DIAMETER et ses Applications
Principes, Architecture et Services

EFORT
http://www.efort.com

Contrairement à RADIUS, acronyme de Remote Authentication Dial-In User Service, le nom du protocole DIAMETER est un jeu de mot, signifiant diamètre en anglais, qui est le double du rayon (radius en anglais).
Le protocole DIAMETER successeur du protocole RADIUS est un protocole AAA (Authentication, Authorization, Accounting). Il permet aux opérateurs d'authentifier des utilisateurs, de leur autoriser certains services et de collecter des informations sur l'utilisation des ressources. Il s'agit du protocole le plus à même de satisfaire les nouveaux besoins suscités par la mobilité. En particulier, il permet aux opérateurs d'authentifier un utilisateur ayant souscrit un abonnement auprès d'un autre opérateur. DIAMETER est un protocole en particulier utilisé par le 3GPP pour ses architectures LTE (Long Term Evolution of 3G) et IMS (IP Multimedia Subsystem). Il permet entre autres l'authentification, l'autorisation et la taxation online et offline des clients LTE et IMS.
Le paragraphe 1 introduit le protocole de base DIAMETER et décrit les différentes applications DIAMETER définies par le monde des télécommunications notamment pour ses architectures LTE et IMS. Le paragraphe 2 présente les différents types de nœud DIAMETER, i.e., client, agent et serveur. Le paragraphe 3 décrit le format des messages DIAMETER et des AVPs (Attribute Value Pair) qui sont les paramètres des messages DIAMETER.

1 Le protocole DIAMETER est ses applications dans le monde des télécommunications

Le protocole DIAMETER a été conçu comme une version améliorée du protocole RADIUS.
Un des objectifs était de maximiser la compatibilité et faciliter la migration de RADIUS à DIAMETER. Par exemple, un message DIAMETER comme un message RADIUS transporte un ensemble de paires <attribut, valeur>.
DIAMETER est défini à travers un protocole de base et un ensemble d'applications. Cette conception permet une extension du protocole de base pour de nouvelles applications. Le protocole de base fournit des mécanismes pour un transport fiable, la livraison des messages et le traitement des erreurs.
Le protocole de base doit être utilisé conjointement avec une application DIAMETER. Chaque application s'appuie sur les services du protocole de base.

DIAMETER est en particulier utilisé dans le monde des télécommunications par les architectures LTE et IMS.

La LTE (Long Term Evolution of 3G) est un projet mené par l'organisme de standardisation 3GPP visant à rédiger les normes techniques de la future quatrième génération en téléphonie mobile. Elle permet le transfert de données à très haut débit, avec une portée plus importante et une latence plus faible.
En terme de vocabulaire, le futur réseau de quatrième génération s'appelle EPS (Evolved Packet System). Il est constitué d'un nouveau réseau d'accès appelé LTE (Long Term Evolution) et d'un nouveau réseau coeur appelé SAE (System Architecture Evolution).

L'EPS (Evolved packet System) a les caractéristiques suivantes :

- Il possède une architecture plate et simplifiée comparée à celle hiérarchique 2G/3G puisque la fonction de contrôleur d'antenne disparaît. La seule entité présente dans l'accès LTE est l'eNodeB qui peut être assimilé à un nodeB avec des fonctions du RNC.
- Il s'agit d'une architecture uniquement paquet comparée à l'architecture 2G/3G circuit et paquet.
- Il permet une connectivité permanente tout-IP (appelée default bearer) comparée à des contextes PDP temporaires ou permanents en 2G/3G dans le domaine paquet
- Son interface radio est totalement partagée entre tous les usagers en mode ACTIF comparée à des ressources dédiées et partagées dans l'architecture 2G/3G. Les appels voix et visiophonie requièrent des ressources dédiées en 3G.
- Il permet des handover vers les réseaux 2G/3G et CDMA/CDMA2000 afin d'assurer des communications sans couture en environnement hétérogène.

L'IMS (IP Multimedia Subsytem) normalisé par l'organisme 3GPP est une architecture de réseau et de service qui permet le contrôle de sessions multimédia sur un réseau IP. Elle supporte des sessions temps réels (voix, vidéotéléphonie, conférence, IPTV), pseudo temps réel (tchat, push to talk) et non temps réel (SMS). Un seul cœur de réseau (IP + IMS) supportant des services multimédia (Services IMS) servira des usagers sur différents accès large bande (xDSL, LTE, 3G+, Câble, FTTH, etc). L'IMS intègre de plus le concept de convergence des services multimédia.
L'IMS normalise déjà un ensemble de capacités de service telles que la présence, le messaging, la conférence, les hosted enterprise services, l'IPTV, les multimedia telephony services qui correspondent aux services complémentaires de la téléphonie, la voice call continuity, etc.

3GPP définit pour LTE et IMS un nombre d 'applications basées sur le protocole DIAMETER qui supportent les interfaces suivantes :

- S6 (LTE) : S6 est une interface entre l'entité de gestion de la mobilité LTE appelée MME (Mobility Management Entity) et la base de données globale LTE appelée HSS (Home Subscriber Server)
- S13 (LTE) : S13 est l'interface entre l'entité MME et l'entité EIR (Equipment Identity Register) dans la LTE
- Gx (LTE) : Gx est l'interface permettant à l'entité de commutation de paquet dans la LTE appelée PDN-GW (Packet Data Network Gateway) d'obtenir des règles de taxation auprès de l'entité PCRF (Policy and Charging Rules Function) et ainsi taxer l'usager sur la base des flux de services et non pas sur le volume.
- Gy (LTE) : Gy est l'interface de taxation online entre le PDN-GW et l'OCS (Online Charging System)
- Gz (LTE) : Gz est l'interface de taxation offline entre le PDN-GW et l'Offline Charging System
- S9 (LTE) : S9 est l'interface entre le PCRF du réseau visité et le PCRF du réseau nominal dans le cas où la taxation est prise en charge par le réseau visité.
- Rx (LTE) : Rx est l'interface permettant à l'IMS de demander au réseau LTE (entité PCRF) de réserver des ressources à l'accès pour garantir la qualité de service des sessions IMS.
- Cx (IMS) : Cx est l'interface entre les entité de contrôle de session IMS appelées I-CSCF et S-CSCF (Interrogating et Serving Call State Control Function) et la base de données IMS appelée HSS afin d'authentifier, d'autoriser et de localiser l'usager IMS.
- Dx (IMS) : Dx est l'interface entre l'I-CSCF ou le S-CSCF et l'entité SLF (Subscription Locator Function) afin de localiser le HSS de l'usager.
- Sh (IMS) : Sh est l'interface entre l'Application Server (AS) SIP et le HSS afin que l'AS obtienne les données de service permettant l'exécution du service par l'AS.
- Dh (IMS) : Dh est l'interface entre l'AS et le SLF afin de localiser le HSS de l'usager.

- Rf (IMS) : Rf est l'interface entre les entités IMS et l'entité CCF (Charge Collection Fuction) pour la taxation offline.
- Ro (IMS) : Ro est l'interface entre les entités IMS et l'entité Online Charging System (OCS).

L'application DIAMETER SIP spécifiée dans le RFC 4740 définit une application DIAMETER qui peut être utilisée par un serveur SIP afin d'authentifier les usagers et les autoriser à utiliser différentes ressources SIP. L'application DIAMETER SIP a une spécification proche de celle de l'interface Cx en terme de fonctions, mais elle a été conçue afin d'être suffisamment générique et ainsi être utilisée par d'autres scénarii de déploiement SIP en dehors de l'IMS.
L'Application DIAMETER Credit Control spécifiée dans le RFC 4006 est utilisée pour la taxation temps réel (online charging) d'un grand nombre de services. Elle est similaire à l'interface Ro DIAMETER définie dans l'IMS.

2 Types de nœud DIAMETER

Un nœud DIAMETER est un hôte qui implante le protocole DIAMETER.
Un client DIAMETER est un nœud à la frontière du réseau qui réalise un contrôle d'accès. Des exemples de clients DIAMETER sont les Network Access Servers (NAS), MME, S4-SGSN.
Un serveur DIAMETER prend en charge les demandes d'authentification, d'autorisation et de taxation pour un domaine donné (appelé realm). Un exemple de serveur est le HSS.
Un agent DIAMETER est un nœud DIAMETER qui fournit des services de relai, de proxy ou de traduction.
Un agent relai route les messages DIAMETE sur la base de l'information présente dans les messages. Les agents sont transparents. Un agent relai peut modifier les messages DIAMETER uniquement en insérant et retirant des informations de routage mais ne peut pas modifier les autres éléments d'information du message.
Un agent proxy comme un agent relai route le message DIAMETER. Toutefois un agent Proxy peut modifier les messages afin de réaliser un contrôle d'accès, un contrôle de politiques, etc. Un exemple d'agent proxy est l'entité PCRF dans l'architecture LTE.
Un agent de redirection fournit aussi une fonction de routage. Il sert de directory permettant généralement la traduction de Nom de domaine → Adresse du serveur. A la différence des autres types d'agent (relai et proxy) qui acheminent les messages DIAMETER, l'agent de redirection retourne un type particulier de réponse à l'émetteur de la requête. La réponse contient l'information de routage afin que l'émetteur puisse retransmettre son message directement au serveur destinataire. Un exemple d'agent de redirection est l'entité SLF dans l'architecture IMS.
Un agent de traduction traduit les protocoles DIAMETER en RADIUS, DIAMETER en MAP, etc. Un exemple d'agent de traduction est l'entité IWF de l'architecture LTE qui traduit DIAMETER en MAP.
A la figure 1, le chemin de la requête et de la réponse est 1, 4, 5 et 6 dans le cas du traitement uniquement par des agents relai/proxy. Le chamin devient 1, 2, 3, 4, 5, et 6 si l'agent de redirection est aussi impliqué.

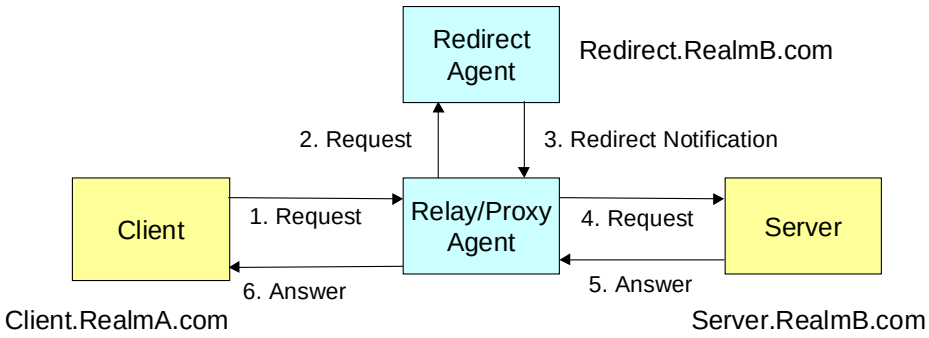

Figure 1 : Types de nœud DIAMETER

3 Message DIAMETER et AVP DIAMETER

Le protocole DIAMETER comprend un protocole de base qui définit le format du PDU (Protocol Data Unit), quelques primitives, et des services de sécurité de base. Le PDU est structuré en AVP (Attribute Value Pair), les 256 premiers AVPs étant réservés pour faciliter la migration de RADIUS à DIAMETER.
Un message DIAMETER consiste en un en-tête de taille fixe (20 octets) suivi par un nombre variable d'AVPs. Le format du message est montré à la figure 2.

- Le champ « Version » indique le numéro de version de DIAMETER. La valeur de ce champ est positionnée à 1.
- Le champ « Message length » indique la longueur du message en octets.
- Le fanion de commande spécifie 4 bits R, P, E et T:
  - R : Le bit R signifie Request. Il indique si le message est une requête ou une réponse. 1 Request; 0=Réponse.
  - P : Le bit P signifie Proxiable. Il indique si le message peut être routé par un agent proxy, un agent relai ou un agent de redirection ou s 'il doit être traité localement.
  - E : Le bit E signifie Error. Il indique si le message contient des erreurs protocolaires ou sémantiques. Lorsque la requête génère une erreur protocolaire, le message de réponse est retourné avec son bit E positionné à la valeur 1 indiquant une erreur protocolaire.
  - T : Le bit T signifie reTransmitted. Il indique si le message a été retransmis suite à un failover ou est utilisé pour supprimer à la réception des message dupliqués.
  - r(eserved) - Les bits r sont réservés pour usager futur. Ils sont positionnés à 0 et ignorés par le récepteur.
- command-code (4 octets) est utilisé pour communiquer la commande associée au message. Chaque message DIAMETER doit contenir un code de commande afin que le récepteur sache identifier l 'action à réaliser pour chaque message
- Application-ID (4 octets) identifie l 'application spécifique à laquelle appartient le message, tel que Mobile IP, Accounting, etc.
- Hop-by-hop identifier transporte un identificateur utilisé afin d 'associer la requête et la réponse sur ce saut (hop). L 'émetteur de la réponse doit s 'assurer que la valeur de cet identificateur est la même que celle présente dans la requête correspondante.
- End-to-end identifier est utilisé afin de détecter des messages dupliqués. L 'identificateur dans la réponse doit être identique à celui de la requête correspondante. L 'identification doit être unique pour au moins 4 minutes. Cet identificateur ainsi que l 'AVP Origin-Host (décrit plus tard) sont utilisés ensemble afin de détecter des duplications de message. Une requête dupliquée ne doit pas conduire à l 'envoi de deux réponses.

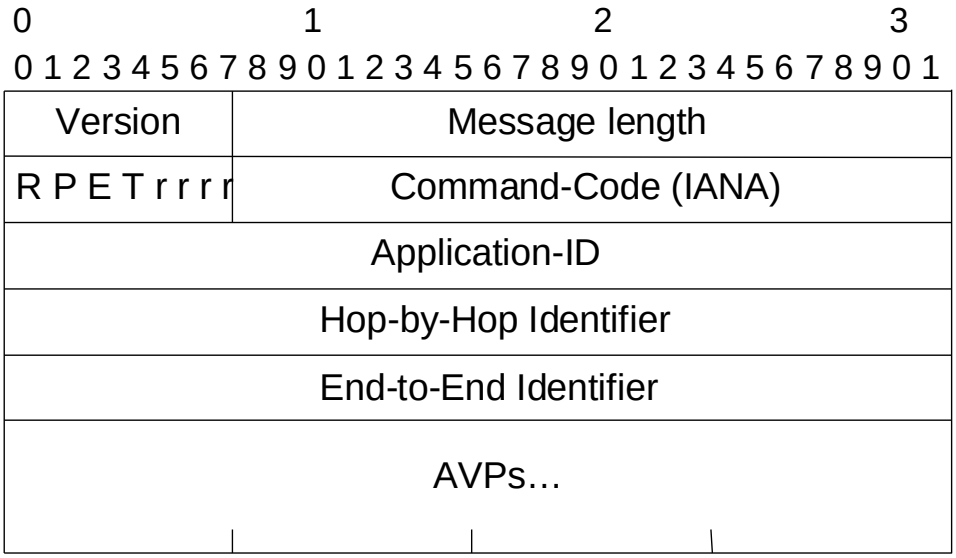

Figure 2 : Format de message DIAMETER

A titre d'exemple, considérons l'interface Cx entre l'I-CSCF ou le S-CSCF et le HSS dans l'architecture IMS.

Cette interface permet :
- L'autorisation d'enregistrement pour l'usager (I-CSCF → HSS)
- La demande des vecteurs d'authentification pour l'usager (S-CSCF → HSS)
- La notification d'état d'enregistrement (register / de-register) (S-CSCF → HSS)
- L'annulation d'enregistrement initiée par le réseau (HSS → S-CSCF)
- La demande de localisation de l'usager (I-CSCF → HSS)
- La mise à jour du profil de l'usager (HSS → S-CSCF).

Tous les messages DIAMETER défins par cette interface ont leur champ « Application-ID » positionné à la valeur 16777216.
Les messages UAR et UAA (Command-Code 300) appartiennent à la transaction d'autorisation. Le message UAR émis par l'entité I-CSCF est acquitté par une réponse UAA qui contient les informations d'enregistrement de l'usager (si celui-ci est déjà enregistré) ou la décision sur la permission de traitement de l'enregistrement (rejeter ou accepter).
Le message MAR est utilisé afin d'obtenir les vecteurs d'authentification pour un usager donné auprès du HSS. La réponse MAA contient un ou plusieurs vecteurs d'authentification générés pour l'usager. Les messages MAR et MAA ont leur champ « Command-Code » positionné à la valeur 303.
Le message SAR est émis par le S-CSCF à l'entité HSS afin de mettre à jour dans le profil de l'usager son S-CSCF courant. L'entité HSS répond par le message SAA en indiquant le nouvel état d'enregistrement de l'usager ainsi que son profil de service. Les messages SAR et SAA ont pour Command-Code la valeur 301.
L'annulation d'enregistrement de l'usager par le réseau est réalisée à l'aide du message RTR émis par le HSS. Le S-CSCF l'acquitte par une réponse RTA. Le Command-Code de RTR et RTA a pour valeur 304.
Le message LIR est émis par l'entité I-CSCF au HSS afin de localiser le S-CSCF courant de l'usager. L'entité HSS répond par un message LIA contenant le nom du S-CSCF ou une valeur d'état indiquant que l'usager n'est pas connu dans ce HSS ou n'est pas actuellement enregistré. Les messages LIR et LIA ont pour Command-Code la valeur 302.
Enfin, le message PPR est utilisé par le HSS afin de mettre à jour un profil d'usager dans le S-CSCF. Ce message est acquitté par le S-CSCF par une réponse PPA. Le Command-Code de PPR et PPA est égal à 305.

Transaction	Emis par
UAR User authorization request	I-CSCF
UAA User authorization answer	HSS
MAR Multimedia authentication request	S-CSCF
MAA Multimedia authentication answer	HSS
SAR Server assignment request	S-CSCF
SAA Server assignment answer	HSS
RTR Registration termination request	HSS
RTA Registration termination answer	S-CSCF
LIR Location info request	I-CSCF
LIA Location info answer	HSS
PPR Push profile request	HSS
PPA Push profile answer	S-CSCF

Figure 3 : Message DIAMETER de l'interface Cx

AVP est l'objet le plus important dans le protocole DIAMETER ; il est utilisé pour fournir toutes les données. Certains AVPs sont nécessaires à DIAMETER lui-même pour fonctionner, alors que d'autres fournissent des données liées aux applications exploitant DIAMETER. Les AVPs contenant l'information spécifique à une application peuvent être arbitrairement ajoutés aux messages DIAMETER, dès lors que les AVPs nécessaires sont présents et que ceux qui doivent être ajoutés ne sont pas explicitement interdits par les règles du protocole.
Les AVPs transportent les informations d 'authentification, d 'autorisation, de sécurité, de comptabilité ainsi que des informations de configuration.
Le format de l 'en-tête de l 'AVP est donné à la figure 4. Il contient les champs suivants :
AVP-Code (4 octets): identifie l 'AVP de manière unique. Les 256 premiers numéros sont réservés pour la compatibilité avec RADIUS. Les suivants sont utilisés par le protocole de base et ses extensions (numéros devant être alloués par l 'IANA).
Fanions (5 bits):
– "V" bit, connu comme Vendor-Specific bit, indique si le champ optionnel Vendor-ID est présent dans l 'en-tête de l 'AVP. Quand positionné, le code AVP appartient à l espace d 'adressage des codes de ce constructeur.
– "M" bit: Le bit M signifie « Mandatory » bit. Il indique si le support de cet AVP est obligatoire. Ainsi si un AVP dont le bit « M »est égal à 0 indique que cet AVP est informationnel, et par conséquent qu 'il peut être ignoré.
– "P" bit: Le bit P signifie « Protected ». Il indique la nécessité d 'un encryptage pour une sécurité de bout en bout. Le protocole de base DIAMETER spécifie quels AVPs doivent être protégés.En pratique ce bit est positionné à la valeur 0.
Les bits rrrrr sont réservés et positionnés à la valeur 0.
Vendor-ID (4 octets) identifie le constructeur à l 'origine de cet AVP propriétaire. La présence de ce champ est précisés par le bit V du champ Fanion (Flags)
Data : Longueur variable.

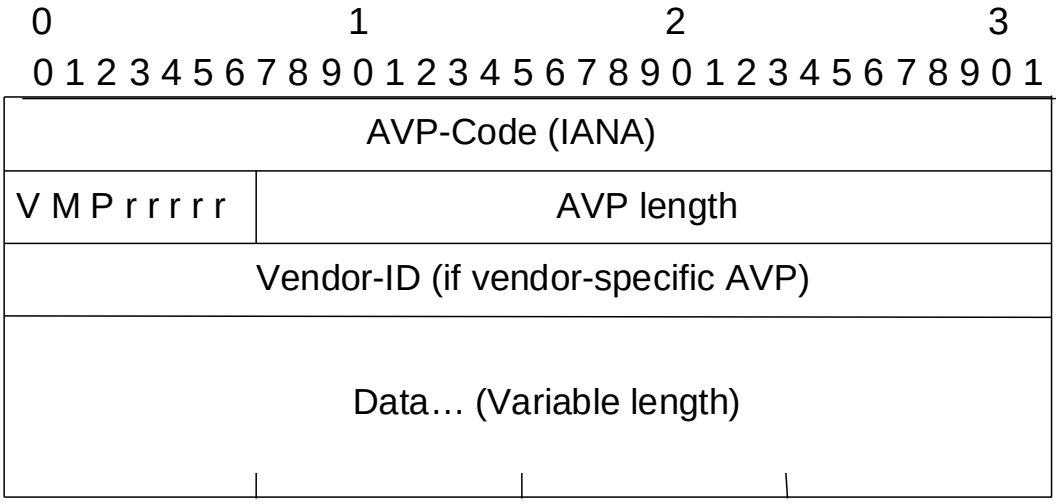

Figure 4 : Format d'AVP DIAMETER

Parmi les AVPs définis par le protocole de base DIAMETER figurent :

- Origin-Host AVP: Cet attribut est ajouté par le client qui génère le message DIAMETER et ne peut pas être modifier par les agents DIAMETER. Il doit être présent dans tous les messages DIAMETER.
- Origin-Realm AVP: Cet AVP contient le Realm (Nom de domaine) de l'émetteur du message DIAMETER et doit être présent dans tous les messages DIAMETER. Les agents Relai ne doivent pas modifier cet AVP.
- Destination-Host AVP: Cet AVP qui peut être présent dans un message DIAMETER émis par un client est utilisé afin de router un message au serveur identifié par cet AVP. L'absence de cet AVP dans un message DIAMETER aura pour conséquence l'envoi du message à n'importe quel serveur DIAMETER supportant l'application et appartenant au domaine spécifié par Destination-Realm AVP.
- Destination-Realm AVP: Cet AVP contient le Realm auquel doit être routé le message DIAMETER. Lorsqu'il est présent, cet AVP permet de réaliser des décisions de routage.

Références

3GPP TS 29.229, Cx and Dx interfaces based on the Diameter protocol; Protocol details, Sept 2007.
RFC 3588, P. Calhoun et al., Diameter Base Protocol, Sept 2003.

Les formations proposées par EFORT présentent outre les aspects architecturaux, protocolaires (SIGTRAN, SIP, DIAMETER, RTP, MEGACO/H.248, etc.) et
normatifs de l'IMS et de l'EPS, les éléments nécessaires à l'élaboration de stratégies de déploiement de business de services sur IP basée sur IMS et EPS: