Architectures and Supporting Protocols for VOIP/3G

Diameter and its use cases
Diameter is the new AAA protocol for the Internet and 3G

- Applications include:
  - Network Access Servers for dial-up with PPP/SLIP,
  - Mobile IPv4 Foreign Agents,
  - Roaming 3G and Internet users (SIP Application).
  - Credit Control
  - Vendor specific applications: e.g. 3G policy and charging control
- Provides **Authentication** of users, **Authorization** and **Accounting** of use
- Carried over TCP or SCTP (or TLS over TCP/SCTP)

![Diagram of Diameter protocol components]

- **Client**
  - NAS: Network Access Server
  - Mobile IPv4 FA
  - S-CSCF

- **Agent**
  - Relay Proxy
  - Redirect Agent

- **Server**
  - e.g. Policy server
  - HSS

  - REQ Answer
  - Request Answer
  - Server Msg e.g. stop service now
Summary of Diameter scalability cmp.

Radius

Radius is the current/legacy standard for AAA in the Internet. E.g. when an ISP user accesses the Internet thru a modem line, the POP uses Radius to contact a DB in order to check access rights. Radius problems are: vulnerability to certain attacks, limited set of attributes are supported and the architecture was designed based on the Client-Server Model.

Add mobile roaming users: Users can roam in many networks owned by hundreds or even thousands of Operators all over the world. The set of offered services is extended – a lot of attributes are needed to describe authorization. The visited network should know about the visitor as little as possible but still be able to route AAA –requests to the home network.

The solution is DIAMETER: introduces proxies, relays, redirect servers + a very flexible protocol message coding + base protocol and extensions architecture. Also Diameter is reliable, runs over TCP or SCTP rather than UDP, less vulnerable to attacks and fraud than Radius.

Challenge is to introduce Diameter when the existing infra is based on Radius. Interoperability of the two protocols becomes key to deployment of Diameter.
Overall Diameter Architecture

**Network Access Server Application**
- EAP Application
- Mobile IPv4 Application
- SIP Application
- Diameter Credit Control Application
- Various 3GPP Apps...

Diameter Base Protocol (RFC 6733)

**EAP** - Extensible Authentication Protocol
NB: The current de-facto solution to AAA is Radius – Diameter for example in 3G

3GPP has created Policy and Charging Control (PCC) Application + HSS and SLF talk Diameter….
Now, DIME has specified the NAT Control Application, QoS Application …
DIME RFCs (4.01.2014)

RFC 5447 Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction (PS)
RFC 5624 Quality of Service Parameters for Usage with Diameter (PS)
RFC 5729 Clarifications on the Routing of Diameter Requests Based on the Username and the Realm (PS)
RFC 5777 Traffic Classification and Quality of Service (QoS) Attributes for Diameter (PS)
RFC 5778 Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction (PS)
RFC 5779 Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server (Proposed Standard)
RFC 5866 Diameter Quality-of-Service Application (PS)
RFC 6408 Diameter Straightforward-Naming Authority Pointer (S-NAPTR) Usage (PS)
RFC 6733 Diameter Base Protocol (PS) Updated by RFC7075
RFC 6734 Diameter Attribute-Value Pairs for Cryptographic Key Transport (PS)
RFC 6735 Diameter Priority Attribute-Value Pairs (PS)
RFC 6736 Diameter Network Address and Port Translation Control Application (PS)
RFC 6737 The Diameter Capabilities Update Application (PS)
RFC 6738 Diameter IKEv2 SK: Using Shared Keys to Support Interaction between IKEv2 Servers and Diameter Servers (PS)
RFC 6942 Diameter Support for the EAP Re-authentication Protocol (ERP) (PS)
RFC 7068 Diameter Overload Control Requirements (Informational)
RFC 7075 Realm-Based Redirection In Diameter (PS)
DIME active drafts (4.01.2014)

draft-ietf-dime-app-design-guide-21 Diameter Applications Design Guidelines (subm pub)
draft-ietf-dime-e2e-sec-req-01 Diameter AVP Level Security: Scenarios and Requirements
draft-ietf-dime-group-signaling-02 Diameter Group Signaling
draft-ietf-dime-ovli-01 Diameter Overload Indication Conveyance
draft-ietf-dime-pmip6-lr-18 Diameter Support for Proxy Mobile IPv6 Localized Routing (subm pub)
draft-ietf-dime-rfc4005bis-14 Diameter Network Access Server Application (subm pub)
draft-tschofenig-dime-e2e-sec-req-01 Diameter AVP Level Security: Scenarios and Requirements
   (Adopted by a WG)

The work of DIME has ended (18.2.2015)
Diameter features include:

- Delivery of attribute value pairs: AVPs
- Capability negotiation
- Error Notification
- Extensibility
- Sessions and Accounting

User Authentication
- Service specific authentication info -> grant service or not

Resource usage information
- accounting and capacity planning is supported

Relay, proxy and redirect of requests thru a server hierarchy
Diameter operation model

**Local Realm**
- Client
- Relay
  - Routing
- Security Association
  - TCP/SCTP
- Roaming Relationship

**Home Realm**
- Proxy
  - Policy
- Home Server
- Security Association
  - SCTP/TCP

**User Session**
- Accounting Relationship

**NAI – Network Access Identifier = user’s-identity + realm**

Raimo Kantola – S – 2015
Diameter terms and definitions

Accounting
The act of collecting information on resource usage for the purpose of capacity planning, auditing, billing or cost allocation.

Authentication
The act of verifying the identity of an entity (subject).

Authorization
The act of determining whether a requesting entity (subject) will be allowed access to a resource (object).

AVP
The Diameter protocol consists of a header followed by one or more Attribute-Value-Pairs (AVPs).
AVP = header encapsulating protocol-specific data (e.g. routing information) + AAA information.

Broker
A broker is a business term commonly used in AAA infrastructures. A broker is either a relay, proxy or redirect agent, and MAY be operated by roaming consortiums. Depending on the business model, a broker may either choose to deploy relay agents or proxy agents.

Diameter Agent = Diameter node that provides either relay, proxy, redirect or translation services.

Diameter Client = a device at the edge of the network that performs access control. Examples are a Network Access Server (NAS) or a Foreign Agent (FA).

Diameter Node = a host process that implements the Diameter protocol, and acts either as a Client, Agent or Server.
More Diameter terms

Diameter Security Exchange = a process through which two Diameter nodes establish end-to-end security.

Diameter Server = one that handles AAA requests for a particular realm. By its very nature, a Diameter Server MUST support Diameter applications in addition to the base protocol.

End-to-End Security
TLS and IPsec provide hop-by-hop security, or security across a transport connection. When relays or proxy are involved, this hop-by-hop security does not protect the entire Diameter user session. End-to-end security is security between two Diameter nodes, possibly communicating through Diameter Agents. This security protects the entire Diameter communications path from the originating Diameter node to the terminating Diameter node.

Home Realm = the administrative domain with which the user maintains an account relationship.

Interim accounting
An interim accounting message provides a snapshot of usage during a user's session. It is typically implemented in order to provide for partial accounting of a user's session in the case of a device reboot or other network problem prevents the reception of a session summary message or session record.

Local Realm
A local realm is the administrative domain providing services to a user. An administrative domain MAY act as a local realm for certain users, while being a home realm for others.
Still more terms

Network Access Identifier or NAI [NAI] = a user's identity + realm.
The identity is used to identify the user during authentication and/or authorization, the realm is used for message routing purposes.

Proxy Agent or Proxy
- forward requests and responses,
- proxies make policy decisions relating to resource usage and provisioning. This is typically accomplished by tracking the state of NAS devices.
- proxies typically do not respond to client Requests prior to receiving a Response from the server,
- they may originate Reject messages in cases where policies are violated.
- proxies need to understand the semantics of the messages passing through them, and
- may not support all Diameter applications.

Real-time Accounting
Real-time accounting involves the processing of information on resource usage within a defined time window. Time constraints are typically imposed in order to limit financial risk.

Relay Agent or Relay
- Relays forward requests and responses based on routing-related AVPs and realm routing table entries.
- do not make policy decisions, they do not examine or alter non-routing AVPs.
- relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs,
- are capable of handling any Diameter application or message type.
- do not keep state on NAS resource usage or sessions in progress.
The last terms

Redirect Agent
- refer clients to servers and allow them to communicate directly.
- do not sit in the forwarding path → they do not alter any AVPs transiting between client and server.
- do not originate messages and
- are capable of handling any message type, although they may be configured only to redirect messages of certain types, while acting as relay or proxy agents for other types.
- do not keep state with respect to sessions or NAS resources.

Roaming Relationships
Roaming relationships include relationships between companies and ISPs, relationships among peer ISPs within a roaming consortium, and relationships between an ISP and a roaming consortium.

Security Association
A security association is an association between two endpoints in a Diameter session which allows the endpoints to communicate with integrity and confidentially, even in the presence of relays and/or proxies.

Session = a related progression of events devoted to a particular activity. Each application SHOULD provide guidelines as to when a session begins and ends. All Diameter packets with the same Session-Identifier are part of the same session.

Sub-session represents a distinct service (e.g. QoS or data characteristics) provided to a given session. These services may happen concurrently (e.g. simultaneous voice and data transfer during the same session) or serially. These changes in sessions are tracked with the Accounting-Sub-Session-Id.

Translation Agent performs protocol translation between Diameter and another AAA protocol, such as RADIUS.
Access is broken into sessions:
Diameter authorizes sessions

Client

Initial Request for Authentication/authorization: IRA
[Session-id]
whatever
[Session-id]
\vdots
\vdots
whatever
[Session-id]

Session Termination Request: STR [Session-id]

Session Termination Answer: STA [Session-id]

Server
A diameter node has a peer table

<table>
<thead>
<tr>
<th>Host identity</th>
<th>Status</th>
<th>Stat/Dyn</th>
<th>Expiration time</th>
<th>TLS enabled</th>
<th>Additional Security info</th>
</tr>
</thead>
</table>

The peer table is referenced by Realm Routing Table. The peer relationship may be dynamically established – will have an expiration time.
Diameter peer discovery helps scalability: order is as follows

- Search manually configured peer agent list
- Use SLPv2 (service location protocol)
- NAPTR query to DNS ("AAA+D2x where x=T|S, T=tcp, S=sctp") – gives the preferred SRV record, a new query gives the IP address
- query `_diameter._sctp`.realm and `_diameter._tcp`.realm, where realm is the destination realm
Realm Routing Table describes the actions of a Diameter Node

A node can act as proxy for some user connections and as a relay for others. The Routing Table is configuration information.
Redirect server helps to centralize Diameter request routing in a roaming consortium

Use Example:
Service Location Function:
SLF in 3G to locate HSS
A node must watch over its peers to achieve security

- Capability negotiation tells a node what to expect of a peer
- Authorization means taking a business risk, limited by Credit limit agreed by the peer realms.
**Diameter header is designed for max flexibility**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version=1</td>
<td>Message Length</td>
</tr>
<tr>
<td>Command Flags</td>
<td>Command-Code</td>
</tr>
<tr>
<td>Application-ID</td>
<td></td>
</tr>
<tr>
<td>Hop-by-Hop Identifier</td>
<td></td>
</tr>
<tr>
<td>End-to-End Identifier</td>
<td></td>
</tr>
</tbody>
</table>

- **AVPs**
  - **R** (equest) – if 0 = Answer
  - **P** (requestable) – if 0 msg must be locally processed
  - **E** (error) – only set in Answer msgs.
  - **T** (potentially re-transmitted message - set after failover to help remove duplicate messages

- **Application-ID**: e.g. 3GPP application
  - Normally +1 increasing number on a connection
  - Same for Request and the corresponding Answer
  - Client sets to locally unique value (4 min) even over Reboots
  - Server copies from Request to Answer
Base Diameter protocol Requests and Answers

For each Command-code
Spec contains exact possible flags, required and optional AVPs and their nr.

Applications introduce additional command-codes and their exact syntax.

Applications may extend these Messages.

Diameter node

Abort-Session-Request: ASR

Abort-Session-Answer: ASA

Accounting-Request: ACR

Accounting-Answer: ACA

Capabilities-Exchange-Request: CER

Capabilities-Exchange-Answer: CEA

Device-Watchdog-Request: DWR

Device-Watchdog-Answer: DWA

Disconnect-Peer-Request: DPR

Disconnect-Peer-Answer: DPA

Re-Auth-Request: RAR

Re-Auth-Answer: RAA

Session-Termination-Request: STR

Session-Termination-Answer: STA
Base protocol AVPs

AVPs have a common header

<table>
<thead>
<tr>
<th>AVP Code</th>
<th>VP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMPrrrrr</td>
<td>AVP Length</td>
</tr>
<tr>
<td>Vendor-ID (opt)</td>
<td></td>
</tr>
</tbody>
</table>

Data...

V-vendor-id present
M-Mandatory AVP
P-encryption for e-2-e sec

In AVPs e.g. the following items may appear:
- IPaddress
- Time
- UTF8String
- Diameter Identity = FQDN
  (fully qualified domain name)
- Diameter URI such as
  "aaa://" FQDN [port] [transport] [protocol]
  aaa://host.example.com:1813;transport=sctp; protocol=radius
- IPFilterRule such as
  action dir proto from src to dst [options], where
  action =permit|deny
  dir=in|out (in = from the terminal)
  src/dst = <address/mask> [ports]

You can specify firewall rules in Diameter.

UTF-8 is an 8-bit encoding for text (NB: ASCII is 7-bit encoding)
A diameter node operation is described as a set of state machines

- Peer state machine
- Authorization Session State Machines (4)
  - Server maintains session state: client FSM and server FSM
  - Server does not maintain session state: client FSM and server FSM
- Accounting Session State Machines
  - Client state machine
  - Server state machines: stateless and stateful
  - may be overridden by applications
Server may require 
Re-authentication/authorization

Use example: enforcing a credit limit on a user during a long telephone call.
NASREQ defines an authentication and authorization application

In Capabilities exchange peers agree to understand NASREQ commands.

NAS (PoP) initiates a new session.

HMS may challenge the user.

User has to respond to challenge

Additional rounds | Accounting, Re-Auth…

AAR and AAA have loads of AVPs!
NASREQ messages (RFC 4005)

<table>
<thead>
<tr>
<th>Command</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA-Request</td>
<td>AAR</td>
</tr>
<tr>
<td>AA-Answer</td>
<td>AAA</td>
</tr>
<tr>
<td>Re-Auth-Request</td>
<td>RAR</td>
</tr>
<tr>
<td>Re-Auth-Answer</td>
<td>RAA</td>
</tr>
<tr>
<td>Session-Termination-Request</td>
<td>STR</td>
</tr>
<tr>
<td>Session-Termination-Answer</td>
<td>STA</td>
</tr>
<tr>
<td>Abort-Session-Request</td>
<td>ASR</td>
</tr>
<tr>
<td>Abort-Session-Answer</td>
<td>ASA</td>
</tr>
<tr>
<td>Accounting-Request</td>
<td>ACR</td>
</tr>
<tr>
<td>Accounting-Answer</td>
<td>ACA</td>
</tr>
</tbody>
</table>

**EAP Application extends NASREQ and provides**

- Command-Name: Abbrev.
- Diameter-EAP-Request: DER
- Diameter-EAP-Answer: DEA
Diameter SIP Application

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Abbr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Authorization-Request</td>
<td>UAR</td>
</tr>
<tr>
<td>User-Authorization-Answer</td>
<td>UAA</td>
</tr>
<tr>
<td>Server-Assignment-Request</td>
<td>SAR</td>
</tr>
<tr>
<td>Server-Assignment-Answer</td>
<td>SAA</td>
</tr>
<tr>
<td>Location-Info-Request</td>
<td>LIR</td>
</tr>
<tr>
<td>Location-Info-Answer</td>
<td>LIA</td>
</tr>
<tr>
<td>Multimedia-Auth-Request</td>
<td>MAR</td>
</tr>
<tr>
<td>Multimedia-Auth-Answer</td>
<td>MAA</td>
</tr>
<tr>
<td>Registration-Termination-Request</td>
<td>RTR</td>
</tr>
<tr>
<td>Registration-Termination-Answer</td>
<td>RTA</td>
</tr>
<tr>
<td>Push-Profile-Request</td>
<td>PPR</td>
</tr>
<tr>
<td>Push-Profile-Answer</td>
<td>PPA</td>
</tr>
</tbody>
</table>

This application is used in 3G IMS

3GPP TS 29.228 V7.4.0 (2006-12)
IP Multimedia (IM) Subsystem Cx and Dx interfaces;
Signalling flows and message contents(Release 7)
Diameter Credit Control Application

• The Diameter CC Application provides
  – support for prepaid services
  – real time credit control for the service

• Two mandatory messages
  – CCR – Credit Control Request
  – CCA – Credit Control Answer

• The CC Server can be different from the
  rest of Diameter AAA servers
IMS has several Call Session Control Function elements

• I-CSCF = (I =interrogating) on the boundary of an IMS domain. Hides the domain and routes IMS requests to the processing CSCF elements

• S-CSCF = (S-serving) the real thing. Creates the services to a user in the domain

• P-CSCF =(P=proxy) first point of contact in the visited IMS domain. Enforces local policy on the visiting user based on roaming agreement.
3G IMS Diameter SIP Application

User-Authorization-Req: UAR
User-Authorization-Ans: UAA
Location-Info-Req: LIR
Location-Info-Ans: LIA
Cx interface runs over SCTP

Server-Assigment-Req: SAR
Server-Assigment-Ans: SAA
Multimedia-Auth-Req: MAR
Multimedia-Auth-Ans: MAA
Registration-Termination-Req: RTR
Registration-Termination-Ans: RTA
Push-Profile-Request: PPR
Push-Profile-Answer: PPA
Registration – user not registered

Source: 29228-740.doc

1. Register (SIP message)
2. Register
3. UAR
4. UAA
5. Register
6. MAR
7. MAA
8. 401 Unauthorised, RAND||AUTN
9. 401 Unauthorised
10. 401 Unauthorised
11. Register, RES
12. Register
13. UAR
14. UUA
15. Register
16. SAR
17. SAA
18. OK, CK||IK
19. OK
20. OK

S-CSCF selection
Authe Vector Selection
Authentication
Registration – user currently registered

- Registration may need to be refreshed from time to time.
- Location changes may require re-registration.
- Mobile Initiated de-registration looks exactly the same!
Many ways/reasons to de-register

1. Timer Expires
2. SAR
3. SAA
4. 200 OK
5. Notify (reg)
6. Notify (reg)
1. RTR
2. RTA
3. Notify (reg)
4. 200 OK
5. Notify (reg)
6. Notify (reg)
7. SAA
8. 200 OK

Visited Network
UA
P-CSCF

Home Network
HSS
S-CSCF

Registration timeout
Remove S-CSCF address from HSS
Administrative de-registration
Both P-CSCF and the terminal have subscribed to the reg state!
De-registration initiated by Service Platform

1. Service Control
2. De-register
3. UE Inform
4. 200 OK
5. 200 OK
6. SAR
7. SAA
8. 200 OK

Raimo Kantola – S – 2015
Mobile Terminated SIP Session Set-up is similar to MAP MT call

1. INVITE
2. LIR
3. LIA
4. INVITE

HSS knows the name (and address) of S-CSCF – no RoutingNumber is needed from ”VLR”. So there is a difference in how routing and addressing operates in GSM and in 3G IMS.

1. INVITE
2. LIR
3. LIA
4. S-CSCF Selection
5. INVITE

6. SAR
7. SAA

8. Service Control further actions

Initiation of a session to a non-registered user.

When there is a change in the user profile HSS issues Push-Profile-Request: PPR and S-CSCF answers by PPA. This transaction is unrelated to any SIP signaling.
Policy and charging control architecture in 3G

- Documents (status of 12-2007)
  - 3GPP TS 23.203 V7.5.0 - Policy and charging control architecture (Release 7)
  - 3GPP TS 29.212 V7.3.0 - Policy and Charging Control over Gx reference point (Release 7)
- Up-to release 6, COPS protocol was used
- Now a new Diameter Application
SIP Sessions require policy control

- Parties can release the “call session” but since they have obtained each others IP-addresses, they can continue sending media streams to each other!!
- How to push INVITE to B-party, if B-party does not have a permanent IP address which is most often the case!

Integration of Proxy with Firewall and NAT
Cmp Circuit and Packet Service Flow

**Circuit Switching**
- Hop by hop path
- Concent
- Thru connect
- Charging

**Packet Switching**
- Callee Discovery
- Parameters & Concent
- Media Flow
- Charging

Signaling is not needed for media flow.
Idea of Carrier Grade Service

- Service is provided by an operator or a set of operators in concert
  - If several operators involved – business agreements are in place
- Service instance is provided to one or more users: user A, user B – these users are known to the operator exactly
  - No way address or ID spoofing is allowed
- What is provided is defined clearly and the operator gives some guarantee of Quality
  - This requires that the services environment is at least somewhat predictable, 3rd parties should not be able to interfere with the service instance of A and B; No DDoS etc…

IMS strives to provide these kind of services. Internet is not carrier grade at all!
QoS – Integrated Serv. and DiffServ help resolving the QoS issue in VOIP and 3G IMS

- **Integrated Services**
  - Different treatment to different flows
  - State info stored in network, routers examine packets!!!(not good)
  - Reservation merging
  - RSVP protocol – for reservation of resources
  - Idea was the QoS would be provided per user – this does not scale

- **DiffServ**
  - Defines a small nrof traffic classes with different priority levels
  - Packets tagged with level tags at the beginning(ingress)
  - Routers just examine tags (diffServ code points)
  - Better scaling – QoS for a class of flows
  - Requires policy management: e.g. which packets to assign to which class.
  - Managing class weights remains an issue = if any class has too many packets, class QoS is poor irrespective of how the class is named.
A Solution for QoS

- Best Effort Service for greedy and even malevolent users.
- Real-time or background traffic classification.
  - It is a good idea to let the network do the classification based on the "nature" of the traffic flow. If flows of different burstiness properties are put to a single class, quality assurance is poor.
- Policy-based management of allocated bandwidth at the edge.
  - Policy enforcement at the edge is possible, because each device handles only a limited set of users.
  - This is where users interfere with each other (e.g., one greedy p2p user blocks the traffic of all other users of a shared link at the edge).
- Adaptive scheduling for managing class weights and thus bandwidth allocations at least in edge (access) routers.
- Statistical multiplexing in the Core (= ordinary BE Service).
  - Makes the core simpler and thus less expensive. At the speeds, the core needs to transfer packets, the nodes do not have time per packet to more than just the simplest BE service.
Scope of Policy and Charging Control in IMS

• Diameter is used to create a harmonized solution for
  ➢ Flow Based Charging, including charging control and online credit control;
  ➢ Policy control (e.g. gating control, QoS control, etc.).
• Flow based charging control gives a fine granularity control over charging for service flows
• Policy control allows assigning QoS, Firewall rules etc per service
Policy and charging control are about Authorization of user services

- Authorization takes place on the level of service and packet flows.
  - So defining exactly what is being authorized is a complex issue
  - When a service is allowed (=authorized), this may incur charges, information for charging purposes needs to be collected. For prepaid or credit limited customers, permission may be with a condition (until credit limit) and that condition needs to be enforced.
- The idea is that even data services are charged based on usage or on transactions (e.g. an MM message costs xy cents but the bytes are not counted towards volume based charges for other data services such as Internet access)
- How useful this is going to be remains to be seen. The nature of best effort data services is that it is economically efficient to charge a flat rate independent of usage (look at the history of Internet charging – it confirms this theoretic statement). One should also notice that this usage based charging functionality is not cheap – cost of usage based charging for an operator is high.
- Experience shows that when flat rate for data services is offered, traffic and usage grow quickly. Adoption is 10 x as compared to volume charging. This means that it may be better for the operator to introduce flat rate but keep it sufficiently high rather than insist on volume charging
Key terms for PCC – policy and charging control

**Packet flow:** a sequence of packets with identical parameters such as IP-protocol, source-IP address, source port, destination IP address, destination port, etc

**Service data flow:** An aggregate set of packet flows.

**Service data flow filter:** A set of IP header parameter values/ranges used to identify one or more of the packet flows constituting a service data flow. A service data flow filter of a PCC rule that is predefined in the PCEF may use parameters that extend the packet inspection beyond the IP 5-tuple (s-IP,d-IP, s-port, d-port, protocol).

**Service data flow template:** The set of service data flow filters in a PCC rule, required for defining a service data flow.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FBC</td>
<td>Flow Based Charging</td>
</tr>
<tr>
<td>IP-CAN</td>
<td>IP Connectivity Access Network</td>
</tr>
<tr>
<td>OFCS</td>
<td>Offline Charging System</td>
</tr>
<tr>
<td>OCS</td>
<td>Online Charging System</td>
</tr>
<tr>
<td>PCC</td>
<td>Policy and Charging Control</td>
</tr>
<tr>
<td>PCEF</td>
<td>Policy and Charging Enforcement Function</td>
</tr>
<tr>
<td>PCRF</td>
<td>Policy and Charging Rules Function</td>
</tr>
<tr>
<td>PDF</td>
<td>Policy Decision Function</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>SBLP</td>
<td>Service Based Local Policy</td>
</tr>
<tr>
<td>SPR</td>
<td>Subscription Profile Repository</td>
</tr>
</tbody>
</table>
Relationship of service data flow, packet flow, service data flow template and service data flow filter is implemented at PCEF
PCC requirements

The PCC architecture discards packets that don't match any service data flow filter of the active PCC rules. It is possible for the operator to define PCC rules, with wild-carded service data flow filters, to allow for the passage and charging for packets that do not match any service data flow filter of any other active PCC rules.

The PCC architecture allows the charging control to be applied on a per service data flow basis, independent of the policy control.

The PCC architecture supports a binding method that allows the unique association between service data flows and their IP-CAN bearer.

A single service data flow template is used to detect a service data flow, for the purpose of both policy control and flow based charging.

A PCC rule may be predefined or dynamically provisioned at establishment and during the lifetime of an IP-CAN session. The latter is referred to as a dynamic PCC rule.

**Background: A mobile device based Firewall does not make sense!**
PCC elements

SPR example – HSS
AF example P-CSCF
PCEF example – GGSN
or PDG for WLAN access

Gx supports
- Initialisation and maintenance of connection (IP-CAN session);
- Request for PCC decision from PCEF to PCRF;
- Provision of PCC decision from PCRF to PCEF;
- Negotiation of IP-CAN bearer establishment mode (UE only or NW only);
- Termination of connection (IP-CAN session).

PCC usage in the visited network is based on proxying of Gx messages between the V-PCEF and the H-PCRF by the V-PCRF.

Raimo Kantola – S – 2015
IP-CAN session establishment for PCC

1. Establish IP-CAN Bearer Request
2. Indication of IP-CAN session establishment
3. Profile Request
4. Profile Response
5. Policy Decision
6. Acknowledge IP-CAN session establishment
7. Credit Request
8. Credit Response
9. IP-CAN Bearer Signaling
10. Establish IP-CAN Bearer Response

This is a logical Information flow that is used as a basis for protocol design
IP-CAN session termination for PCC

1. Remove IP-CAN Bearer Request

2. Indication of IP-CAN Session Termination

3. Identify what Policy and Charging Rules are affected.

4. Remove all Policy and Charging Rules

5. Notify loss of transmission.


7. Acknowledge IP-CAN Session Termination

8. Credit Final Report

9. Credit Acknowledge

10. Remove IP-CAN Bearer Request

11. Cancel Subscribed Notification Request

12. Cancel Subscribed Notification Response

Also GW(PCEF) Initiated IP-CAN Session Termination is supported (not shown)
Proxying rules to visited network
Policy and Charging Control over Gx interface

GW: PCEF

PCRF

If RAR has no rules, PCEF will send CCR

Re-Auth Request

Re-Auth Answer

CC Request

CC Answer

RAR and RAA extended from The Base Protocol allow installing and managing the state of rules in PCEF.

CCR and CCA extended from CC Application

3GPP TS 29.212 V8.3.0 (2009-03)
Use of Diameter in 3G IMS

- 3GPP uses the Diameter SIP Application to handle roaming.
- Cx and Dx interfaces are the same. The difference is that Dx points to a Diameter Redirect Agent and Cx to a Diameter Server (HSS).
- ”Cellular” Location management maps into MAP operations in SGSN +GGSN+ Registration/De-Registration in SIP terms maps to Authorization-Request/-Answer in Diameter + S-CSCF obtaining Subcr data = Diameter SAR/SAA etc.
  - User-Location-Query is used to obtain S-CSCF identity
  - I-CSCF can use Diameter Redirect capability in SLF (Dx interface):
    Server-Location-Function to select S-CSCF/user-identity
  - I-CSCF is stateless, so SLF has to be used for every query
  - S-CSCF is stateful and will cache HSS address for the session.
- There is also a Diameter Application for AS to HSS interface (Sh Interface). This is vendor specific where 3GPP is the vendor.
- The newest usage is for harmonized Policy and Charging Control (Gx Application in Diameter = Vendor/3GPP specific application)

AS – Application Server
Authentication and charging

• For an operator, the motivation to authenticate reliably is linked with charging
  – Usage based charging requires knowledge of whom to send the bill and the amount of usage
  – Transaction based charging – the same thing
• If the only method to collect money is a flat rate monthly tariff – why bother authenticating individual users and create additional cost for the operator for no gain?
• Claim: for an operator to authenticate users reliably – the only 2 motivations are mobile service and usage based billing
Summary

• IP telephony requires many supporting protocols.
• Many IETF protocols overlap with GSM protocols (e.g. Diameter with MAP) in terms of functionality
  – This overlap was created because of the move from CS to PS services
  – Supported data differs
• Diameter follows a client-agent-server model
• Diameter has Base-protocol + Diameter Apps structure; each App introduces a new use case for Diameter
• Diameter is central for providing carrier grade control to services provisioning