Diameter 协议研究

邱锡鹏　刘海鹏
(复旦大学计算机科学与工程系　上海200433)

Research on Diameter Protocols

QIOU Xi-Peng　LIU Hai-Peng
(Department of Computer Science and Engineering, Fudan University, Shanghai 200433)

Abstract Diameter is the next authentication, authorization and accounting protocol currently developed in the IETF AAA working group, which will replace the widely and successfully deployed Radius protocol. In the paper, the motivations and backgrounds of Diameter protocols are firstly introduced. The following is a detailed description of the Diameter base protocol and its applications, such as mobile IP, NASREQ. Then the comparisons and analysis between Diameter and Radius are given.

Keywords Diameter protocols, Radius protocol, SCTP, AAA protocol

1 引言

Radius(Remote Access Dial In User Services)协议[1]已经被成功而广泛地应用在拨号 PPP/IP 和移动 IP 网络中，用以提供鉴别、授权和计费 AAA(Authentication Authorization and Accounting)服务。但是，由于 Radius 协议内在的缺陷，不但使其在功能日益强大的路由器和网络接入服务器中的应用受到限制，而且不能满足新兴应用对 AAA 服务扩展功能的要求。当前，IETF 的许多工作组正在或已经指定许多新兴应用对 AAA 协议的需求：

(1)IETF 的移动 IP 工作组(IP Routing for Wireless/Mobile Hosts)制定了移动 IP 在域间切换时对 AAA 的需求[2]。

(2)电信工业协会(the telecommunication industry association)TR-45.6下属的无线包数据技术(wireless packet data technology)工作组制定了 CDMA2000蜂窝网络对 AAA 的需求[3]。在 TR-45.6工作的基础上，3GPP2已经决定采取两个阶段在无线蜂窝网络中实现 IETF 制定的协议；第二阶段对 AAA 功能的要求不是 Radius 所能支持的。

(3)IETF 的接入访问服务需求 NASREQ(the NAS requirements)工作组对下一代接入访问服务 AAA 的要求进行了制定[4,5]。

(4)IETF 的漫游操作 ROAMOPS(the roaming operations)工作组制定了对漫游网络的需求[6]。

这些新兴应用直接推动 Diameter 协议的出现。作为 Radius 协议的增强版本，Diameter 协议在许多方面保持与 Radius 的兼容性，以方便移植。例如，Diameter 消息包含属性值对 AVP，这一点与 Radius 消息的 TLV(Type Length Value)非常相似。Diameter 包括一个基础协议和一个或若干个应用，这种设计结构便于协议的扩展，以适应新的网络接入技术。

2 背景知识

2.1 Radius 协议简介

Radius 协议[1]是上世纪90年代初设计的用于解决网络接入服务器 NAS 对拨号用户的鉴别、授权与计费问题。Radius 工作在 Client/Server 模式，使用 UDP 作为传输层协议。Radius 的功能简要介绍如下：

(1)Radius 采用 UDP 协议，使得服务器端的实现比较简单，在一定时间内未收到响应消息后可以马上重发一个 UDP 消息而不需要关心前一个消息是否到达，使得对用户的鉴别可以在很短的时间内完成，但 UDP 由于没有出错重发机制，影响了鉴别的可靠性。

(2)Radius 提供多种服务类型，支持 PAP, CHAP, Unix login 等多种鉴别机制，这样针对不同用户的安全性需求，可灵活、方便地制定安全策略。由于结合了共享密钥、数字签名等技术，Radius 既可以验证用户的身份又不致于在网络上暴露用户的秘密口令，克服了传统的单纯"用户名－口令"鉴别方式。

(3)Radius 支持 Proxy 功能，既可以转发由 NAS 发过来的 Radius 请求消息，也可以转发由其 Radius 服务器发出的响应消息。

(4)Radius 将鉴别和服务部分分开，用户数据集中存放便于维护和升级，增加服务或改变接入方式时不需要再改变鉴别系统。

2.2 流控制传输协议 SCTP

Diameter 协议使用具有流量控制、传输确认和重传功能的 SCTP 或 TCP 传输协议。流传输控制协议 SCTP[7](stream control transmission protocol)是较新的传输层协议，与 UDP 和 TCP 位于同一层次。SCTP 在有些方面与 TCP 相似，如：

(1)SCTP 在两个端节点之间提供一种面向连接的传输服务；

(2)SCTP 提供可靠传输，确保数据的按序发送，无丢失和无重复；

(3)SCTP 提供完全的双向数据传输功能；

(4)SCTP 利用滑动窗口机制进行流量控制。

另一方面，SCTP 提供了下述 TCP 不具备的功能：

(1)SCTP 在两个端节点之间能提供多个数据流。对于每一个数据流，均能保证报文的无丢失、无重复和按序发送。单独的数据交换可以在多个流上同时进行，其中一个流上的报

文丢失并不影响其它流的数据传输。TCP 只能提供一个流的数据传输，单个报文的丢失会影响后续报文的发送，这种现象称为线头阻塞(head-of-line blocking)问题。减少线头阻塞是SCTP 的功能之一，这种特性非常有利于 Diameter 协议。

(2)SCTP 是面向报文的，SCTP 保持报文边界，并能为上层协议发送完整的报文。TCP 是面向字节的，在传输的字节流中不能保持报文边界，需要上层协议自己处理。

(3)SCTP 能识别并能利用多址主机(multi-homed host)提供的功能。多址主机具有一个或多个 IP 接口。在初始化阶段，对等 SCTP 节点可以交换自己的 IP 接口地址池。需要重发的 SCTP 消息可以使用另外一个 IP 接口进行发送，从而增强发生网络故障时 SCTP 会话的恢复能力。SCTP 利用多址的目的是进行冗余，而非负载平衡。相对而言，TCP 会话在端节点只能使用单一的 IP 地址，IP 接口的失效将导致整个会话的失败。

3 Diameter 基础协议

Diameter 基础协议[8](Diameter base protocol)是在 Radius 协议的基础上，针对移动 IP、NASREQ 等应用的需求，为网络接入用户提供基本的鉴别、授权、计费框架。Diameter 基础协议提供四种功能：AVPs(Attribute Value Pair)的传输、对等节点能力的协商、错误通知和新功能及新应用扩展的方法。Diameter 基础协议定义四种功能节点：

(1)本地节点，该节点可以直接处理 Diameter 消息，不需要转发消息到其它节点。

(2)中继节点，接收的 Diameter 消息必须转发到下一节点进行处理，中继节点不能修改非路由 AVPs 的任何信息。

(3)代理节点，Diameter 消息必须转发到下一节点进行处理，代理节点根据本身的管理策略，可以在路由 AVPs 前增加自己的 AVPs。

(4)重定向节点，重定向节点可以向发送消息的对等节点返回特殊的响应消息，该消息包含路由信息，从而使对等节点重新发送请求到合适的目的服务器。

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。同时，对用户会话状态的维护和控制也给出十分具体的定义。Diameter 基础协议使用 TCP 和 SCTP 传输服务。在对等节点建立连接时，优先使用 SCTP 服务。当前，Diameter 基础协议中 TCP 和 SCTP 的服务端口为 TBD(To Be Determined)。

3.1 Diameter 协议头格式

Diameter 基础协议定义了新的数据包格式，协议头格式见图1。

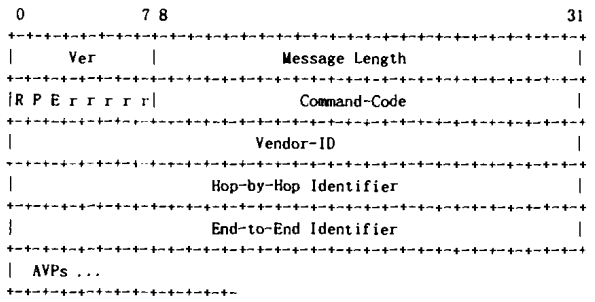

图1 Diameter 协议头格式

图1中，Ver 是版本号，必须为1。Message Length 为整个 Diameter 消息的字节数。命令标志字节：R 比特，置位是请求消息，复位是响应消息；P 比特，置位表示消息可以被中继或代理，复位表示只能本地节点处理；E 比特，置位表示消息中包含出错信息 AVPs。Command-Code，命令代码。Vendor-ID，厂商标识。Hop-by-Hop Identifier，逐跳标识，用于中间节点对请求和响应消息的匹配。End-to-End Identifier，端到端标识，用于发送或接收端检测重复消息。AVPs，属性-值对。

Diameter 基础协议对节点连接状态维护、用户会话状态控制、用户鉴别、计费定义了命令代码，如节点能力协商请求 Capabilities-Exchange-Request、节点能力协商响应 Capabilities-Exchange-Answer，计费请求 Accounting-Request 、计费响应 Accounting-Answer 等。在 Diameter 基础协议中，各命令消息采用 ABNF(Augmented Backus-Naur Form)描述。

3.2 AVP 头格式描述

在 Diameter 基础协议中，用户的鉴别、授权和计费等信息，节点间资源利用情况，路由信息等均通过 AVPs 来传输，图2给出 AVP 的头格式。

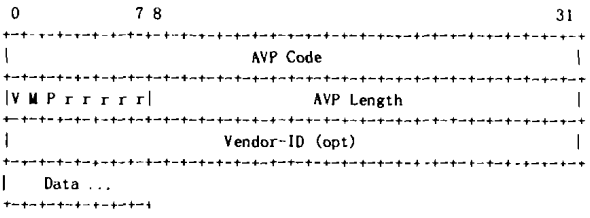

图2 AVP 头格式

图2中，AVP Code，AVP 属性标识，前256属性标识保留给 Radius 协议。AVP 标志字节：V 比特，置位，Vendor-ID 域存在；M 比特，置位表示该 AVP 不能被忽略，必须被 Diameter 节点正确处理，否则出错；P 比特，置位表示该 AVP 受完整性保护。AVP Length，整个 AVP 的字节数。Diameter 基础协议对数据 Data 定义了多种标准和扩展格式，Integer32、Unsigned32、Integer64、Unsigned64、Float32、Float64、Float128、OctetString 和组类型(Grouped)。组类型 AVP 的数据由一系列 AVPs 构成。Diameter 同时定义了衍生的数据类型，包括枚举 enumerated(derived from integer32)、Diameter 标识符 DiameterIdentity(derived from octetstring)、时间 time (derived from unsigned32)、UTF8String (derived from octetstring)、IPFilterRule (derived from octetstring)、QosFilterRule (derived from octetstring)。AVP 同样采用 ABNF 格式来描述。

3.3 Diameter 标识符

运行 Diameter 进程的每一个主机动态产生或被静态配置一个 Diameter 标识符。Diameter 标识符符合通用资源标识符 URI(universal resource identity)语法规定：其中一部分字符串代表主机 FQDN(fully qualified domain name)；某一个端口用于侦听到来的连接；传输字段指明侦听的连接类型，如 SCTP 或 TCP；AAA 字段指明 AAA 服务类型，Diameter 或 Radius；传输层安全字段指明是否利用 TLS。下面是一个符合语法的 Diameter 主机标识符：

aaa: // host. abc. com: 1812; transport = tcp; protocol = diameter

由于 Diameter 标识符包含主机的 FQDN，同时单一主机的多个 Diameter 进程不可能在同一协议的相同端口上侦听

到来的连接，因此任何进程的 Diameter 标识符是唯一的。

3.4 Diameter 消息内容和路由

Diameter 消息由固定长度的头和可变长度的 AVPs 组成，消息有两种类型：请求和响应。由于极少情况下发生请求消息被无记载丢弃，因此通常情况下，发送一个请求消息，总会得到一个响应消息。每一个响应消息包含一个结果代码 AVP，其值是一个整型代码，表明处理的请求是成功、部分成功或发生错误。每一个 Diameter 消息必须在原始主机 AVP (origin-host AVP)中包含创建该消息进程的 Diameter 标识符。每一个 Diameter 消息也必须在原始域 AVP(origin-realm AVP)中包含创建该消息进程所在的域。通过设置消息头的标记字段，可以将请求消息设置为可以代理(proxiable)或不可以代理(non-proxiable)。不可以代理的请求消息必须被下一节点处理，不能被转发；可以代理的消息则能在域中进行转发处理。每一个可以代理的请求消息必须在目的域 AVP (destination-realm AVP)中表明目的域。属于一个用户会话的 Diameter 消息包含会话标识符 AVP(session-id AVP)，其值在会话期间保持不变。会话标识符 AVP 的值是一个全球唯一的字符串，目的是唯一标识一个用户会话而不需要其它信息。会话标识符 AVP 的值由发起会话的 Diameter 客户创建。在 Diameter 消息中 AVPs 的排列顺序上，会话标识符 AVP 紧随 Diameter 标识符。

3.5 Diameter 对等节点

Diameter 对等节点，与给定 Diameter 节点直接通信的 Diameter 节点，可以静态配置或通过其它动态方式确定。两个 Diameter 节点建立传输层连接后的第一个 Diameter 消息是能力交换(capabilities exchange)消息，该消息包含对等节点的 Diameter 标识符和能力，如协议版本号、支持的 Diameter 应用等。Diameter 节点只传输对等节点 Diameter 应用中支持的命令。

消息Device-Watchdog-Request和Device-Watchdog-Answer 是应用层定时检测消息，用于主动发现传输层错误。当对等连接空闲，且存在及时响应消息没有收到时，便定时发送这些检测消息。如果检测到一个对等节点出现传输层错误，Diameter 节点就试图切换到另一个对等节点，这样，所有等待原错误对等节点处理的请求消息便转发到该节点。此后，Diameter 节点会试图定时去重新建立与出错节点的传输层连接；一旦成功建立连接，Diameter 节点就重新起用该对等节点转发消息。

3.6 计费

计费支持和计费消息被规定为基础协议的一部分。计费协议基于服务器控制模型，以支持实时计费信息的发送。在这种模型下，产生计费数据的客户接收来自授权服务器或计费服务器的关于对计费记录的要求，如计费间隔。Diameter 目前不支持没有应用前途的批量计费功能。CMS 安全可以应用于 Diameter 计费消息，以提供计费数据强大的鉴别和完整性保护。Diameter 基础协议定义了一些计费请求消息必须的 AVPs，如会话标识符 AVP、用户名 AVP。每一种 Diameter 应用，如 NASREQ、移动 IP 必须另外定义自己的计费 AVPs。会话标识符 AVP 可以用来区分用户会话间的计费消息；另外对于需要多个计费子会话的应用，可以使用计费子会话标识符 AVP(accounting-sub-session-id AVP)。更进一步，如果一个用户从多种接入设备得到服务，用户标识符各不相同，这种情况可以利用计费多会话标识符 AVP(accounting-multi-session-id AVP)。

3.7 CMS 安全

Diameter 协议可以利用 IPSec 或 TLS 在两个节点之间建立逐跳的完整性和机密性。但是，Diameter 端节点有可能需要通过中间节点，如代理、中继进行通信，这样，端到端的安全性不能得到保证。Diameter CMS(cryptographic message syntax)安全[9]在 AVP 这一层次提供了端到端的鉴别、完整性、机密性和不可否认性。Diameter CMS 安全主要利用了两种技术：数字签名提供鉴别、完整性、不可否认性，加密提供机密性。CMS 安全为两个 Diameter 节点之间建立安全关联定义了所需的消息和 AVPs。

4 基于 Diameter 的应用

Diameter 基础协议自身不能单独使用，必须至少与一种基于 Diameter 的应用结合才能使用，图3示例了 Diameter 的协议结构。

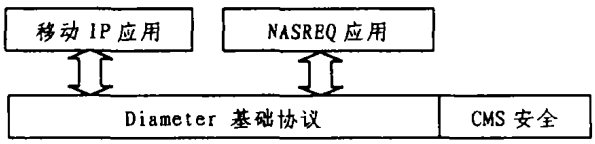

图3 Diameter 协议结构

4.1 移动 IP 应用

利用基础协议提供的功能，基于 Diameter 的移动 IP[10]应用比较完善地解决了移动 IP 面临的问题。在基于 Diameter 的移动 IP 应用中，AAA 服务器作为密钥分配中心，为移动节点、外部代理和归属代理动态创建和分配会话密钥，从而便于移动节点在外部网络得到接入服务。同时，基于 Diameter 的移动 IP 应用规定了 Diameter 服务器节点如何对得到移动 IP 服务的 MN 进行鉴别、授权和计费，这些功能通过引入四个新的命令代码和相应的 AVPs 来实现。在基于 Diameter 的应用中，移动 IP 的应用标识为4。

4.2 NASREQ 应用

Diameter NASREQ 应用[11]为拨号 PPP 用户提供 AAA 服务，是 Radius 协议的下一代替代产品。NASREQ 应用可以尽可能地使用与现有 Radius 兼容的属性来传输数据，这样减轻当前 Radius 到 Diameter 移植的难度，同时降低 Radius/Diameter 网关的协议转换工作量。利用扩展鉴别协议 EAP(extensible authentication protocol)，NASREQ 应用能提供安全的鉴别。NASREQ 应用定义了 Diameter-EAP-Request 和 Diameter-EAP-Answer 消息，用于传输 EAP 载荷。在 NASREQ 应用中，AA-Request 消息等同 Radius 中的 Access-Request，AA-Answer 等同于 Radius 中的 Access-Accept、Access-Reject 消息。另外，NASREQ 应用对作为 Radius-Diameter 网关的服务器作了初步规定。

5 分析与比较

作为新一代的鉴别、授权和计费协议，Diameter 相对 Radius 具有许多优势，分析和比较如下：

(1)属性数据的长度 Radius 属性，即{属性类型，属性长度，属性值}三元组作为可变长度被包含在 Radius 消息中。属性长度仅为1字节，因此限制属性值数据的最大长度为255字节。Diameter 属性作为五元组{属性类型，标记，属性长度，

厂商标识符，属性值）被包含在 Diameter 消息中，属性长度为3字节，单一属性值数据长度可以超过16,000,000字节。

（2）*待处理消息的数目* Radius 数据包头的标识符(identifier)字段用于识别消息的重传，但是该标识符为1字节，使得 Radius 客户和服务器之间同时交互的消息数最大为255个。Diameter 消息包中，端到端标识符(end to end identifier)用来识别重传；标识符长度为4字节，允许客户端同时发送40亿个 Diameter 消息。

（3）*流量控制能力* Radius 使用 UDP 传输协议，一种简单的面向无连接的协议，接收节点缺乏对发送节点数据流的控制能力。Diameter 使用 TCP 或 SCTP 这些面向连接的传输协议，具备完善的流控和拥塞控制机制。

（4）*服务器失效检测能力* 对于一个 Radius 请求，NAS 不能及时收到响应的原因有多种多样，如网络拥塞、NAS 到 AAA 服务器路径上的临时网络失效、下一跳代理服务器的失效、AAA 服务器的失效等。对于基于 UDP 的 Radius 协议，NAS 不能区分响应失败的原因，只能假设是下一跳代理服务器的失效，然后选择其它的下一跳代理服务器进行重传。这种错误恢复机制可能不是最好。在面向连接协议和 Diameter 消息保活(keepalive message)功能的支持下，Diameter 节点能检测局部对等节点的失效。

（5）*数据包的丢失处理* 对于由于各种错误原因而丢失的消息包，Radius 进行的处理只是无记载丢弃(silently discarded)。这样，NAS 假设 AAA 服务器没有收到消息，接着进行无意义的重传，直到最终放弃该请求。除了极少数错误原因，Diameter 节点多数情况下会返回响应消息。

（6）*服务器错误恢复能力* 许多 NAS 在实现上配置为可以访问多个 Radius 服务器，一个主服务器和若干个备用服务器。但是当发生错误而切换到备用服务器时，NAS 并不知道该备用服务器是否可用。这些有可能延迟终端得到接入服务，直到某一备用服务器的确可用。Diameter 节点可以有效支持服务器间的错误恢复。当主服务器恢复可用时，消息处理可以立即从备用服务器切换回来，对请求消息的时延影响很小。

（7）*代理环境中 Radius 服务器利用的低效* 在 Radius 环境中，NAS 进行所有的重传工作，代理服务器并不重传 Radius 请求。在不知道错误是本地还是外地的情况下，NAS 有可能不适当地选择下一跳节点进行重传。而 Diameter 基础协议规定，处于消息原始节点到最终节点传输路径中的所有节点，均可以进行对等节点错误检测、错误恢复和消息重传。这样，错误就可以本地发生，本地恢复。

（8）*服务器主动发送消息的能力* Radius 协议不允许服务器主动发送消息到 NAS。当服务器需要主动请求时，要么厂商提供 Radius 协议之外的其它解决措施，如简单网络管理协议 SNMP；要么对 Radius 采用私有的扩展方案，从而导致相互厂商产品间的不兼容。Diameter 允许服务器主动发送消息请求，基础协议定义了两条这类消息，一是请求 Diameter 客户终止某一用户的会话，二是请求 Diameter 客户对某一用户重新进行鉴别或授权。

其它 Diameter 协议与 Radius 协议的功能比较见表1：

表1 Diameter 与 Radius 其它功能比较

	重放攻击	端到端安全	厂商专有命令	对齐方式	共享密钥
Radius	X	X	X	字节对齐	必须存在
Diameter	√	√	√	32比特对齐	不必须

总结和展望 本文主要介绍 Diameter 基础协议，基于 Diameter 的移动 IP 和 NASREQ 应用。通过对 Diameter 协议和 Radius 协议的分析比较，表明 Diameter 克服了 Radius 在 AAA 服务领域的不足和缺陷，完全满足新兴应用对 AAA 服务的要求。随着 Diameter 协议及其应用的成熟和标准化，对未来移动通信系统和宽带接入系统的发展将起到巨大的推动作用。

参 考 文 献

1 Rigney C, Rubens A, et al. Remote Authentication Dial In User Service (Radius). IETF RFC2865, June 2000

2 Glass S, Jacobs S, et al. Mobile IP Authentication, Authorization, and Accounting Requirements. IETF RFC 2977, Oct. 2000

3 Hiller T, Walsh P, et al. CDMA2000 Wireless Data Requirements for AAA. IETF RFC 3141, June 2001

4 Aboba B, Calhoun P, et al. Criteria for Evaluating AAA Protocols for Network Access. IETF RFC 2989, Nov. 2000

5 Beadles M, Mitton D. Criteria for Evaluating Network Access Server Protocols. IETF RFC 3169, Sept. 2001

6 Aboba B, Zorn. Criteria for Evaluating Roaming Protocols. IETF RFC 2477, Jan. 1999

7 Stewart R, Xie Q, et al. , Stream Control Transmission Protocol. RFC2960, Oct. 2000

8 Calhoun P, Akhtar H, et al. Diameter Base Protocol. IETF Internet Draft (draft-ietf-aaa-diameter-09. txt), March 2002. Work in progress

9 Calhoun P, Bulley W, et al. Diameter CMS Security Application. IETF Internet Draft (draft-ietf-aaa-diameter-cms-sec-04. txt), March 2002. Work in progress

10 Calhoun P, Perkins C. Diameter Mobile IPv4 Application. IETF Internet Draft (draft-ietf-aaa-diameter-mobileip-09. txt), March 2002. Work in progress

11 Calhoun P, Bulley W, et al. Diameter NASREQ Application, IETF Internet Draft (draft-ietf-aaa-diameter-nasreq-09. txt), March 2002. Work in progress