ICS 33.040.40
M 31

YD

中华人民共和国通信行业标准

YD/T 1469-2006

用于 IP 网络的 Diameter 基础协议技术要求

Technical Requirements for Diameter Base Protocol in IP Network

（IETF RFC 3588：2003，Diameter Base Protocol，MOD）

2006-06-08 发布　　2006-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“Diameter协议”系列标准之一，是其他Diameter扩展协议的基础协议。本系列的标准结构和名称预计如下：

1. 《用于IP网络的Diameter基础协议技术要求》；
2. 《AAA系统传输要求》；
3. 《Diameter NAS应用扩展要求》；
4. 《Diameter移动IP应用扩展要求》；
5. 《Diameter信用控制应用扩展要求》；
6. 《Diameter EAP应用扩展要求》；
7. 《Diameter SIP应用扩展要求》。

本标准对应于IETF RFC 3588（2003）。本标准与IETF RFC 3588（2003）的一致性程度为修改采用，主要差异如下：

——按照汉语习惯对一些编排格式进行了修改；

——将一些适用于国际标准的表述改为适用于我国标准的表述；

——根据GB/T 1系列的要求，增加了第1章、第2章和第3章，其中第3.1节的定义均来自RFC 3588的第1.3节；

——本标准的第4.1节、第4.2节根据需要增加了对Diameter协议的整体性、简要性描述；

——本标准的第4.3.1节、第4.3.2节、第4.3.3节、第4.3.4节、第4.3.5节、第4.5节、第4.6节、第4.7节分别与RFC 3588 第2.4节、第2.5节、第2.8节、第2.6节、第2.7节、第2.2节、第2.3节、第2.10节保持一致；

——本标准的第4.4节在RFC 3588 第2.1节的基础上，根据技术需要参考了IETF RFC 3539《认证、授权和计费（AAA）传输轮廓》，补充了技术细节要求；

——本标准的第5.1节和第5.2节分别与RFC 3588的第3章和第4章保持一致；

——本标准的第6章与RFC 3588的第5章保持一致；

——本标准的第7.1节、第7.2节、第7.3节分别与RFC 3588的第6章、第7章、第8章保持一致；

——本标准的第8章和第9章与RFC 3588的第9章和第13章保持一致；

——本标准的附录B和附录C与RFC 3588的第10章和第12章保持一致；

——本标准的附录D、附录E、附录F分别对应RFC 3588的Appendix A、Appendix B、Appendix C；

——本标准的附录A是根据技术需要增加的内容，主要参考了IETF RFC 4004《Diameter 移动IPv4应用》、IETF RFC 4005《Diameter网络接入服务器应用》、IETF RFC 4006《Diameter信用控制应用》、IETF RFC 4072《Diameter扩展认证协议（EAP）应用》。

本标准附录A、附录B、附录C是规范性附录，附录D、附录E、附录F是资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院

本标准主要起草人：谢　玮　刘　清　武　静　刘　述　姜吕良

用于IP网络的Diameter基础协议技术要求

1 范围

本标准规定了Diameter协议的体系结构、Diameter基本功能、Diameter基础协议通信模式、Diameter基础协议信令流程以及安全机制等方面的要求。

本标准适用于我国IP网络中AAA（认证、授权和计费）系统和AAA相关设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC 0793	传输控制协议（TCP）
IETF RFC 2165	业务位置协议（SLP）
IETF RFC 2234	扩展 BNF 语法规范（ABNF）
IETF RFC 2407	用于 ISAKMP 的 IPSec 域的翻译（IPSecDOI）
IETF RFC 2409	因特网密钥交换（IKE）
IETF RFC 2915	命名权威点 DNS 资源记录
IETF RFC 2960	流控制传输协议
IETF RFC 3588	Diameter 基础协议
IETF RFC 3539	认证、授权和计费（AAA）传输轮廓
IETF RFC 4004	Diameter 移动 IPv4 应用
IETF RFC 4005	Diameter 网络接入服务器应用
IETF RFC 4006	Diameter 信用控制应用
IETF RFC 4072	Diameter 扩展认证协议（EAP）应用
ANSI/IEEE 754-1985	二进制浮点运算

3 定义和缩略语

3.1 定义

下列定义适用于本标准。

- 计费（Accounting）

收集资源使用信息的动作，以用于能力规划、审核、营业额或成本分配。

- 计费记录（Accounting Record）

一条计费记录表述了一个用户在整个会话过程中资源消费的总结。

- 认证（Authentication）

核实某个实体（客体）身份的动作。

• 授权（Authorization）

决定一个提出请求的实体（客体）是否被允许访问资源（主体）的动作。

• AVP（Attribute-Value-Pairs）

Diameter协议由一个头以及跟随的一个或多个属性值对（AVP）组成。一个AVP包含一个头和用来封装特定协议的数据（例如，路由信息），以及认证、授权或计费信息。

• Diameter 代理（Diameter Agent）

Diameter代理是一个Diameter节点，它提供中继、Proxy、重定向或翻译服务。

• Diameter 客户（Diameter Client）

Diameter客户是位于网络边缘的一个设备，执行接入控制。Diameter客户的典型范例就是网络接入服务器（NAS）或外地代理（FA）。

• Diameter 节点（Diameter Node）

Diameter节点是实现Diameter协议的主机程序，它既可以作为客户也可以作为代理或服务器。

• Diameter 对等端（Diameter Peer）

Diameter对等端是一个Diameter节点，该节点和另一个特定的Diameter节点有一个直接的传输连接。

• Diameter 安全交换（Diameter Security Exchange）

Diameter安全交换是两个Diameter节点建立端到端安全的过程。

• Diameter 服务器（Diameter Server）

Diameter服务器负责处理某个特殊域的认证、授权和计费请求。除基本协议以外，Diameter服务器还必须支持Diameter应用扩展。

• 下行（Downstream）

用于标识由归属服务器发往接入设备的特定Diameter消息的方向。

• 端到端安全（End-to-End Security）

TLS和IPSec提供逐跳安全，或者跨一个传输连接的安全。当中继或Proxy参与进来时，逐跳安全无法保证整个Diameter用户会话的安全。端到端安全是指可能通过Diameter代理进行通信的两个Diameter节点之间的安全。端到端安全可以保证从发起Diameter节点到终结Diameter节点之间整个Diameter通信路线的安全。

• 归属域（Home Realm）

归属域是可管理域，通过它可以与用户保持一个账户关系。

• 归属服务器（Home Server）

位于归属地的Diameter服务器。

• 中间计费（Interim Accounting）

中间计费消息提供一个用户会话过程中资源使用的快照。在设备重启动或者其他网络故障，而无法得到会话总结消息或会话记录时，它通常用于用户会话的分段计账。

• 本地域（Local Realm）

本地域是为某用户提供服务的可管理域（Domain）。一个可管理域可以作为某些用户的本地域（Realm），也可以同时是其他用户的归属域（Realm）。

• 多会话（Multi-session）

一个多会话表现为若干会话的一个逻辑链接。多会话通过采用Acct-Multi-Session-Id来辨识。多会话的一个举例可以是一个多链路PPP束。该PPP束的每一个分支都是一个会话，而整个PPP束则是一个多会话。

• 网络接入标识符（Network Access Identifier）

可以简称为NAI，在Diameter协议中用来摘录某个用户的身份和域（Realm）的信息。身份用来在认证和/或授权过程中标识该用户，而域则用于消息的路由。

• Proxy 代理/Proxy（Proxy Agent or Proxy）

Proxy代理除了转发请求和响应外，还根据与资源使用和配置相关的策略作出决定。该工作通常通过跟踪NAS设备的状态来完成。Proxy代理在收到服务器响应之前一般不会响应客户请求。当需要转发的请求和响应违反策略时，它可以生成拒绝（Reject）消息。因此，Proxy代理必须理解通过它们的消息语义；不一定支持所有的Diameter应用。

• 域（Realm）

NAI中紧跟在“@”字符后面的字符串。NAI域名必须是惟一的，并且遵从DNS命名空间的管理。Diameter采用Realm（也可以泛指Domain）来决定消息是否本地处理，还是必须将其路由或重定向。

• 实时计费（Real-time Accounting）

实时计费包括在一个定义好的时间窗口内处理资源采用的信息。时间约束的使用通常是由于财政风险的限制。

• 中继代理/中继（Relay Agent or Relay）

中继根据与路由相关的AVP和域路由表列表转发请求和响应。由于中继不作策略决定，它们不检查或改变非路由AVP。因此，中继从不生成消息，也不须理解消息或非路由AVP的语义，并且能够处理任何Diameter应用或消息类型。由于中继根据路由AVP和域转发表中的信息作决定，它们不会保留NAS资源使用或会话的状态。

• 重定向代理（Redirect Agent）

重定向代理将客户引导到服务器，使得它们可以直接通信。由于重定向代理不在转发路径上，它们不会改变在客户和服务器之间传送的任何AVP。重定向代理不生成消息，能够处理任何消息类型。重定向代理不保留与会话或NAS资源有关的状态。

• 漫游关系（Roaming Relationships）

漫游关系包括公司和ISP之间的关系、在一个漫游联盟（Roaming Consortium）中对等端ISP之间的关系、以及一个ISP与一个漫游联盟之间的关系。

• 安全联盟（Security Association）

指一个Diameter会话中的两个端点之间的关联，该会话保证端点间通信的保密性和完整性，即使通信在有中继和/或Proxy的情况下进行的。

• 会话（Session）

会话是一个与某个特定动作参与事件的相关过程。每个应用应提供指南例如会话的开始和结束时间。所有拥有相同会话ID的Diameter数据包，都被认为属于同一个会话。

• 会话状态（Session State）

状态代理通过跟踪所有经过授权的活动会话，保留会话状态信息。每个经过授权的会话都与某特殊的业务绑定，其状态为活动，一直到被通知改变为其他状态，或到期为止。

• 子会话（Sub-session）

表示一个提供给已有会话的独特的业务（例如，QoS或数据特性）。这些业务可以同时（例如，在同一会话过程中同时传送语音和数据）或连续发生。会话中的这些改变通过Accounting-Sub-Session-Id来表征。

• 事务状态（Transaction State）

Diameter协议要求代理维护事务状态，以用于失败处理。

• 翻译代理（Translation Agent）

一个有状态的Diameter节点，执行Diameter和其他AAA协议（如RADIUS）之间的协议翻译。

• 传输连接（Transport Connection）

指两个Diameter对等端之间已有的直接TCP或SCTP连接，也称为端到端连接。

• 上行（Upstream）

用于标识从接入设备到归属服务器的特定Diameter 消息的传送方向。

• 用户（User）

要求或使用某些资源以支持Diameter客户生成一个请求的实体。

3.2 缩略语

下列缩略语适用于本标准。

AAA	Authentication，Authorization and Accounting	认证、授权和计费
ABNF	Augmented BNF for Syntax Specifications	扩展BNF语法规范
AVP	Attribute Value Pairs	属性值对
CMS	Cryptographic Message Syntax	密码消息语法
EAP	Extensible Authentication Protocol	可扩展认证协议
IP	Internet Protocol	互联网协议
NASREQ	Network Access Server Requirements	网络接入服务器请求
NAPTR	The Naming Authority Pointer（NAPTR）DNS Resource Record	命名权威指针DNS资源记录
PPP	Point to Point Protocol	点对点协议
RADIUS	Remote Authentication Dial-In User Service	远端拨入用户验证服务
RAS	Registration，Admission and Status	注册、允许和状态协议
SLIP	Serial Line IP	串行IP
SCTP	Stream Control Transmission Protocol	流控制传输协议
SLP	Service Location Protocol	业务位置协议
TCP	Transmission Control Protocol	传输控制协议
TACACS	Terminal Access Controller Access Control System	终端接入控制者接入控制系统协议
TLS	Transport Layer Security	传输层安全

4 Diameter 的体系结构

4.1 Diameter 总体框架及协议概述

4.1.1 Diameter 协议的设计目的

Diameter协议的设计目的是创建一个能够充分满足网络访问控制要求的AAA协议。Diameter设计要求的具体内容如下：

—— 具有良好的网络适应性和可扩展性；
—— 统一且良好的失败控制和检测机制；
—— 完整的传送层安全保证（包括域内和域间）；
—— 数据传输可靠性保证机制；
—— 支持各种类型的代理，包括 Proxy 代理、重定向代理以及中继代理等；
—— 支持服务器发起的消息，即允许服务器主动发送消息给其客户端；
—— 与现有网络协议的良好可互操作性；
—— 支持节点间的能力协商机制；
—— 支持动态对等端发现和配置机制；
—— 支持安全和可扩展的漫游。

4.1.2 Diameter 协议的框架结构

Diameter包含基础协议、传送协议、不同的应用扩展，如NASREQ和移动IP，如图1所示。所有应用和服务共用的基本功能都在基础协议中实现，而应用特定的功能则会在不同的应用中实施。

Diameter基础协议注重能力协商，消息发送以及对等端如何最终被拒绝。基础协议还规定了特定规则以用于Diameter节点之间所有的消息交换。Diameter基础协议旨在提供一个AAA框架，以用于各种应用。基础协议还定义了所有Diameter应用使用的，并且所有Diameter设备都必须支持的消息格式、传输、差错报告和安全服务。

为了给不同业务提供符合该业务特征的功能，Diameter协议必须支持适用于各种不同业务的不同的实施方案。

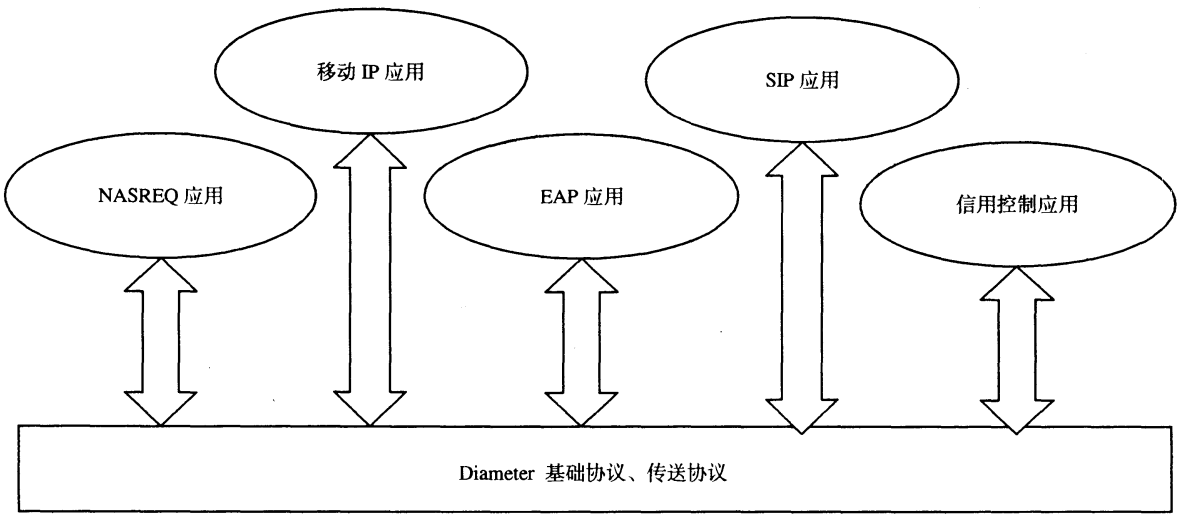

图1 Diameter 协议结构

图1给出了Diameter协议结构的示意图，Diameter基础协议是AAA系统实施的基本协议要求；传输机制主要定义Diameter协议传输层的问题及解决方法，还包括失败检测算法和状态机；其他拥有各种不同功能的应用都必须支持基础协议。

Diameter基础协议可以直接用于计费应用，但如果用于认证和授权，则必须进行特定的应用扩展，如NASREQ应用、移动IP应用等。

NASREQ应用定义了一个Diameter应用，其允许Diameter服务器用于NAS作为主要接入手段的网络环境中。其中给出了需要在Diameter和RADIUS之间进行协议转换的服务器需要注意的问题。移动IP应用定义了一个Diameter应用，其允许Diameter服务器对一个移动节点执行用于移动IP业务的AAA功能。SIP应用是Diameter协议应用与SIP环境中的要求一样。EAP应用是Diameter为支持EAP所应具有的扩展要求。信用控制（Credit Control）是一种可以与一个账户进行实时交互、控制并监视，并对特定服务进行收费的机制，其相应的Diameter扩展规定了Diameter协议为支持该功能所定义的扩展要求。Diameter应用扩展要求参见本标准附录A。

4.1.3 Diameter 实体对协议的支持

Diameter客户必须支持基础协议。另外它们还必须根据客户业务实施的需要，支持任何Diameter应用扩展。如果Diameter客户不同时支持所有应用扩展，则必须明确表示为“Diameter *X*客户”，其中*X*表示它所支持的应用。

Diameter服务器必须支持基础协议。另外它们还必须根据其所提供的业务需要，支持任何Diameter应用扩展。如果Diameter服务器不同时支持所有应用扩展，则必须明确表示为“Diameter *X*服务器”，其中*X*表示它所支持的应用。

Diameter中继代理和重定向代理是透明传输协议，必须透明支持Diameter基础协议以及所有Diameter应用。

Diameter Proxy代理必须支持基础协议。另外，它还必须完全支持实现采用Proxy业务所需要的任何Diameter应用。如果Diameter Proxy不同时支持所有应用扩展，则必须明确表示为“Diameter *X* Proxy”，其中*X*表示它所支持的应用。

4.2 Diameter 基础协议的功能概述

Diameter基础协议提供以下功能：

—— AVP（属性值对）的发送；

—— 能力协商；

—— 差错通知；

—— 可扩展性，通过增加新命令和 AVP 来实现；

—— 扩展应用的基本业务需求，例如，用户会话或计费处理。

4.3 Diameter 相关概念释义

4.3.1 应用标识符

每一个Diameter应用都必须拥有一个应用标识符。由于对基础协议的支持是强制性的，因此基础协议不需要应用标识符。在能力交换过程中，Diameter节点告知对等端本地所支持的应用，并且，所有Diameter消息都包含一个应用标识符，在消息向前转发的过程中使用。

规定范围0x00000001～0x00ffffff为标准应用预留，而0x10000001～0xfffffffe为运营商自行定义的应用预留。目前定义了的应用标识符见表1。

表1 Diameter 应用标识符

应用标识符	值
Diameter 通用消息	0
NASREQ	1
移动 IP	2
Diameter 基础计费	3
中继	0xffffffff

中继和重定向代理必须广播中继应用标识符，同时所有其他Diameter节点必须广播本地支持的应用。广播中继服务的能力交换消息的接收者必须假设发送者支持所有现有的和将要有的应用。

Diameter中继和Proxy代理负责寻找一个上行服务器，以支持某个特殊消息的应用。如果没有发现，将返回差错消息，其中的结果代码AVP设置为DIAMETER_UNABLE_TO_DELIVER。

4.3.2 连接和会话

连接是两个对等端之间的一个传输层连接，用于发送和接收Diameter消息。会话是一个应用层的逻辑概念，在一个接入设备和一个服务器之间共享，并且通过会话ID AVP来标识。图2给出了Diameter连接和会话的区别。

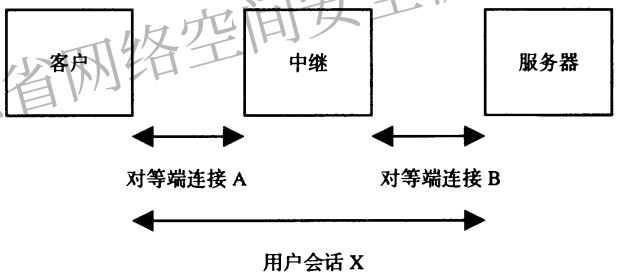

图2 Diameter 连接和会话示例

需要明确的是，连接和会话之间并没有关系，一个会话可以跨越多个连接，而用于多会话的Diameter消息也可以在一个单独的连接中传送。

4.3.3 Diameter 代理

除了客户和服务器，Diameter协议还引入了中继代理、Proxy代理、重定向代理和翻译代理。这些Diameter代理的主要作用如下：

—— 可以将系统管理分配为可调配的组，包括安全联盟的维护。

—— 可以用于集中大量相关或分布式的NAS设备，以作为一个用户组。

—— 能够对请求或响应进行增值处理。

—— 能够用于负载平衡。

一个复杂的网络将拥有多个认证源，它们可以过滤请求并将请求前转给正确的目标。

Diameter协议要求代理保持事物状态，以用于失败替代（Failover）。事物状态意味着前转某个请求，要保存其逐跳标识符；该字段被一个本地惟一的标识符替代，当收到相应的应答时，再将该字段恢复为其原始的值。该请求的状态在收到应答时被释放。无状态的代理就是仅保持事物状态。

Proxy-Info AVP允许无状态代理给一个Diameter请求添加本地状态，当然必须保证在对应的应答中也必须出现相同的状态。该协议的失败替代过程要求代理保持未获得请求的副本。

通过持续跟踪所有的已授权的激活会话，有些状态代理可以保持会话状态信息。每个已授权会话都是绑定在特定的业务上，它的状态一直都是激活的，除非它得到通知，或者生命期到期。每个已授权会话都有一个生命期，通过Session-Timeout AVP 告知Diameter服务器。

保持会话状态在某些特定应用中会非常有用，例如：

—— 协议翻译（如RADIUS<——>Diameter）；

—— 给某个特定用户有限的资源授权；

—— 每用户或事物审计。

一个Diameter代理可以对于某些请求是有状态的，而其他请求则是无状态的。一个Diameter实施也可以对于某些请求是一种类型的代理，而对于其他请求是另一种类型的代理。

4.3.3.1 中继代理

中继代理是一个Diameter代理，用来接收请求并根据在消息中发现的信息（例如，目的地域Destination-Realm）路由去往其他Diameter节点的消息。该路由决定是利用所支持的域和已知对等端的列表完成的。该表被称作域路由表，详见第4.3.5节。

中继可以用于聚合来自在一个地理区域（POP）内的多个网络接入服务器（NAS）的请求。使用中继可以避免NAS与在其他域的Diameter服务器的通信，同时还可以减少Diameter服务器在NAS增加、变化或删除时的配置负担。

中继会通过插入以及删除路由信息等动作修改Diameter消息，但是不会修改消息的其他任何部分。中继不维护会话状态，但必须维护事务状态。

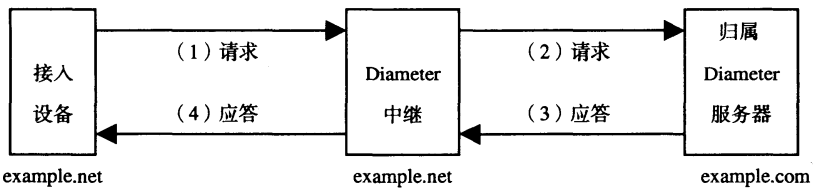

图3 Diameter 消息的中继过程

图3给出了一个Diameter消息的中继过程。接入设备为用户bob@example.com产生一个请求。在发出请求前，接入设备先利用“example.com”作为关键字，执行Diameter路由查询，然后决定该消息应被送到Diameter中继。Diameter中继执行同样的路由查询，并将该消息中继给“example.com”的归属Diameter服务器。归属服务器判断该请求可以在本地处理，则进行对该请求的认证和／或授权，并返回应答。该应答通过保存的事务状态，被路由回接入设备。

由于中继不执行任何应用级别的程序，它们提供的中继服务可以用于所有Diameter的应用，因此它们必须广播中继应用标识符。

4.3.3.2 Proxy 代理

与中继类似，Proxy代理应用Diameter路由表来路由Diameter消息。它们不同之处在于，Proxy代理修改消息以达到策略的强制实施。这要求Proxy保持它们下行对等端（例如，接入设备）的状态以执行资源的应用，提供准入控制和预配置。

必须重点指出的是，尽管Proxy可以为NAS提供增值功能，但它们的存在使得接入设备无法应用端到端安全，因为对消息的修改将使端到端的加密工作无法完成。

Proxy可以用在呼叫中心或接入ISP中，它们能够监视正在使用的端口号码和类型，并根据它们的配置作出资源分配和允许进入的决定。

执行资源限制的Proxy必须保持会话状态。所有Proxy必须保持事务状态。

由于执行策略需要了解提供的业务，Proxy仅需广播它们支持的Diameter应用。

4.3.3.3 重定向代理

重定向代理在Diameter路由需要集中配置的情况下非常有用。重定向代理为某个集团的所有成员提供服务，但不希望负担域间消息中继的任务。这种方案优势在于，当某个成员的结构发生变化时，无需集团向它的成员提供路由更新。

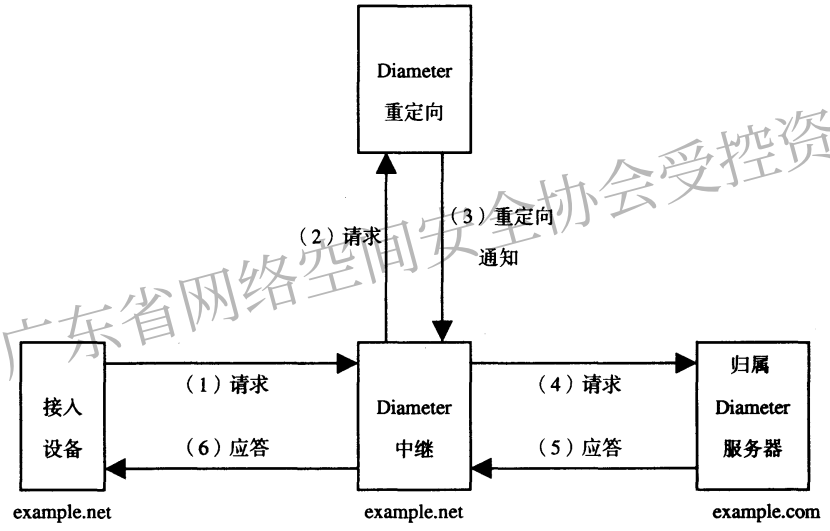

图4 重定向一个 Diameter 消息

在图4中，接入设备为用户bob@example.com产生一个请求。该消息由接入设备发送到其中继，但该中继的Diameter路由表中没有example.com的路由入口。Diameter中继的缺省路由配置为重定向代理，重定向代理返回一个重定向通知中继，同时还有相关归属服务器的联系信息。收到重定向通知后，中继建立与归属服务器的传输连接，并将请求转发给中继。

由于重定向代理不中继消息，仅返回一个应答，其中包括Diameter代理间直接通信所需要的信息，它们不修改消息。重定向代理不接收应答消息，所以它们不用保持会话状态。而且重定向代理从来不会中继请求，它们也不需要保持事务状态。

由于重定向代理不执行任何应用级别的程序，它们为所有Diameter应用提供服务，因此必须广播中继应用标识符。

4.3.3.4 翻译代理

翻译代理是提供两种协议（例如，RADIUS与Diameter、TACACS与Diameter）之间翻译的设备。翻译代理通常用来聚合服务器以和一个Diameter基础设施进行通信。

Diameter协议引入了永久（long-lived）授权会话的概念，翻译代理必须保持会话状态和事务状态。

翻译代理必须仅广播它们本地支持的应用。

4.3.4 对等端表（Peer Table）

在消息前转过程中应用Diameter对等端表，同时还要参考域路由表（Realm Routing Table）。对等端表包含以下字段：

—— 主机标识。格式遵循在本标准第 5.2.3 节中定义的 DiameterIdentity 扩展 AVP 数据格式。该字段包含在 CER 或 CEA 消息中发现的源主机 AVP 的内容。

—— 状态。对等端入口状态，必须与本标准第 6.6 节中列举的某个值相匹配。

—— 静态或动态。指定某个对等端入口是静态配置的还是动态发现的。

—— 生命期。指定动态发现的对等端表入口被刷新或到期的时间。

—— TLS 有效。指定对等端通信时是否采用 TLS。

—— 附加安全信息（可选）。例如，关键字、证书等。

4.3.5 基于域的路由表（Realm-Based Routing Table）

所有基于域的路由查找都是依靠域路由表来执行的。域路由表入口包含以下字段：

—— 域名。该字段通常用作路由表查询中的主关键字。注意，某些实际应用在执行查询时是基于“从右端最长匹配”的原则，而不要求完全匹配。

—— 应用标识符。一个应用是由运营商 ID 和应用 ID 来标识的。目前运营商 ID 均定为“0”。一个路由入口基于消息中的应用标识 AVP 可能拥有不同的目的地。应用标识符必须用作路由表查询的第二关键字字段。

—— 本地动作。本地动作字段用来标识一个消息将被如何处理。支持以下动作：

- Local：本地动作设置为Local的Diameter消息可以在本地处理，无需被路由到其他服务器。
- Relay：所有属于本类型的Diameter消息必须被路由到下一跳的服务器，无需修改任何非路由AVP。
- Proxy：所有属于本类型的Diameter消息必须被路由到下一跳的服务器。本地服务器可以在路由之前通过将新的AVP插入到该消息中，实行本地策略。
- Redirect：所有属于本类型的Diameter消息必须附加归属Diameter服务器的标识，并且返回给消息的发送者。

—— 服务器标识符。消息会被路由到一个或多个服务器。这些服务器也必须出现在对等端表中。当本地动作设置为 Relay 或 Proxy 时，该字段包含消息必须被路由到的服务器的标识符。当本地动作设置为 Redirect 时，该字段包含消息将被重定向到的一个或多个服务器的标识符。

—— 静态或动态。指定某个路由入口是静态配置的还是动态发现的。

—— 生命期。指定某个动态发现的路由表入口的到期时间。

必须重点指出，Diameter代理必须至少支持Local、Relay、Proxy或Redirect操作模式之中的一种。为了与协议规定一致，代理不需要支持所有的操作模式。中继代理和Proxy不允许重排AVP。

路由表可以包括一个默认入口，为任何与其他入口都不匹配的请求采用。路由表可以仅包含这样一个入口。

当请求被路由时，目标服务器必须已经为特定的消息广播应用标识符，或者标明自己是一个中继或Proxy代理。否则，将返回一个差错，其结果码AVP设置为DIAMETER_UNABLE_TO_DELIVER。

4.4 Diameter 传输协议

Diameter基本协议运行在TCP和SCTP传输协议的端口3868上。Diameter客户必须支持TCP或SCTP（RFC 2960），而代理和服务器必须两者都支持。本标准以后版本将强制客户支持SCTP。

4.4.1 SCTP 的特征

SCTP与TCP相同点是：

—— SCTP 提供面向连接的传输服务；

—— SCTP 提供可靠的传输，保证数据按顺序到达，并且没有丢失或重复；

—— SCTP 是全双工的；

—— SCTP 应用窗口机制以提供流控。

SCTP还提供一些TCP不具备的能力：

—— SCTP 提供两端点之间的多数据流传送。在每个数据流内，消息都会按序到达，并且没有丢失和重复。

—— SCTP 是面向消息的；即 SCTP 负责维护消息分界并分发完整消息（PDU），而 TCP 则是面向比特的。

—— SCTP 采用多宿主主机的概念。一个多宿主主机是拥有多个 IP 接口的主机。在初始化时，SCTP 两端交换它们的 IP 接口地址列表。一个要求重传的 SCTP 消息可以被发送到备选的 IP 地址，这样可以在发生网络失败时，提高 SCTP 会话复原的能力。而 TCP 会话在每个端点只能处理单个 IP 地址。

4.4.2 Diameter 传输协议要求

Diameter协议必须能够在可以提供重传策略的传输层上运行，以使其能够在对等端不可达时，有效地转换另一个主机。与RADIUS相反，Diameter协议要求代理链上的每一个节点都应在“传输层”对请求或响应进行确认。由于Diameter运行在提供可靠传输的SCTP上，代理链上的每个节点都有责任对没有确认的消息进行重传。

Diameter节点可以从一个源端口上初始化连接，该端口可以不是其声明接受连接请求的端口，同时Diameter节点必须时刻准备在端口3868上接收连接。一个特定的Diameter对等端状态机的实例不允许采用多个传输连接与一个已知的对等端通信，除非该对等端出现多个实例，这种情况下，允许每个进程一个连接。

当一个对等端不存在与之相关的传输连接时，应当定期进行连接尝试。该行为通过Tc定时器控制，建议该值为30s。该规则还有特定的例外，比如一个对等端已经结束了传输连接，表明其不希望通信等。

当连接一个对等端，且定义了0个或多个传输时，应首先尝试采用SCTP，然后是TCP。参见6.2节“对等端发现机制”中的信息。

Diameter实施（Implementation）应能够将ICMP协议“端口不可达消息”解释为明确地指示“服务器不可达”。Diameter实施也应当能够将传输和超时连接尝试，解释为重置。

如果Diameter接收到来自上行TCP的数据，该数据不能解析或鉴别为一个对等端造成的Diameter差错，则表明该数据流受到安全威胁且不能恢复。必须使用一个Reset呼叫（发送一个TCP RST比特）或一个SCTP Abort消息关闭该传输连接。

以下是对支持SCTP的Diameter实施的要求：

1）关于协同工作能力：所有 Diameter 节点必须准备接收在联盟（Association）中的任何 SCTP 流上的 Diameter 消息。

2）对于预防拥塞：所有 Diameter 节点应当运用所有对于联盟有效的 SCTP 流来防止 head-of-the- line 拥塞。

4.5 Diameter 消息的加密

Diameter客户，例如，网络接入服务器（NAS）和各种代理必须支持IPSec，并且可以支持TLS。Diameter服务器必须支持TLS和IPSec。不允许在没有任何安全机制（TLS或IPSec）的情况下采用Diameter协议。

推荐在边缘和域内业务流量中可以将IPSec作为首选，例如，在NAS和本地AAA Proxy之间采用预共享（pre-shared）密钥。这也放松了对NAS支持证书的要求。同时还建议域间流量应首先采用TLS。IPSec和TLS采用的具体内容参见本标准第9.1和9.2节。

4.6 Diameter 应用顺从

应用标识符在能力交换阶段被广播，参见6.3节。广播支持某个应用表示发送者支持规范中描述的所有命令码，以及相关联的ABNF中规定的AVP。

一个实施可以给在某个应用中定义的任何命令增加任意的非强制AVP，包括运营商定义的AVP。

4.7 Diameter 路由授权

Diameter要求在每一个连接上应用传输层安全（TLS或IPSec）。因此，每个连接都需要认证、重放和完整性保护以及基于分组的加密。

除了认证每个连接，每个连接以至于整个会话也都必须经过授权。在一个连接开始之前，Diameter对等端必须检查它的对等端是否被授权承担其角色。例如，一个Diameter对等端可能是可信任的，但是这并不意味着它被授权作为一个可以广播一组Diameter应用的Diameter服务器。

在建立一个连接之前，应对沿途每个连接进行授权检查。Diameter能力协商（CER/CEA）也必须执行，以决定每个对等端支持什么Diameter应用。Diameter会话必须仅由授权过的节点进行路由，该节点被广播支持该会话所要求的Diameter应用。

一个中继或Proxy代理必须在其前转的所有请求后面增加一个路由记录（Route-Record）AVP。该AVP包含该请求来自的对等端的标识。

在授权一个会话之前，归属Diameter服务器必须检查路由记录AVP，以确保该请求穿过的路由是可接受的。例如，归属域内的管理员也许不希望请求被路由通过一个不可信任的域。通过授权一个请求，该归属Diameter服务器含蓄的指出其希望参与该事务，正如服务器和上一跳（Hop）之间的约定中规定的那样。如果该请求穿过的路由不可接受，则发送一个DIAMETER_AUTHORIZATION_REJECTED差错消息。

归属域也可能希望检查每个与Diameter响应授权会话相应的计费请求消息。没有相应授权响应的计费请求应当接受更多的安全检查，同时计费请求应当表明要求和提供的服务之间的区别。

类似地，在接收一个授权某会话的Diameter响应时，本地Diameter代理必须检查路由记录（Route-Record）AVP，以确保该响应经过的路由是可接受的。在每一步，前转授权响应被认为是进行与该会话相关的财政冒险的表现。本地域可能希望限制这种暴露，例如，通过建立对中间域的信用限制，以及拒绝接受违反那些限制的响应等手段。通过发布一个对应于该授权响应的计费请求，本地域含蓄的表示其同意提供授权响应中指出的服务。如果本地域不能提供该服务，则必须在计费请求中发送一个

DIAMETER_UNABLE_TO_COMPLY的差错消息；Diameter客户接收到其不能实现的服务的授权响应时，不可以另一个服务替换，并且随后发送计费请求申请另一个替换的服务。

5 Diameter 协议格式

5.1 Diameter Header

图5给出了Diameter头的格式。这些字段是以网络字节顺序传送的。

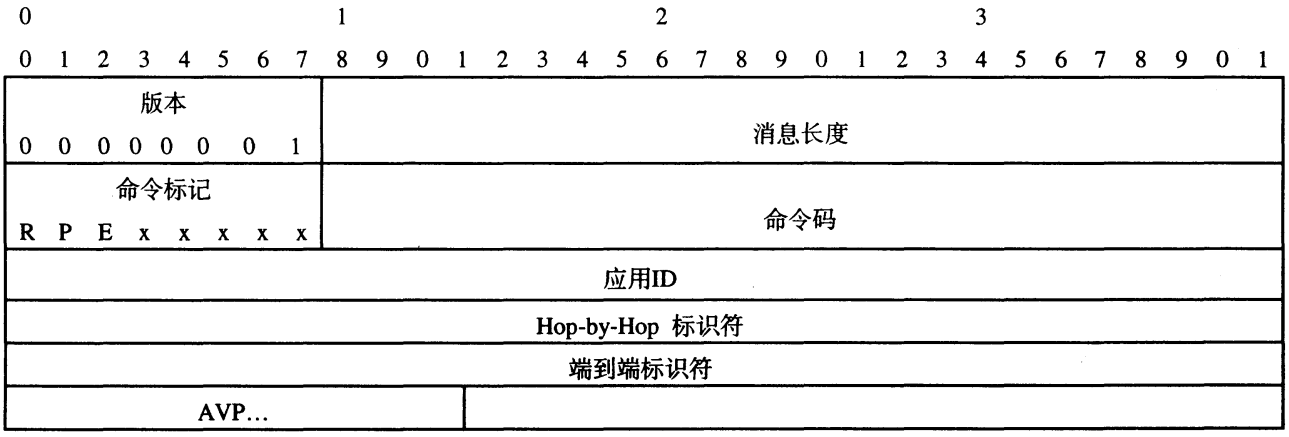

图5 Diameter 头格式

1）版本：该版本字段必须置为1，表明Diameter版本1。

2）消息长度：该消息长度字段为3个八位组，指明该Diameter消息的字节长度，包括头字段。

3）命令标记：该命令标记字段为8比特。已经分配的比特位如下：

```
 0 1 2 3 4 5 6 7
 +-+-+-+-+-+-+-+-+
 |R P E T r r r r|
 +-+-+-+-+-+-+-+-+
```

—— R（equest）：如果设置，表明该消息是一个请求。如果清0，该消息是一个应答。

—— P（roxiable）：如果设置，表明该消息可以被Proxy、中继或者重定向。如果清0，该消息必须在本地处理。

—— E（rror）：如果设置，表明该消息包含一个协议差错，且该消息与ABNF中描述的该命令不一致。“E”比特设置的消息一般当作差错消息。在请求消息中不能设置该比特。参见本标准第7.2.2节。

—— T（Potentially re-transmitted message）：该标记在链路失败过程后被设置，以帮助除去重复的请求。当重发请求还没有被确认时，需要设置该比特，以作为链路失败而造成的可能的重复包指示。当第一次发送一个请求时，该比特必须被清0，否则发送者必须设置该比特。Diameter代理仅需要关心它们发送的同一请求消息的遍数；其他实体进行的重传无须考虑。Diameter代理接收到一个T比特设置为1的请求，必须在前转该请求时保持T标记的设置。如果接收到一个以前消息的差错消息（如协议差错），则不可以设置该标记。该标记只有在没有接收到任何来自服务器的该请求的应答，且该请求再次被发送的情况下才能被设置。该标记不能在应答消息中设置。

—— r（eserved）：这些标记比特为将来应用预留，必须设置为0，接收者应当忽略。

4）命令码：该命令码字段为3个八位组，用于表明与该消息相关联的命令。该24位地址空间由IETF的IANA负责分配管理。命令码值16、777、214和16、777、215（16进制的FFFFFE ~ FFFFFF）被预留为实验使用。

5）应用ID：应用ID为4个八位组，用于标识该消息可适用于哪个应用。该应用可以是一个认证应用。头中的应用ID必须与该消息中包含的其他相关AVP相同。

6）Hop-by-Hop标识符：Hop-by-Hop标识符为一个32比特无符号整数字段（按网络字节顺序），用来帮助匹配请求和响应。发送者必须保证请求中的Hop-by-Hop标识符在特定的连接上在任何特定的时间是惟一的，并且保证该数字在经过重启动后仍然惟一。应答消息的发送者必须确保Hop-by-Hop标识符字段维持与相应的请求相同的值。Hop-by-Hop标识符通常是单调升序的数字，其开始值是随机生成的。一个带有未知Hop-by-Hop标识符的应答消息必须被丢弃。

7）端到端标识符：端到端标识符是一个32比特无符号整数字段（按网络字节顺序），用来检测重复消息。重启动实施可以设置高位12比特为包含当前时间的低位12比特，低位20比特为随机值。请求消息的发送者必须为每一个消息插入一个惟一的标识符。该标识符必须维持本地惟一至少4min，即使经过重启动。应答消息的生成者必须确保该端到端标识符字段包含与相应的请求相同的值。端到端标识符不可以被Diameter代理以任何原因修改。源主机AVP（Origin-Host，参见7.1.3节）和该字段的结合可以用于检测重复。重复请求会造成相同应答的传输，并且不可以影响任何状态的设置，当处理原始请求时。应当在本地被消除的重复应答消息将会被忽略（参见7.1.2节）。

8）AVP：AVP是封装与Diameter消息相关信息的一种方法，参见第5.2节。

5.1.1 命令码

每个请求/应答命令对分配给一个命令码、子类型（sub-type），例如，请求或应答，通过Diameter头的命令标记字段中的“R”比特来标识。

每个Diameter消息必须在其头中的命令码（Command-Code）字段里包含一个命令码，用来决定对特定消息采取的动作。表2是Diameter基础协议规定的命令码。

表2 Diameter基础协议规定的命令码

命令名	缩写	编码	参考章节
Abort-Session-Request	ASR	274	7.3.5.1
Abort-Session-Answer	ASA	274	7.3.5.2
Accounting-Request	ACR	271	8.7.1
Accounting-Answer	ACA	271	8.7.2
Capabilities-Exchange- Request	CER	280	6.3.1
Capabilities-Exchange- Answer	CEA	280	6.3.2
Device-Watchdog-Request	DWR	280	6.5.1
Device-Watchdog-Answer	DWA	280	6.5.2
Disconnect-Peer-Request	DPR	282	6.4.1
Disconnect-Peer-Answer	DPA	282	6.4.2
Re-Auth-Request	RAR	258	7.3.3.1
Re-Auth-Answer	RAA	258	7.3.3.2
Session-Termination- Request	STR	275	7.3.4.1
Session-Termination- Answer	STA	275	7.3.4.2

5.1.2 ABNF 定义的命令码

每个定义的命令码必须包含一个相应的ABNF规范，以用于规定必须或可能出现的AVP。在定义中采用下列格式：

```
command-def         = command-name "::=" Diameter-message
command-name        = Diameter-name
Diameter-name       = ALPHA *（ ALPHA / DIGIT / "-" ）
Diameter-message    = header  [ *fixed] [ *required] [ *optional]
                      [ *fixed]
header              = "<" Diameter-Header:" command-id
                      [r-bit] [p-bit] [e-bit] ">"
command-id          = 1*DIGIT
                      ；给该命令分配的命令码
r-bit               = ", REQ"
                      ；如果出现，命令标记中的“R”比特被设置，表明该消息是一个请求，
                      ；相反则是一个应答。
p-bit               = ", PXY"
                      ；如果出现，命令标记中的“P”比特被设置，表明该消息可以被Proxy。
e-bit               = ", ERR"
                      ；如果出现，命令标记中的“E”比特被设置，表明该应答消息包含一个
                      ；“协议差错”级别的结果码Result-Code AVP。
fixed               = [qual] "<" avp-spec ">"
                      ；规定AVP的固定位置
required            = [qual] "{" avp-spec "}"
                      ；该AVP必须出现，且能够在该消息的任何地方出现。
optional            = [qual] "[" avp-name "]"
                      ；在“optional”规则下的avp-name不能赋予
                      ；包括在fixed或required规则下的任何AVP名的值。
                      ；该AVP可以在消息中的任何地方出现。
qual                = [min] "*" [max]
                      ；见ABNF约定，RFC 2234第6.6节。
                      ；任何限定范围的缺失，取决于它是否领先于fixed，required，或optional
                      ；规则。如果一个fixed或required规则没有限定范围，
                      ；则必须出现准确的那个AVP。如果optional规则没有
                      ；限定词，则可能出现0或1这样的AVP。
                      ；
                      ；注：“［”和“］”拥有与在ABNF中不同的含义。
                      ；这些括号不能用于表示optional fixed规则（例如在结尾的optional
```

; ICV）。惯例是“0*1fixed”。

min = 1*DIGIT

; 可能出现的最小数。缺省值是0。

max = 1*DIGIT

; 可能出现的最大数。缺省值是无限大。

; 0表示该AVP不可以出现。

avp-spec = Diameter-name

; avp-spec必须是一个在Diameter基础或扩展规范中定义的AVP名。

avp-name = avp-spec / "AVP"

; 字符串“AVP”代表*any*任意AVP名，其不能与

; 在命令码定义中规定了required或fixed位置的AVP不冲突。

以下是一个假设的命令码定义：

Example-Request ::= < "Diameter-Header: 9999999，REQ，PXY >

{ User-Name }

* { Origin-Host }

* [AVP]

5.1.3 Diameter 命令命名惯例

Diameter命令名通常包括一个或多个英文单词，其后跟随动词请求（Request）或应答（Answer）。每个英文单词以连字符分界。同时也通常会采用三个字母缩写来表示请求和应答。

以下示例是用来结束一个会话的消息。命令名是Session-Terminate-Request和Session-Terminate-Answer，其缩写分别是STR和STA。

用于一个已知命令的请求和应答共享相同的命令码。该请求通过将Diameter头中的R（Request）比特设置为1来标识，以要求完成某个特定的动作，比如授权一个用户或终结一个会话。一旦该接收者完成了该请求，它将发出相应的应答，其中包括一个结果码，内容可以是以下几种：

—— 请求成功；

—— 请求失败；

—— 必须发送附加的请求以提供对等端先前要求的信息，这样才能返回成功或失败应答；

—— 接收者不能处理该请求，但可以提供一个能够处理该请求的Diameter对等端的信息，称为重定向。

在AVP中，编码的附加信息也可以包含在应答消息中。

5.2 Diameter AVP

Diameter AVP携带特定的认证、计费、授权、路由和安全信息以及请求和应答的配置细节。

某些AVP可能被列举了不止一次。这种AVP的作用是特定的，由AVP描述在每种情况中具体指定。

每个OctetString类型的AVP必须将32比特位填充满，而其他的AVP类型则可以自然排列。AVP数据字段结尾添加若干值为0的字节，直到到达一个字（Word）的边界。填充字节的长度不计入AVP长度字段内。

5.2.1 AVP 头

AVP头中的字段必须按网络字节顺序发送。头的格式如图6所示。

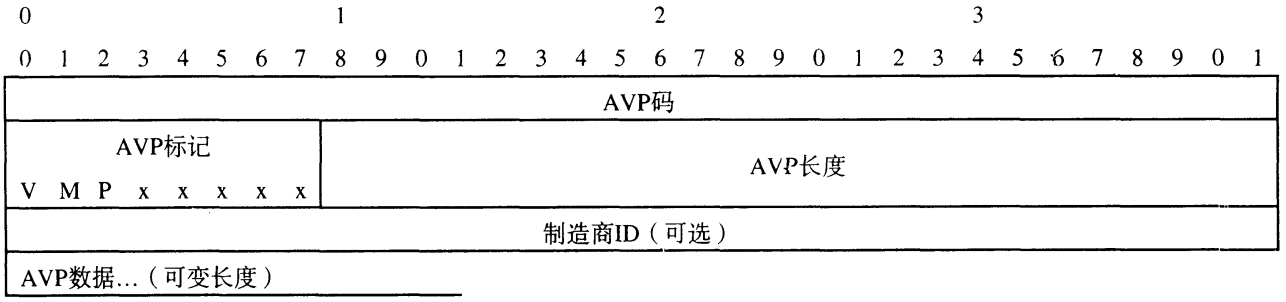

图6 AVP 头格式

1）AVP 码

AVP码与制造商ID 结合，可以惟一标识属性。AVP中1~255为前向兼容RADIUS预留，无需设置制造商ID字段。≥256的AVP用于Diameter，由IANA负责分配。

2）AVP 标记

AVP标记字段告知接收者如何处理每个属性。“r”（预留）比特不使用，应设置为0。

表示以后的Diameter应用可以在AVP头中定义附加的比特，一个未被承认的比特应被看作差错。“P”比特指明为保证端到端安全需要加密。

“M”比特，称为强制比特，指明对该AVP的支持是否是必需的。如果Diameter客户、服务器、Proxy或者翻译代理接收到一个AVP，其“M”比特设置为1，且该AVP或其值为未知，该消息必须被拒绝。Diameter中继和重定向代理不可以拒绝带有未知AVP的消息。

“M”比特必须按照包含它的AVP规定的规则进行设置。为了保证互用性，Diameter 实施必须能够从一个Diameter消息中剔除掉任何强制AVP，这些AVP既不是在Diameter基础协议中定义的，也不是在任何管理该消息的Diameter 应用规范中定义的。

它可以通过以下方式之一实现：

——如果一个消息被拒绝，由于该消息包含一个强制AVP，其既没有在Diameter基础标准中定义，也没有在任何管理该消息的Diameter应用规范中定义，该实施可以重新发送不带该AVP的消息，也可以同时插入附加的标准AVP来替代。

——可以在系统范围内提供一个配置选项，每个对等端或每个域将允许／拒绝特定的强制AVP。这样管理者能够改变配置以避免互用性的问题。

要求Diameter实施支持遵循消息正式语法的、或者在Diameter基础标准中定义、或者在管理该消息的Diameter应用规范中定义的所有强制AVP。

“M”比特清0的AVP仅是信息提示性的，接收者接收到其不支持的（包括不支持其值）“M”比特为0的AVP，可以简单忽略该AVP。

“V”比特，称作制造商定义（Vendor-Specific）比特，指明在AVP头中是否出现可选的制造商ID字段。当设置时，该AVP码属于某特定制造商编码地址空间。

除非另外注明，AVP将拥有以下缺省AVP标记字段设置：

“M”比特必须设置。“V”比特不可以设置。

3）AVP长度

AVP长度字段为三个八位组，指明在这个AVP中的八位组的数量，包括AVP码、AVP长度、AVP标

记、Vendor-ID字段（如果出现）以及AVP数据。如果接收到一个消息，其带有无效属性长度，该消息应被拒绝。

5.2.1.1 可选的头元素

AVP头包含一个可选字段。该字段仅在与其有关的比特标记有效时出现。

1）制造商ID（Vendor-ID）

如果在AVP标记字段中设置了“V”比特，则会出现制造商ID字段。可选的4个八位组的制造商ID字段包含IANA分配的“SMI网络管理私有企业码”值，按网络顺序编码。

任何希望实现制造商定义（Vendor-Specific）Diameter的制造商必须使用他们自己的制造商ID，顺着他们的私有管理AVP地址空间，以保证他们与其他制造商的Vendor-SpecificAVP 以及将来的IETF应用的AVP都不会冲突。制造商ID值为0符合IETF采用的AVP值，由IANA管理。

由于制造商ID字段缺失暗示该AVP不是制造商定义的，实施时不可以使用值为0的制造商ID。

5.2.2 基本 AVP 数据格式

数据字段为0到多个八位组，包含属性定义的信息。数据字段的格式和长度由AVP码和AVP长度字段决定。数据字段的格式必须是以下基本数据类型中的一种，或者是基本数据类型导出的一个数据类型。当需要一个新的基本AVP数据格式时，必须重新修订本标准。

1）OctetString

该数据包含任意可变长数据。除非另外注明，AVP长度字段必须至少设置为8（如果“V”比特有效，则为12）。这种类型的AVP值的长度如果不是4个八位组的倍数，应按照需要填充，这样下一个AVP（如果有）才能够在一个32比特边界开始。

2）Integer32

32比特有符号值，按照网络字节顺序。AVP长度字段必须设置为12（如果“V”比特有效，则为16）。

3）Integer64

64比特有符号值，按照网络字节顺序。AVP长度字段必须设置为16（如果“V”比特有效，则为20）。

4）Unsigned32

32比特无符号值，按照网络字节顺序。AVP长度字段必须设置为12（如果“V”比特有效，则为16）。

5）Unsigned64

64比特无符号值，按照网络字节顺序。AVP长度字段必须设置为16（如果“V”比特有效，则为20）。

6）Float32

该类型表示单精度浮点值，遵循IEEE 754-1985中关于浮点的描述。该32比特值按网络字节顺序送。AVP长度字段必须设置为12（如果“V”比特有效，则为16）。

7）Float64

该类型表示双精度浮点值，遵循IEEE 754-1985中关于浮点的描述。该64比特值按网络字节顺序传送。AVP长度字段必须设置为16（如果“V”比特有效，则为20）。

8）Grouped

该数据字段定义为一个AVP序列。这些AVP按其定义的顺序排列，每一个都包括它们的头和填充位。AVP长度字段值设置为8（如果“V”比特有效，则为12），加上所有序列内的AVP的长度总和。因此Grouped类型的AVP的长度字段总是4的倍数。

5.2.3 导出 AVP 数据格式

除了采用基本AVP数据格式以外，应用可以定义从基本AVP数据格式导出的数据格式。定义新的AVP导出数据格式的应用必须包括一个名称为“导出AVP数据格式”的部分，采用和下面相同的定义格式。每一个新定义必须或者定义其格式，或者列出定义其格式的参考标准。

以下是常用的导出AVP数据格式。

1）Address

地址格式是从OctetString AVP基本格式导出的。它与其他数据格式不同，例如，需要区分32比特（IPV4）或128比特（IPV6）地址。地址AVP的头两个八位组为AddressType，其包含一个在［IANA的“地址家族号码”］中定义的地址家族。AddressType用来区别剩下八位组的内容和格式。

2）Time

时间格式是从OctetString AVP基本格式导出的。该字符串必须包含4个八位组，与NTP时间戳格式的前4个字节格式相同。NTP时间戳在NTP协议规范（RFC 2030）第3章中定义。

本格式描述的时间，从通用协调时间（UTC）1900年1月1日0：00点开始。

在UTC时间2036年2月7日6：28：16，时间值将溢出。SNTP规范中描述了将时间扩展到2104年的程序，所有Diameter节点都必须支持该程序。

3）UTF8String

UTF8String格式是从OctetString AVP基本格式导出的。该格式采用ISO/IEC IS 10646－1字符集表示的人类可读的字符串，采用RFC 2279中描述的UTF-8转换格式，编码为一个OctetString。

由于标准10646不断在更新版本中增加附加编码点，实施必须能够处理0x00000001~0x7fffffff之间的任何编码点。字节顺序不符合UTF-8字符集中编码点的有效编码或者超出该范围都是被禁止的。

不应当允许采用控制符编码。但当需要另起一个新行时，可以采用控制符编码CR LF。

应避免采用先导或尾随空白字符。

由于用户接口硬件或软件并不直接支持编码点，可以提供其他替换的登录和显示方法，如十六进制。

对于7比特US-ASCII编码的信息，UTF-8字符集与US-ASCII字符集相同。

UTF-8可以要求多个字节表示一个字符／编码点，因此一个UTF8String的长度（以八位组计）可能与编码字符的个数不同。

注意，UTF8String的AVP长度字段是以八位组衡量的，不是字符。

4）DiameterIdentity

DiameterIdentity格式是从OctetString AVP基本格式导出的。

DiameterIdentity = FQDN

DiameterIdentity值惟一标识一个Diameter节点，以用于重复连接和路由环路检测。

字符串的内容必须是Diameter节点的FQDN。如果多个Diameter节点在同一台主机上运行，每个Diameter节点必须分配惟一的DiameterIdentity。如果一个Diameter节点可以由若干个FQDN标识，其中一个FQDN应在启动时被挑选出来，并作为该节点惟一的DiameterIdentity。

5）DiameterURI

DiameterURI必须遵循以下规定的统一资源标识符（URI）语法规则：

"aaa://" FQDN [port] [transport] [protocol]

; 没有传输安全

"aaas://" FQDN [port] [transport] [protocol]

; 采用传输安全

FQDN = Fully Qualified Domain Name

port = ":" 1*DIGIT

; 端口中的一个用来监听进来的连接。如果没有，假定为缺省Diameter端口（3868）

transport = ";transport=" transport-protocol

; 传输层协议中用来监听外来的连接请求。如果没有，则缺省为SCTP协议。如果aaa-protocol字段设置为Diameter，则不能采用UDP。

transport-protocol = ("tcp" / "sctp" / "udp")

protocol = ";protocol=" aaa-protocol

; 如果没有，缺省的AAA协议是Diameter

aaa-protocol = ("Diameter" / "radius" / "tacacs+")

以下是有效的Diameter主机标识示例：

aaa://host.example.com;transport=tcp

aaa://host.example.com:6666;transport=tcp

aaa://host.example.com;protocol=Diameter

aaa://host.example.com:6666;protocol=Diameter

aaa://host.example.com:6666;transport=tcp;protocol=Diameter

aaa://host.example.com:1813;transport=udp;protocol=radius

6）Enumerated

Enumerated是从Integer32 AVP基本格式导出的。该定义包含一个有效值的列表和它们的解释，并在引入该AVP的Diameter应用中有所描述。

7）IPFilterRule

IPFilterRule格式是从OctetString AVP基本格式导出的。其应用ASCII字符集。分组数据报可能基于以下与其相关的信息被过滤：

方向 （in或者out）

源和目的IP地址 （可能有掩码）

协议

源和目的端口 （列表或范围）

TCP标记

IP片段标记

IP选项

ICMP类型

适当方向的规则是按顺序评估的，通过首字匹配原则终结评估。每个分组评估一次。如果没有规则匹配成功，当最后一条规则允许某类分组通过时，该分组被丢弃；当最后一条规则拒绝某类分组通过时，该分组被转发。

IPFilterRule过滤器必须遵循以下格式：

Action dir proto从src到dst [options]

① action:

——permit　允许匹配该规则的分组通过。

——deny　丢弃匹配该规则的分组。

②dir: "in"是来自终端的，"out"是到终端的。

③proto: 通过数字定义的IP协议。关键字"ip"表示任何协议都可匹配。

④src and dst: <address/mask> [ports]

<address/mask>可以按照如下方式定义：

——ipno　以点或规范的IPv6格式分隔的IPv4或IPv6地址。

只有这个严格要求IP地址应匹配规则。

——ipno/bits　和上面一样的IP地址，带一个掩码长度，格式为1.2.3.4/24。在这种情况下，所有从1.2.3.0到1.2.3.255的IP数字将匹配。比特宽度必须对于IP版本有效，IP数字不可以设置超出掩码范围。

为了匹配，必须在用来描述该IP地址的分组中出示相同的IP版本。为了测试一个特定的IP版本，该比特部分可以被设置为0。

关键字"any"是0.0.0.0/0或者等价的IPv6地址。

关键字"assigned"是分配给终端的地址或地址组。

对于IPv4，一个典型的首要规则通常是"deny in ip! assigned"。

匹配的含义可以通过在前面增加一个修饰语（!）倒转，以使得所有其他地址匹配。这并不影响端口号的选择。

对于TCP、UDP和SCTP协议，可选端口可以定义如下：

{port/port-port}[，ports[，...]]

'-'符号规定了端口的范围（包括边界）。

拥有非0位移的分段分组（即不是第一个分段）将永远不匹配有一个或多个端口规定的规则。匹配分段分组的详细信息，参见可选项frag。

可选项如下：

①frag

如果该分组是一个分组片段，且不是数据包的第一个分段，则匹配。

如果与tcpflags 或TCP/UDP 端口规范冲突，Frag可不使用。

②ipoptions spec

如果IP头包含逗号分割的本标准中规定的可选项列表，则匹配。

支持的IP可选项有：ssrr（严格源路由）、lsrr（松散源路由）、rr（记录分组路由）以及ts（时间戳）。特定可选项缺失，可以利用'!'表示。

③tcpoptions spec

如果TCP头包含逗号分割的本标准中规定的可选项列表，则匹配。

支持的TCP可选项有：mss（最大分段尺寸）、window（tcp窗口广告）、sack（选择确认selective ack）、ts（rfc1323时间戳）和cc（rfc1644 t/tcp连接数量）

特定可选项缺失，可以利用'!'表示。

④established

仅用于TCP分组。匹配RST或ACK比特设置为1的分组。

⑤setup

仅用于TCP分组。匹配SYN比特设置为1但未设置ACK比特的分组。

⑥tcpflags spec

仅用于TCP分组。如果TCP头包含逗号分割的本标准中规定的标记列表，则匹配。支持的TCP标记有：fin、syn、rst、psh、ack和urg。特定标记缺失，可以利用'!'表示。

包含tcpflags规定的规则可以永远不匹配非0位移的分段分组。

匹配分段分组的详细信息，t参见可选项frag。

⑦icmptypes types

仅用于ICMP分组。如果列表类型中有ICMP类型，则匹配。

该列表可以是用逗号分隔的范围或个别类型的任何组合

下面列出的数字值和符号值都可以使用。支持的ICMP类型如下：

echo reply（0），destination unreachable（3），source quench（4），redirect（5），echo request（8），router advertisement（9），router solicitation（10），time-to-live exceeded（11），IP header bad（12），timestamp request（13），timestamp reply（14），information request（15），information reply（16），address mask request（17）和address mask reply（18）。

有一种分组，接入设备必须总丢弃，就是分段位移是1的IP分段。这是一个有效分组，但其只有一种用处，试图包围防火墙。

不能理解或应用某个拒绝规则的接入设备必须终结该会话。不能理解或应用某个允许规则的接入设备可以采用一个更为严格的规则。接入设备可以在采用提供的规则之前采用自己的拒绝规则，例如，为保护接入设备拥有者的基础设施。

规则语法是来自FreeBSD的改良的ipfw（8）子集，ipfw.c 编码可以为实施提供一个有用的基础。

8）QoSFilterRule

QoSFilterRule格式是从OctetString AVP基本格式导出的。其采用ASCII字符集。分组可能基于以下其相关的信息被过滤：

方向	（in或者out）
源和目的IP地址	（可能有掩码）
协议	
源和目的端口	（列表或范围）
DSCP值	（没有掩码或范围）

适当方向的规则是按顺序评估的，通过首字匹配原则终结评估。每个分组评估一次。如果没有规则匹配，该分组被视为尽力而为。不能理解或适用某QoS规则的接入设备，不应当终结该会话。

QoSFilterRule过滤器必须按照以下格式：

①Action dir proto从src到dst [options]

——tag：采用一个特定的DSCP［RFC 2474］标记分组。必须包括DSCP选项。

——meter： Meter流量。必须包括metering选项。

②dir：该格式遵照IPFilterRule中的描述。

③Proto：该格式遵照IPFilterRule中的描述。

④Src和dst： 该格式遵照IPFilterRule中的描述。

5.2.4 组合 AVP 值

Diameter协议允许“Grouped”类型的AVP值。其表示该数据字段实际上是一个AVP序列。其可能包括带有一个Grouped类型的AVP，即嵌套。一个组合类型AVP中的AVP与非组合类型AVP的添加（padding）要求是一样的。参见第5.2节。

一个组合AVP中的所有AVP的AVP编码数字空间与非组合AVP也是一样的。此外，如果封装在一个组合AVP中的任何一个AVP的“M”比特设置为1，则组合AVP自己必须也将其“M”比特设置为1。

每个定义的组合AVP必须包括一个相应的语法，采用ABNF，如下所示。

```
grouped-avp-def     = name "::=" avp
name-fmt            = ALPHA * ( ALPHA / DIGIT / "-" )
name                = name-fmt
                      ; 该名称必须是一个在Diameter基础或扩展规范中定义的AVP名称。
avp                 = header [ *fixed] [ *required] [ *optional]
                      [ *fixed]
header              = "<" "AVP-Header:" avpcode [vendor] ">"
avpcode             = 1*DIGIT
                      ; 该AVP编码分配给组合AVP
vendor              = 1*DIGIT
                      ; 分配给组合AVP的运营商ID。如果缺失，缺省使用0。
```

5.2.4.1 带一个组合数据类型的 AVP 举例

示例AVP（AVP编码为999999）是组合类型，用于表明组合AVP值是如何工作的。组合数据字段遵循如下ABNF语法：

```
Example-AVP   ::= < AVP Header: 999999 >
                    { Origin-Host }
                  1*{ Session-Id }
                   *[ AVP ]
```

后面跟随一个带组合数据的示例AVP。

其中Origin-Host AVP是必需的。本例中：Origin-Host = “example.com”。

后面必须跟随一个或多个Session-Id。本例中有两个：

Session-Id = “grump.example.com:33041;23432;893;0AF3B81”

Session-Id = “grump.example.com:33054;23561;2358;0AF3B82”

可选AVP为：

1）Recovery-Policy = <binary>

2163bc1d0ad82371f6bc09484133c3f09ad74a0dd5346d54195a7cf0b35
2cabc881839a4fdcfbc1769e2677a4c1fb499284c5f70b48f58503a45c5
c2d6943f82d5930f2b7c1da640f476f0e9c9572a50db8ea6e51e1c2c7bd
f8bb43dc995144b8dbe297ac739493946803e1cee3e15d9b765008a1b2a
cf4ac777c80041d72c01e691cf751dbf86e85f509f3988e5875dc905119
26841f00f0e29a6d1ddc1a842289d440268681e052b30fb638045f7779c
1d873c784f054f688f5001559ecff64865ef975f3e60d2fd7966b8c7f92

2）Futuristic-Acct-Record = <binary>

fe19da5802acd98b07a5b86cb4d5d03f0314ab9ef1ad0b67111ff3b90a0
57fe29620bf3585fd2dd9fcc38ce62f6cc208c6163c008f4258d1bc88b8
17694a74ccad3ec69269461b14b2e7a4c111fb239e33714da207983f58c
41d018d56fe938f3cbf089aac12a912a2f0d1923a9390e5f789cb2e5067
d3427475e49968f841

可选AVP被表示为十六进制，是由于Diameter实施在该示例AVP组定义的时候并不知道这些AVP的格式，而且很可能在该AVP实例被解释的时候也不是已知的，除非Diameter实施支持相同的AVP集合。该编码举例说明了如何使用填充，以及如何计算长度字段。同时也说明了AVP可以表示为接收者不能翻译的组合AVP值（本例中是Recover-Policy和Futuristic-Acct-Record AVP）。

本例AVP编码见表3。

表3 示例 AVP 的编码

```
    0       1       2       3       4       5       6       7
+-------+-------+-------+-------+-------+-------+-------+-------+
 0 |      示例AVP头（AVP码 =999999），长度 =468                   |
+-------+-------+-------+-------+-------+-------+-------+-------+
 8 |      Origin-Host AVP头（AVP码 =264），长度 =19                |
+-------+-------+-------+-------+-------+-------+-------+-------+
16 |  'e'  |  'x'  |  'a'  |  'm'  |  'p'  |  'l'  |  'e'  |  '.'  |
+-------+-------+-------+-------+-------+-------+-------+-------+
24 |  'c'  |  'o'  |  'm'  |填充   |       Session-Id AVP Header   |
+-------+-------+-------+-------+-------+-------+-------+-------+
32 |（AVP码 = 263），长度 = 50    |  'g'  |  'r'  |  'u'  |  'm'  |
+-------+-------+-------+-------+-------+-------+-------+-------+
                          . . .
+-------+-------+-------+-------+-------+-------+-------+-------+
64 |  'A'  |  'F'  |  '3'  |  'B'  |  '8'  |  '1'  |填充   |填充   |
+-------+-------+-------+-------+-------+-------+-------+-------+
72 |       Session-Id AVP头（AVP 码 = 263），长度= 51              |
+-------+-------+-------+-------+-------+-------+-------+-------+
80 |  'g'  |  'r'  |  'u'  |  'm'  |  'p'  |  'l'  |  'e'  |  'x'  |
+-------+-------+-------+-------+-------+-------+-------+-------+
                          ...
+-------+-------+-------+-------+-------+-------+-------+-------+
104 |  '0'  |  'A'  |  'F'  |  '3'  |  'B'  |  '8'  |  '2'  |填充   |
+-------+-------+-------+-------+-------+-------+-------+-------+
112 |   Recovery-Policy头（AVP码 = 8341），长度 = 223              |
+-------+-------+-------+-------+-------+-------+-------+-------+
120 |  0x21 | 0x63  | 0xbc  | 0x1d  | 0x0a  | 0xd8  | 0x23  | 0x71  |
+-------+-------+-------+-------+-------+-------+-------+-------+
                          ...
+-------+-------+-------+-------+-------+-------+-------+-------+
320 |  0x2f | 0xd7  | 0x96  | 0x6b  | 0x8c  | 0x7f  | 0x92  |填充   |
+-------+-------+-------+-------+-------+-------+-------+-------+
328 |  Futuristic-Acct-Record头（AVP码 = 15930），长度 = 137        |
+-------+-------+-------+-------+-------+-------+-------+-------+
336 |   0xfe | 0x19  | 0xda  | 0x58  | 0x02  | 0xac  | 0xd9  | 0x8b  |
+-------+-------+-------+-------+-------+-------+-------+-------+
                          . . .
+-------+-------+-------+-------+-------+-------+-------+-------+
464 |  0x41 |填充   |填充   |填充   |
+-------+-------+-------+-------+
```

5.2.5 Diameter 基础协议 AVP

表4描述了在基础协议中定义的Diameter AVP，包括它们的AVP编码值、类型、可能的标记值，以及该AVP是否可以被加密等。对于Diameter消息的发起者，“Encr”（加密）表示如果发送一个包含该AVP的消息经由一个Diameter代理（Proxy、重定向或中继），则该消息不可以被发送，除非在发起者和接受者之间提供端到端安全，并且对该AVP提供完整性／保密性保护，或者该发起者有本地信任配置指明不需要端到端安全。同样，对于Diameter消息的发起者，在“MAY”一栏中的“P”表示如果发送包含该AVP的消息经由一个Diameter代理（Proxy、重定向或中继），则该消息不可以被发送，除非在发起者和接受者之间提供端到端的安全，并且对该AVP提供完整性／保密性保护，或者该发起者有本地信任配置指明不需要端到端的安全。

表4中DiamIdent表示DiameterIdentity。

表4 Diameter 基础协议 AVP

属性名	AVP 编码	定义的章节	数据类型	AVP标记规则				
				MUST	MAY	SHLD NOT	MUST NOT	MAY Encr
Accounting-Interim-Interval	85	8.8.2	Unsigned32	M	P		V	Y
Accounting-Realtime-Required	483	8.8.7	Unsigned32	M	P		V	Y
Acct-Multi-Session-Id	50	8.8.5	UTF8String	M	P		V	Y
Accounting-Record-Number	485	8.8.3	Unsigned32	M	P		V	Y
Accounting-Record-Type	480	8.8.1	Enumerated	M	P		V	Y
Accounting-RADIUS-Session-Id	44	8.8.4	OctetString	M	P		V	Y
Accounting-Sub-Session-Id	287	8.8.6	Unsigned64	M	P		V	Y
Acct-Application-Id	259	7.1.9	Integer32	M	P		V	N
Auth-Application-Id	258	7.1.8	Integer32	M	P		V	N
Auth-Request- Type	274	7.3.7	Enumerated	M	P		V	N
Authorization- Lifetime	291	7.3.9	Unsigned32	M	P		V	N
Auth-Grace- Period	276	7.3.10	Unsigned32	M	P		V	N
Auth-Session- State	277	7.3.11	Enumerated	M	P		V	N
Re-Auth-Request- Type	285	7.3.12	Enumerated	M	P		V	N
Class	25	7.3.20	OctetString	M	P		V	Y
Destination-Host	293	7.1.5	DiamIdent	M	P		V	N
Destination- Realm	283	7.1.6	UTF8String	M	P		V	N
Disconnect-Cause	273	6.4.3	Enumerated	M	P		V	N
E2E-Sequence AVP	300	7.1.15	Grouped	M	P		V	Y
Error-Message	281	7.2.3	UTF8String		P		V, M	N
Error-Reporting- Host	294	7.2.4	DiamIdent		P		V, M	N

表4（续）

属性名	AVP编码	定义的章节	数据类型	AVP标记规则				
				MUST	MAY	SHLD NOT	MUST NOT	MAY Encr
Event-Timestamp	55	7.3.21	Time	M	P		V	N
Experimental- Result	297	7.2.6	Grouped	M	P		V	N
Experimental-Result-Code	298	7.2.7	Unsigned32	M	P		V	N
Failed-AVP	279	7.2.5	Grouped	M	P		V	N
Firmware- Revision	267	6.3.4	Unsigned32				P, V, M	N
Host-IP-Address	257	6.3.5	Address	M	P		V	N
Inband-Security-Id	299	7.1.10	Unsigned32					
Multi-Round-Time-Out	272	7.3.19	Unsigned32	M	P		V	N
Origin-Host	264	7.1.3	DiamIdent	M	P		V	N
Origin-Realm	296	7.1.4	UTF8String	M	P		V	N
Origin-State-Id	278	7.3.16	Unsigned32	M	P		V	N
Product-Name	269	6.3.7	UTF8String				P, V, M	N
Proxy-Host	280	7.1.7.3	DiamIdent	M			P, V	N
Proxy-Info	284	7.1.7.2	Grouped	M			P, V	N
Proxy-State	33	7.1.7.4	OctetString	M			P, V	N
Redirect-Host	292	7.1.12	DiamURI	M	P		V	N
Redirect-Host-Usage	261	7.1.13	Enumerated	M	P		V	N
Redirect-Max-Cache-Time	262	7.1.14	Unsigned32	M	P		V	N
Result-Code	268	7.2.1	Unsigned32	M	P		V	N
Route-Record	282	7.1.7.1	DiamIdent	M			P, V	N
Session-Id	263	7.3.8	UTF8String	M	P		V	Y
Session-Timeout	27	7.3.13	Unsigned32	M	P		V	N
Session-Binding	270	7.3.17	Unsigned32	M	P		V	Y
Session-Server-Failover	271	7.3.18	Enumerated	M	P		V	Y
Supported- Vendor-Id	265	6.3.6	Unsigned32	M	P		V	N
Termination- Cause	295	7.3.15	Enumerated	M	P		V	N
User-Name	1	7.3.14	UTF8String	M	P		V	Y
Vendor-Id	266	6.3.3	Unsigned32	M	P		V	N
Vendor-Specific-Application-Id	260	7.1.11	Grouped	M	P		V	N

6 Diameter 对等端通信模式

6.1 连接建立

一个Diameter节点具有和多个对等端通信的能力，但与所有对等端均建立连接则不是有效的方法。基于每个域，一个Diameter节点应该与两个对等端建立连接，即首要对等端和次要对等端。如果认为有必要，Diameter节点还可以建立其他连接。一般发送至域的所有消息均会发送到首要对等端，但是当失败替代（Failover）程序被调用时，所有未处理的请求均会被发送至次要对等端。然而，实施对两个对等端之间的负载平衡请求是自由的。一个假定对等端既可以作为一个假定域的首要对等端，又可以作为其他域的次要对等端。

当一个对等端不可信时，可能有多种原因，其中包括在指定的时间内未接收到DWA，此时不能向该对等端转发新的请求，而是启动Failover过程。当对等端的模式由活动（Active）模式变为不可信模式时，则需要建立额外的连接用以保证活动连接存在的必要数目。

有两种方法可以将对等端从不可信对等端列表中删除：

1）对等端为不可到达，导致传输连接被关闭。对等端的状态转变为关闭状态；

2）三条监控消息与可接受的往返次数交换，与该对等端建立的连接被视为稳定的。

不管被删除的对等端是首要对等端还是次要对等端，都使用备选对等端替代被删除的对等端。若被删除的对等端是首要对等端，则备选对等端则成为首要对等端，若被删除的对等端为次要对等端，则备选对等端则成为次要对等端。

6.2 对等端发现机制

动态的Diameter代理发现机制使得Diameter业务实施更为简化，更为可靠。下述机制描述用于提高Diameter 对等端发现机制的互操作性，这些机制是基于已有的IETF标准的。Diameter的所有节点都必须支持首选项（手工配置），后两个选项（SLP和DNS）为可选支持。

Diameter对等端发现机制可以在如下两种情况下应用：首先是当Diameter客户端需要发现一个第一跳Diameter代理；其次是Diameter代理需要发现用于进一步处理Diameter 操作的代理。在这两种情况下，推荐以下“查询顺序”：

1）若存在静态配置的Diameter代理位置列表，Diameter 实施则会查询该列表。

2）Diameter实施采用SLPv2发现Diameter业务。Diameter业务模板见附录D。

建议应用SLPv2安全机制，SLPv2安全机制要求给SLPv2 代理分配密钥。在附录D进行详细论述。SLPv2安全机制用于保证被发现的对等端是经过安全原则授权的。在附录D中进一步介绍SLPv2。

3）Diameter实施会采用NAPTR查询在指定域中的服务器。该实施必须预先知道在哪个域中寻找它的Diameter 代理。该域可以由一些参数推导出，例如，从NAI的“Realm”字段中，Diameter实施可以推断出需要完成的Diameter操作。

a）与传输协议选择业务相关的NAPTR业务字段的值为“AAA + D2x”，这里x表示主域支持的传输协议类型。本标准定义D2T表示传输协议为TCP协议，D2S表示传输协议为SCTP协议。为NAPTR业务名称与传输协议之间的映射已在IANA登记。

NAPTR记录提供由域到SRV记录的映射，SRV记录用于联络NAPTR业务字段中具有指定传输协议的服务器。资源记录会包含一个空规则表达和一个可变值（Replacement），可变值就是对应传输协议的SRV

记录。服务器支持多种传输协议，则会有多个NAPTR记录，每一个记录会有不同的业务值。按照RFC 2915（DNS资源记录NAPTR的标准），客户端丢弃任何业务字段不可用的记录。

b）客户端必须丢弃所有不是“D2X”的标识解析业务的业务字段，X值表示客户端支持的传输协议类型。NAPTR处理过程除了解析出服务器的SRV记录外，还会得到服务器首选同时也是客户端都支持的传输协议。NAPTR可变值中包含的域名后缀应该与查询请求的域名匹配。

4）如果未发现NAPTR记录，请求者查询目的地址的地址记录，'diameter. _ sctp' . realm或者'diameter._tcp' .realm。地址记录中包括的A RR's`和AAAA RR's`或者其他类似记录是根据请求者的网络协议能力选择的。如果DNS服务器没有返回地址记录，请求者则放弃。

如果服务器采用站点证书，在查询中的主域名称和在可变字段中的主域名称均必须基于站点证书是有效的，站点证书在TLS或者IKE交换过程中由服务器分发。同样，在SRV查询中的主域名称和在SRV记录中的目标中的主域名称必须基于相同站点证书是有效的。否则，攻击者能够修改DNS记录，给可变值赋上其他的域名，客户端则无法分辨是正常行为还是攻击行为。

Diameter对等端必须检验被发现的对等端的角色是否经过授权。不能仅通过IKE方式、TLS方式的鉴权，或者通过DNSSEC的方式确认DNS RRs。例如，一个Web服务器可以包含一个有效的TLS 证书，DNS可以包含可靠的RRs，但这不意味着它被授权成为Diameter服务器。

授权能够通过配置一个Diameter服务器CA完成。另一个方法就是由在TLS或者IKE证书内部定义OID，以此来表示Diameter服务器授权。

动态发现对等端会在对等端列表中建立一个新的表项。注意，由DNS建立的列表必须在DNS TTL过期前失效或者更新。如果在本地域范围外发现对等端，则会为对等端的域建立路由表。路由表的过期必须与对等端的过期值相匹配。

6.3 能力交换

两个Diameter对等端建立传输连接时，必须按照对等端状态机中规定的交换能力交换信息。能力交换消息允许了解对等端的标识和能力（协议版本号、支持的Diameter应用、安全机制等）。接收端仅给它的对等端发布应用程序对应的命令，该命令是对等端已经通告的自己所支持的Diameter 应用。一个Diameter节点必须缓存对等端所支持的应用，以确保未被识别的命令和AVP不会发送给它的对等端。

如果能力交换请求（Capabilities-Exchange-Req（CER））消息的接收端与它的发送端没有任何共同支持的应用程序，则必须返回result - code AVP为DIAMETER_NO_COMMON_APPLICATION的能力交换回答（Capabilities-Exchange-Answer（CEA）），而且要终止与相互间的传输层连接。注意从某对等端（宣告自己为中继，参见本标准第4.3.1节）接收CER和CEA，必须被认为与该对等端拥有公共应用。

类似地，收到（Capabilities-Exchange-Req（CER））消息的接收端如果与发送端没有任何安全机制的话，必须返回Result-Code AVP设为DIAMETER_NO_COMMON_SECURITY的能力交换回答（Capabilities-Exchange-Answer（CEA）），并且应该终止传输层连接。

由未知对等端处发送的CER消息可以被悄悄丢弃，或者可以通过将Result-Code AVP 设为DIAMETER_UNKNOWN_PEER发布CEA消息。在这两种情况下，传输层连接均要被关闭。如果本地策略允许接收未知主机发送的CER消息，则返回成功CEA消息。如果用成功的CEA消息回复未知对等端的CER消息，对等端实体的生命期等于传输连接的生命期。如果传输失败，所有目的地为未知对等端的等待处理的交互事务（Pending Transactions）能够被丢弃。

CER和CEA消息不许被Proxy、重定向或中继。

由于CER/CEA消息不能够被Proxy，上游代理有可能接收到没有有效的对等端去处理与消息中命令代码对应的应用程序的消息。在这种情况下，在回答消息中的E比特设为本，同时result - code AVP被置位为DIAMETER_UNABLE_TO_DELIVER，以提示下游采取相应措施（例如，向备选的对等端重新进行路由请求。）。

除了能力交换请求消息，还有一种类型包括Auth - Application - Id或者Acct - Application - Id AVP的请求消息，或者含有指定应用程序命令代码的请求消息，只能被转发到明确通告支持该应用程序的主机处（或者该主机已通告中继应用标识符）。

6.3.1 能力交换请求消息（Capabilities-Exchange-Request）

发送命令代码为257、命令标记“R”比特置位的能力交换请求消息交换本地能力。一旦检测到传输失败，则这条消息不可以被发送到备选对等端处。

当Diameter运行在SCTP协议上（注：SCTP协议允许连接建立在多个接口和多个IP地址之上），能力交换请求消息必须为每一个潜在的IP地址包含一个Host- IP-Address AVP。潜在的IP地址可以用于传输Diameter消息。

消息格式如下：

```
<CER> ::= < Diameter Header: 257，REQ >
                { Origin-Host }
                { Origin-Realm }
              1* { Host-IP-Address }
                { Vendor-Id }
                { Product-Name }
                [ Origin-State-Id ]
              * [ Supported-Vendor-Id ]
              * [ Auth-Application-Id ]
              * [ Inband-Security-Id ]
              * [ Acct-Application-Id ]
              * [ Vendor-Specific-Application-Id ]
                [ Firmware-Revision ]
              * [ AVP ]
```

6.3.2 能力交换应答消息（Capabilities-Exchange-Answer）

命令代码为257、清除“R”比特命令标记的能力交换应答消息（CEA）用于应答CER消息。

当Diameter运行在SCTP协议上，能力交换应答消息必须为每个潜在的IP地址包含一个主机IP地址（Host-IP-Address）AVP，这些IP地址可以在本地传输Diameter消息时采用。

消息格式如下：

```
<CEA> ::= < Diameter Header: 257 >
                { Result-Code }
                { Origin-Host }
```

{ Origin-Realm }
1* { Host-IP-Address }
{ Vendor-Id }
{ Product-Name }
[Origin-State-Id]
[Error-Message]
* [Failed-AVP]
* [Supported-Vendor-Id]
* [Auth-Application-Id]
* [Inband-Security-Id]
* [Acct-Application-Id]
* [Vendor-Specific-Application-Id]
[Firmware-Revision]
* [AVP]

6.3.3 设备制造商 Id AVP（Vendor-Id AVP）

Vendor－Id AVP（AVP 代码为266）类型是Unsigned32，包含分配给Diameter应用程序的设备制造商的IANA“SMI 网络管理私有企业代码（SMI Network Management Private Enterprise Codes）”值。与Supported-Vendor-Id AVP相结合，可以用于知道哪些设备制造商的特定属性可以被发送至对等端，还可以预先将设备制造商Id、产品名称、软硬件修复AVP相结合提供非常有用的跟踪信息。

在CER和CEA消息中的vendor－Id数值0是被预留的，并且这个字段是被忽略的。

6.3.4 固件修订（Firmware-Revision）AVP

固件修订AVP（AVP 代码 267）类型是Unsigned 32，用于提示Diameter 对等端的发布设备的固件修订。

没有固件修订的设备（例如，运行Diameter软件模块的通用计算机），可以报告Diameter软件模块的修订。

6.3.5 主机 IP 地址（Host-IP-Address ）AVP

主机IP地址（Host-IP-Address）AVP（AVP 代码 257）用于提示Diameter对等端的发送端IP地址。Diameter节点若希望采用SCTP协议，则所有源地址必须在CER和CEA消息中被通告，通过为每一个地址包含一个主机IP地址AVP来实现。这个AVP仅在CER和CEA消息中应用。

6.3.6 支持的设备制造商 Id（Supported-Vendor-Id）AVP

Supported-Vendor-Id AVP（AVP 代码 265）类型是Unsigned 32，包含分配给除设备制造商以外的制造商的IANA“SMI 网络管理私有企业代码”值。这个AVP应用在CER和CEA消息中，提示对等端该发送端支持由本AVP对应的制造商定义的AVP。

6.3.7 产品名称（Product-Name）AVP

产品名称AVP（AVP 代码 269）是UTF8字符串类型，包含制造商分配给产品的名称。相同产品名称AVP应该保持不变，即便经过多次固件修订。

6.4 对等端连接拆除

当Diameter节点拆除其传输连接中的某一个时，它的对等端无法知道拆除连接的原因，则通常会假设出现了连通性的问题，或者认为该节点在重新启动。在这种情况下，该对等端可以周期性地尝试重新连接，见4.4.2节。如果是因为缺乏内部资源中断连接，或者仅因为该Diameter节点预计在短期内将不会向其对等端转发任何Diameter消息，那么周期性的连接请求会被该节点拒绝。Disconnection-Reason AVP包含Diameter节点先前发布Disconnect-Peer-Request消息的原因。

Diameter节点采用Disconnect-Peer-Request消息提示对等端自己将拆除传输层连接，并且要求对等端不要再与自己重新连接，除非该对等端有合法理由（例如，有需要前转的消息）。对等端收到拆除对等端连接请求消息，即返回给发送端Disconnect-Peer-Answer消息，如果该消息近期已经被转发过，则会在消息中包含错误信息，否则会出现紊乱。Disconnect-Peer-Answer消息的接收端会拆除传输连接。

6.4.1 拆除对等端连接请求（Disconnect-Peer-Request）

拆除对等端连接请求（Disconnect-Peer-Request（DPR）），命令代码为282，命令标记“R”比特置位。将此消息发送至对等端，提示对方自己将关闭传输连接。如果检测到传输失败，该消息不可以被发送到备选对等端。

消息格式如下：

<DPR> ::= < Diameter Header: 282，REQ >
{ Origin-Host }
{ Origin-Realm }
{ Disconnect-Cause }

6.4.2 拆除对等端连接应答（Disconnect-Peer-Answer）

拆除对等端连接的应答消息（Disconnect-Peer-Answer（DPA）），命令码为282，命令标记“R”比特清除，应答Disconnect-Peer-Request消息。当接收到这条消息时，传输连接关闭。

消息格式如下：

<DPA> ::= < Diameter Header: 282 >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[Error-Message]
* [Failed-AVP]

6.4.3 拆除连接原因（Disconnect-Cause）AVP

拆除原因AVP（AVP代码 273）是列举类型（enumerated）。Diameter节点必须在Disconnect-Peer-Request消息中包括这个AVP，提示对等端关闭传输连接的原因。应该支持下列原因值：

1）REBOOTING 0

即将进行预定中的重启。

2）BUSY 1

对等端的内部资源受到限制，因此该对等端决定需要关闭该传输连接。

3）DO_NOT_WANT_TO_TALK_TO_YOU 2

对等端在近期内不希望与此对等端交换任何消息，因此决定不需要该传输连接。

6.5 传输差错检测

由于Diameter协议本身的特点，建议能够尽快检测出传输差错。检测出差错可以降低将消息发送至无效代理的机会，减少不必要的时延，并且提供更好的Failover 性能。本章定义的Device-Watchdog-Request和Device-Watchdog-Answer消息就可以用于提前检测出传输差错。

6.5.1 设备监控请求消息（Device-Watchdog-Request）

Device-Watchdog-Request（DWR），命令码为280，命令标记“R”比特置位，当两个对等端之间没有流量交互时，发送至对等端（见6.5.3）。一旦检测到传输差错，则该消息不允许发送至备选对等端。

消息格式如下：

<DWR> ::= < Diameter Header: 280，REQ >
{ Origin-Host }
{ Origin-Realm }
[Origin-State-Id]

6.5.2 设备监控应答消息（Device-Watchdog-Answer）

设备监控应答消息Device-Watchdog-Answer（DWA），命令码为280，命令标记“R”比特位清除，回复Device-Watchdog-Request消息时发送。

消息格式如下：

<DWA> ::= < Diameter Header: 280 >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[Error-Message]
* [Failed-AVP]
[Original-State-Id]

6.5.3 传输失败算法

传输失败算法在RFC 3539《认证、授权和计费（AAA）传输轮廓》中定义。所有Diameter实施必须支持该标准中定义的算法。

6.5.4 失败替代（failover）和失败回溯（failback）过程

如果检测出与对等端间的传输失败，所有等待转发的请求消息需要被转发到另一备选代理。这就是通常所说的失败替代。

Diameter节点为完成失败替代规程，需要为一个给定的对等端维护一个等待消息队列。当接收到应答消息时，队列中的通信请求则会被删除。逐跳（Hop-by-Hop）标识符字段被用于将应答与排队的请求进行匹配。

当检测到传输失败时，如果可能的话，队列中的所有消息将被发送至备选代理，并将消息中的T标记置位。在Diameter客户端或代理启动过程中，任何还在非易失性存储器中传送着的记录上的T标记也将被置位。在另外一种情况下，如果消息有固定的目的地，且失效的对等端是消息的最终目的地（参见Destination-Host AVP），客户端或代理不能将消息转发至备选服务器。这种错误要求代理返回将E比特置位的应答消息，Result - Code AVP设置为DIAMETER_UNABLE_TO_DELIVER。

需要重点指出的是，接收到多个相同的请求或应答可以被视为失败替代的结果。Diameter头中端到端ID字段和Origin-Host AVP必须用于鉴别重复的消息。

应该周期性地尝试向失败对等端发送连接请求，以便重新建立传输连接。一旦成功建立连接，就可以再次将消息转发至该对等端。这通常被称作失败回溯（Failback）。

6.6 对等端状态机

所有的Diameter实施必须遵守本节所描述的有限状态机。任何Diameter节点与任何对等端通信时，都必须遵循下面描述的状态机。多个动作（Action）由逗号分隔开，并且可以占用连续的多行。同样地，状态和下一个状态可以扩展占用多行。

这个状态机与RFC 3539《认证、授权和计费（AAA）传输轮廓》中描述的状态机是紧密结合的，RFC 3539中的状态机用于打开、关闭、失败替代、探测和重新打开传输连接。需要特别注意的是，RFC 3539要求采用监控Watchdog消息探测连接。对于Diameter，则采用DWR和DWA消息。

I为前缀：表示发起侧（连接）连接；R为前缀：表示应答侧（监听）连接。没有前缀意味着事件或者动作是相同的，不管事件发生在哪个连接上。

状态机中的稳定状态可以是关闭（Closed）、I－open和R－open，其余的状态是中间状态。无论初始化侧还是应答侧传输连接被用于通信时，I－open和R－open都是一样的。

连接请求成功完成后，会立即在初始化连接上发送CER消息。在有两条连接的情况下，两条连接中的一条通过选举将会被关闭。如果应答方Diameter实体的Origin-Host高于其对等端，则应答侧连接会被保留。如果对等端的Origin-Host高于发起方Diameter实体，则发起方的连接会被保留。所有后继的消息都会在保留下来的连接上被发送。注意，在一个对等端上的选举结果，一定会是另一个对等端上选举结果的反转。

对于TLS的应用，当两个端点均为打开状态时，TLS握手开始。如果TLS握手成功，所有后续的消息均会通过TLS发送。如果握手失败，两个端点同时转移到关闭状态。

状态机仅约束Diameter实施的行为。

通常认为产生相同结果的任何实施都是相兼容的。

对等端状态机见表5。

表5 对等端状态机

状　态	事　件	动　作	下一状态
Closed	Start	I-Snd-Conn-Req	Wait-Conn-Ack
	R-Conn-CER	R-Accept	R-Open
		Process-CER	
		R-Snd-CEA	
Wait-Conn-Ack	I-Rcv-Conn-Ack	I-Snd-CER	Wait-I-CEA
	I-Rcv-Conn-Nack	Cleanup	Closed
	R-Conn-CER	R-Accept	Wait-Conn-Ack/
		Process-CER	Elect
	Timeout	Error	Closed
Wait-I-CEA	I-Rcv-CEA	Process-CEA	I-Open

表5（续）

状　态	事　件	动　作	下一状态
	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/	I-Rcv-Conn-Ack	I-Snd-CER，Elect	Wait-Returns
Elect	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
Wait-Returns	Win-Election	I-Disc，R-Snd-CEA	R-Open
	I-Peer-Disc	I-Disc	R-Open
		R-Snd-CEA	
	I-Rcv-CEA	R-Disc	I-Open
	R-Peer-Disc	R-Disc	Wait-I-CEA
	R-Conn-CER	R-Reject	Wait-Returns
	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

表5（续）

状　态	事　件	动　作	下一状态
	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

6.6.1　输入连接

当接收到Diameter 对等端发送来的连接请求时，一般情况下并不知道该对等端的身份，直到接收到对等端发送来的CER消息时才可能知道对等端的身份。这是因为主机和端口决定Diameter 对等端的身份，一个输入连接的源端口是任意的。根据收到的CER消息，对等端的身份能够通过Origin-Host完全确定。

基于该原因，Diameter对等端应用某种逻辑方法接收连接请求、接受请求、等待CER消息，这些过程必须与状态机无关。一旦在新连接上接收到CER消息，则采用标识对等端的Origin－Host定位与该对等端相关联的状态机，新连接和CER消息被传递给状态机，这就是一个R－Conn－CER事件。

如果任何消息在CER之前到达，或者在收到CER消息之前，实施定义的定时器超时，则处理输入连接的逻辑方法应该关闭并且丢弃该连接。

6.6.2　事件

自动机中的转移和动作由事件引起。本节中，我们忽略I－和R－前缀，因为实际事件将会是相同的，只是仅会在两个可能的连接中的一个发生。

Start：Diameter应用发出信号，应该发起与对等端的连接。

R-Conn-CER：接收到的确认消息声明传输连接已经建立，相关的CER消息也已经到达。

Rcv-Conn-Ack：接收到一个肯定的确认消息，证实传输连接已经建立。

Rcv-Conn-Nack：接收到否定的确认消息声明传输连接未被建立。

Timeout：一个定义的应用定时器在等待某些事件时超时。

Rcv-CER：接收到对等端发来的CER消息。

Rcv-CEA：接收到对等端发来的CEA消息

Rcv-Non-CEA：接收到对等端发来的非CEA的消息。

Peer-Disc：接收到对等端发来的拆除连接指令

Rcv-DPR：接收到对等端发来的DPR消息。

Rcv-DPA：接收到对等端发来的DPA消息。

Win-Election：举行选举时，本地节点为获胜者。

Send-Message：消息要被发送。

Rcv-Message ：接收到除了CER、CEA、DPR、DPA、DWR、DWA消息外的消息。

Stop：Diameter应用程序发出信号，通知应该中断一个连接（例如，系统关闭）。

6.6.3 动作（action）

在自动机中的动作由事件引发，并且指示分组传输和将要在连接上采取的动作。本节中，我们忽略I－和R－前缀，因为实际动作将会是相同的，只是将会在两个可能的连接中的一个发生。

Snd-Conn-Req：开始发起与对等端的一个传输连接。

Accept：接受作为应答侧连接的与R-Conn-CER相关联的输入连接。

Reject：拆除与R-Conn-CER相关联的输入连接。

Process-CER：处理与R-Conn-CER相关联的CER消息。

Snd-CER：将CER消息发送至对等端。

Snd-CEA：将CEA消息发送至对等端。

Cleanup：如果需要，连接被关闭，任何本地资源均被释放。

Error：传输层连接可以被Politely或者Abortively拆除，以响应一个错误条件Condition。本地资源被释放。

Process-CEA：处理接收到的CEA消息。

Snd-DPR：将一条DPR消息发送至对等端。

Snd-DPA：将一条DPA消息发送至对等端。

Disc：拆除传输层连接，本地资源被释放。

Elect：一次选举发生。

Snd-Message：一条消息被发送。

Snd-DWR：一条DWR消息被发送。

Snd-DWA：一条DWA消息被发送。

Process-DWR：DWR消息被处理。

Process-DWA：DWA消息被处理。

Process ：消息被处理。

6.6.4 选举过程

在应答侧完成选举。应答侧将自己的Origin-Host与对等端发送的CER消息中的Origin-Host进行比较。如果本地Diameter列表的Origin-Host高于对等端的Origin-Host，则本地发布win－election事件。

在比较过程中，应将较短的字节串用0填充，以使它的长度与较长的字节串相同，然后从高位字节完成逐字节无符号的比较。任何保留的字节均被认为值是0x80。

7 Diameter 协议流程

7.1 Diameter 消息处理

这一节描述了Diameter请求与应答消息如何产生与处理。

7.1.1 Diameter 请求消息寻路概述

向目的地发送的请求消息中的Destination-Realm AVP与Destination-Host AVP组合有如下三种应用方式：

—— 不能被 Proxy 的请求（比如 CER）不可以包含 Destination-Realm 或 Destination-Host AVP。

—— 一个请求需要发送给为某特定域服务的归属服务器，但并不针对某个特定服务器（比如一系列往复消息中的第一个请求），则该请求中必须包括 Destination-Realm AVP，且不可以包含 Destination-Host AVP。

—— 否则，一个请求发送给为某特定域服务的一个特定的归属服务器，该请求必须同时包含 Destination-Realm 与 Destination-Host AVP 两个参数。

Destination-Host AVP用于描述上述组合中请求的目的地为固定时的情况。包括：

—— 认证请求要进行多次往复。

—— Diameter 消息在源与目的间采用了预先共享的会话密钥来建立安全机制。

—— 服务器产生的消息必须由一个特定的 Diameter 客户端接收（如接入设备），比如 Abort-Session-Request 消息，用来申请终止某个用户的会话。

注意：当且仅当主机在对等端表（见4.3.4节）中时，一个代理才可以把一个请求前转到Destination-Host AVP里描述的主机处。否则，该请求消息将只根据Destination-Realm进行寻址（参见7.1.1.6节）。

如果一个消息可以被Proxy，就必须有Destination-Realm AVP。将由Diameter代理（Proxy、重定向、中继）转发的请求消息必须有一个 Acct-Application-Id AVP、一个Auth-Application-Id AVP或Vendor-Specific-Application-Id AVP。不可由Diameter代理（Proxy，重定向与中继）的消息在它的ABNF中必须不能包括Destination-Realm AVP。这个Destination-Realm AVP值可能从User-Name AVP中提取，或采用其他与应用相关的方法。

当收到消息时，消息会按下述方式进行处理：

1）如果消息是到本地主机的，处理过程如 7.1.1.4 节所述。

2）如果消息是发向一个 Diameter 对等端，并且本地主机能直接与之通信，处理过程如 7.1.1.5 节所述。这个处理过程称为请求前转。

3）在 7.1.1.6 节中的处理过程称为请求寻路。

4）如果上述的处理过程均不成功，则返回一个应答消息，应答消息中的 Result-Code 设为 DIAMETER_UNABLE_TO_DELIVER，同时设置 E 比特。

对于在一个管理域内Diameter消息的寻路，所有域内的Diameter节点必须建立对等关系。

注：这一节里包括的处理规则是作为Diameter开发者的一般性指导。具体实施可能采用与这里描述完全不同的方法，但仍符合协议规范。差错处理详见第7.2节。

7.1.1.1 产生一个请求

当创建一个请求时，除了遵循在应用定义中描述的、对于特定请求的所有处理过程以外，还必须遵循下述的处理过程：

—— Command-Code 设成适当的值。

—— R 比特置位。

—— 端到端标识符设成本地惟一的值。

—— Origin-Host 与 Origin-Realm AVP 必须设成适当的值，用来标识消息的源。

—— Destination-Host 与 Destination-Realm AVP 必须设置适当的值，参见 7.1.1。

—— 如请求消息需要经过代理，则必须包括 Acct-Application-Id AVP、Auth-Application-Id 或 Vendor-Specific-Application-Id AVP。

7.1.1.2 发送请求

当发送一个请求时，不论该请求是本地产生的，还是前转或寻路的一个结果，都必须遵循下述的处理过程：

—— 逐跳标识符应设为本地惟一的值；

—— 消息应保存在未决请求列表中。

作用于该消息的其他行为（基于代理正在担任的特殊任务）将在下面的章节中描述。

7.1.1.3 接收请求

一个中继或Proxy收到请求时必须检查前转环路，当服务器发现自己的标识在Router-Record AVP中时，就检测到环路。当这种情况发生时，代理必须发送一个带有Result-Code AVP设为DIAMETER_LOOP_DETECTED的应答消息。

7.1.1.4 处理本地请求

当下述情况之一发生时，这个请求认为是本地的。

—— Destination-Host AVP 为本地主机的标识；

—— 如果没有 Destination-Host AVP，Destination-Realm AVP 参数里的域（Realm）被配置成本地处理，同时本地也支持该 Diameter 应用；或

—— Destination-Host 与 Destination-Realm 都没有。

当一个请求在本地处理时，应根据7.1.2节中的规则产生相应的应答。

7.1.1.5 请求消息前转

完成请求前转需要依靠Diameter对等端列表。Diameter对等端列表包括所有本地节点可以直接进行通信的对等端。

当收到一个请求时，请求中的Destination-Host AVP中的主机在对等端列表中，这个消息应前转到对等端。

7.1.1.6 请求消息寻路

Diameter请求消息寻路是通过域与相关应用来完成的。一个可能由Diameter代理（Proxy、重定向或中继）前转的Diameter消息，它必须在Destination-Realm AVP及某个应用标识符（Auth-Application-Id、Acct-Application-Id 或 Vendor-Specific-Application-Id）AVP中包含目标域。域可以从User-Name AVP中提取，这个AVP的格式为网络接入标识符（NAI）。NAI中的域相关部分插入到Destination-Realm AVP中。

Diameter代理可能有一个本地支持的域与应用列表，也可能有一个外部支持的域与应用列表。当收到一个请求时，它所包含的域与/或应用本地不支持，这个消息会经过寻路到域路由列表中列出的对等端（见4.3.4节）。

7.1.1.7 请求消息重定向

当重定向代理收到一个请求时，其寻路列表设为REDIRECT。重定向代理必须回应一个设置了E比特的应答消息，同时维护信息头中的逐跳标识，并把Result-Code AVP设为

DIAMETER_REDIRECT_INDICATION。每一个与寻路列表相关的服务器都加入到一个Redirect-Host AVP中。

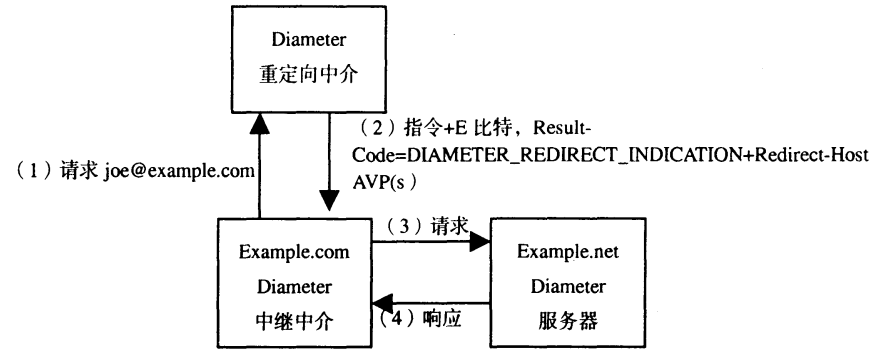

图7 Diameter 重定向代理

E比特置位，且Result-Code设为DIAMETER_REDIRECT_INDICATION的应答消息的接收者采用Diameter头中逐跳标识符的值，来标识在未决消息队列中要进行重定向的消息（见6.3节）。如果与新的代理间没有传输连接，就建立一个，然后直接把请求发送给对方。

多重Redirect-Host AVP是允许的。E比特置位的应答消息的接收者从这些主机里选取一个作为重定向消息的目的地。

7.1.1.8 中继与 Proxy 请求消息

一个中继或Proxy代理必须把Route-Record AVP加入到所有前转的请求中。这个AVP参数里有接收这个请求的对等端标识符。

请求消息中的逐跳标识符被保存，并用本地惟一的值代替。请求消息的源亦被保存，它包含有IP地址、端口与协议。

如果一个中继或Proxy代理收到相应的响应时需要对本地状态信息进行存取，可能在请求消息中包括Proxy-Info AVP。Proxy-Info AVP涉及一些安全问题，应包含一个带有本地节点密钥的嵌入式HMAC。另一种方案是，设备可能用本地存储来保存状态信息。

该消息根据域路由表，发送到下一跳。

图8是用本节中消息寻路处理过程的实例。

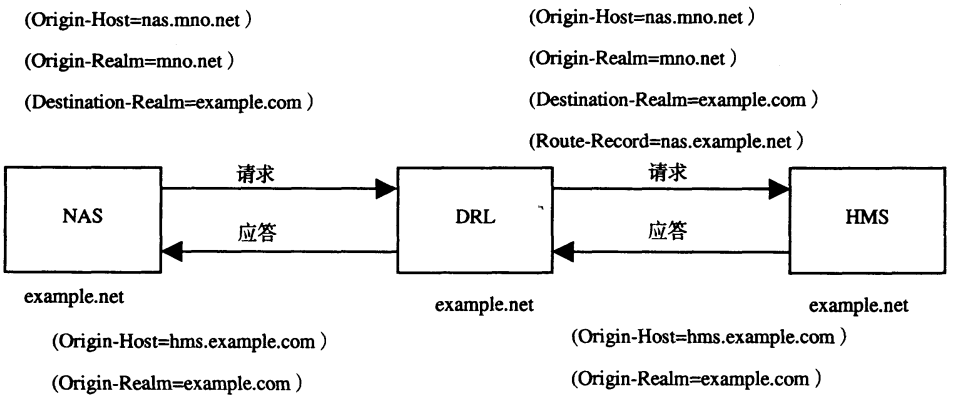

图8 Diameter 消息的寻路

7.1.2 Diameter 应答消息处理

当在本地处理一个请求时，要产生一个相关的应答消息，除了应遵循Diameter应用所定义的命令处理过程外，还必须符合下述处理过程：

—— 在应答消息中的逐跳标识符与请求消息中的相同。

—— 本地主机的标识写在 Origin-Host AVP 中。

—— Destination-Host 与 Destination-Realm AVP 必须不能出现在应答消息中。

—— 加上 Result-Code AVP 以表明成功与否。

—— 如果请求消息里有 Session-Id，应答消息里也必须有。

—— 如果请求消息里有的任何 Proxy-Info AVP 必须加到应答消息里，顺序同请求消息中的一致。

—— P 比特与请求消息中的相应比特一致。

—— 应答消息中端到端标识符与请求消息中的一致。

注意：差错消息（见7.2.3节）也遵从上述处理过程。

7.1.2.1 处理收到的应答消息

Diameter客户端或Proxy服务器必须把应答消息的逐跳标识符与一组待处理请求消息进行比较，相应的消息应从待处理消息队列中移除。与已知的逐跳标识均不匹配的应答消息应被忽略。

7.1.2.2 中继与 Proxy 应答消息

如果一个应答是被Proxy或中继过的请求应答，代理必须恢复原来Diameter头中逐跳标识符的值。

如果消息中最后一个Proxy-Info AVP指向本地的Diameter服务器，该AVP必须在被前转前删除。

如果一个中继或Proxy代理收到应答消息的Result-Code AVP表明请求失败，它必须不能修改AVP中的内容。必须记录任何检测到的其他本地错误，但不能在Result-Code AVP中反映出来。如果代理收到的应答消息中Result-Code AVP显示成功，它想把这个AVP进行修改以显示一个差错，它必须把发往接入设备的消息中的Result-Code AVP改成相应的差错，同时加入一个Error-Reporting-Host AVP，并代表接入设备发送一个STR。

代理必须向发出请求消息的主机发送应答消息。

7.1.3 Origin-Host AVP

Origin-Host AVP（AVP编号264）为DiameterIdentity类型，必须出现在每一个Diameter消息中。这个AVP表明产生Diameter消息的源点。中继代理不可改变此AVP。

Origin-Host AVP的值在一个单机上是惟一的。

注：Origin-Host AVP在Diameter对等端支持多于一个地址时，可能会解析成多个地址。

此AVP应尽量放置在离Diameter头较近的位置。

7.1.4 Origin-Realm AVP

Origin-Realm AVP（AVP编号296）为DiameterIdentity类型，此AVP包含任一Diameter消息产生者所在域，应出现在所有的消息中。

此AVP应尽量放置在离Diameter头较近的位置。

7.1.5 Destination-Host AVP

Destination-Host AVP（AVP编号293）为DiameterIdentity类型，此AVP必须出现在所有主动提供服务的代理发起消息中，可能出现在请求消息中，但不可出现在应答消息中。

如果没有Destination-Host AVP会导致消息发送到任意一个在Destination-Realm AVP中定义的域中支持相应应用的服务器上。

此AVP应尽量放置在离Diameter头较近的位置。

7.1.6 Destination-Realm AVP

Destination-Realm AVP（AVP编号283）为DiameterIdentity类型，包含有消息寻址的域。Destination-Realm AVP不可在应答消息中出现。Diameter客户把User-Name AVP的域相关部分插入到此AVP中。发起一个请求消息的Diameter服务器用从目标主机收到的Origin-Realm AVP填写此AVP（除非它知道此前的值）。当这个AVP出现时，Destination-Realm AVP用于消息寻路的判决。

一个请求消息，其ABNF没有把Destination-Realm AVP当作必选AVP列出，应被认为是不可寻路的消息。

此AVP应尽量放置在离Diameter头较近的位置。

7.1.7 Routing AVPs

本节定义的AVP用于消息寻路。这些AVP在Diameter消息经代理处理时发生变化，因此无法受到端到端的安全保护。

7.1.7.1 Route-Record AVP

Route-Record AVP（AVP编号282）为DiameterIdentity类型。此AVP中的标识必须与收到的能力交换消息中的Origin-Host一致。

7.1.7.2 Proxy-Info AVP

Proxy-Info AVP（AVP编号284）为Grouped类型。Grouped类型数据域符合ABNF语法：

```
Proxy-Info ::= < AVP 头: 284 >
                    { Proxy-Host }
                    { Proxy-State }
                   * [ AVP ]
```


7.1.7.3 Proxy-Host AVP

Proxy-Host AVP（AVP编号280）为DiameterIdentity类型。此AVP包含填加Proxy-Info AVP的主机标识符。

7.1.7.4 Proxy-State AVP

Proxy-State AVP（AVP编号33）类型为OctetString，包含有本地的状态信息，必须当做不透明的数据进行处理。

7.1.8 Auth-Application-Id AVP

Auth-Application-Id AVP（AVP编号258）类型为Unsigned32，用于通告应用对认证、授权部分的支持。Auth-Application-Id必须在所有的认证或/与授权消息中出现，这些消息在其他的Diameter规范中定义，并分配相应的应用ID。

7.1.9 Acct-Application-Id AVP

Acct-Application-Id AVP（AVP编号259）类型为Unsigned32，用于通告应用对计费部分的支持。Acct-Application-Id AVP必须出现在所有计费消息中。惟一的Auth-Application-Id可能与多个Acct-Application-Id同时存在。

7.1.10 Inband-Security-Id AVP

Inband-Security-Id AVP（AVP编号299）类型为Unsigned32。用于通告应用对安全部分的支持。

当前支持下述的值，但有足够的空间添加新的安全标识。

1）NO_INBAND_SECURITY 0

对等端不支持TLS，如果此AVP不存在，这是默认的值

2）TLS 1

此节点支持TLS安全，遵循TLS标准RFC 2246中的定义

7.1.11 Vendor-Specific-Application-Id AVP

Vendor-Specific-Application-Id AVP（AVP编号260）为Grouped类型，用于通告厂商定义的Diameter应用。惟一的Auth-Application-Id与多个Vendor-Specific-Application-Id可能同时出现。

此AVP必须为厂商自定义的应用中所有试验性指令的第一个AVP。

此AVP应尽量放置于与Diameter头较近处。

AVP格式如下：

<Vendor-Specific-Application-Id> ::= < AVP头: 260 >

1* [Vendor-Id]

0*1{ Auth-Application-Id }

0*1{ Acct-Application-Id }

7.1.12 Redirect-Host AVP

如果一个应答消息的E比特被设置，Result-Code设为DIAMETER_REDIRECT_INDICATION必须有一个或多个此AVP。

根据上述收到的消息，接收Diameter节点应把请求消息直接前转到此AVP中列出的一个主机处。从Redirect-Host AVP中选出的服务器应在整个会话过程使用。

7.1.13 Redirect-Host-Usage AVP

Redirect-Host-Usage AVP（AVP编号261）为Enumerated类型。此AVP可能出现在一个E比特置位、Result-Code AVP为DIAMETER_REDIRECT_INDICATION的应答消息中。

当此AVP出现时，它指明如何应用受重定向主机影响的寻路列表。支持下述取值：

1）DONT_CACHE 0

Redirect-Host AVP中定义的主机不应进行缓存，这是默认值。

2）ALL_SESSION 1

所有会话中的消息，由于有相同的Session-ID AVP，可能会发向Redirect-Host AVP中定义的主机。

3）ALL_REALM 2

所有请求同一目的域的消息可能会发往Redirect-Host AVP中定义的主机。

4）REALM_AND_APPLICATION 3

所有到同一域中同一应用的消息可能发送到Redirect-Host AVP中定义的主机。

5）ALL_APPLICATION 4

所有针对一应用的消息可能发往Redirect-Host AVP中定义的主机。

6）ALL_HOST 5

所有产生重定向主机的消息可能会发往Redirect-Host AVP中定义的主机。

7）ALL_USER 6

对于请求用户的所有消息可能会被发送到Redirect-Host AVP中定义的主机。

7.1.14 Redirect-Max-Cache-Time AVP

Redirect-Max-Cache-Time AVP（AVP编号262）类型为Unsigned32。此AVP必须出现在一个E比特被设置，Result-Code AVP设为DIAMETER_REDIRECT_INDICATION，且Redirect-Host-Usage AVP非0的应答消息中。

此AVP包含对等端列表与路由列表（这两个列表的出现是重定向主机Redirect-Host的结果）入口被缓存的最大秒数。注：当用于重定向的主机不能到达时，所有相关的对等端列表与路由表列表均必须删除。

7.1.15 E2E-Sequence AVP

E2E-Sequence AVP（AVP编号300）提供了端到端消息反重演（Replay）的保护，为Grouped类型。它包含一个随机值（一个临时的OctetString）与一个计数器（整型）。对于每一个端到端的对等端，必须用不同的随机值，计数器初始为0并随AVP向对等端发送时加1，此AVP必须包括在所有使用端到端保护的消息中（比如CMS签名与加密）。

7.2 Diameter 差错处理

在Diameter中有两类差错：协议差错与应用差错。协议差错发生在基本协议层，可能需要每一跳都引起注意（例如消息的选路错误）。应用差错总的来说是由于Diameter应用中指定的一个功能的错误（例如，用户鉴权，丢失AVP）。

Result-Code AVP的值用来报告协议差错，此参数必须在设置了“E”比特的应答消息中出现。当收到一个引起协议差错的请求消息时，返回一个“E”比特置位的应答消息，且在Result-Code AVP里设置适当的协议差错值。消息后向发送给请求的发起者时，每一个Proxy代理或中继代理都可能对这个消息进行处理。

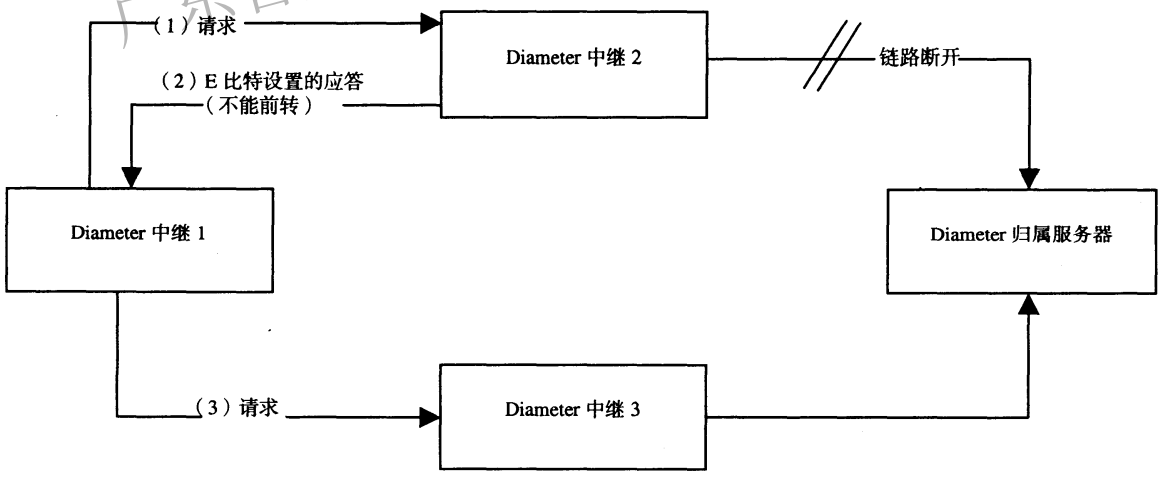

图9 Diameter 中继前向前转消息举例

图9提供了一个消息由Diameter中继上行前转的例子，当中继2接收到消息时，它检测到自己不能把请求消息前转给归属服务器，它返回一个消息，这个消息中“E”比特被置位，且Result-Code AVP设置成DIAMETER_UNABLE_TO_DELIVER。图10中给出的这个差错属于协议差错范畴，中继1会采取特别的行动，它会尝试把消息通过替代的中继3前转。

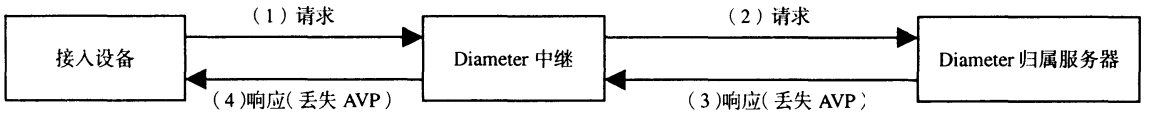

图10 Diameter 消息导致应用差错的实例

图10提供了一个Diameter消息导致应用差错的实例。当产生应用差错时，报告差错的Diameter实体将命令标记中的 “R” 比特置0，并添加带有正确值的Result-Code AVP。应用差错与任何Proxy代理或中继代理无关，因此这个消息会后向转发给请求消息的产生者。

有一些Result-Code AVP应用差错需要其他的AVP也出现在应答中。在这些情况下，Diameter节点设置Result-Code AVP来指示差错必须加上相应的AVP。例如：

—— 收到一个 “M” 比特置位（必选比特）但不可识别的 AVP，会导致应答消息中把 Result-Code AVP 设置成 DIAMETER_AVP_UNSUPPORTED，并把该不可识别的 AVP 放到 Failed-AVP AVP 中。

—— 收到含有不可识别值的 AVP 时，会导致返回的应答消息中 Result-Code AVP 设置成 DIAMETER_INVALID_AVP_VALUE，并把包含错误 AVP 放到 Failed - AVP 参数中。

—— 收到一个命令，其中的一个 AVP 缺失，可是根据命令的 ABNF，这个参数是必选的。接收者发送的应答消息中的结果代码中设置 DIAMETER_MISSING_AVP，并创建一个 AVP，该 AVP 中的代码与其他值字段设成希望原消息中缺少 AVP 所应设置的值，再把创建的这个 AVP 放到 Failed-AVP AVP 中。

Result-Code AVP用于描述Diameter节点在其处理消息过程中遇到的各种差错。在有多个错误的情况下，Diameter节点必须只报告第一个遇到的差错（可能在与具体执行相关的执行顺序中检测到）。

7.2.1 Result-Code AVP

Result-Code AVP（AVP代码268）是一个Unsigned32数值，指示某特定的请求是否成功完成或是否发生了错误。所有标准应用中定义的Diameter应答必须包括Result-Code AVP。如果Result-Code AVP中主机的设置与Origin-Host AVP的标识不一致，一个非成功的Result-Code AVP（数值为除了DIAMETER_REDIRECT_INDICATION以外、非2xxx）必须包括一个Error-Reporting-Host AVP。

结果代码数值字段包括了一个IANA分配的32比特地址空间，用来表示差错。Diameter提供了下列类型的差错，所有的值为十进制表示的千位数。

—— 1xxx（报告）

—— 2xxx（成功）

—— 3xxx（协议错误）

—— 4xxx（暂时故障）

—— 5xxx（永久故障）

一个不识别的类（最高位数字未在这一节中定义的）必须被视为永久故障。

7.2.1.1 信息

在这个范畴内的错误用来通知请求者，请求不能被满足，在接受接入请求前，还需要其他的行动。

DIAMETER_MULTI_ROUND_AUTH 1001

这个信息性的错误由Diameter服务器返回，用于通知接入设备采用的认证机制还要进行多次交互，为了接受接入请求，还需要发送后续的请求消息。

7.2.1.2 成功

在这个范畴中的错误用来通知对方请求被成功完成。

1）DIAMETER_SUCCESS 2001

请求消息被成功完成。

2）DIAMETER_LIMITED_SUCCESS 2002

当返回这个消息，请求消息已成功完成，但应用还要进一步处理，以为用户提供服务。

7.2.1.3 协议差错

在这个范畴内的差错应在每一跳中都被处理，如果可能的话，DiameterProxy可能会尝试修正这个差错。注意有且仅有这些差错必须在应答消息中设置“E”比特。

1）DIAMETER_COMMAND_UNSUPPORTED 3001

该请求包括一个命令码，这个指令码不被识别或支持。当Diameter节点收到一个试验性的命令，但它并不能识别，这个差错消息必须被采用。

2）DIAMETER_UNABLE_TO_DELIVER 3002

这个差错在Diameter不能把消息发送的目的地时使用。不能送达的原因是在支持请求应用的域内没有主机空闲来外理请求，或给出了Destination-Host AVP却没给出相关的Destination-Realm AVP。

3）DIAMETER_REALM_NOT_SERVED 3003

请求消息中的字段不能被识别。

4）DIAMETER_TOO_BUSY 3004

当返回这个差错时，Diameter节点应尝试向其他可选的对等端发送消息。该差错必须仅在请求了特定的服务器，但它却不能提供请求的服务时采用。

5）DIAMETER_LOOP_DETECTED 3005

一个代理在试图得到发往接收者的消息时，检测到有环路。如果可能，该消息可发向可选的对等端，不过报告错误的对等端被认为有配置的问题。

6）DIAMETER_REDIRECT_INDICATION 3006

一个重定向代理判断该请求不能在本地得到满足，请求的发起者应把请求直接定向到服务器，关于服务器的相关信息加到响应中。当设置了这个差错时，必须同时具备Redirect-Host AVP。

7）DIAMETER_APPLICATION_UNSUPPORTED 3007

为某个应用而发送的请求不被支持。

8）DIAMETER_INVALID_HDR_BITS 3008

收到一个请求，该请求消息的Diameter头设置成非法的组合，或值与指令代码定义不一致。

9）DIAMETER_INVALID_AVP_BITS 3009

收到一个请求，这个请求中包括了一个标记比特设置成不可识别的值，或与AVP定义不一致的AVP。

10）DIAMETER_UNKNOWN_PEER 3010

从一个不知道的对等端收到CER消息。

7.2.1.4 暂时故障

这些差错属于暂时故障范畴中，用于通知对等端，收到的请求在收到时不能得到满足，但有可能在将来予以满足。

1）DIAMETER_AUTHENTICATION_REJECTED 4001

用户认证过程失败，很有可能因为用户使用了错误密码。仅当向用户提示输入密码时才进一步进行尝试。

2）DIAMETER_OUT_OF_SPACE 4002

Diameter节点收到计费请求但因为临时缺少空间不能把数据写入稳定的存诸设备中。

3）ELECTION_LOST 4003

对等端判断它在选举中失败，因此切断传输连接。

7.2.1.5 永久故障

这些差错属于永久故障范畴，用来通知对等端请求失败，不要再进行尝试。

1）DIAMETER_AVP_UNSUPPORTED 5001

对等端接收到一个消息，此消息中有不能识别或不支持的AVP，且这个AVP被标记了M比特。有这个差错的Diameter消息必须有一个或多个Failed-AVP AVP来报告出错的AVP。

2）DIAMETER_UNKNOWN_SESSION_ID 5002

请求里含有不识别的Session-Id。

3）DIAMETER_AUTHORIZATION_REJECTED 5003

收到一个请求，此请求的用户不能被授权。这个差错在如果请求的服务不允许该用户接入时发生。

4）DIAMETER_INVALID_AVP_VALUE 5004

请求中有一个AVP在数值部分中带有非法的值。用于指示这个差错的Diameter消息必须包括带有出错AVP的Failed-AVP AVP。

5）DIAMETER_MISSING_AVP 5005

请求消息里没有命令代码定义所需要的AVP。如果这个值是在Result-Code AVP里发送的，这个消息里面还要包括一个Failed-AVP AVP。如果可能，这个AVP必须包括带有缺失的AVP并带有Vendor-Id。缺失的AVP中的值字段应为允许的最短长度，包含若干0。

6）DIAMETER_RESOURCES_EXCEEDED 5006

收到一个请求，该请求不能被授权，因为用户已消耗了允许的资源。这个差错的例子是一个用户被限制只能用一个拨号PPP端口，但该用户试图建立第二个PPP连接。

7）DIAMETER_CONTRADICTING_AVPS 5007

归属Diameter服务器检测到请求中AVP相互矛盾，不能为用户提供服务。在这种情况下一个或多个Failed-AVP AVP必须被返回，这些AVP中包含有相互矛盾的AVP。

8）DIAMETER_AVP_NOT_ALLOWED 5008

收到的一个消息中带有必须不能包含的AVP，Failed-AVP AVP必须在返回消息中，并包含引起差错的AVP。

9）DIAMETER_AVP_OCCURS_TOO_MANY_TIMES 5009

收到的消息中有一个AVP，其出现的次数多于消息定义中允许的次数。Failed-AVP AVP必须在返回消息中，并包含那个首次超出允许次数的错误AVP。

10）DIAMETER_NO_COMMON_APPLICATION 5010

这个差错在收到一个CER消息后，且在对等端间没有共同的应用被支持时返回。

11）DIAMETER_UNSUPPORTED_VERSION 5011

收到一个请求，不支持这个请求中的版本号，这时返回这个差错。

12）DIAMETER_UNABLE_TO_COMPLY 5012

这个差错在因为未定义的原因拒绝一个请求时返回。

13）DIAMETER_INVALID_BIT_IN_HEADER 5013

这个差错在Diameter消息头中不可识别的比特设为1时返回。

14）DIAMETER_INVALID_AVP_LENGTH 5014

请求包含一个长度无效的AVP。指出这个差错的Diameter消息必须在Failed-AVP AVP包含这个出错的AVP。

15）DIAMETER_INVALID_MESSAGE_LENGTH 5015

该差错在收到一个无效的消息长度时返回。

16）DIAMETER_INVALID_AVP_BIT_COMBO 5016

请求中包含一个，其AVP标记字段中有不允许的值。指出这个差错的Diameter消息必须在Failed-AVP AVP包含这个出错的AVP。

17）DIAMETER_NO_COMMON_SECURITY 5017

当收到CER消息时返回这个差错，并且在对等端间没有共同的安全机制。必须返回一个Capabilities-Exchange-Answer（CEA）消息，且其中的Result-Code AVP必须设置为DIAMETER_NO_COMMON_SECURITY。

7.2.2 差错比特

当一个请求导致了与协议相关的差错时，应设置Diameter头中的E比特（见7.2.1.3节）。一个设置了E比特的消息不可以作为一个应答消息的响应发送。注意，设置了E比特的消息仍遵循7.1.2中定义的处理过程。当设置了这个比特，对一个命令的应答消息不会遵循ABNF规范，而与下面的ABNF格式相符。

消息格式如下：

```
<应答消息> ::= < Diameter头: 编码，差错 [PXY] >
                    0*1< Session-Id >
                       { Origin-Host }
                       { Origin-Realm }
                       { Result-Code }
                       [ Origin-State-Id ]
                       [ Error-Reporting-Host ]
                       [ Proxy-Info ]
                     * [ AVP ]
```

注意：在头里用的编码与请求消息中的相同，但R比特被清除而E比特被设置。头中的P比特设成与请求消息相同。

7.2.3 Error-Message AVP

Error-Message AVP（AVP Code 281）为UTF8String类型。它可以和一个Result-Code AVP结合作为一个可读的差错消息。Error-Message AVP不能在实时情况下应用，且不应期望能够为网络实体解析。

7.2.4 Error-Reporting-Host AVP

Error-Reporting-Host AVP（AVP Code 294）为DiameterIdentity类型。仅当设置Result-Code的主机与Origin-Host AVP中的不同时，该AVP包含发送Result-Code AVP（值不是成功2001）的Diameter主机的标识符。该AVP用于发现并处理故障，当Result-Code AVP指出一个失败时，必须将其置位。

7.2.5 Failed-AVP AVP

Failed-AVP AVP（AVP Code 279）是Grouped类型，提供Debug信息，以防由于特定AVP中的错误信息而造成请求被拒绝或者没有完全执行。Result-Code AVP的值将为Failed-AVP AVP提供原因信息。

该AVP可能的原因是出现构造不正确的AVP、不支持或不认识的AVP、无效的AVP值、必需的AVP冗长、出现明确被拒绝接受的AVP（参见附录B中的表）、或者被限制只许出现0次、1次、或0到1次的AVP出现了两次或多次。

Diameter消息可以包含一个Failed-AVP AVP，包含不能被正确处理的完整的AVP。如果失败原因是必需的AVP冗长，则必须增加带有缺失AVP码的AVP、缺失的制造商ID以及为达到AVP缺省最小要求的长度而填充的0。

AVP格式：

<Failed-AVP> ::= < AVP Header: 279 >

1* {AVP}

7.2.6 Experimental-Result AVP

Experimental-Result AVP（AVP Code 297）是Grouped类型，指明某个特殊的制造商定义的（vendor-specific）请求是否被正确完成或者是否出现差错 。其数据字段拥有以下ABNF语法：

AVP格式：

Experimental-Result ::= < AVP Header: 297 >

{ Vendor-Id }

{ Experimental-Result-Code }

本组合AVP中的Vendor-Id AVP（参见6.3.3节）标识了负责结果编码分配的制造商。所有在vendor-specific应用中定义的Diameter应答消息必须或者包括一个Result-Code AVP或者包括一个Experimental-Result AVP。

7.2.7 Experimental-Result-Code AVP

Experimental-Result-Code AVP（AVP Code 298）类型是Unsigned32，包含一个制造商分配的（vendor-assigned）值以表示处理该请求的结果。

建议该制造商分配的结果编码遵循Result-Code AVP的惯例，参照结果编码和差错控制的不同类型（非2xxx的值）。

7.3 Diameter 用户会话

Diameter能够为应用提供两种类型的服务。第一种涉及认证和授权，并可选择的使用计费。第二种只使用计费。

当一个服务使用应用的认证和授权部分时，并且一个用户请求接入网络，Diameter客户端向本地服务器发送一个认证请求。该认证请求由特定的Diameter应用来定义（如NASREQ）。该请求包含Session-Id AVP，这个AVP在用户会话相关消息中使用。Session-Id AVP提供了让客户端和服务器把Diameter消息和用户会话联系起来的方法。

当Diameter服务器授权用户在一定时间内使用网络资源，以及将通过以后的请求来扩展授权，它必须在应答消息中包含Authorization-Lifetime AVP。Authorization-Lifetime AVP定义了在服务器需要的另一个授权请求之前，用户可以使用资源的最大时间。Auth-Grace-Period AVP中包含了授权时间到期后的一段时间（s），在这段时间之后，服务器将释放用户会话相关的所有状态信息。注意，如果服务费用由用户归属域的服务域来支付，Authorization-Lifetime AVP加上Auth-Grace-Period AVP意味着归属域愿意为会话支付的最大时间长度。超过Authorization-Lifetime 和Auth-Grace-Period时间的服务由接入设备支付。当然，实际的服务费用的计算超出了本标准的范围。

如果接入设备不愿向服务器发送重新授权或者会话终止请求，那么可以把Auth-Session-State AVP的值设置为 NO_STATE_MAINTAINED，作为给服务器的暗示。如果服务器接受了这个暗示，它同意由于一旦提供给用户的服务终止，它将不会接收到会话终止消息，因此服务器不会保存该会话的状态。如果服务器的应答消息在Auth-Session-State AVP包含了另外的值，接入设备必须服从服务器的指令。注意，NO_STATE_MAINTAINED不能在后续的重新认证请求和应答中设置。

Diameter基础协议中并不包含任何的授权请求消息，因为这些是应用相关的，并在Diameter应用文档中定义。然而，Diameter基础协议确实定义了终止用户会话的消息。这些消息用来让维护状态信息的服务器释放资源。

当一个服务只采用Diameter协议的计费部分时，即使是在应用中结合采用，Session-Id仍然被用来标识用户会话。然而，由于终止会话是通过发送停止计费消息来实现的，因此并没有采用会话终止消息。

7.3.1 授权会话状态机

本节包含了一系列的有限状态机，表示了Diameter会话的生命周期，采用了认证/授权部分的Diameter应用必须遵守这些状态机。术语“服务指定”表示Diameter应用中定义的消息（如移动IPv4、NASREQ）

在Diameter 基础协议中支持4种不同的授权会话状态机。前两个定义了服务器维持会话状态的会话，用Auth-Session-State AVP的值（或者缺省）表示。一个从客户端角度定义了会话，另一个从服务器角度。后两个状态机在服务器不维护状态信息时应用。也是一个从客户端角度定义会话，另一个从服务器角度。

当会话转移到空闲状态时，任何会话相关的资源分配都必须被释放。任何在状态机中没有列出的事件必须被视为错误条件，如果可行的话，应答消息必须返回给消息产生者。

在状态表中，事件“发送X失败”表示Diameter代理无法向期望的目的地发送命令X。这可能因为对等端死机，或者由于对等端在相应的应答命令的Result-Code AVP中发送回一个表示瞬时失败或临时协议错误的通知 DIAMETER_TOO_BUSY 或 DIAMETER_LOOP_DETECTED。事件“X成功被发送”是“发送X失败”的补充。

当服务器为会话维护状态时，客户端遵守表6中的规定。

表6 客户机，STATEFUL

状 态	事 件	行 为	新状态
空闲	客户机或者设备请求接入	发送服务特定的认证请求	等待
空闲	接收到未知会话的ASR	发送 ASA，其中Result-Code为UNKNOWN_SESSION_ID	空闲
等待	接收到成功的服务指定授权应答，其中包含缺省Auth-Session-State值	授权接入	打开
等待	接收到成功的服务指定授权应答，但服务无法提供	发送STR	断开
等待	成功的服务指定授权应答处理出错	发送STR	断开
等待	接收到失败的服务指定授权应答	清除	空闲
打开	客户机或者设备请求接入服务	发送服务指定的认证请求	打开
打开	接收到成功的服务指定授权应答	提供服务	打开
打开	接收到失败的服务指定授权应答	断开用户/设备连接	空闲
打开	接入设备会话时间到	发送STR	断开
打开	接收到ASR，客户机将遵循请求而中断会话	发送ASA，Result-Code = SUCCESS，发送STR	断开
打开	接收到ASR，客户机将不按照请求的要求中断会话	发送ASA，Result-Code≠SUCCESS	打开
打开	Authorization-Lifetime + Auth-Grace-Period在接入设备上超时	发送STR	断开
断开	接收到ASR	发送ASA	断开
断开	接收到STA	断开用户/设备	空闲

当服务器为会话维护状态时，服务器需要遵守表7中的规定。

表7 服务器，STATEFUL

状 态	事 件	行 为	新状态
空闲	接收到服务指定的授权请求,并且用户认证授权通过	发送成功的服务指定授权应答	打开
空闲	接收到服务指定的授权请求,但用户认证授权没有通过	发送失败的服务指定授权应答	空闲
打开	接收到服务指定的授权请求,并且用户认证授权通过	发送成功的服务指定授权应答	打开
打开	接收到服务指定的授权请求,但用户认证授权没有通过	发送失败的服务指定授权应答，并清除资源	空闲
打开	归属服务器需要终止服务	发送ASR	断开
打开	在归属服务器上的授权时间（包括Auth-Grace-Period）到期	清除	空闲
打开	在归属服务器上的会话超时	清除	空闲
断开	发送ASR失败	等待，重发ASR	断开
断开	发送ASR成功，并且接收到带有Result-Code的ASA	清除	空闲
非断开	接收到ASA	空	不改变
任何	接收到STR	发送STA，并清除	空闲

当服务器不维护状态时，客户端要遵守表8中的规定。

表8 客户机，STATELESS

状 态	事 件	行 为	新状态
空闲	客户机或者设备接入请求	发送服务指定授权应答	未决
等待	接收到成功的服务指定授权应答，Auth-Session-State设置为NO_STATE_MAINTAINED	授权接入	打开
等待	接收到失败的服务指定授权应答	清除	空闲
打开	接入设备会话时间到	用户/设备断开	空闲
打开	用户服务终止	断开	空闲

当服务器不维护状态时，服务器要遵守表9中的规定。

表9 服务器，STATELESS

状 态	事 件	行 为	新状态
空闲	接收到服务指定的授权请求，并且处理过程成功	发送服务指定授权应答	空闲

7.3.2 计费会话状态机

有计费部分的应用或者只需要计费服务的应用都必须支持下面的状态机。第一个状态机（表8）是客户机必须遵守的。

计费命令码参见8.7节，计费AVP参见8.8节。

计费状态机的服务器端与特定应用相关。Diameter 基础协议定义了一个缺省的状态机，没有指定必须遵守其他状态机的所有应用。这是本节下文中的第二个状态机（表9）。

缺省的服务器端状态机需要接受任何顺序和任何时间的计费记录，并没有规定处理这些记录时的任何标准要求。Diameter实施可能执行检查、排序、关联、查错和其他基于这些记录的任务。作为这些任务的一部分，Diameter基础协议的AVP和应用指定的AVP都可能被检查。这些任务能够在接受记录之后立即进行，也可以在后期处理阶段进行。但是，这些任务是与典型的应用或策略相关的，它们没有被Diameter规范所标准化。应用可以基于Accounting-Realtime-Required AVP的值、信用界限检查等来定义何时接受计费记录的需求。

然而，Diameter基础协议定义了一个可选的服务器端状态机（表11和表12）。需要在计费服务器上跟踪会话状态的应用可以遵循该状态机。注意，这样的跟踪与维持长时连接性的能力相矛盾。因此，这样的状态机建议只在Accounting-Realtime-Required AVP的值是DELIVER_AND_GRANT的应用中采用，而且必须为正在使用服务的用户中断解决计费连接行问题。否则，连接重建后，客户机产生的记录会被不再接受这些记录的服务器所丢失。这个状态机是本节中的第三种状态机（表10）。这个状态机被监督会话定时器Ts监视，它的值会合理的高于Interim_Record_Interval。Ts可能被设置成两倍于Interim_Record_Interval，以避免Diameter服务器的计费会话在短暂的网络失败后变成空闲状态。

表10 客户机，计费

状 态	事 件	行 为	新状态
空闲	客户机或设备请求接入	发送开始计费请求	PendingS
空闲	客户机或设备申请一次性服务	发送计费事件请求	PendingE
空闲	在存储器中记录	发送记录	PendingB
PendingS	接收到成功的计费开始应答		打开

表10（续）

状　态	事　件	行　为	新状态
PendingS	发送失败、有可用的缓冲区空间且实时不等于DELIVER_AND_GRANT	存储开始记录	打开
PendingS	发送失败、没有可用的缓冲区空间且实时等于GRANT_AND_LOSE		打开
PendingS	发送失败、没有可用的缓冲区空间且实时不等于GRANT_AND_LOSE	用户/设备断开	空闲
PendingS	接收到失败的计费开始应答，并且实时等于GRANT_AND_LOSE		打开
PendingS	接收到失败的计费开始应答，并且实时不等于GRANT_AND_LOSE	用户/设备断开	空闲
PendingS	用户服务终止	保存停止记录	PendingS
打开	过渡时间结束	发送计费过渡记录	PendingI
打开	用户服务终止	发送停止计费请求	PendingL
PendingI	接收到成功的计费过渡应答		打开
PendingI	发送失败、（可用的缓冲区空间或者旧的记录可以被覆盖）且实时不等于DELIVER_AND_GRANT	存储过渡记录	打开
PendingI	发送失败、没有可用的缓冲区空间，且实时等于GRANT_AND_LOSE		打开
PendingI	发送失败、没有可用的缓冲区空间，且实时不等于GRANT_AND_LOSE	用户/设备断开	空闲
PendingI	接收到失败的计费过渡应答，并且实时等于GRANT_AND_LOSE		打开
PendingI	接收到失败的计费过渡应答，并且实时不等于GRANT_AND_LOSE	用户/设备断开	空闲
PendingI	用户服务终止	储存停止记录	PendingI
PendingE	接收到成功的计费事件应答		空闲
PendingE	发送失败并且缓冲区可用	存储事件记录	空闲
PendingE	发送失败并且没有缓冲区可用		空闲
PendingE	接收到失败计费事件应答		空闲
PendingB	接收到成功的计费应答	删除记录	空闲
PendingB	发送失败		空闲
PendingB	接收到失败的计费应答	删除记录	空闲
PendingL	接收到成功的计费停止应答		空闲
PendingL	发送失败并且缓冲区可用	保存停止记录	空闲
PendingL	发送失败并且没有缓冲区可用		空闲
PendingL	接收到失败的计费停止应答		空闲

表11 服务器，STATELESS ACCOUNTING

状 态	事 件	行 为	新状态
空闲	接收到开始计费请求并且处理成功	发送开始计费应答	空闲
空闲	接收到计费事件请求并且处理成功	发送计费事件应答	空闲
空闲	接收到过渡记录并且处理成功	发送计费过渡应答	空闲
空闲	接收到计费停止请求，并且处理成功	发送计费停止应答	空闲
空闲	接收到计费请求，没有储存记录的空间	发送计费应答，Result-Code=OUT_OF_SPACE	空闲

表12 服务器，STATEFUL ACCOUNTING

状 态	事 件	行 为	新状态
空闲	接收到开始计费请求并且处理成功	发送开始计费应答，开始Ts	打开
空闲	接收到计费事件请求并且处理成功	发送计费事件应答	空闲
空闲	接收到计费请求，没有储存记录的空间	发送计费应答，Result-Code=OUT_OF_ SPACE	空闲
打开	接收到过渡记录，并且处理成功	发送计费过渡应答，重启动Ts	打开
打开	接收到计费停止请求，并且处理成功	发送计费停止应答，停止Ts	空闲
打开	接收到计费请求，没有储存记录的空间	发送计费应答，Result-Code=OUT_OF_SPACE，停止Ts	空闲
打开	会话监督定时器Ts到期	停止 Ts	空闲

任何在状态机中没有列出的事件必须被视为错误条件，如果可能，应答消息必须返回给消息的产生者。

在状态表中，事件“发送失败”表示Diameter客户机无法与期望的目的地通信。这可能因为对等端死机，或者由于对等端在计费应答命令的Result-Code AVP中发送回一个表示瞬时失败或临时协议错误的通知 DIAMETER_TOO_BUSY 或 DIAMETER_LOOP_DETECTED。

事件“失败的应答”表示Diameter客户端在计费应答命令中接收到了非瞬时的错误通知。注意，如果给定的应用既有认证/授权部分，又有计费部分，那么 “Disconnect user/dev” 的行为必须对授权会话状态表产生影响，例如，导致发送STR消息。

状态PendingS、PendingI、PendingL、PendingE 及 PendingB分别表示等待计费请求的应答状态开始（Start）、 过渡时期（Interim）、停止（Stop）、 事件（Event）和 缓冲记录。

7.3.3 服务器发起的重认证/授权

Diameter服务器可以通过发出一个Re-Auth-Request（RAR）来发起重新认证/授权服务。

例如，对于预付费服务，初始授权的Diameter服务器可能需要确定用户是否还在使用这个服务。

如果服务支持重认证/授权，接收到RAR消息且其中的Session-Id与当前的会话活动相同的接入设备必须向用户发起重认证/授权。

7.3.3.1 重新认证/授权请求（Re-Auth-Request）

Re-Auth-Request（RAR）用命令码设置为258，消息标志“R”设置来表示。该命令可以由任何服务器发送给提供会话服务的接入设备，来请求对用户进行重新认证/授权。

消息格式如下：

```
<RAR>  ::= < Diameter Header: 258, REQ, PXY >
           < Session-Id >
           { Origin-Host }
           { Origin-Realm }
```

{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
{ Re-Auth-Request-Type }
[User-Name]
[Origin-State-Id]
* [Proxy-Info]
* [Route-Record]
* [AVP]

7.3.3.2 重新认证/授权应答（Re-Auth-Answer）

Re-Auth-Answer（RAA）用命令码设置为258，消息标志“R”清除来表示。该命令用来应答RAR消息。Result-Code AVP必须出现，表示请求消息的处理结果。

一个成功的RAA消息必须有跟随着的应用指定的认证/授权消息。

消息格式如下：

<RAA> ::= < Diameter Header: 258，PXY >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Origin-State-Id]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
* [Redirected-Host]
[Redirected-Host-Usage]
[Redirected-Host-Cache-Time]
* [Proxy-Info]
* [AVP]

7.3.4 会话终止

对于授权某个会话并维护其状态的Diameter服务器而言，当会话不再活跃时，该服务器必须得到通知，以用于跟踪并使得代理服务器（能够保存会话状态的服务器）释放它们为用户会话所提供的资源。对于不维护状态的会话，则不需要。

当一个需要Diameter授权的用户会话结束时，提供服务的接入设备必须向授权该服务的Diameter服务器提交一个Session-Termination-Request（STR）消息，通知它这个会话不再活跃。当用户会话终止时，必须发送STR消息，不论会话终止的原因是用户登出、会话超时、管理行为、接收到Abort-Session- Request（参见7.3.5节）还是接入设备顺序关闭。

接入设备还必须为某个已经授权，但从未真正开始的会话提交STR。这种情况可能发生，例如，由于接入设备资源意外缺乏，或者因为接入设备不愿提供授权中申请的服务类型，或者接入设备不支持授权返回中的某个强制AVP等。

也可能某个会话已经被授权，但由于Proxy的行为而从未真正启动。例如，Proxy可能修改一个授权应答，在把消息转发给接入设备之前把结果由成功改为失败。如果应答不包含设置为NO_STATE_MAINTAINED 的Auth-Session-State AVP，由于接入设备无法得知该会话已经被授权，所以导致授权的会话没有启动的Proxy必须向授权这个会话的Diameter服务器发送一个STR，已终止该会话。接收到STR消息的Diameter服务器必须清除STR中的Session-Id相关的资源，并且返回Session-Termination-Answer。

Diameter服务器必须在会话超时，或者当授权时间和Auth-Grace-Period AVP过期而没有收到重新认证/授权请求时清除资源，而不管是否收到这个会话的STR消息。接入设备不能在这些定时器超时后继续提供服务。因此，这些定时器中的某个超时意味着接入设备无法预测的关闭。

7.3.4.1 会话终止请求（Session-Termination-Request）

Session-Termination-Request（STR）由命令码275和设置消息标志“R”来表示。它由接入设备发送，以通知Diameter服务器认证/授权的会话需要终止。

消息格式如下：

```
<STR> ::= < Diameter Header: 275，REQ，PXY >
          < Session-Id >
          { Origin-Host }
          { Origin-Realm }
          { Destination-Realm }
          { Auth-Application-Id }
          { Termination-Cause }
          [ User-Name ]
          [ Destination-Host ]
        * [ Class ]
          [ Origin-State-Id ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        * [ AVP ]
```

7.3.4.2 会话终止应答（Session-Termination-Answer）

Session-Termination-Answer（STA）由命令码275和清除消息标志“R”来表示。它由Diameter服务器发送，以响应会话终止的通知。Result-Code AVP必须出现，可能包含处理STR过程中出现错误的提示。

当发送或接收到STA时，Diameter服务器必须释放由Session-Id AVP指定的Session相关资源。如果需要的话，任何Proxy链上的中间服务器也要释放资源。

消息格式如下：

```
<STA>   ::= < Diameter Header: 275，PXY >
```

< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
* [Class]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
[Origin-State-Id]
* [Redirect-Host]
[Redirect-Host-Usase]
[Redirect-Max-Cache-Time]
* [Proxy-Info]
* [AVP]

7.3.5 中断会话

Diameter服务器可能通过发送Abort-Session-Request（ASR）来请求接入设备停止为某个会话提供服务。

例如，为某个会话初始授权的Diameter服务器可能会被请求中断该会话，因为当会话开始授权时无法预知信用额度等原因。另一方面，运营商可以维护一个管理服务器，用来管理性的把用户从网络中去除而发送ASR。

一个接入设备接收到与当前活动的会话具有相同的Session-ID的ASR消息时，可以停止这个会话。不论接入设备是否停止该会话都依赖于实施和/或配置，例如，接入设备可能只接受特定的代理发送的ASR。在任何情况下，接入设备必须返回Abort-Session-Answer，其中包括一个表示其采取行为的Result-Code AVP。

注意，如果接入设备确实因为接受了ASR消息而停止会话，它必须向授权的服务器（可能是，也可能不是发送ASR的代理）发送STR消息。

7.3.5.1 中断会话请求（Abort-Session-Request）

Abort-Session-Request（ASR）由命令码274和设置消息标志“R”来表示，它由任何服务器向提供接入服务的接入设备发送，来请求中断Session – Id表示的会话。

消息格式如下：

<ASR> ::= < Diameter Header: 274，REQ，PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }

{ Auth-Application-Id }
[User-Name]
[Origin-State-Id]
* [Proxy-Info]
* [Route-Record]
* [AVP]

7.3.5.2 中断会话应答（Abort-Session-Answer）

Abort-Session-Answer（ASA）由命令码274和清除消息标志“R”来表示，是应答ASR的消息。Result-Code AVP必须出现，表示请求的处理结果。

如果以ASR中Session – Id表示的会话成功终止，返回值设置为DIAMETER_SUCCESS。如果会话当前不活跃，那么返回值为DIAMETER_UNKNOWN_SESSION_ID。如果接入设备因为某种原因并没有停止会话，则返回值是DIAMETER_UNABLE_TO_COMPLY。

消息格式如下：

<ASA> ::= < Diameter Header: 274，PXY >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Origin-State-Id]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
* [Redirected-Host]
[Redirected-Host-Usage]
[Redirected-Max-Cache-Time]
* [Proxy-Info]
* [AVP]

7.3.6 从 Origin-State-Id 推断会话终止

Origin-State-Id用来允许快速检测因为不曾预料的接入设备关闭而导致终止，却没有发送STR的会话。

通过在CEA/CER消息中加入Origin-State-Id，接入设备允许下一跳的服务器立即确定是否该设备从上次连接后已经丢失了它的会话。

通过在请求消息中加入Origin-State-Id，接入设备也允许通过Proxy连接的服务器作出类似的决定。但是，没有直接连接该接入设备的服务器无法发现该接入设备已经重启，直到它从该设备接收到新的请求。因此，采用这种机制跨越Proxy并不完全可靠，但是有用。

当Diameter服务器接收到同一个发送者发来的、比上次Origin-State-Id更大的Origin-State-Id，它可以假定发送者从上次消息后已经丢失了状态，并且在先前的低的Origin-State-Id下所有的会话已经终止。

Diameter服务器可以清除与这些丢失的会话相关的会话状态，并可以向授权这些丢失会话的上游服务器发送STR，允许清除全局范围的会话状态。

7.3.7 Auth-Request-Type AVP

Auth-Request-Type AVP（AVP Code 274）类型为Enumerated，包含在应用指定的认证/授权请求中，来通知对等端用户是否只需要认证，或只需要授权，还是两者都需要。注意，除了两者都需要以外，其他的值可能导致RADIUS兼容性问题。

1）AUTHENTICATE_ONLY 1

只在认证时发送本请求，并且必须包含Diameter服务器为认证用户所需的相关应用指定认证AVP。

2）AUTHORIZE_ONLY 2

只在授权时发送本请求，并且必须包含为标识请求/提供的服务所需的相关应用指定授权AVP。

3）AUTHORIZE_AUTHENTICATE 3

本请求同时包含认证和授权请求。本请求必须包含相关的应用指定认证信息，以及为标识请求/提供的服务所需的授权信息。

7.3.8 Session-Id AVP

Session-Id AVP（AVP Code 263）类型是UTF8String，用来标识一个特定的会话。所有的属于一个会话的信息必须包含惟一的Session－Id，并且在会话生命期中保持一致。当出现时，Session－Id应该紧接着出现在Diameter头部之后（参见第5.2节）。

Session－Id必须保持全局和永远惟一，它不用参考其他信息就能惟一的标识一个用户会话，可以用来联系历史认证信息和计费信息。Session－Id包含一个必须的部分和一个实施定义的部分。推荐的实施定义部分在下面介绍。

Session－Id必须由以DiameterIdentity类型编码的发送者标识开始。剩下部分用“；”分隔，可以是客户机保证永远惟一的任何序列。但是，推荐下面的格式（[]表示可选部分）：

<DiameterIdentity>;<high 32 bits>;<low 32 bits>[;<optional value>]

<high 32 bits>和<low 32 bits>是一个单调增加的64位值的高32位和低32位十进制表示。这个64位值分成两部分是为了简化32位处理器的处理格式。开始时，高32位值可以初始化为时间，低32位值初始化为0。假定重启动时间大于1s，这种方法可以消除重启动后Session-Id重叠的可能性。替代方法是，实施可以持续跟踪存储在非易失存储器中的递增值。

<optional value>是实施指定的，但可能包含如modem设备Id、第二层地址、时间戳等。

例如，没有可选项的值：

accesspoint7.acme.com;1876543210;523

例如，有可选项的值：

accesspoint7.acme.com;1876543210;523;mobile@200.1.1.88

Session-Id由Diameter初始化这个会话的Diameter应用创建，在多数情况下是由客户机创建。注意，Session-Id在给定应用中可能同时用于认证和授权。

7.3.9 Authorization-Lifetime AVP

Authorization-Lifetime AVP（AVP Code 291）类型是Unsigned32，包含了用户需要重新认证/授权前，服务能够提供的最大时间。确定授权时间值的大小时必须特别注意，因为一个很小的值会导致大量的Diameter流量，可能导致网络和代理的拥塞。

把值设为0意味着接入设备需要立即的重新认证。典型的应用是采用多种认证方式的场合，并且一个该AVP设置为0的成功认证/授权应答表示下一个认证方法需要立即启动。没有这个AVP或者值设置为全1，表示不需要重新认证/授权。

如果这个AVP和Session-Timeout AVP同时出现在一个消息中，后者的值不能小于前者。

Authorization-Lifetime AVP可能在重新授权消息中出现，包含从接入设备接收到重新授权应答消息起，用户被授权使用服务的时间。

这个AVP可以由客户机提供，以暗示它愿意接受的最大生命期。但是，服务器可以返回大于、等于、小于客户机提供的时间。

7.3.10 Auth-Grace-Period AVP

Auth-Grace-Period AVP（AVP Code 276）类型是Unsigned32，包含着在授权时间到期后，Diameter服务器在清除会话资源之前将等待的时间。

7.3.11 Auth-Session-State AVP

Auth-Session-State AVP（AVP Code 277）类型为Enumerated，表明对一个会话而言是否要保存状态。客户机可能在请求消息中包含这个AVP，作为对服务器的暗示。但是在服务器的应答消息中的值才有约束力。支持下面的值：

1）STATE_MAINTAINED 0

这个值表示会话状态需要保持，接入设备必须在用户终止时发送会话终止消息，是缺省值。

2）NO_STATE_MAINTAINED 1

这个值用来表示当授权时间超时时，接入设备不用发送会话终止消息。

7.3.12 Re-Auth-Request-Type AVP

Re-Auth-Request-Type AVP（AVP Code 285）的类型是Enumerated，包含在应用指定的应答消息中，用来通知客户机在授权时间到期时应该采取的行动。如果应答消息中包括了值为正数的授权时间AVP，Re-Auth-Request-Type AVP必须在应答消息中出现。定义了下面的值：

1）AUTHORIZE_ONLY 0

在授权时间到期后，只需要授权。如果应答消息中包括授权时间但没有这个AVP的话，这是缺省值。

2）AUTHORIZE_AUTHENTICATE 1

授权时间到期后，需要认证和授权。

7.3.13 Session-Timeout AVP

Session-Timeout AVP（AVP Code 27）（RFC 2865，RADIUS）类型是Unsigned32，包括了在会话终止之前，提供服务给用户的时间（s）。当Session-Timeout和Authorization-Lifetime 在应答消息中同时存在时，前者必须大于等于后者。

因为Session-Timeout到期而在接入设备上终止的会话必须发送STR，除非接入设备和归属服务器事先协商不发送会话终止消息（参见7.3.9节）。

Session-Timeout AVP可能在重新授权应答消息中出现，包含从重新认证起的剩余时间（s）。

该AVP的值为0，或者没有这个AVP，表示在终止前，会话具有无限时间。

这个AVP可能有客户机提供来表示它愿意接受的最大超时。但是服务器可以返回大于、等于、小于客户机提供的时间。

7.3.14 User-Name AVP

User-Name AVP（AVP Code 1）（RFC 2865，RADIUS）类型是UTF8String，包含了用户名称，与NAI规范 [NAI]的格式一致。

7.3.15 Termination-Cause AVP

Termination-Cause AVP（AVP Code 295）类型为Enumerated，用来指示在接入设备上会话终止的原因。定义了如下的值：

1）DIAMETER_LOGOUT 1

用户发起的中断。

2）DIAMETER_SERVICE_NOT_PROVIDED 2

当用户在接收到授权应答消息之前断开时使用本值。

3）DIAMETER_BAD_ANSWER 3

表示接入设备收到的授权应答处理不成功。

4）DIAMETER_ADMINISTRATIVE 4

因为管理原因，如接收到Abort-Session-Request消息等，用户没有获得接入授权或断开。

5）DIAMETER_LINK_BROKEN 5

与用户的通信突然断开。

6）DIAMETER_AUTH_EXPIRED 6

因为授权的会话时间到期，用户的接入终止。

7）DIAMETER_USER_MOVED 7

用户从另外的接入设备接受服务。

8）DIAMETER_SESSION_TIMEOUT 8

用户的会话超时，服务已经终止。

7.3.16 Origin-State-Id AVP

Origin-State-Id AVP（AVP Code 278）类型是Unsigned32，是一个单调递增的值，每次Diameter实体丢失以前的状态重新开始时都要增加，如重启动。Origin-State-Id可以包含在任何Diameter消息中，包括CER。

一个发出这个AVP的Diameter实体每次状态重置时必须生成一个更高的值。一个Diameter实体可以把Origin-State-Id设为启动时间，也可以采用在非易失内存中保存的递增计数器来跨越重启动。

如果Origin-State-Id出现，则必须反映Origin-Host所代表的实体的状态。如果一个Proxy修改Origin-Host，它必须同时去除Origin-State-Id，或者将其改为适当的值。

典型的情况是，Origin-State-Id由开始没有会话活动的接入设备采用。也就是说，任何重启动之前的会话活动都已经丢失。通过把Origin-State-Id包含在消息中，允许任何Diameter实体推测出与较低序号的

Origin-State-Id相关的会话已经不再活动。如果接入设备不愿让其他实体得到这样的推测，它必须在消息中不包括Origin-State-Id，或者把值设置为0。

7.3.17 Session-Binding AVP

Session-Binding AVP（AVP Code 270）类型是Unsigned32，可以在应用指定的授权应答消息中出现。如果出现，这个AVP通知Diameter客户机以后该会话的应用相关的重认证消息必须发送给同一个授权服务器。这个AVP也可以指定该会话的会话终止请求消息必须发送给同一个服务器。

该字段是位掩码（bit mask），定义了如下的位：

1）RE_AUTH 1

当该位设置时，以后的该会话重新认证/授权消息不能包含Destination-Host AVP。当本位清除，即缺省值，Destination-Host AVP必须在该会话所有的重新认证/授权消息中出现。

2）STR 2

当该位设置时，以后的该会话的STR消息不能包含Destination-Host AVP。当本位清除，即缺省值，Destination-Host AVP必须在该会话的所有STR消息中出现。

3）ACCOUNTING 4

当该位设置时，以后的该会话的计费消息不能包含Destination-Host AVP。当本位清除，即缺省值，Destination-Host AVP必须在该会话的所有计费消息中出现。

7.3.18 Session-Server-Failover AVP

Session-Server-Failover AVP（AVP Code 271）类型为Enumerated，可以出现在不包括Session-Binding AVP或者包括任何位都设置为0的Session-Binding AVP的应用指定授权应答消息中。如果该AVP出现，它可以通知Diameter客户机：如果因为传送原因，导致重认证或者STR消息失败，这个Diameter客户机应该发送没有Destination－Host的后续消息。当缺少这个AVP时，缺省的值是REFUSE_SERVICE。

支持以下的值：

1）REFUSE_SERVICE 0

如果重新认证/授权消息或者STR消息传送失败，终止用户服务，并且不做后续尝试。

2）TRY_AGAIN 1

如果重新认证/授权消息或者STR消息传送失败，重新发送不包含Destination-Host AVP的失败的消息。

3）ALLOW_SERVICE 2

如果重新认证/授权消息传送失败，假设重新授权成功。如果STR消息发送失败，终止会话。

4）TRY_AGAIN_ALLOW_SERVICE 3

如果重新认证/授权消息或者STR消息传送失败，重新发送不包含Destination-Host AVP的失败消息。如果第二次传送重新认证/授权消息传送失败，假设重新授权成功。如果第二次STR消息发送失败，终止会话。

7.3.19 Multi-Round-Time-Out AVP

Multi-Round-Time-Out AVP（AVP Code 272）类型为Unsigned32，应该在Result-Code AVP 设置为DIAMETER_MULTI_ROUND_AUTH的应用指定授权应答消息中出现。这个AVP包含接入设备必须提供给用户认证请求响应的最大秒数。

7.3.20 Class AVP

Class AVP（AVP Code 25）类型为OctetString，被Diameter服务器用来给接入设备返回状态信息。当一个或更多的Class AVP在应用指定的授权应答消息中出现时，它们必须在后续的重新授权、会话终止和计费消息中出现。在重新授权应答消息中出现的Class AVP覆盖了在以前的授权应答消息中出现的同类AVP。Diameter服务器的实施不应该返回需要在Diameter客户机占用超过4096字节存储的Class AVP。一个接收到超过本地可用存储的Class AVP的Diameter客户机必须终止该会话。

7.3.21 Event-Timestamp AVP

Event-Timestamp（AVP Code 55）类型为Time，可以在计费请求和计费应答消息中出现，以1970年1月1日00：00：00 UTC起的秒数的形式来记录汇报事件发生的时间。

8 Diameter 计费

本计费协议基于具有实时传送计费信息能力的服务器指向模型。在协议中采用了一些弹性容错方法，用来在各种错误情况和假设设备具有不同的能力下减少计费数据的丢失。

8.1 服务器指向模型

服务器指向模型表示生成计费数据的设备要根据计费数据转发的方向，从授权服务器或计费服务器处获得信息。这个信息包括对计费记录时间性的要求。

计费数据的实时传递是必需的，比如实行信用限度检查和欺骗检测。注意，批处理计费消息则不是必需的，因此Diameter并不支持。如果将来需要批处理计费，就要创建一个新的Diameter应用，或者由其他协议来处理。但是，即使在Diameter层的计费请求是一个个按顺序处理的，Diameter下层的传输协议在网络负担沉重时，通常在一个数据包中批处理多个请求。这对于许多应用来讲足够了。

授权服务器（链）基于对用户的了解和漫游关系的合作来指导选择合适的传输策略。服务器（或代理）采用Acct-Interim-Interval 和 Accounting-Realtime-Required AVPs来控制作为客户机的Diameter对等端的操作。当Acct-Interim-Interval AVP出现时，指示作为客户机的Diameter节点产生持续的计费信息，即使是同一个会话中。Accounting-Realtime-Required AVP用来在从Diameter客户机传送的计费记录传输延时或者失败时，控制客户机的行为。

Diameter计费服务器可以通过在计费应答消息中包含Acct-interim-Interval或者Accounting-Realtime-Required AVP覆盖过渡时期的间隔或实时需求。当其中的一个AVP出现时，在同一个会话以后的计费活动中将采用最近收到的值。

8.2 协议消息

Diameter节点如果接收到从归属AAA服务器发送的成功的认证和/或授权消息，就必须收集该会话的计费消息。计费请求消息用来向归属AAA服务器发送计费消息，归属AAA服务器必须回复计费应答消息来确认接受。计费应答消息包含Result-Code AVP来表示计费消息中出现的错误。一个被拒绝的计费请求消息可能导致用户的会话中断，这取决于先前接收到的、用于本会话的Accounting-Realtime-Required AVP的值。

为了减少网络带宽的使用，可以压缩Diameter计费协议的消息。如果采用了IPSec和IKE来保证Diameter会话，可以采用IP压缩，并且IKE可以用来协商压缩参数。如果TLS用来保护Diameter会话，也可以采用TLS压缩机制。

8.3 对扩展应用标准文档的要求

每个Diameter应用（例如，NASREQ、移动IP），必须在“计费AVP”一节（8.8节）中定义计费请求消息中必须出现的服务指定的AVP。这个应用必须假设本文档中定义的AVP将在所有的计费消息中出现，所以只需要在这一节中定义它们各自的服务指定的AVP。

8.4 差错恢复

Diameter 基础协议机制可以用来克服一些小的消息丢失和网络临时失败。

作为客户机的Diameter对等端必须实现采用Failover来保护服务器失败和某些网络失败。作为代理或者相关的离线处理系统的Diameter对等端必须检测重复的计费消息，这可能由向多个服务器发送同一个记录或者在传输中的消息复制造成。这个检测必须基于检查Session-Id 和 Accounting-Record-Number AVP对。附录F讨论了重复检测的需求和实现问题。

Diameter客户机可以有非易失内存，用来在系统重启、网络失败、网络划分、服务器失败等情况下保存计费记录。如果这样的内存可用，客户机应该在产生新的计费记录和接收到Diameter服务器明确的响应消息之间把新的计费记录存贮在该内存中。在重启时，客户机必须开始向计费服务器发送在非易失内存中的记录、对终止原因、会话长度和记录中的其他相关信息进行适当的修改。

关于这个协议的更深入的应用可以包括采用AVP来控制在Diameter客户端最多存储的计费记录个数，而不用把它们提交给非易失内存或者传给Diameter服务器。

客户机不应该在接收到正确的计费应答之前从任何内存区域删除计费数据。客户机可以在资源耗尽的情况下删除旧的、没发送的或者没有被响应的计费数据。客户机在这种情况下如何接收新的会话是一个与实施相关的问题。

8.5 计费记录

在所有的计费记录中，Session-Id AVP必须出现；如果对Diameter客户机可行，User-Name AVP也必须出现。如果需要经过代理的强（Strong）认证过程，则认证需要采用端到端的安全机制。

应当根据实际的计费服务类型以及用于过渡计费的授权服务器的指示，来发送不同类型的计费记录。如果计费服务是一次性事件，这意味着事件的开始和停止是同时进行的，所以Accounting-Record-Type AVP必须出现，并且值为EVENT_RECORD。如果计费服务有可测量的长度，该AVP必须采用START_RECORD、STOP_RECORD值，可能的话，采用INTERIM_RECORD。如果授权服务器没有指示对这个会话采用过渡计费，则必须产生两个计费记录以用于每个类型会话的服务。当发送了给定会话的初始计费请求，计费记录类型AVP必须设置为START_RECORD。当最后的计费请求发送后，该值为STOP_RECORD。

如果授权服务器允许过渡计费，Diameter客户机必须在START_RECORD 和 STOP_RECORD之间产生附加的记录，标记为INTERIM_RECORD。这些记录的生成受Acct-interim-Interval和会话中其他重新认证/授权的指示。如果在同一个会话中生成了新的记录，Diameter客户机必须覆盖本地存储准备发送的以前的过渡计费记录。这样保证在接入设备上给定的会话只有一个等待的过渡记录。

Accounting-Sub-Session-Id的一个特定值除了重传以外，必须只能在从Diameter客户端来的计费记录序列中出现。发送的一个序列必须是设置成EVENT_RECORD的Accounting-Record-Type AVP，或者是以START_RECORD开始，随后的若干个INTERIM_RECORD和一个STOP_RECORD。一个特定的Diameter应用规范必须定义其必须使用的序列类型。

8.6 计费记录的相互关系

Diameter协议的全局惟一Session-Id AVP用来在授权阶段标识一个特定的会话。无需授权的服务也要采用Session-Id AVP来标识会话。计费消息可以采用与授权消息中不同的会话标识。特定的应用可以为计费消息请求不同的Session-ID。

然而，存在需要多个计费子会话的特定应用。这样的应用将发送固定Session－Id的消息，但是，有不同的Accounting-Sub-Session-Id。在这些情况下，用Session－Id来建立联系。需要特别注意的是，当在START_RECORD消息中最初采用子会话时，接收到没有Accounting-Sub-Session-Id AVP的STOP_RECORD意味着所有的子会话要被终止。

而且，存在一个用户从不同的接入设备接收服务的应用（例如，移动IPv4），每个都有一个独立的惟一Session－Id。在这些情况下，Acct-Multi-Session-Id AVP用来做关联。在授权过程中，判断为现有会话的请求的服务器应该包括Acct-Multi-Session-Id AVP，每个接入设备必须在所有的后续计费消息中包括这个AVP。

Acct-Multi-Session-Id可以包括初始的Session-Id。其内容是实施特定的，但必须在其他Acct-Multi-Session-Id间保持全局惟一，并且不可以在会话的生存期间改变。

Diameter扩展应用标准文档中必须定义正在计费的会话的精确概念，同时可以定义多个会话的概念。例如，NASREQ DIAMETER应用把一个与网络接入服务器间的PPP连接视为一个会话，把多个多链路PPP会话视为一个多会话。

8.7 计费命令码

本节定义了所有支持计费服务的Diamter实施必须支持的命令码。

8.7.1 Accounting-Request

Accounting-Request（ACR）命令，由命令码为271并且设置命令标志“R”表示，由作为客户端的Diameter节点发送，为了和对等端交换计费信息。

Acct-Application-Id 和 Vendor-Specific-Application-Id AVP必须有一个出现。如果Vendor-Specific-Application-Id组（grouped）AVP出现，其中必须包含Acct-Application-Id。

下面列出的AVP应该包括服务指定的计费AVP，参见8.3节。

消息格式如下：

<ACR> ::= < Diameter Header: 271，REQ，PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Accounting-Record-Type }
{ Accounting-Record-Number }
[Acct-Application-Id]
[Vendor-Specific-Application-Id]
[User-Name]
[Accounting-Sub-Session-Id]
[Accounting-Session-Id]

[Acct-Multi-Session-Id]
[Acct-interim-Interval]
[Accounting-Realtime-Required]
[Origin-State-Id]
[Event-Timestamp]
* [Proxy-Info]
* [Route-Record]
* [AVP]

8.7.2 Accounting-Answer

Accounting-Answer（ACA）命令，由命令码为271并且清除命令标志“R”表示，用来应答计费请求命令。计费应答命令包含同样的Session－Id。如果用端到端的安全机制保护计费请求，对应的ACA消息必须也用端到端的安全机制来保护。

只有作为归属Diameter服务器的目标Diameter服务器才应以Accounting-Answer命令应答。

Acct-Application-Id 和 Vendor-Specific-Application-Id AVPs 之一必须出现。如果Vendor-Specific-Application-Id grouped AVP出现，其中必须包含Acct-Application-Id。

以下列出的AVP应该包括服务指定的计费AVPs，参见8.3节。

消息格式如下：

<ACA> ::= < Diameter Header: 271，PXY >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
{ Accounting-Record-Type }
{ Accounting-Record-Number }
[Acct-Application-Id]
[Vendor-Specific-Application-Id]
[User-Name]
[Accounting-Sub-Session-Id]
[Accounting-Session-Id]
[Acct-Multi-Session-Id]
[Error-Reporting-Host]
[Acct-interim-Interval]
[Accounting-Realtime-Required]
[Origin-State-Id]
[Event-Timestamp]
* [Proxy-Info]
* [AVP]

8.8 计费 AVPs

本节包括描述与某个特定会话相关的计费采用信息的AVP。

8.8.1 Accounting-Record-Type AVP

Accounting-Record-Type AVP（AVP Code 480）类型为Enumerated，包括发送的计费记录类型。以下的值在Accounting-Record-Type AVP中定义：

1）EVENT_RECORD 1

用来指示一次性事件发生的计费事件记录（表示事件的开始和结束同时发生）。这个记录包括了所有的服务相关的信息，并且是服务的惟一记录。

2）START_RECORD 2

计费开始、过渡、停止记录用来表示已经提供可测长度的服务。一个计费开始记录用来表示一个计费会话，并包括关于会话起始的计费信息。

3）INTERIM_RECORD 3

过渡计费记录包括了一个存在的计费会话的累计计费信息。过渡计费记录应该在每次重新认证和重新授权发生时发送。而且，特定的Diameter应用可以定义附加的过渡记录。

4）STOP_RECORD 4

停止计费记录在终止计费会话时发送，并且包括关于一个存在的会话累计的计费信息。

8.8.2 Acct-interim-Interval AVP

Acct-interim-Interval AVP（AVP Code 85）类型为Unsigned32，由Diameter归属授权服务器向Diameter客户机发送。客户机采用本AVP中的信息来判断生成计费记录的时间和方式。随着这个AVP的值不同，根据归属机构的需求，服务会话可以导致一个、两个、或者2 + *N*个计费记录。以下的计费记录生成行为由本AVP指示：

1） 略Acct-interim-Interval AVP或者把值设置为0表示事件记录（EVENT_RECORD），开始记录（START_RECORD）和停止记录（STOP_RECORD）的生成。

2） 括这个AVP并把值设置为非0表示必须在开始记录和停止记录之间包括过渡记录。这个AVP的值是在记录间的名义上的间隔时间（s）。产生这些计费信息的Diameter节点，即客户机，必须在从开始时起，过了名义上的间隔时间后，产生第一个过渡记录，下一个记录在间隔到期时产生。诸如此类，一直到会话结束，产生停止记录。

客户机必须保证过渡记录生成次数随机化，因此避免在记录之间或者公共的服务开始时生成大量的计费消息风暴。

8.8.3 Accounting-Record-Number AVP

Accounting-Record-Number AVP（AVP Code 485）类型为Unsigned32，表示这个记录在一个会话中。因为Session-Id是全局惟一，Session-Id与Accounting-Record-Number的组合也是全局惟一，并且可以在匹配计费记录时采用。一个产生惟一号码的简单方法是把类型为EVENT_RECORD和 START_RECORD值设为0，并把第一个INTERIM_RECORD的值设置为1，第二个设置为2，依此类推，直到STOP_RECORD，STOP_RECORD比最后一个INTERIM_RECORD多1。

8.8.4 Accounting-Session-Id AVP

Accounting-Session-Id AVP（AVP Code 44）类型为OctetString，只在RADIUS/Diameter转换时采用，该AVP包含了RADIUS Accounting-Session-Id属性的内容。

8.8.5 Acct-Multi-Session-Id AVP

Acct-Multi-Session-Id AVP（AVP Code 50）类型为UTF8String，遵循7.3.8节的格式。Acct-Multi-Session-Id用来连接多个相关的计费会话。每个会话都有惟一的Session-Id，但Acct-Multi-Session-Id相同。这个AVP可能在Diameter服务器的授权应答中出现，必须在给定会话的所有计费消息中出现。

8.8.6 Accounting-Sub-Session-Id AVP

Accounting-Sub-Session-Id AVP（AVP Code 287）类型为Unsigned64，包含计费子会话的标识。Session-Id和这个AVP的组合必须为每个子会话惟一，并且该AVP的值必须为每个新的子会话增加1。除了Accounting-Record-Type 设置为STOP_RECORD 的Accounting-Request外，本AVP的缺乏暗示没有采用中的子会话。没有Accounting-Sub-Session-Id出现的停止记录消息将终止一个给定的Session-Id的所有的子会话。

8.8.7 Accounting-Realtime-Required AVP

Accounting-Realtime-Required AVP（AVP Code 483）类型为Enumerated，是从Diameter归属授权服务器发送给Diameter客户机，或者是在计费服务器的计费应答消息中。客户机采用本AVP中的信息来判断，在向计费服务器发送计费记录时出现如网络问题的临时失败时，应该如何处理。

1）DELIVER_AND_GRANT 1

设置为DELIVER_AND_GRANT，表示必须只能在与计费服务器有连接的情况下，才能授权服务。注意，在这种情况下，可选择的计费服务器集合被视为一个服务器。向备份服务器移动计费记录不能是终止用户服务的原因。

2）GRANT_AND_STORE 2

设置为GRANT_AND_STORE，表示如果这里存在连接，或者如果能够存储记录（参见8.4节）就应该授权服务。这是授权服务器应答的缺省值。

3）GRANT_AND_LOSE 3

设置为GRANT_AND_LOSE，表示即使不存在连接，或者无法存储记录也应该授权服务。

9 Diameter的安全机制

Diameter基础协议假设消息采用IPSec或者TLS进行安全保护。该安全机制在没有可靠的第三方Proxy的环境中是可接受的。在其他情况下，需要端到端安全。

Diameter客户，例如，网络接入服务器和移动性Proxy必须支持IPSec，并且可以支持TLS。Diameter服务器必须同时支持TLS和IPSec。 Diameter实施必须在每条链接上采用某种类型（IPSec或TLS）的传输层安全。

如果一个Diameter连接无法得到IPSec的保护，则CER／CEA交换必须包括一个带TLS值的Inband-Security-ID AVP。对于TLS应用，在CER/CEA交换结束后，且两端都在开放状态时，开始TLS握手。如果TLS握手成功，所有进一步的消息都将通过TLS发送。如果握手失败，两端都变为关闭状态。

建议IPSec主要在边缘用于域间交换。对于没有证书支持的NAS设备，预共享密钥可以在NAS和本地AAA Proxy之间应用。

TLS推荐用于保护域内交换。

9.1 IPSec 的使用

在采用非空密码和认证算法以提供每分组认证、完整性保护和机密性的传输方式中，所有Diameter实施必须支持IPSec ESP，并且必须支持IPSec的重演（Replay）保护机制。

Diameter实施必须利用IPSec DOI［RFC 2407］，支持IKE以用于对等端认证、安全联盟的协商以及密钥管理。Diameter实施必须支持采用预共享密钥的对等端认证，可以支持采用数字签名的、基于证书的对等端认证。IKE规范［RFC 2409］的5.2和5.3节中描述的采用公共密钥加密方式的对等端认证，在本标准中应不采用。

兼容实施必须同时支持IKE Main Mode和Aggressive Mode。当认证采用预共享密钥时，应采用IKE Aggressive Mode，而不应采用IKE Main Mode。当认证采用数字签名时，既可以采用IKE Main Mode也可以采用IKE Aggressive Mode。

当数字签名用于完成认证时，IKE协商应采用IKE证书请求有效载荷来规定根据本地策略可信任的证书权威（CA）。IKE协商者应在接受IKE认证规程中采用的PKI证书之前，采用有关的证书撤回检查。

用于协商保护Diameter连接的快速方式交换的阶段2必须明确承载Identity Payload字段（Idci和IDcr）。DOI提供多种类型的认证数据。当在兼容实施中应用时，每个ID载荷必须承载一个单个的IP地址和一个单个的非0端口号，并且不可以采用IP子网或IP地址范围格式。这允许阶段2安全联盟符合TCP和SCTP连接的规定。

由于IPSec加速硬件可以仅能够控制有限数量激活IKE阶段2 SA，阶段2删除消息可能发送给空闲SA，以保持激活SA的数量最小。IKE阶段2删除消息不应当解释为释放Diameter连接的一个原因。更可取的方法是保持该连接，如果在上面发送附加流量，应由另外的IKE阶段2 SA来保护它。这样可以避免潜在不断的连接建立和释放。

9.2 TLS 的使用

发起一个到其他Diameter节点连接的Diameter节点，承担TLS客户的角色，接受连接的Diameter节点承担TLS服务器的角色。作为TLS会话建立的一部分，采用TLS来保证安全的Diameter节点必须互相认证。为了保证互相认证，承担TLS服务器角色的Diameter节点必须向承担TLS客户角色的Diameter节点请求证书，承担TLS客户角色的Diameter节点必须准备提供相应的证书。

Diameter节点必须能够协商以下TLS密码组：

—— TLS_RSA_WITH_RC4_128_MD5

—— TLS_RSA_WITH_RC4_128_SHA

—— TLS_RSA_WITH_3DES_EDE_CBC_SHA

Diameter节点应当能够协商以下TLS密码组：

—— TLS_RSA_WITH_AES_128_CBC_SHA

Diameter节点可以协商其他TLS密码组。

9.3 对等端到对等端的考虑

在采用任何对等端到对等端协议的时候，Diameter对等端内信任模型的正确配置对于安全是非常重要的。当采用证书的时候，需要配置该Diameter对等端信任的根证书授权机构（CA）。这些根CA很可能是惟一用于Diameter的，是与用于其他用途的（如Web浏览）可信任根CA区别开的。通常希望，配置那

些根CA以能够反映拥有Diameter对等端的组织与其他组织之间的交易关系。因此，Diameter对等端将不配置为允许与任何任意的对等端连接。当证书认证时，可能预先不知道Diameter对等端，因此需要对等端发现机制。

注意，通常认为在配置根CA时，IPSec相对于TLS来说缺乏灵活性。因为IKE阶段1中，端口标识的应用是被禁止的，在IPSec中，不可能单独为每一个应用惟一配置可信任的根CA；必须为所有的应用配置相同的策略。这意味着一个用于Diameter的可信任根CA必须也可以用来保护SNMP。这些限制很难实现。由于TLS支持证书策略中的应用层粒度，TLS应用来保护管理域之间的Diameter连接。当加密机制采用预共享密钥时，IPSec是最适合于域间采用的。

当IPSec采用预共享密钥认证来保护Diameter，Diameter对等端配置惟一的预共享密钥，该Diameter对等端用其IP地址（Main Mode方式下）标识，也可能是其FQDN（Aggressive Mode方式下）。因此需要预先知道Diameter对等端集合。这样基本上就不需要对等端发现机制了。

以下提供该问题的一些指导。

推荐Diameter对等端对跨越所有其对等端到对等端的连接执行相同的安全机制（IPSec或TLS）。采用不一致的安全机制将造成应用冗余安全机制（例如TLS在IPSec之上）或者更糟，形成潜在的安全弱点。当Diameter采用IPSec时，用于带外流量的传统安全策略为“初始化IPSec，从我到任何Diameter目的端口”，对于带内流量，策略为“请求IPSec，从我到任何Diameter目的端口”。

该策略导致无论何时Diameter对等端初始一个连接到另一个Diameter对等端，都需要采用IPSec，无论何时出现一个带内Diameter连接，都会被请求采用IPSec。该策略是非常吸引人的，因为它不要求为每个对等端设置策略，或者在一个每一次新的Diameter连接建立时动态修改；基于一个简单静态策略自动创建一个IPSec SA。因为在大多数平台上IPSec扩展通常对于Socket API是无效的，并且IPSec策略国内是单独实施的，采用简单静态策略对于能够应用IPSec的Diameter实施是最经常且路由最简单的。

该推荐的策略暗示，如果一个节点同时采用TLS和IPSec，没有方便的方法能够在不为TLS应用预留一个附加端口的同时，或者采用TLS或者采用IPSec，而不是同时。因为Diameter为TLS和非TLS应用采用相同的端口，当应用了推荐的IPSec策略，受保护的TLS连接将与该IPSec策略匹配，并且同时采用TLS和IPSec保护该Diameter连接。为了避免这样，需要静态或动态地检讨（Plumb）对等端定义的策略。

如果IPSec保证Diameter对等端到对等端连接的安全，IPSec策略应设置为要求IPSec保护带内连接，并且发起IPSec保护以用于带外连接。这可以通过带内和带外过滤策略的应用来实现。

附 录 A
（规范性附录）
Diameter 应用扩展

A.1 NAS应用扩展要求

Diameter协议在以网络接入服务器（NAS）作为主要接入手段的网络环境中提供认证、授权和计费（AAA）服务时，除了需要遵循基本协议的要求外，还必须有相应的应用扩展要求。网络接入服务器应用扩展规范和Diameter基本协议要求、传输轮廓要求（RFC 3539）、以及可扩展认证协议（EAP）（RFC 2284bis）规范结合在一起，才能够满足传统网络接入业务的AAA要求。

由于传统网络接入业务目前绝大多数采用RADIUS协议来提供AAA服务，Diameter协议在最初应用时，必须考虑与现有网络中的RADIUS协议并存的问题。为了尽量减轻RADIUS和Diameter协议转换的负担，NAS应用扩展要求中充分考虑了该问题的解决，例如，NAS应用扩展中包括RADIUS属性空间，以避免完成很多属性翻译。

NAS应用扩展要求包括Diameter NAS应用操作的描述、定义相应的Diameter消息命令码、列举在这些消息中采用的AVP（包括会话鉴定、认证、授权、隧道和计费AVP），以及与RADIUS互操作和前向兼容要求。

A.2 移动IP应用扩展要求

Diameter移动IP应用允许Diameter服务器对移动节点的移动IP业务进行认证、授权、采集计费信息。结合diameter基础协议的域间能力（Inter-Realm capability），这个应用允许移动节点接收外部服务器提供的业务。外部代理和归属代理采用Diameter计费消息将有用信息传送给diameter服务器。

移动IP定义了移动节点在改变因特网接入点时仅有最小的业务受到干扰的一种方法。移动IP对穿越分离的行政主域不提供任何特殊的支持。在分离的行政主域之间切换，限制了移动IP在IPv4商业用途中的应用。移动IP规范建议移动节点采用静态归属地址和归属代理。然而，在某些应用中却不是很现实。最近，IETF允许移动IP中的移动节点不完全采用静态归属代理和归属地址。另外，MIPNAI规范允许移动节点采用网络接入标识符替代归属地址，NAI更适合目前的管理实际。

移动IP协议规定了一种安全模式，即移动节点和归属代理之间共享一个预先存在的安全联盟。这个安全联盟引出了扩展和配置问题。本标准定义了Diameter的功能，即允许AAA服务器作为密钥分配中心（Key Distribution Center，KDC）。为保护移动IP注册消息的安全性，KDC可以建立动态会话密钥，并且将密钥分发给移动实体。要求强健的认证和会话密钥的机密性，并由TLS或IPSec方式认证。

根据Diameter 基础协议，实现移动IP应用的AAA服务器能够处理在网络接入标识符格式中提供的用户标识符，网络接入标识符用于Diameter 消息路由选择。移动节点包括在注册消息中的NAI。NAI的应用方法与ROAMOPS工作组定义的域模型是相一致的。

基于移动IP特点，重认证消息由移动节点侧发起，并不参与Diameter消息交互。因此Daiemeter服务器发起的重认证不适用于本应用。

移动节点可以在不同的外部代理之间进行切换。为保证注册用户始终终结在相同的初始AAAH，移动节点应该一直包含AAAH 网络接入标识符。最后，为协助AAAH将消息路由到移动节点的归属代理，

移动节点应该总包含HA网络接入标识符。如果移动节点不支持移动IP AAA NAI扩展，可以限制提供给这样的移动节点的功能。

A.3 SIP应用扩展要求

Diameter 会话初始化协议应用是与会话初始化协议（SIP）结合在一起使用的，在SIP服务器中提供Diameter客户端功能，SIP服务器必须能够请求Diameter服务器认证用户，授权SIP资源使用。Diameter SIP应用不要求与移动IP Diameter提供的其他认证服务或网络接入服务器Diameter应用（Network Access Server Diameter applications）相关。

Diameter SIP应用扩展允许Diameter客户端向Diameter服务器为基于IP多媒体业务的初始会话协议（SIP）请求认证、授权信息。假定SIP服务器和Diameter客户端位于相同节点，SIP服务器能够接收、处理SIP请求消息和回答消息，分别基于为认证SIP请求消息和授权特定SIP业务的AAA体系结构。

当SIP协议用于初始和终结多媒体会话时，或者SIP协议用于非会话相关的应用时，Diameter SIP应用扩展提供Diameter规程，用于实现特定功能。这个应用扩展既不要求Mandate将SIP规程特定映射到Diameter SIP应用规程，也不要求SIP协议与Diameter协议之间事件的特定顺序。本标准提供了一些应用示例，描述SIP与Diameter SIP应用之间的互操作，完成预想功能。

Diameter SIP应用扩展了Result-Code Attribute-Value-Pair（AVP）新数值。这个应用定义了一些新的AVP。

Diameter SIP应用扩展假定了一个通用体系结构，即归属域由一个或多个实现Diameter或SIP功能的节点构成。其中，至少有一个这样的节点实现Diameter 服务器功能。Diameter服务器有权应用用户数据库。特定用户的用户数据储在用户数据库中一个单独的节点中。网络中可以有多余一个的Diameter 服务器，所有的Diameter服务器均有权应用用户数据库。但在特定时间内，Diameter服务器返回的数据是不依赖于Diameter服务器返回的信息。

这个体系结构的中心就是在网络中的一个单独的节点中存储用户数据。这个限制并不要求特殊实现，可能在运行Mirror模式下，提供冗余时实现数据库丛Clusters。Diameter 服务器有权应用的用户数据是作为一个单独的用户数据库存储的。

本标准允许归属域有多种配置。在其中一种配置情况下，SIP服务器被分配给用户，用于触发和执行业务。用户在网络中进行注册时动态分配SIP服务器。在这种配置情况下，要求有一个位于网络边缘的SIP服务器，支持对SIP请求和回答消息的路由算法。SIP服务器节点实现Diameter客户端功能。

在另一种配置情况下，SIP 输出代理被配置为SIP端点。在SIP输出代理节点中的输出Diameter 客户端认证用户、为SIP请求消息要求授权并完成计费活动。

Diameter SIP应用能够在SIP环境中使用。在SIP环境中要求有一个AAA基础框架结构接口，采用这个接口进行认证、授权、提供计费信息。

A.4 EAP应用扩展要求

EAP是在RFC 2284bis中定义的一种支持多种认证机制的认证框架结构。EAP可用于专线、交换线路，有线与无线链路上。

Diameter为了支持EAP增加了两个命令Diameter-EAP-Request与Diameter-EAP-Answer及几个相应的AVP：EAP-Payload AVP、EAP-Reissued-Payload、EAP-MTU、EAP-Master-Session、Accounting-EAP-Auth-Method AVP。

当发起一个EAP会话建立时，接入设备会向Diameter发起一个EAP-Payload为空的Diameter-EAP-Request消息表示EAP-Start。如果Diameter服务器接受EAP认证方式，它用Diameter-EAP-Answer进行应答，其中EAP-Payload AVP里包含有相应的EAP数据包，Result-Code设为DIAMETER_MULTI_ROUND_AUTH，表明等待后续的数据包。EAP-Payload里的内容由接入服务器前转给EAP有客户端。如图A.1所示。

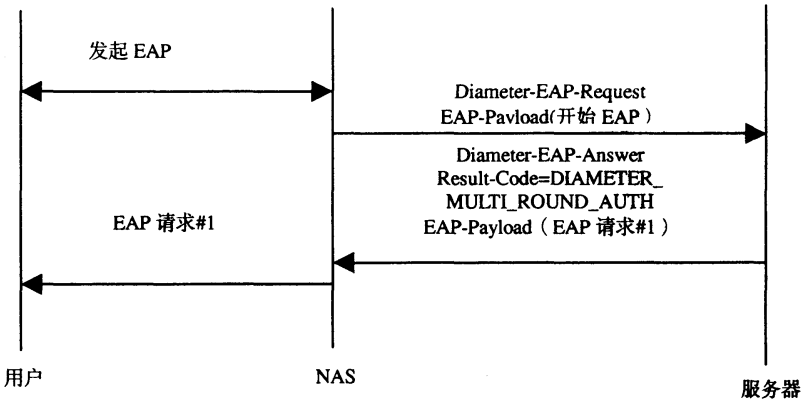

图 A.1 EAP 会话建立

此对话会一直进行下去，直到Diameter服务器发出的Diameter-EAP-Answer消息中的Result-Code AVP表明成功或失败。接入设备根据Result-Code AVP来决定是否为EAP用户提供服务。

如果需要授权，Diameter-EAP-Answer的Result-Code设为DIAMETER_SUCCESS，同时必须包括服务所需要的相应授权AVP。

A.5 信用控制应用扩展要求

信用控制（Credit-Control）是一种可以与一个账户进行实时交互、控制并监视，对一服务进行收费的机制。信用控制包括对检查一账户是否存在、续费、当一个服务结束时从账户中扣除相应收取的费用与退还余下的金额等处理。

Diameter 信用控制服务器可以看作预付费服务器，进行实时的计费与信用控制。Diameter信用控制客户端是与信用控制服务器进行交互的实体，它监视由服务器端返回的允许金额的使用状况。

Diameter消息针对信用控制应用扩充了两个消息：Credit-Control-Request与Credit-Control-Answer，分别用于信用控制的请求与应答并相应加入了若干AVP。

在信用控制应用中，有两种模式，一种是信用控制服务器对用户请求进行评估，从用户的账户上划转一定数额的钱，并返回相应的信用度。此处的信用度不一定用钱衡量，也可能用其他单位（比如数据量）。收到成功的信用授权后，信用控制客户端向用户提供服务，并监视允许资源的使用情况，在资源消耗完、服务完成或服务终结后，客户端向服务器返回报告；服务器从用户账户相应扣除。

另一种方式是收到了信用授权请求后，服务器端直接从用户账户里扣除相应的数额，客户端收到服务器返回的信用控制授权应答后为终端用户提供服务。这一过程只有一个时间事件就完成了，不维护会话的状态。

附 录 B
（规范性附录）
已定义的 AVP 表

表B.1给出了本标准中定义的AVP，该AVP可能出现的Diameter消息。注意，只能在一个组合AVP中出现的AVP不在本标准列出。

本表使用以下符号：

a） 该AVP不可以在该消息中出现。

0+：该AVP的0或多个实例可能在该消息出现。

0－1：该AVP的0或一个实例可能在该消息出现。多于1个该AVP的实例将被认为是差错。

1：该AVP的0或多个实例必须在该消息出现。

1+：至少一个该AVP的实例必须在该消息出现。

B.1 基础协议命令AVP表

表B.1仅限于本标准中定义的非计费命令码。

表 B.1 基础协议命令 AVP 表

	命令码											
属性名	CER	CEA	DPR	DPA	DWR	DWA	RAR	RAA	ASR	ASA	STR	STA
Acct-Interim-Interval	0	0	0	0	0	0	0－1	0	0	0	0	0
Accounting-Realtime-Required	0	0	0	0	0	0	0－1	0	0	0	0	0
Acct-Application-Id	0+	0+	0	0	0	0	0	0	0	0	0	0
Auth-Application-Id	0+	0+	0	0	0	0	1	0	1	0	1	0
Auth-Grace-Period	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Request-Type	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Session-State	0	0	0	0	0	0	0	0	0	0	0	0
Authorization-Lifetime	0	0	0	0	0	0	0	0	0	0	0	0
Class	0	0	0	0	0	0	0	0	0	0	0+	0+
Destination-Host	0	0	0	0	0	0	1	0	1	0	0-1	0
Destination-Realm	0	0	0	0	0	0	1	0	1	0	1	0
Disconnect-Cause	0	0	1	0	0	0	0	0	0	0	0	0
Error-Message	0	0－1	0	0－1	0	0－1	0	0－1	0	0－1	0	0－1
Error-Reporting-Host	0	0	0	0	0	0	0	0-1	0	0-1	0	0-1
Failed-AVP	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+
Firmware-Revision	0－1	0－1	0	0	0	0	0	0	0	0	0	0

表 B.1（续）

属性名	命令码											
	CER	CEA	DPR	DPA	DWR	DWA	RAR	RAA	ASR	ASA	STR	STA
Host-IP-Address	1+	1+	0	0	0	0	0	0	0	0	0	0
nband-Security-Id	0+	0+	0	0	0	0	0	0	0	0	0	0
Multi-Round-Time-Out	0	0	0	0	0	0	0	0	0	0	0	0
Origin-Host	1	1	1	1	1	1	1	1	1	1	1	1
Origin-Realm	1	1	1	1	1	1	1	1	1	1	1	1
Origin-State-Id	0 – 1	0 – 1	0	0	0 – 1	0 – 1	0 – 1	0 – 1	0 – 1	0 – 1	0 – 1	0 – 1
Product-Name	1	1	0	0	0	0	0	0	0	0	0	0
Proxy-Info	0	0	0	0	0	0	0 +	0+	0+	0+	0+	0+
Redirect-Host	0	0	0	0	0	0	0	0+	0	0+	0	0+
Redirect-Host-Usage	0	0	0	0	0	0	0	0-1	0	0-1	0	0-1
Redirect-Max-Cache-Time	0	0	0	0	0	0	0	0-1	0	0-1	0	0-1
Result-Code	0	1	0	1	0	1	0	1	0	0	0	1
Re-Auth-Request-Type	0	0	0	0	0	0	1	0	0	0	0	0
Route-Record	0	0	0	0	0	0	0+	0	0+	0	0+	0
Session-Binding	0	0	0	0	0	0	0	0	0	0	0	0
Session-Id	0	0	0	0	0	0	1	1	1	1	1	1
Session-Server-Failover	0	0	0	0	0	0	0	0	0	0	0	0
Session-Timeout	0	0	0	0	0	0	0	0	0	0	0	0
Supported-Vendor-Id	0+	0+	0	0	0	0	0	0	0	0	0	0
Termination-Cause	0	0	0	0	0	0	0	0	0	0	1	0
User-Name	0	0	0	0	0	0	0 – 1	0 – 1	0 – 1	0 – 1	0-1	0 – 1
Vendor-Id	1	1	0	0	0	0	0	0	0	0	0	0
Vendor-Specific-Application-Id	0+	0+	0	0	0	0	0	0	0	0	0	0

B.2 计费AVP表

表B.2给出了标准中定义的出现在计费消息中的AVP。这些AVP出现的要求可能被在Diameter应用标准中的应用定义要求扩展和/或推翻。

表 B.2　计费 AVP 表

属性名	命令码	
	ACR	ACA
Acct-Interim-Interval	0 – 1	0 – 1
Acct-Multi-Session-Id	0 – 1	0 – 1
Accounting-Record-Number	1	1
Accounting-Record-Type	1	1
Acct-Session-Id	0 – 1	0 – 1
Accounting-Sub-Session-Id	0 – 1	0 – 1
Accounting-Realtime-Required	0 – 1	0 – 1
Acct-Application-Id	0 – 1	0 – 1
Auth-Application-Id	0	0
Class	0+	0+
Destination-Host	0 – 1	0
Destination-Realm	1	0
Error-Reporting-Host	0	0+
Event-Timestamp	0 – 1	0 – 1
Origin-Host	1	1
Origin-Realm	1	1
Proxy-Info	0+	0+
Route-Record	0+	0+
Result-Code	0	1
Session-Id	1	1
Termination-Cause	0 – 1	0 – 1
User-Name	0 – 1	0 – 1
Vendor-Specific-Application-Id	0 – 1	0 – 1

附 录 C
（规范性附录）
Diameter协议相关配置参数

本附录包含本标准中出现的可配置参数。

1）Diameter对等端

一个Diameter实体可以与静态配置的对等端通信。一个静态配置的Diameter对等端应要求IP地址或提供的完全资格域名（FQDN），用作DNS解析。

2）域（Realm）路由表

一个Diameter Proxy服务器基于网络接入标识符（NAI）的域（Realm）部分来路由消息。服务器必须拥有一个域名（Realm Names）表，以及消息必须前转到的对等端的地址。路由表也可以包括一个“缺省路由”，该路由表一般用于不能本地处理的所有消息。

3）Tc计时器

Tc计时器控制到一个没出现动作传输连接的对等端的传输连接尝试的频率。建议值为30s。

附 录 D
（资料性附录）
Diameter 服务模板

以下服务模板描述了属性，这些属性是Diameter服务器用来广播自己的。它简化了选择适当的与自己通信的服务器的程序。Diameter客户可以基于自己想要的Diameter服务器的特征来请求特定的Diameter服务器（例如，一个用于计费的AAA服务器）。

1）提交者的名字：“Erik Guttman” <Erik.Guttman@sun.com> 服务模板的语言：en。

2）安全考虑

Diameter客户和服务器使用不同的密码机制以保护通信的完整性、机密性，同时还执行端点认证。因此没有正确的事先配置好的密码或密钥的攻击者使用SLPv2广播自己并伪装成合法的Diameter对等端，是非常困难的。尽管如此，由于Diameter服务对于网络操作来说是至关重要的，因此非常有必要使用SLPv2认证以阻止攻击者修改或删除合法Diameter服务器的服务广告。

3）模板文字

```
----------------------------------模板开始-------------------------------
template-type=service:diameter
template-version=0.0
template-description=
template-url-syntax=
  url-path=    ；举例：'aaa://aaa.example.com:1812;transport=tcp
   supported-auth-applications= string L M
   # 该属性列举了AAA实施支持的Diameter应用。目前定义的应用如下：
   #     应用名                    所属
   #  ----------------          ----------------------------------
   #  NASREQ                    Diameter网络接入服务器应用
   #  MobileIP                  Diameter移动IP应用
   #
   # 注：
   #    . Diameter实施支持一个或多个应用。
   #    . 附加应用可以在将来定义。届时将创建一个修订的服务模板。
   #
   NASREQ，MobileIP
   supported-acct-applications= string L M
   # 该属性列举了AAA实施支持的Diameter应用。目前定义的应用如下：
   #     应用名                    所属
   #  ----------------          ----------------------------------
   #  NASREQ                    Diameter网络接入服务器应用
```

MobileIP Diameter移动IP应用

#

注：

.Diameter实施支持一个或多个应用。

.附加应用可以在将来定义。届时将创建一个修订的服务模板。

#

NASREQ，MobileIP

supported-transports= string L M

SCTP

该属性列出了所支持的、Diameter实施接受的传输。注意适合的Diameter 实施必须

支持SCTP，尽管其可能也支持其他传输。

SCTP，TCP

----------模板结束----------

附 录 E
（资料性附录）
NAPTR 示例

作为一个示例，假设一个希望解析aaa:ex.com的客户。该客户执行一个用于该域的NAPTR请求，返回以下NAPTR记录：

;;		顺序	前缀	标记	业务	regexp	replacement
	IN NAPTR	50	50	"s"	"AAA+D2S"	""	_diameter._sctp.example.com
	IN NAPTR	100	50	"s"	"AAA+D2T"	""	_aaa._tcp.example.com

这表明服务器支持SCTP和TCP。如果该客户支持SCTP，将采用SCTP，目标是由SRV查找_diameter._sctp.ex.com决定的主机。查找应返回：

;;		优先级	加权值	端口	目标
IN	SRV	0	1	5060	server1.example.com
IN	SRV	0	2	5060	server2.example.com

附 录 F
（资料性附录）
重复检测

计费记录重复检测是基于会话标识符的。重复记录的出现可能由于多种原因：

—— Failover到另一台替换的服务器。由于需要接近实时的性能要求，Failover门限需要保持为“低”，这将可能导致重复记录出现的可能性增加。Failover可能在客户或Diameter代理中出现。

—— 在来自非可变存储器的记录发送之后，客户或代理出现故障，但此时还没有收到一个应用层ACK，并删除该记录。这将导致该记录在客户或代理重启动之后很快被重新发送。

—— 从RADIUS网关接收到重复的记录。由于RADIUS的重传行为并没有在RADIUS的规范（RFC 2865）中定义重复记录的可能性将由于实施的不同而不同。

—— 实施问题和错误配置。

T标记用于作为应用层重传事件（例如，由于Failover到另一台替换的服务器）的标识。其仅为Diameter客户或代理发送的请求消息而定义。举例，重启动后，客户可能不知道在重启动发生之前其是否已经试图发送在非可变存储器中的该计费记录。当处理请求和删除重复消息的时候，Diameter服务器可以使用T标记作为帮助。然而，服务器这样做必须保证，即使第一次发送的请求在重传请求之后到达服务器，也能发现重复消息。它仅在没有收到来自服务器的应答，并且再一次发送请求的情况下（例如，由于一个到替换的对等端的Failover，由于一个恢复主要对等端，或者由于一个在客户或代理重启动之后，重新发送非可变存储器中记录的客户）使用。

在某些情况下，Diameter计费服务器能够延迟重复检测和计费记录的处理，直到后处理阶段（post-processing phase）开始。那时记录通常被根据其包含的用户名（User-Name）排序，这种情况下，重复的删除会很容易。在其他情形下，可能需要执行实时重复检测，例如当使用信用限制或需要实时欺骗检测的时候。

通常，只有Failover或非可变存储器中的记录重发造成的重复能够被Diameter客户或代理可靠地检测到。在这种情况下，Diameter客户或代理能够利用设置T标记来标识可能重复的消息。由于Diameter服务器负责重复检测，它可以选择是否采用T标记，以优化重复检测。由于T标记不会影响协同性，而且某些服务器可能不需要，所以要求Diameter客户和代理必须能够生成T标记，但Diameter服务器则为可以采用。

例如，通常可以假定重复现象会在时间窗口（最长记录网络分区或设备故障的时间窗口）规定的时间内出现，或许是一天。因此，只有这个时间窗口内的记录需要逆向进行检查。其次，哈希算法技术和在接收到的消息中采用T标记等其他机制，可以减少完全搜索。

下面举例说明如何采用T标记检测重复请求。

Diameter服务器通过检查接收到的消息中的T标记判决记录是否可能重复。如果请求消息中T标记置位，服务器在可配置的复制时间窗口内进行前向和后向的检查，搜索是否有重复。这样可以限制数据库仅在T标记置位的记录中进行搜索。在一个运行状况良好的网络中，网络分区和设备故障发生的几率很小，因此这种重复检测进程是一种优化的方法。在失败回溯（Failover）阶段，T标记对记录标记后，由于初始记录和重复记录经过路径的不同网络时延，可能会接收到初始记录。随着这种情况发生次数的增多，失败回溯的间隔会减少。为能够检测出无序的重复，当完成对T标记标记过的请求时，Diameter服务

器应该采用前向和后向时间窗。例如，为留出初始记录退出网络并被计费服务器记录的时间，Diameter服务器可以延迟处理将T标记置位的记录，直到关闭初始传输连接，且TIME _WAIT + RECORD_PROCESSING_TIME时间段结束。在TIME _WAIT + RECORD_PROCESSING_TIME时间段已经过期后，Diameter服务器可以检查T标记标记过的记录，与具有原始记录（如果发送）已经被接收并被记录的相关保证的数据库进行对比。

中华人民共和国
通信行业标准
用于IP网络的Diameter基础协议技术要求
YD/T 1469-2006
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
北京新瑞铭印刷有限公司

*
开本：880×1230　1/16　　2006年9月第1版
印张：5.75　　2006年9月北京第1次印刷
字数：172千字
ISBN 7-115-1281/06-102
定价：45.00元
本书如有印装质量问题，请与本社联系　电话：(010)67114922