响测试结果的正确性。基于同样的原因，由于没有支持 IPv6 接入的路由设备，在本文的实例测试过程中使用配置了双网卡的计算机来模拟接入路由器的功能。

经过对两组用户(可漫游和不可漫游)的测试，移动节点的 AAA 基本过程、在外地接入网络中的动态家乡代理地址分配、密钥分配过程都正确的完成了任务。可以基于该 API 基础之上进一步扩展基于 Diameter 协议的 AAA 服务器对移动 IPv6 的支持。

ABSTRACT

With the development of the network technology and the demand of the various service, the next generation network(NGN),mobile IP and IPv6 have been improved more rapidly and the integration of the three incompatible networks(telephone network, computer network and TV network) has became more and more important. At the same time, IP network becomes the leading power in the process of the integration of the incompatible networks because of its excellent features, such as, the convenient connection method , the low cost and easy expandability of business application and so on. Although the AAA (Authentication , Authorization , Accountting) technology in previous internet network, such as TACACS and RADIUS, has been used in wide fields,they can't work well in the new network condition,especially in the process of AAA for mobile IPv6.Hence,a new protocol for AAA, Diameter protocol, which was recommended by IETF has became the standard protocol for the various applications.

Diameter protocol is the name of a protocol family, a Diameter base protocol and several interrelated application protocols are included in it. In the Diameter base protocol, some base network entities and operations were specified,while the Diameter header,AVP header and the secure demand were also defined in it. Based this Diameter base protocol, some protocols were developed for different application fields, such as mobile IPv4 application, SIP application,NASREQ application and so on.Although MIPv6 application protocol looks like MIPv4 application protocol in the higher level,in fact,there are many differences between them.For instance,there is no foreign agent in MIPv6 protocol,so that mobile node can't visited network resource through foreign agent.

In this thesis, I will specify the protocol profile of the basic process of AAA of MIPv6 node and some enhanced features related with MIPv6 by studied deeply in Diameter protocol family and PANA protocol will be used with Diameter base protocol together for provided authentication and authorization. And then I designed and developed the class library for mobile IPv6 based on the MIPv6 application that is specified previously and the open resource software OpenDiameter. Finally, a simulated network

circumstance for MIPv6 was set up and the correctness of the class library for Diameter MIPv6 application protocol was testified.

Expanding the Diameter base protocol can be fulfilled through defining new Diameter messages and new AVP payload types. In circumstance of MIPv6,I will define four messages (AA-Registration-Request,AA-Registration-Answer, Home-Agent-MIPv6-Request, home-Agent-MIPv6-Answer) and some new AVPs (MIP-Binding-Update,MIP-Binding-acknow -ledgement,MIPv6-Mobile-Node-Address,MIPv6-Home-Agent-Address,MI Pv6-Feature-Vector,Key-Request,MN-Key-Distribution, Key-Distribu -tion) for basic AAA process of mobile IPv6 node, dynamic home agent address assignment in visited domain and Key distribution. In design of this Diameter MIPv6 application protocol, I did my best to reuse the Diameter messages and AVPs which have been defined in Diameter base protocol. Such as,CER/CEA and DER/DEA.

PANA protocol is defined to finish the process of authentication between client (PAC) and server (PAA).This protocol utilize UDP transport protocol, but it defines reliable re-transport mechanism for the correctness of the message exchange. In this protocol, a series of request/answer messages are used in the process of peer-to-peer authentication, and every message is composed by zero or more AVPs payload. The payloads in this protocol are almost EAP messages and used in EAP session between PAC and PAA.In this thesis,PANA protocol will cooperate with Diameter protocol to fulfill the message exchange process between MN and AAA client. Based on PANA protocol framework, Mobile node software acts as PAC and AAA client acts as PAA.At one time,AAA client should communicate with AAA server to exchange Diameter messages, and must have the ability to parse such messages. When AAA servers begin to initialize, it should connect to other AAA servers and learn which service can be supported by other AAA servers through capability exchange request and answer.

Mobile nodes may not own their static IP address at any time, so that dynamic assignment Home Agent address in visited domain is necessary. This mechanism provides a better flexile method to support the roam of the mobile node. In this section, I added a pair of Diameter messages (HOR/HOA) and defined a set of AVPs to solve it.

As identified in the previous sections, many security keys need to be set up and shared between the IPv6 mobile nodes and other network entities, for example, the key between the mobile node and its Home Agent to

authenticate the binding Update and Binding acknowledgement messages. The AAA entities can play a major role in the computation and distribution of these security keys. Two key distribution methods, relying on this AAA infrastructure and allowing authenticated key distribution, are proposed. In this process, two methods can be used, one is based on random number distribution ,and the other is based on Diffie-Hellman key exchange distribution.

In the aspect of implementation, I learn more from OpenDiameter software and reuse quite a few class library which had been done in OpenDiameter software packet. such as, class library for Diameter base protocol,EAP protocol and PANA protocol etc.At present,OpenDiameter is the best software packet, many excellent design patterns that be designed by ACE are used, such as Socket Connector/Acceptor design pattern, thread pool design pattern and so on. Besides such design pattern,OS abstract level developed by ACE is also took by OpenDiameter for independence from the concrete Operation System. Because of the widely using ACE library, OpenDiameter can work well in different OS platform.

From the point of view of the function, the implementation of the Diameter MIPv6 application protocol should include three parts:AAA Server module,AAA client module,Moble Node module. AAA Server module that be a core module will perform such tasks: parsing message,secure transmission,establishing connection with AAA entities,session manage etc.AAA Client module will perform such task:Actting as a PAA entity to perform the authentication process with Mobile Node, communicating with AAA Server and exchanging Diameter messages, collecting the network resource information that is used by Mobile Node and encapsulating it into Diameter message which will be sent to AAA Server after a period.Mobile Node module: listening router advertisement, if the location of MN has changed, it can initialize a re-login process to the visited domain. In this situation, it act as a PAC entity.

Considering the widely deployment of the WINDOWS operation system and the good developing environment, I choose the WINDOWS XP as the platform of programming. At the same time,XP OS has support IPv6 protocol stack completely and can easily install, so that will be helpful to code, compile and test. For being accordance with OpenDiameter software packet, I choose the C++ as the programmed language.

According to the limit of the experiment environment, I integrate the

AAA Server module and AAA Client module as one server software in this example which is designed to testify the correctness of Diameter MIPv6 protocol API.Because the important change of the Diameter MIPv6 application is Diameter messages and AVPs，the communication between Home AAA Server and Visited AAA Server, the process of authentication based on PANA protocol between AAA Client and MN.Sending Diameter messages between AAA Server and AAA client has no different with Diameter base protocol. So this predigestion has no effect on the correctness of the API.As the same reason, I make use of a computer which gets two network cards to replace the router which support IPv6 protocol.

After being tested carefully to the different users(owning roam purview or not),the API of Diameter MIPv6 application protocol can work correctly in the basic process of AAA,dynamic assignment Home Agent address in visited domain and key distribution. The AAA Server based on Diameter protocol can be extend their service capability by this way.

致谢

本文是在我的研究生导师魏达老师的悉心指导下完成的。在这宝贵而难忘的三年硕士学习生涯中，魏老师在生活和学习的方方面面都给了我精心的指导和悉心的帮助。在论文脱稿之际，首先衷心的向我的导师魏老师表示感谢！同时，论文工作中得到了刘衍珩教授的多方面的帮助，使我顺利的完成了毕业设计和学位论文，在这里我向刘衍珩老师表示衷心的感谢！

由于本文的研究与实现过程中大量的借鉴了 OpenDiameter 开源软件包源代码的设计思想并重用了其 Dimaeter 基础协议实现类库，在此向 OpenDiameter 的开发者致以最大的敬意，同时对推动开源软件开发的网站 SourseForge.Net 表示感谢。正是该网站提供的空间以及 Mail List，给大家提供了一个相互交流的平台，使我能迅速得到最新的文档及资讯，并最终完成论文的写作和相关代码的实现。

此外，还要衷心感谢我的父母、妻子，在远方默默的给予我的支持和关怀；还有我可爱的儿子，虽然他不在我和身边，但对他的想念也是激励我前进的动力之一。

最后向所有曾给予我鼓励和帮助的在这里未能提及的老师、同学、朋友以及参考文献的作者们表示最高的敬意！

导师及作者简介

魏达(1964--),性别：男；民族：汉；吉林舒兰人。吉林大学计算机科学与技术学院博士研究生，副教授，主要从事计算机网络管理和网络安全研究。联系方式 Tel: 0431-5690186，E-mail: weida@email.jlu.edu.cn；

李晓东（1976--）, 性别：男；民族：汉；河南郑州人，吉林大学计算机科学与技术学院硕士研究生，主要从事网络和信息安全研究。联系方式 Tel: 13844983008，E-mail: lixiaodong317@ yahoo.com.cn。

在校其间发表论文：

魏达、刘衍珩、李晓东 基于 Diffie-Hellman 密钥交换的 WEB 安全传输，吉林大学学报 信息版 2005 年第三期。