Architectures and Supporting Protocols for VOIP/3G

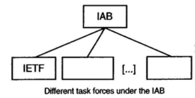
IETF at work
NGN and 3G Network Elements
Numbering and Naming (ENUM)
Session Description Protocol (SDP)
Media Gateway Control (Megaco/MGCP)
Diameter

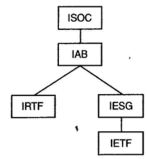
Agenda

- IETF
- Networking framework – 3G, wireline
- Why control what users can do?
  - Justification for 3G IMS architecture
- 3G terminal
- ENUM – naming and addressing

IETF

- IETF toolkit
  - bottom-up approach *("one problem – one protocol")*
  - Protocols should be simple, reusable, scalable, robust



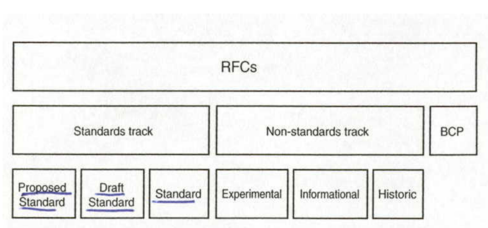


IESG
Internet Engineering
Steering Group

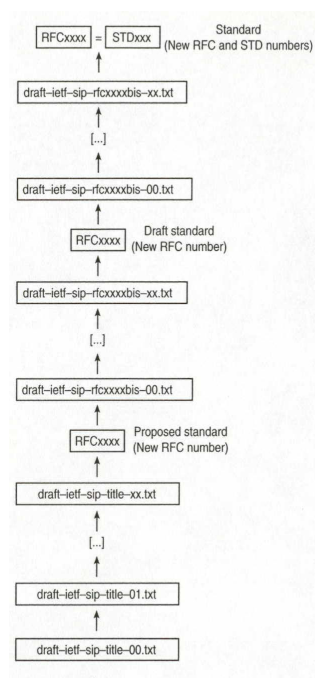
Application Area	General Area	Internet Area	O&M Area	Routing Area	Security Area	Sub-IP Area	Transport Area
… simple			aaa dnsop	bgmp idmr idr manet mpls ospf	ipsec smime tls …		avt enum iptel mmusic sip sipping sigtran

- ➢ over 100 active WGs
- ➢ here are some of them

IETF specifications



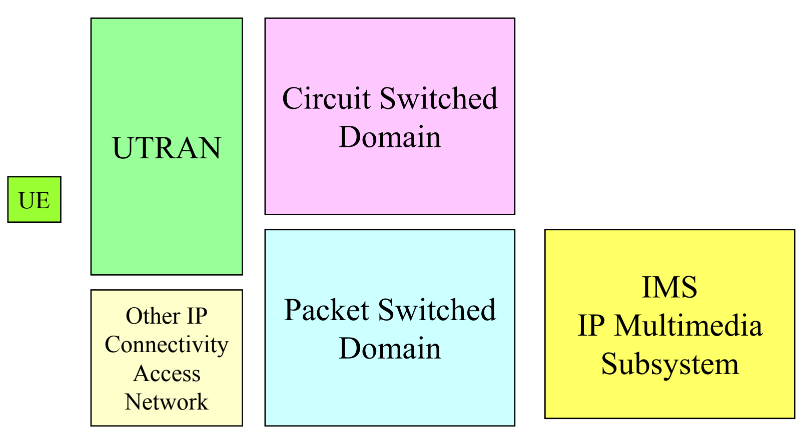
•Every standard follows the route Proposed standard-> Draft Standard-> Standard



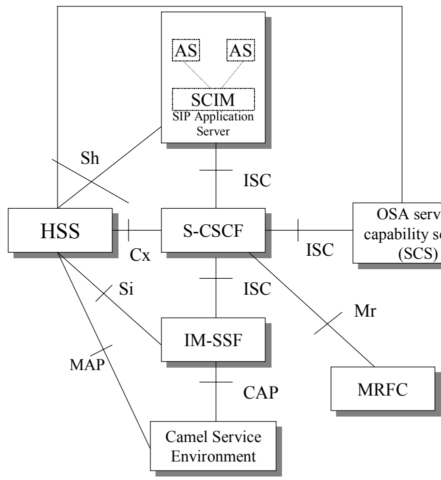
ETSI, etc have delegated the 3G standardisation work to 3GPP

- 3GPP – is the 3G Partnership Project
- this gives a key role to vendors
- site: www.3gpp.org has all their documents!
- The idea is that ETSI etc will rubberstamp 3G documents as standards.

3G is composed of many Subsystems



3G IP Multimedia core network Subsystem (3G IMS)



AS – Application Server
CAP - Camel Application Part
IM-SSF – IP Multimedia Service Switching Function
ISC – IP Multimedia Service Control

S-CSCF – Serving Call Session Control Function
HSS – Home Subscriber Server

MAP - Mobile Application Part
MRFC - Media Resource Function Controller
OSA – Open Service Access
SCIM – Service Capability Interaction Manager
SCS – Service Capability Server

Alternative to IMS?

- With a 3G device a user can access the open Internet and use any services that are available on the Internet: www, e-mail, conferencing, VOIP etc.
  - QoS is the Best Effort QoS of regular Internet
  - Charging can be either volume based or flat rate.
  - Flat rate can lead to overuse of the cellular capacity and poor QoS
- Take the CS domain signaling and call control, map TDM trunks to IP ”connections” → retains the existing CS –domain services control and architecture, replace TDM transport by IP (this is called UMA – universal mobile access)

Motivation for IMS

- IMS = Integration of cellular and Internet worlds. Why, when a user already can take an Internet connection from a cellular device and use all Internet Services?
  - Controlled QoS for Interactive voice and video
  - Proper Charging for QoS and Freedom of charging based on any business model for the services
  - Integration of services on a single packet platform: access to all aspects of sessions from any service.
  - Ease of interworking with Internet Services(?)

Q: Is this enough?
Q: Why should operators switch from circuit based voice services to IMS based voice services in 3G?

IMS Objectives

Support for the following:

1. establishing IP Multimedia Sessions
2. negotiation of QoS
3. interworking with the Internet and the CSN
4. roaming
5. strong conrol by the operator with respect to the services delivered to the end user
6. rapid service creation without requiring strandardization
7. access independence (starting from release 6)

Next Generation Network (NGN) is the ETSI effort to harmonize packet telephony

The network architecture is layered in a much more strict sense than in case of CSN

Services
- IP Applications
- Virtual Home Environment
- Open Service Architecture

Control

Network Specific
- call control
- session management
- mobility management

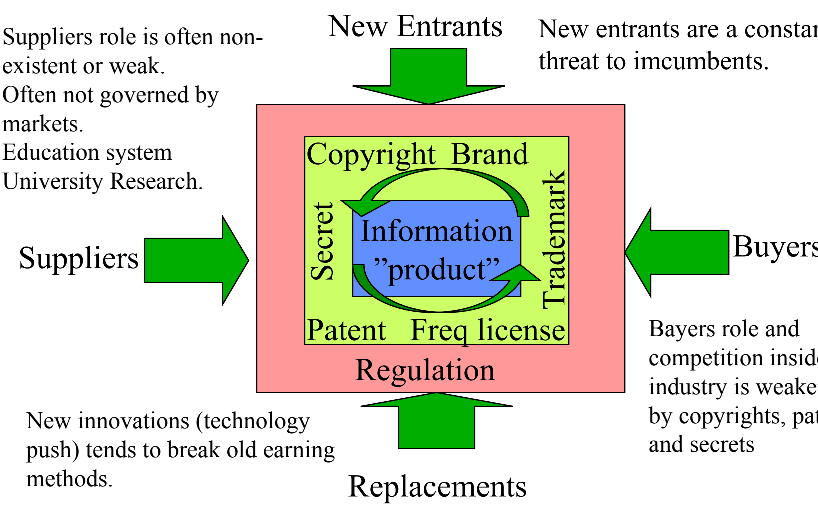
Switching
- Transcoding at the edge
- Switching
- Routing

In practice this means that ETSI has decided to adopt the IMS framework as a basis for services over all kinds of networks wireline or wireless.

Competition in Information Economy – Porter's Five Forces model

Suppliers role is often non-existent or weak.
Often not governed by markets.
Education system
University Research.

New entrants are a constant threat to imcumbents.



Bayers role and competition inside the industry is weakened by copyrights, patents and secrets

New innovations (technology push) tends to break old earning methods.

Competition inside an Industry

- Information creation often happens inside companies
- Competition is limited by
  - Copyright: a product is available from a single source
  - Patent: a problem can often be solved in many ways. A Group of patents, often cross-licenced by key players, may create a new market creating entry barriers for new entrants
  - Frequency licenses. E.g. Cellular.
- The key question is granularity: how big an area is coverned by the monopoly right. The bigger the area, the more inefficiencies it can contain.

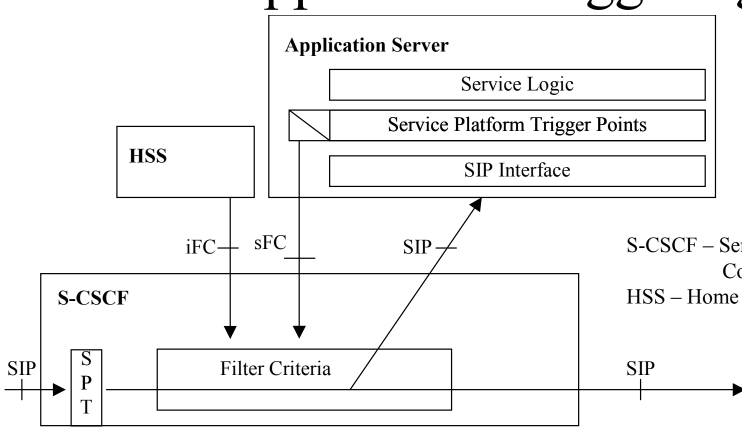
Price = 0

- Information is non-depletable and non-excludable: you give it to somebody, you still have it and as many times as you like
  - Under free market conditions, supply is infinite
  - Copy cost approaches zero
  - According to law of demand and supply, price approaches marginal cost → price of information approaches zero.
- Free market does not support a price that makes creation of information sustainable economically.
- Copyrights, patents, (frequency) licenses and secrets are fundamental for earning money using information.

Examples of information goods

- Internet BE service under over-provisioning is non-depletable
  - Because ISP does not promise any quality
- → Overprovisioned BE networks – economically efficient prices = flat rate
- Difficult to recover investments and make a margin → desire for control by operators
- In the long run, the mentality of free Internet service will lead to consolidation of operators and creation of new monopolies → there is no answer that would be best for all times.

3G Application Triggering



S-CSCF – Serving Call Session Control Function
HSS – Home Subscriber Server

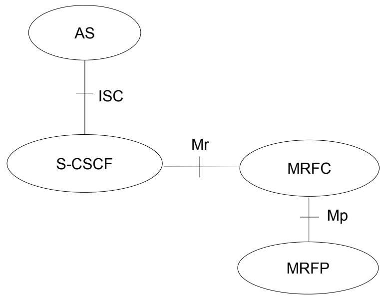
iFC – Initial Filter Criteria
sFC – Subsequent Filter Criteria
SPT – Service Point Trigger

Service processing can be delegated to Application Servers with a fine grained control

sFC is considered historical (obsolete)

The result is the same as in IN: for low penetration services, only one or a few servers need to be upgraded instead of upgrading all CSCF network elements.

Media processing in 3G



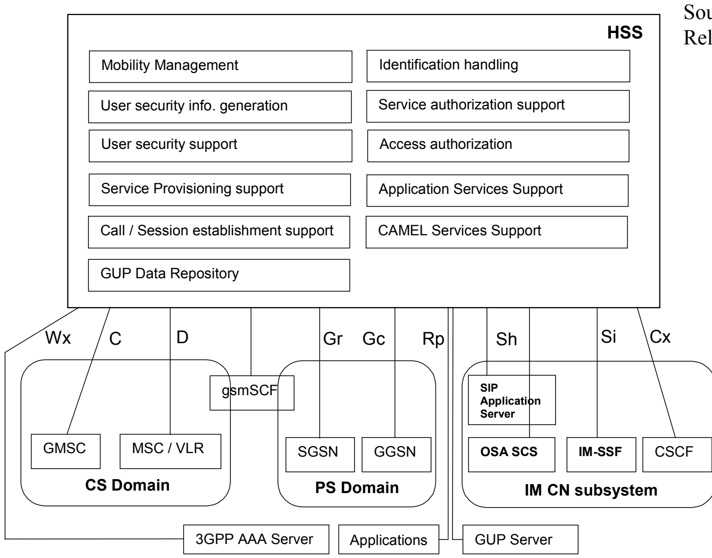
MRFC - Media Resource Function Controller
MRFP – Media Resource Function Processor

MRFC likely to have a general purpose processor,
MRFP has many DSPs – digital signal processors.

All this takes place in the IP domain.
Examples:
- transcoding Wideband AMR/ Narrowband AMR codec
- Multiparty conference media processing

In practice it is convenient to implement MRFP in the same device as the Media Gateway between CS/PS domains

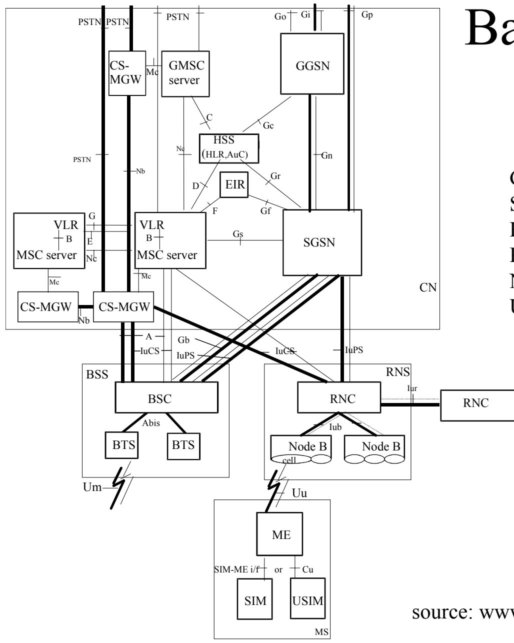
The role of HSS



Source: 23002-700.doc Release 7

GUP –Generic User Profile

Basic Configuration of a PLMN



GGSN – Gateway GPRS Support Node
SGSN – Serving GPRS Support Node
HSS – Home Subscriber Server
RNC – Radio Network Controller
Node B = 3G base station
USIM – UMTS Subscriber Identity Module

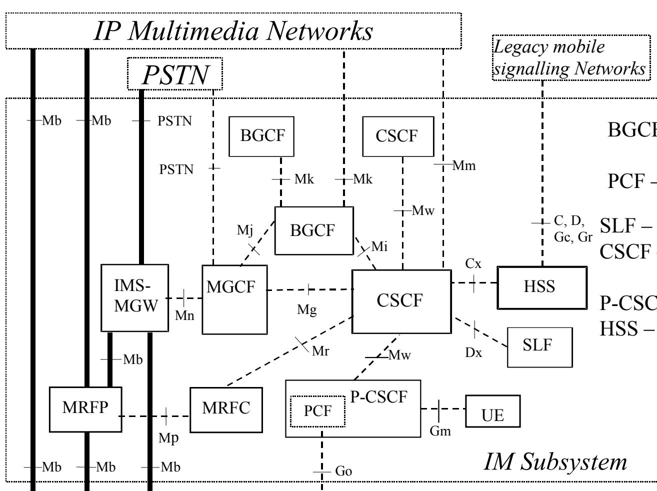
On CS side breakdown of MSC to Media Gateway and MSC server.

3G and GSM/GPRS are based on the same packet core elements.

source: www.3gpp.org/specs/archive/23002-580

The IP Multimedia Subsystem

sits on top of the Packet Core

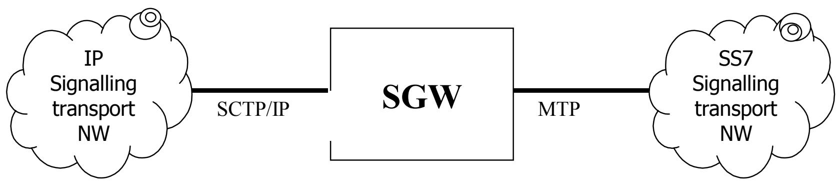


BGCF – Breakout Gateway Control Function
PCF – Policy Control Function

SLF – Service Location Function
CSCF – Call Session Control Function
P-CSCF – Proxy CSCF
HSS – Home Subscriber Server

source: www.3gpp.org/specs/archive/23002-580

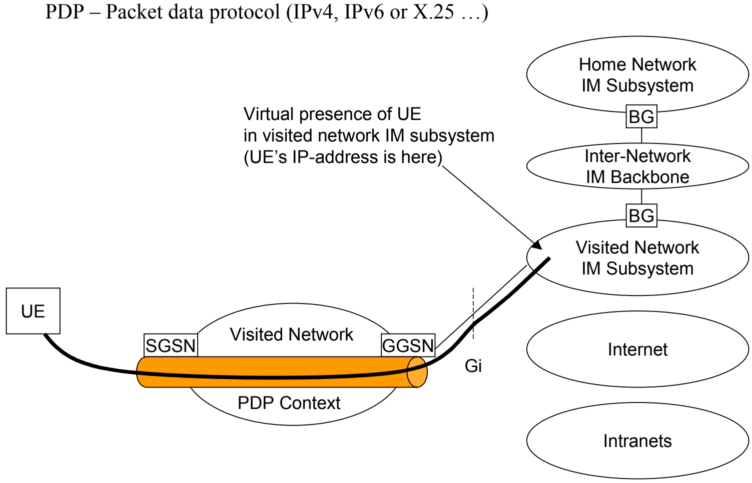
Signaling Gateway maps SS7 MTP to SCTP/IP transport



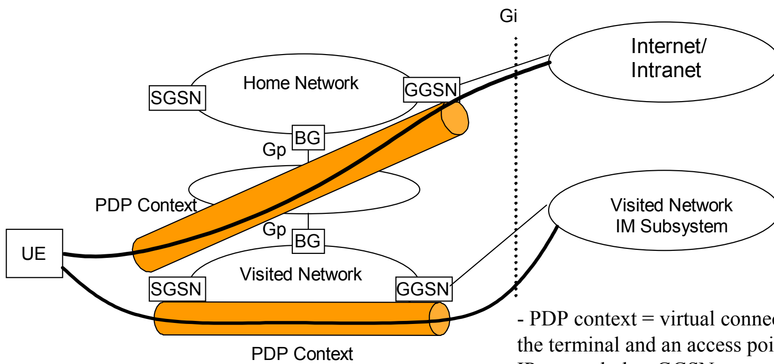
This allows to transfer signaling and service processing responsibility to IP based environment.
NB: The call control protocol on top may be e.g. ISUP on both interfaces, just the message transport is between MTP and IP

UE has a tunnel to visited IMS

PDP – Packet data protocol (IPv4, IPv6 or X.25 …)



3G UE can use several services at the same time

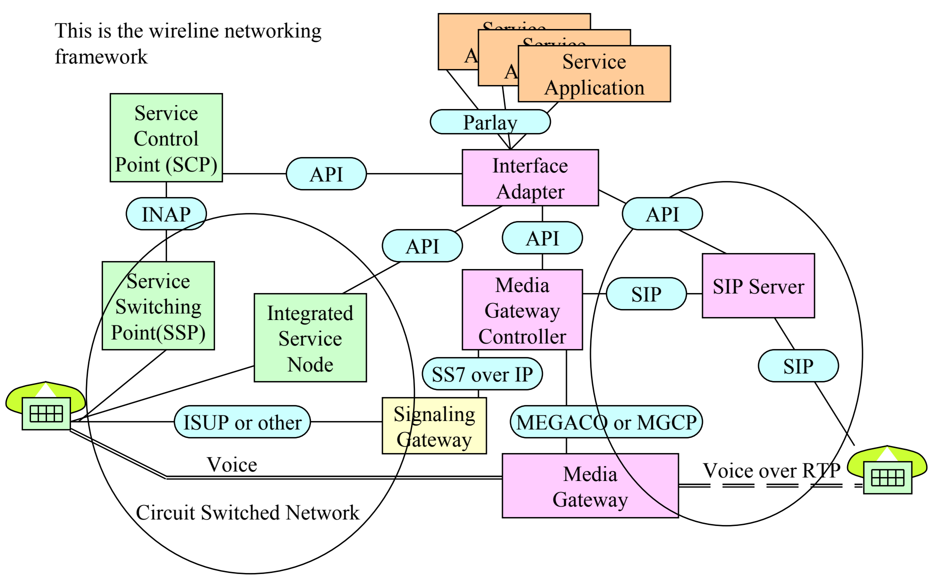


- PDP context = virtual connection between the terminal and an access point to an IP network thru GGSN
- Assigns an IP address for the terminal

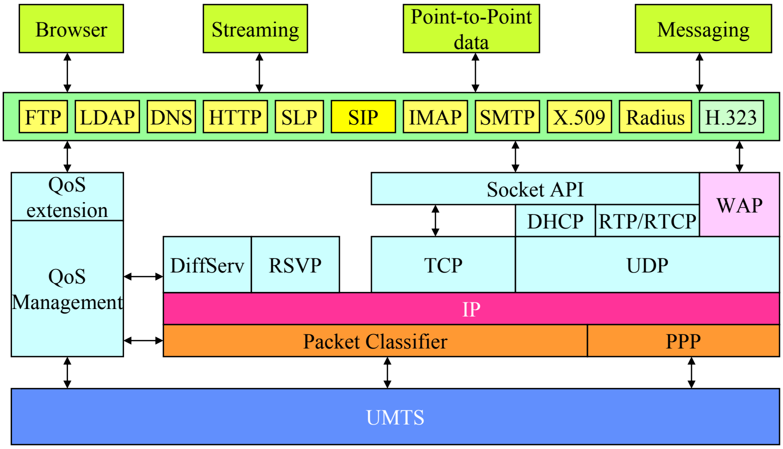
For mobile office applications Intranet connectivity at this level is not popular. Instead IP VPNs are used.

ETSI SoftSwitch Architecture for NGN

This is the wireline networking framework

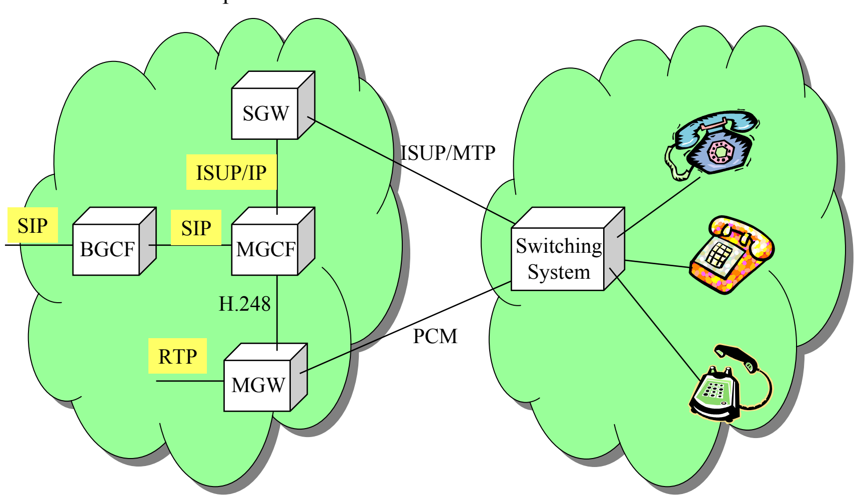


The UMTS terminal functional model

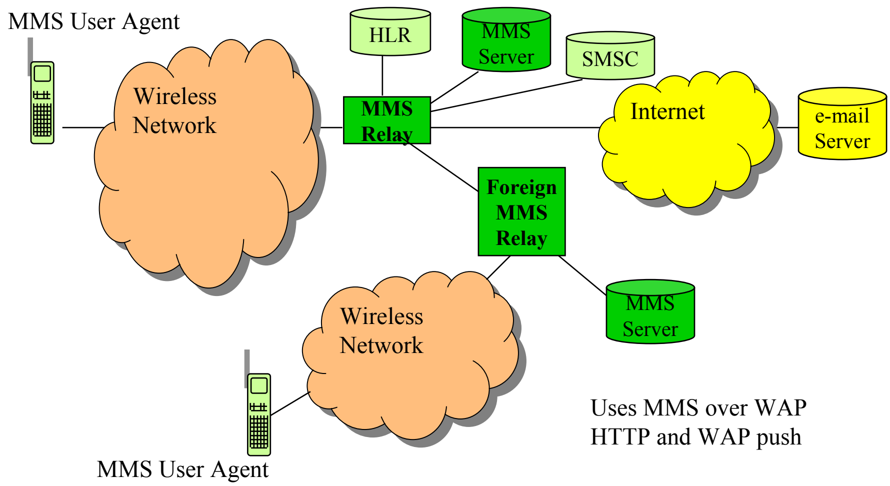


IMS Interworking with the PSTN

- IMS terminals must support CSN services due to Emergency Call requirements, so PSTN interworking can occur thru the CS domain. However, IMS Interworking with PSTN is also possible.



The GPRS and 3G networks implement the Multimedia Messaging Service



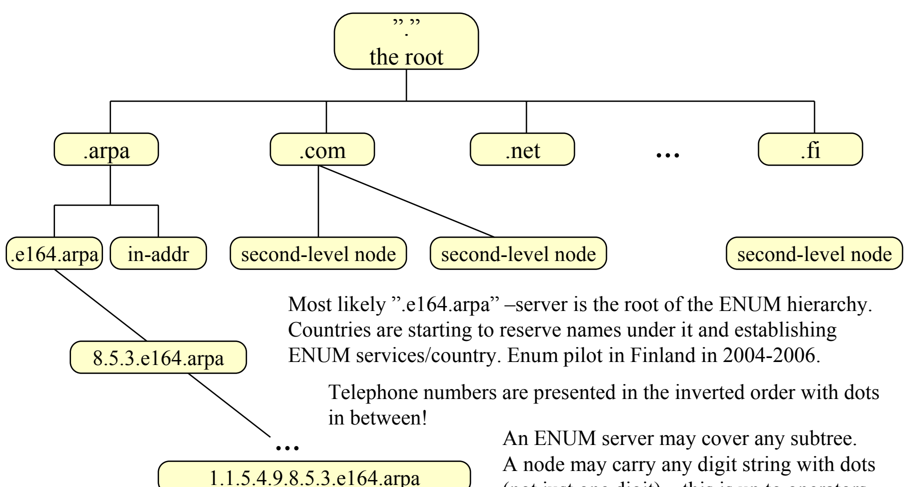
Supporting protocols for IP telephony – wired and wireless

- ENUM – addressing and naming
- Gateway control - Megaco
- Session description – SDP
- AAA - Diameter

Naming and Addressing in NGN and 3G IMS vs. Telephone numbering

- A **Name identifies** a domain, a user or a service. An **address points to** a user or to an interface or to an inlet/outlet in a network.
- Internet heavily relies on the Domain Name System (DNS) to translate names to addresses. The specs of using DNS for Telephony names and addresses is called ENUM – tElephone-NUmber-Mapping.
- ENUM was originally meant for mapping IP telehone numbers (e.g. 3G IMS phonenumbers) to logical names (and IP addresses).
- With Naming and Addressing, at the same time we need to solve the problem of Gateway (CSN/IP) location and Number Portability across the technology boundary.

ENUM uses DNS to store telephone numbers



Most likely ”.e164.arpa” –server is the root of the ENUM hierarchy. Countries are starting to reserve names under it and establishing ENUM services/country. Enum pilot in Finland in 2004-2006.

Telephone numbers are presented in the inverted order with dots in between!

An ENUM server may cover any subtree. A node may carry any digit string with dots (not just one digit) – this is up to operators.

ENUM introduces NAPTR records

RFC 2915 - The Naming Authority Pointer (NAPTR) DNS Resource Record (Sep 2000)

NAPTR – Naming Authority PoinTeR = Record in DNS containing an URI.

E.g. IN NAPTR 10 10 ”u” ”sip+E2U” ”!^.*$!sip:raimo.kantola@sip.elisa.com!”.

Internet

Record type

Order and Pref

expect uri

SIP, E.164 to URI

The URI itself! Can be modified by Regular expression

NAPTR format is: Domain TTL Class Type Order Preference Flags Service Regexp Replacement

Domain=first well known key e.g. <something>.uri.arpa
TTL=Time-To-Live – validity time of the record (time to cache)
Class=IN=Internet
Type=NAPTR=35
Order=low nrs are processed before high, once target found, stop (excepting flags)
Pref=if same order value, all with diff pref can be processed, take lowest first.
Flags=“S”-next lookup for SRV record, “A”-next lookup for A, AAAA or A6 record, “U” – the reminder has an URI+this is the last record, P –protocol specific processing
Service=protocol-name + resolver, resolver is used to resolve the result of regexp
Regexp=replacement-rule for whatever querier is holding.
Replacement=a fully qualified domain name to query next for NAPTR, SRV or address records (“S”, “A”)

Example from RFC 2915

In order to convert the phone number to a domain name for the first iteration all characters other than digits are removed from the telephone number, the entire number is inverted, periods are put between each digit and the string ".e164.arpa" is put on the left-hand side. For example, the E.164 phone number "+1-770-555-1212" converted to a domain-name it would be "2.1.2.1.5.5.5.0.7.7.1.e164.arpa."

For this example telephone number we might get back the following NAPTR records:

```
$ORIGIN 2.1.2.1.5.5.5.0.7.7.1.e164.arpa.
 IN NAPTR 100 10 "u" "sip+E2U"  "!^.*$!sip:information@tele2.se!"     .
 IN NAPTR 102 10 "u" "mailto+E2U" "!^.*$!mailto:information@tele2.se!"  .
```

This application uses the same 'u' flag as the URI Resolution application. This flag states that the Rule is terminal and that the output is a URI which contains the information needed to contact that telephone service. ENUM uses the Service field by defining the 'E2U' service. The example above states that the available protocols used to access that telephone's service are either the Session Initiation Protocol or SMTP mail.

A possible ENUM hierarchy

Tier 1 maps a number of a number block to ENUM op, Tier 2 gives the NATPR records.
(this is the planned deployment model in Finland)

Tier 0

```
$ORIGIN e164.arpa.
    1 IN NS att_enum.com.
  6.4 IN NS sweden_enum.se.
8.5.3 IN NS ficora_enum.fi.
```

358 is delegated to ficora_enum

---

ficora_enum.fi
8.5.3.e164.arpa

Tier 1

```
$ORIGIN 4.9.8.5.3.e164.arpa.
5 IN NS enum.elisa.fi.
6 IN NS enum.elisa.fi.
```

Elisa is chosen as the ENUM operator for HUT numbers 09-45….,
From Oct 2006 will be run by Ficora

---

enum.elisa.fi

Tier 2

```
$ORIGIN 1.7.4.2.1.5.4.9.8.5.3.e164.arpa.
IN NAPTR 10 10 ”u” ”sip+E2U”  ”!^.*$sip:raimo.kantola@sip.netlab.hut.fi!”.
```

My office phone number is mapped to a (non-existing at the moment) SIP server operated by the NETLAB

Tier 3 Corporate numbering schemas…

In Finnish ENUM pilot until oct-2006 only Tier 1 and Tier 2 present!

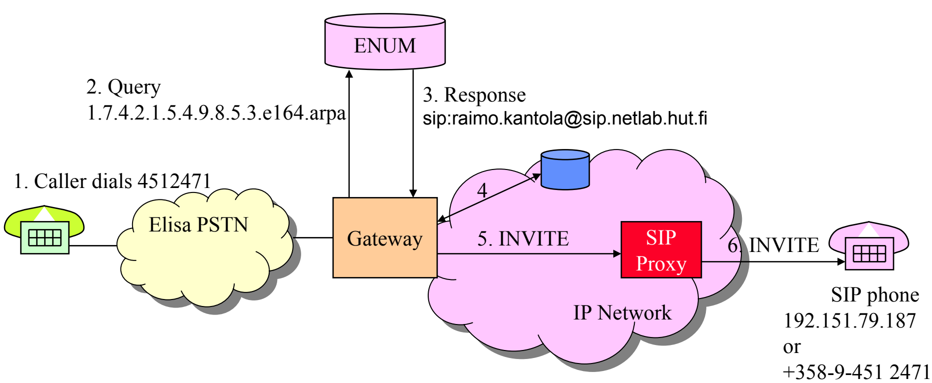
ENUM use and future

- Since DNS is used by everybody, ENUM is a likely surviver, policy routing etc additions may emerge
- Due to Number Portability, the Provision of ENUM service and the provision of VOIP service to end-customers are two independent services.
  - User may need to select the Numbering service provider separately from the VOIP service provider.
- ENUM does not support secret telephone numbers

Use of ENUM in 3G IMS

- If the callee is identified by tel URL (tel: +358-59-345-897), the originating S-CSCF tries to map this to a SIP URI using a NAPTR query to ENUM
  - successful if the target is a VOIP number
  - → if call is made from IMS to GSM, we first try to find the destination in an IP network. This may take a while because the query escalates up in the DNS hierarchy.
- If no mapping is found, it is assumed that the target is a PSTN or any other CSN number and the call signaling is routed to a BGCF (Breakout Gateway Control Function) that is specialised at routing based on telephone numbers.

Call from PSTN to a SIP phone



4 - sip:raimo.kantola@sip.netlab.hut.fi is translated to an IP address of the SIP proxy serving the number by another DNS query that returns an address record.

ENUM issues and problems

- Long chain of DNS servers results in low reliability
- Secret telephone numbers seem to require two ENUM systems: the ”Operator ENUM” with no direct access by users and ”user ENUM”.
- Result is always the same for a number irrespective of from where the call is originating in a domain →Non-optimal routing.
- Number Portability accross technology boundary would require changes in PSTN (link between IN and ENUM)
- Using ENUM for calls from PSTN is difficult because of overlap sending: non-complete numbers are not described in ENUM records (leads to many queries with result: Not Found).
- Management of numbering data. DNS mgt tools are not optimal.
- Security (DNSSec under development…?)
- Nicklas Beijar of Netlab suggests solutions to some of the above problems in his Lic thesis 2004.
- ENUM pilot in Finland until 1.6.2005 now unofficially, from Oct 2006 commercial operation says Klaus Nieminen of Ficora.

IP Telephony Research in the Networking Laboratory

- Technology evaluation
  – Delay measurements breakdown (1997…)
  – SIP call waiting
- Numbering and Routing Information Interoperability with ISDN
  – TRIP (Telephony Routing over IP) and ENUM protocols
  – CTRIP (Circuit TRIP) protocol proposed
  – Database (mySQL) solution to Number Portability (Antti Paju)
  – Nicklas Beijar’s Lic thesis (Spring 2004) on alternative solutions for NP

SDP: Session Description Protocol

- SDP was initially designed for Mbone. Mbone was/is a multicast overlay network on the Internet
- Used to describe sessions (to link the session with media tools)
- Describes conference/session addresses and ports + other parameters needed by RTP, RTSP and other media tools
- SDP is carried by SIP, SAP: Session Announcement Protocol etc.

Multicast

- Several parties involved
  - IPv4 Multicast from 224.0.0.0 – 239.255.255.255
- Saves bandwidth cmp to *n* times p2p connection
- Entity that is sending does not have to know all the participants
- Multicast Routing protocols
  - Dense Mode (shortest-path tree per sender)
  - Sparse Mode (shared tree used by all sources)
- IGMP (Internet Group Management Protocol)
  - For hosts that want to become part of a multicast group
- Mbone – part of Internet that supported multicast
- RTP – transport of real-time data such as voice or video
  - Sequence number, timestamps
- RTCP – controls RTP transport (every RTP session has a parallel RTCP session.)
- Has its direct use as a service in corporate networks and as a service enabler in public networks.

SDP can describe

- Session name and purpose
- Time(s) the session is active
  - start, stop time, repetition (relevant for conferences)
- The media comprising the session
  - video, audio, etc
  - transport protocol: RTP, UDP, IP, H.320 etc
- Parameters to receive media: addresses, ports, formats etc.
  - H.261 video, MPEG video, PCMU law audio, AMR audio
- Approximate bandwidth needed for the session
- Contact info for person responsible

SDP info is <type>=<value> in strict order

<type> is a single, case sensitive character.
<value> is a text string or a nrof fields delimited by a single white space char.
SDP has one session level description and optionally *n* media descriptions.

Session description
- v= (protocol version)
- o= (owner/creator and session identifier).
- s= (session name)
- i=* (session information)
- u=* (URI of description)
- e=* (email address)
- p=* (phone number)
- c=* (connection information - not required if included in all media)
- b=* (bandwidth information)

* = optional

One or more time descriptions (see below)
- z=* (time zone adjustments)
- k=* (encryption key)
- a=* (zero or more session attribute lines)

Zero or more media descriptions (see below)

SDP items continued

Time description
- t= (time the session is active)
- r=* (zero or more repeat times)

Media description
- m= (media name and transport address)
- i=* (media title)
- c=* (connection information - optional if included at session-level)
- b=* (bandwidth information)
- k=* (encryption key)
- a=* (zero or more media attribute lines)

3G document refer to a newer SDP- draft from may 2002.

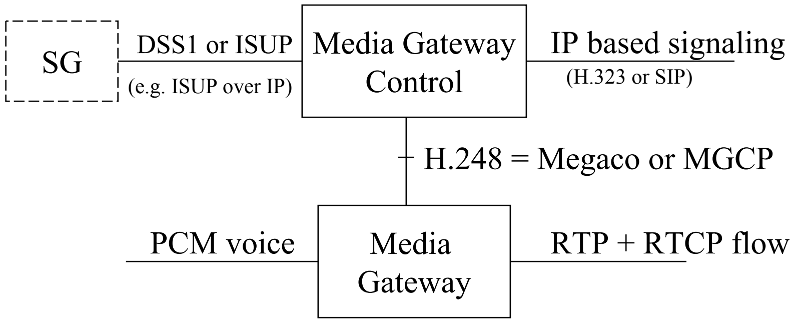
Some SDP documents:

RFC 2327: SDP Session Description Protocol (dated 1998), now Proposed Std
RFC 3407: SDP Simple Capability Declaration
RFC 3264 - An Offer/Answer Model with Session Description Protocol (SDP)
RFC 3266 - Support for IPv6 in Session Description Protocol (SDP)
RFC 3556 SDP Bandwidth modifiers for RTCP

Megaco - Media Gateway Control protocol controls Media Gateways and Media Processing

- MGCP was promoted by Cablelabs = US CATV R&D body as the CATV Telephony standard
- ITU-T has its own variant called Megaco=H.248
- Megaco, MGCP are master-slave protocols by which media gateways can be configured e.g to services - in case of residential media gateway, MGCP becomes a subscriber signalling system

Gateway decomposition

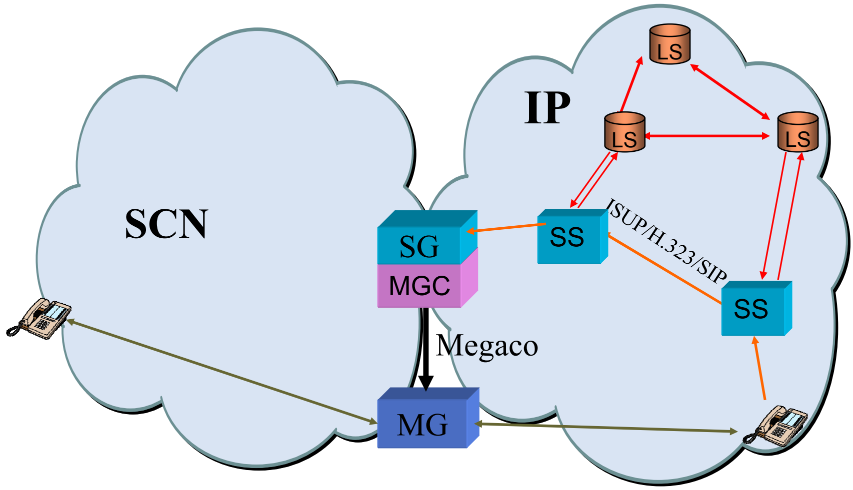


MG - Trunk gateway, residential gateway etc.
Many MGs can be controlled by one MGC, MGCs can be a mated pair --> higher availability performance.

Megaco functions

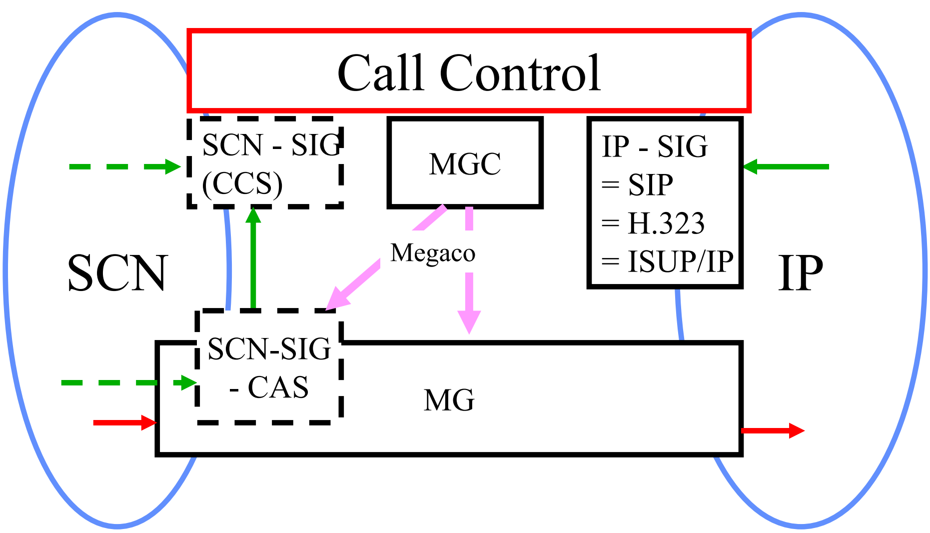
- Establishment of connections between terminations
  - PCM –timeslots for voice
  - ephemeral packet stream terminations: IP-address + source + dest UDP-port number
- Release of connections
- Separation of signaling from voice band in case of CAS and analogue subsc signaling

Current Architecture



SG - Signalling Gateway, MGC - Media Gateway Controller
MG - Media Gateway, SS = Signaling Server, LS = Location Server

Gateway decomposed



Megaco for Residential Gateways

- Residential MG processes analogue subscriber signaling – inband, can not be separated from media plane
- Controller gives a dialling pattern for MG to look for. When detected, report to MGC. MGC gives a new pattern to look for. Etc.
- Real time processing of signals is delegated to the residential gateway, while MGC retains overall control over what is happening and what is the interpretation of the patterns.

NAT Traversal

RFC 3489 Title: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
Author(s): J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy
Status: Standards Track Date: March 2003
See also: http://corp.deltathree.com/technology/nattraversalinsip.pdf
Traversal Using Relay NAT (TURN) draft-rosenberg-midcom-turn-03

- The NAT story that was here is OBSOLETE
- Look at Gonzalo's slides!

Internet is an A-subscriber's Network! B-subscribers are not connected!

Documents of BEHAVE

Internet-Drafts:
Simple Traversal Underneath Network Address Translators (NAT) (STUN) (152616 bytes)
Network Address Port Translator (NAPT) Any-Source Multicast Requirement (14242 bytes)
NAT Behavioral Requirements for TCP (47849 bytes)
Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN) (124751 bytes)
Extension to the Simple Traversal Underneath NAT (STUN) Relay Usage for IPv4/IPv6 Transition (15352 bytes)
NAT Behavioral Requirements for ICMP protocol (48330 bytes)
State of Peer-to-Peer(P2P) Communication Across Network Address Translators(NATs) (81765 bytes)

Request For Comments:
Network Address Translation (NAT) Behavioral Requirements for Unicast UDP (RFC 4787) (68693 bytes)

DO NOT USE THESE SLIDES on NAT → LOOK at Gonzalo's presentation instead!

About NATs and VOIP

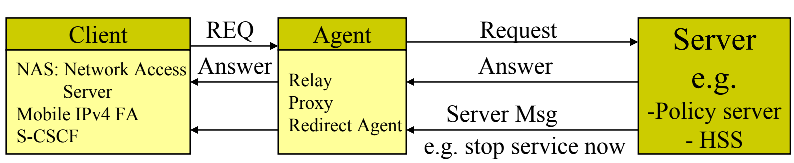
- Users behind a NAT use private addresses. They may e.g. get them from a DHCP server in the private network. E.g. an ADSL modem with several Ethernet ports may contain a NAT and the DHCP server. Private addresses are not unique in the Internet and can not be used for communication across the public Internet.
- When a host in the private network sends a message to the public Internet, the NAT creates a mapping: [priv-source IP add, source port] -> [public source IP addr, source port] and will keep this mapping for a time. If within the time a packet is seen, the timeout is restarted. As a result, non-active hosts do not need to have a public IP address. When the timeout expires, the mapping is deleted. Due to a NAT, a large number of clients can use a single public IP address (how many depends on how many ports each will use simultaneously).
- In client server applications (DNS, e-mail, www etc), communication always starts from the host so NAT traversal is automatic. E.g. using DNS (a server in the public Internet), the client (even behind a NAT) can learn public IP addresses of other communicating parties such as mail server addresses. VOIP is fundamentally a peer-to-peer application, because a VOIP client must be reachable from the public Internet. Clients with private addresses are not reachable from the Internet – they must themselves take the initial step. Moreover, VOIP may send the callers IP add+port information in application messages (in signaling).

Problems created by NATs to VOIP

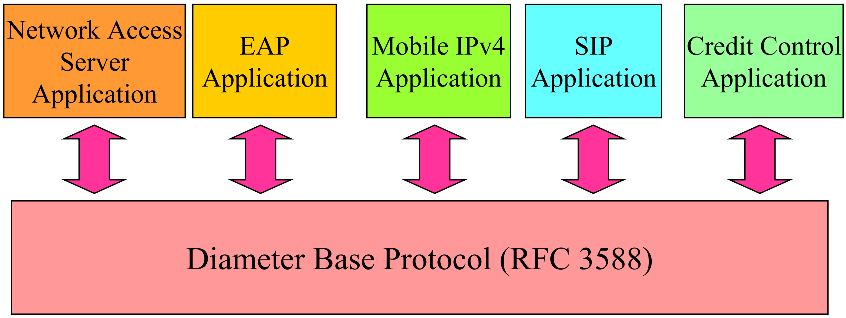
- Invitation (or setup message) can not be sent to a client in a private IP network, i.e. behind a NAT. This does not depend on whether the call comes from a client or a proxy in the public Internet.
  - This means that there are no B-subscribers (callees) in the Internet with NATs
- Even if the invitation goes through, sending voice packets (RTP/UDP/IP) to the B –subscriber is not possible without additional tricks, because RTP can not use the same port as signaling.
- A solution would be that ”B-subscribers” are always registered on some server in the Internet and all packets to the B-subscriber go through the server. For signaling, this might be ok (although it defiets the original purpose of NATs). For voice packets, this creates additional delay and a significant additional cost.

Diameter is the emerging 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



Overall Diameter Architecture



EAP - Extensible Authentication Protocol

NB: The current de-facto solution to AAA is Radius – Diameter for example in 3G

IETF Diameter group has not yet adopted 3G policy and charging control (PCC)…

Diameter Documents

Request For Comments:
Accounting Attributes and Record Formats (RFC 2924) (75561 bytes)
Introduction to Accounting Management (RFC 2975) (129771 bytes)
Criteria for Evaluating AAA Protocols for Network Access (RFC 2989) (53197 bytes)
Authentication, Authorization, and Accounting:Protocol Evaluation (RFC 3127) (170579 bytes)
Authentication, Authorization and Accounting (AAA) Transport Profile (RFC 3539) (93110 bytes)
Diameter Base Protocol (RFC 3588) (341261 bytes)
Diameter Mobile IPv4 Application (RFC 4004) (128210 bytes)
Diameter Network Access Server Application (RFC 4005) (198871 bytes)
Diameter Credit-Control Application (RFC 4006) (288794 bytes)
Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072) (79965 bytes)
Diameter Session Initiation Protocol (SIP) Application (RFC 4740) (174175 bytes)

No Internet drafts (12.1.2007)

Source: http://www.ietf.org/html.charters/aaa-charter.html

Diameter features include

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

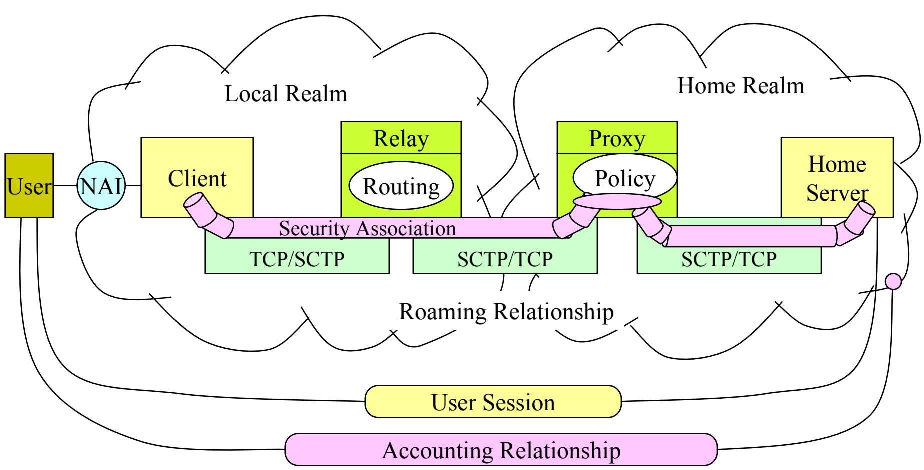
User Authentication

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



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

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.

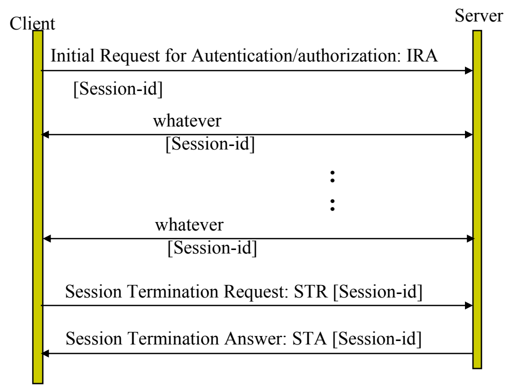
Security Association
A security association is an association between two endpoints in a Diameter session which allows the endpoints to communicate with integrity and confidentially, even in the presence of relays and/or proxies.

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



A diameter node has a peer table

Host identity	Status	Stat/Dyn	Expiration time	TLS enabled	Additional Security info

Host identity:
origin host
-from capability exchange: CER/CEA

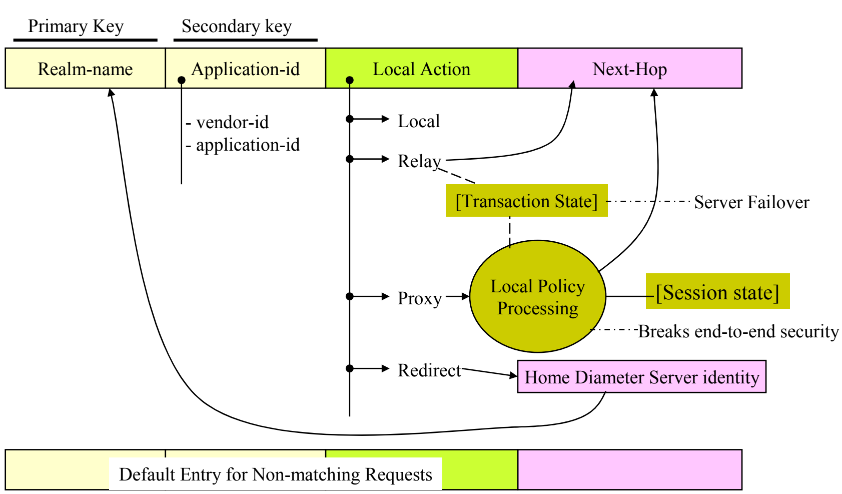
Status:
- Closed
- Wait-conn-ack
- wait-I-CEA
- wait-I-CEA/Elect
- wait-returns
- R-Open
- I- Open
- ….
- …
- Stop
- = state of the "dialogue" with the peer

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

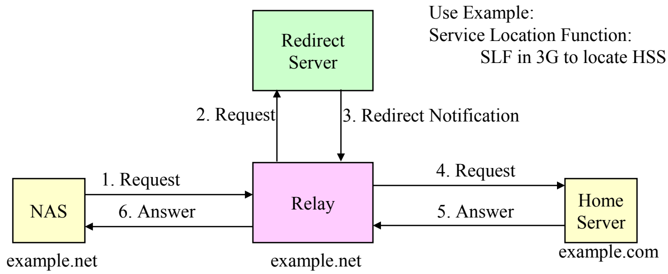
- Search manually configured peer agent list
- Use SLPv2 (service location protocol)
- NAPTR query to DNS (”AAA+D2x where x=T|S, T=tcp, S=sctp) – gives the preferred SRV record, a new query gives the IP address
- query `_diameter._sctp´.realm and `_diameter._tcp´.realm, where realm is the destination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

Realm Routing Table describes the actions of a Diameter Node

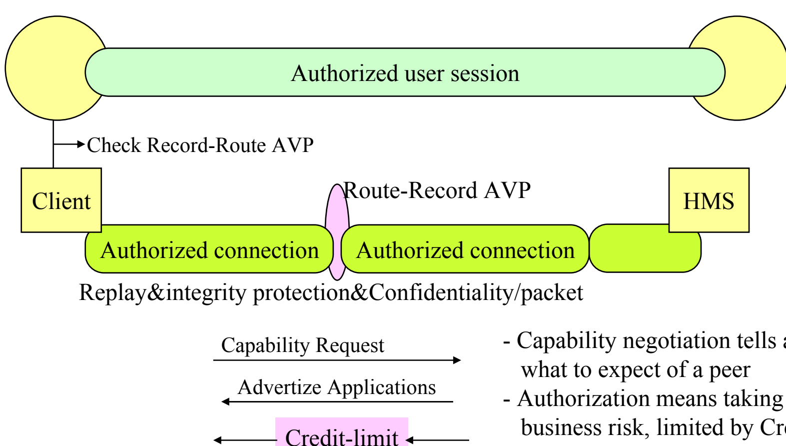


A node can act as proxy for some user connections and as a relay for others.
The Routing Table is configuration information.

Redirect server helps to centralize Diameter request routing in a roaming consortium



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

Version=1	Message Length
Command Flags	Command-Code
Application-ID	
Hop-by-Hop Identifier	
End-to-End Identifier	
AVPs	

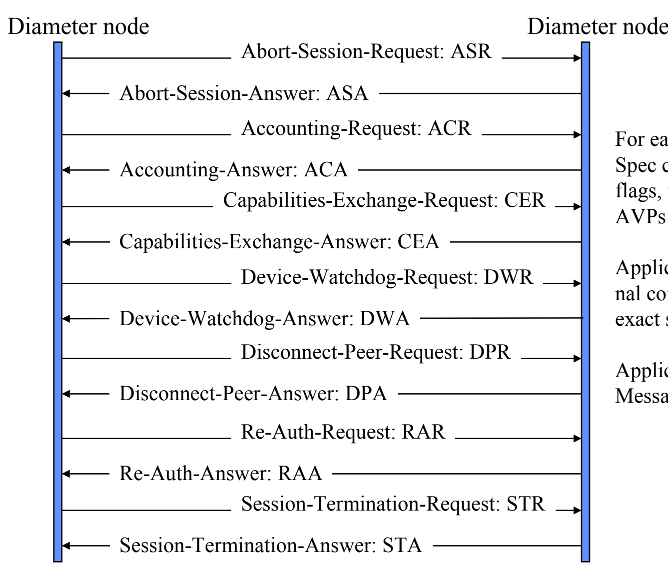
Application-ID: e.g. 3GPP application

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

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

Base Diameter protocol Requests and Answers



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

Applications introduce additio-nal command-codes and their exact syntax.

Applications may extend these Messages.

Base protocol AVPs

AVPs have a common header

AVP Code	
VMPrrrrr	AVP Length
Vendor-ID (opt)	
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.

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

Summary of Diameter scalability cmp. Radius

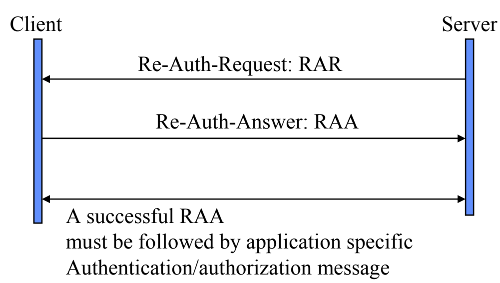
Radius is the current standard for AAA in the Internet. E.g. when an ISP user accesses the Internet thru a modem line, the POP uses Radius to contact a DB in order to check access rights.
Radius problems are: vulnerability to certain attacks, limited set of attributes are supported and the architecture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

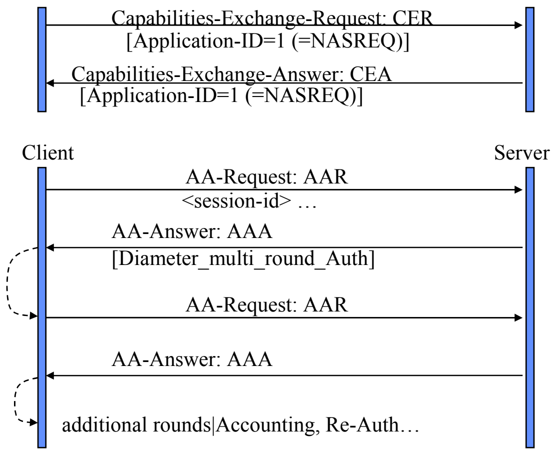
Challenge is to introduce Diameter when the existing infra is based on Radius. Interoperability of the two protocols becomes key to deployment of Diameter.

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

AAR and AAA have loads of AVPs!

NASREQ messages (RFC 4005)

AAR	AA-Request
AAA	AA-Answer
RAR	Re-Auth-Request
RAA	Re-Auth-Answer
STR	Session-Termination-Request
STA	Session-Termination-Answer
ASR	Abort-Session-Request
ASA	Abort-Session-Answer
ACR	Accounting-Request
ACA	Accounting-Answer

Extended from BASE

EAP Application extends NASREQ and provides

Command-Name	Abbrev.
Diameter-EAP-Request	DER
Diameter-EAP-Answer	DEA

Diameter SIP Application

Command Name	Abbr.
User-Authorization-Request	UAR
User-Authorization-Answer	UAA
Server-Assignment-Request	SAR
Server-Assignment-Answer	SAA
Location-Info-Request	LIR
Location-Info-Answer	LIA
Multimedia-Auth-Request	MAR
Multimedia-Auth-Answer	MAA
Registration-Termination-Request	RTR
Registration-Termination-Answer	RTA
Push-Profile-Request	PPR
Push-Profile-Answer	PPA

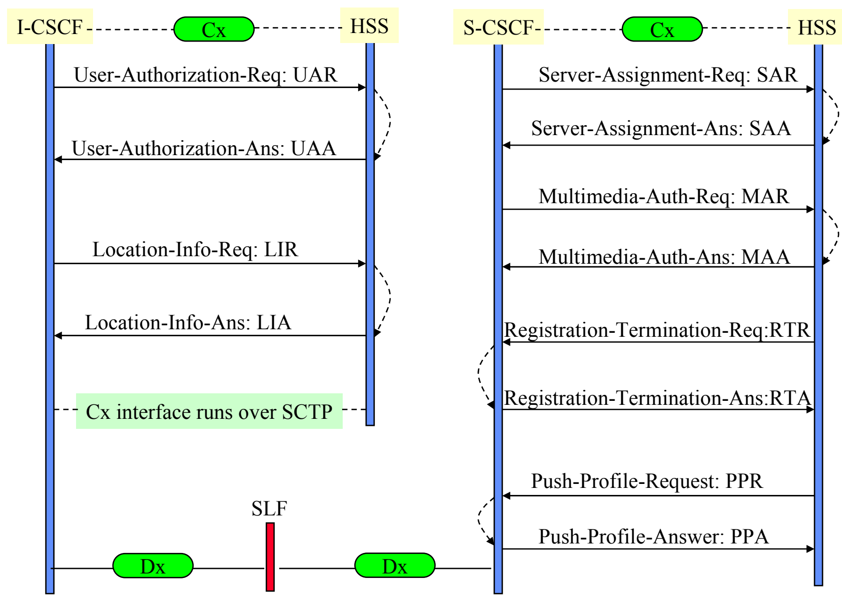
This application is used in 3G IMS

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

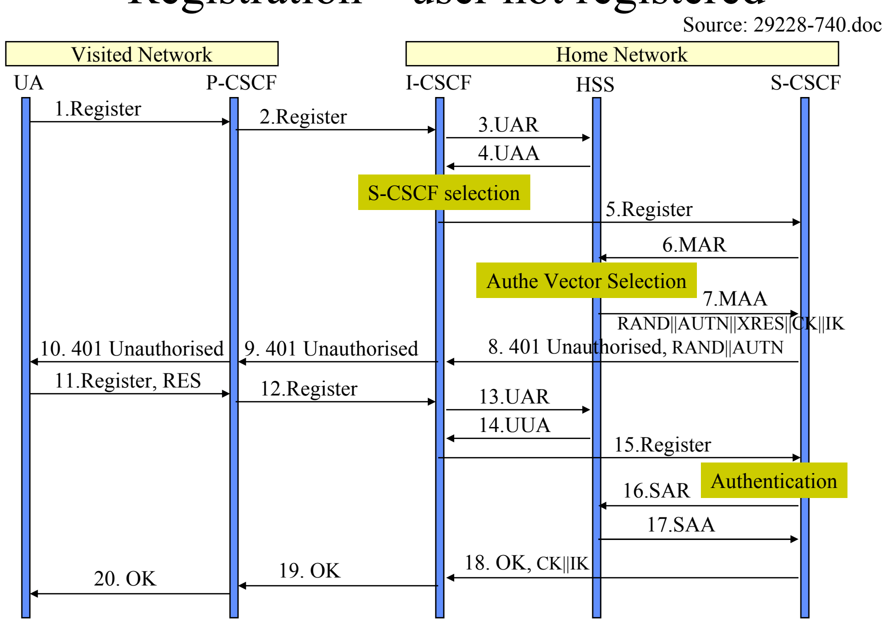
Diameter Credit Control Application

- 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

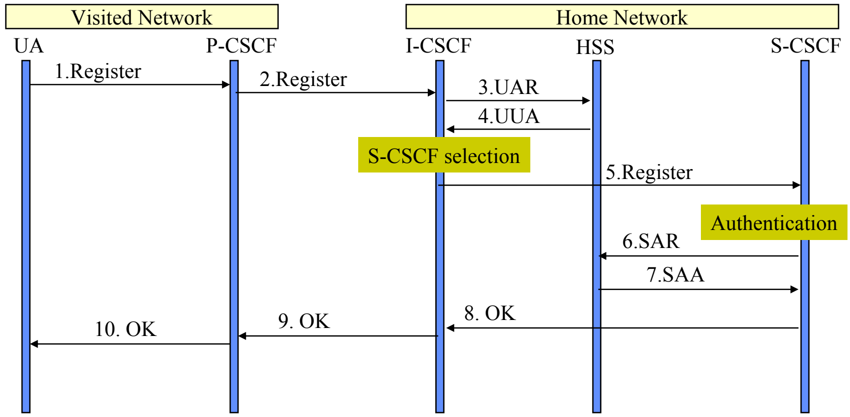
3G IMS Diameter SIP Application



Registration – user not registered

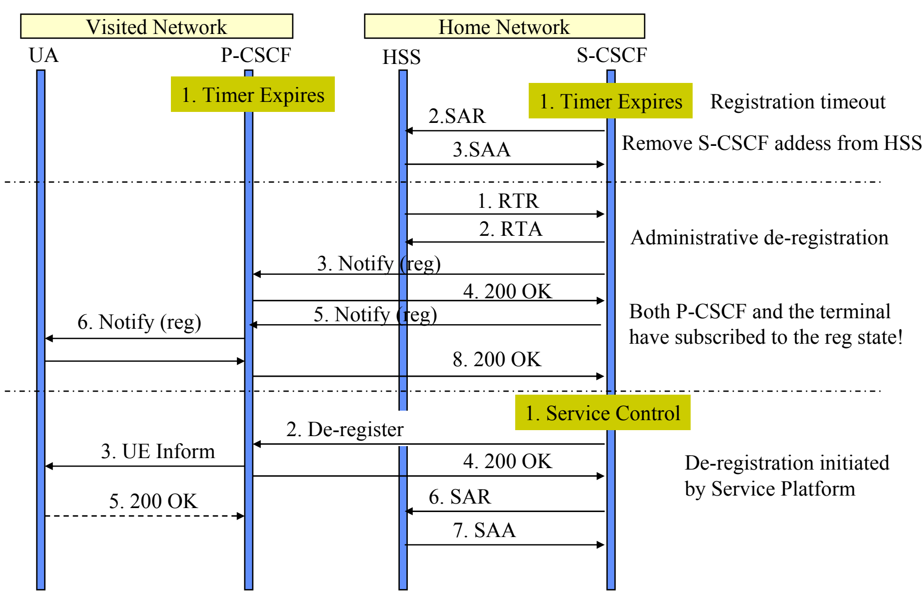


Registration – user currently registered

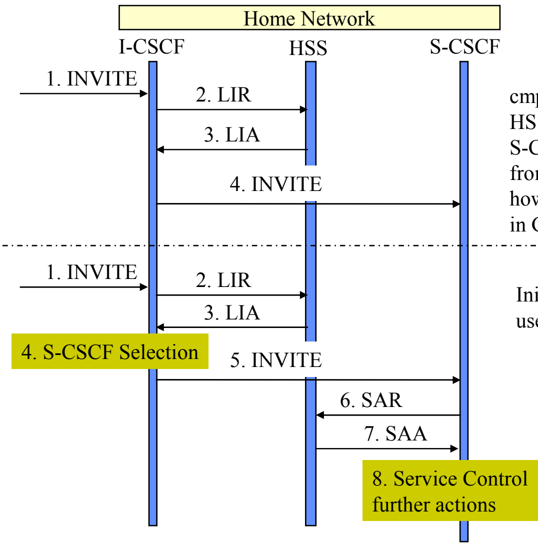


- Registration may need to be refreshed from time to time.
- Location changes may require re-registration.
- Mobile Initiated de-registration looks exactly the same!

Many ways/reasons to de-register



Mobile Terminated SIP Session Set-up is similar to MAP MT call



cmp: SendRoutingInformation of MAP 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.

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
  - 3GPP TS 23.203 V7.1.0 - Policy and charging control architecture (Release 7)
  - 3GPP TS 29.212 V1.0.0 - 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

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
- 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
  - Requires policy management: e.g. which packets to assign to which class.
  - Managing class weights remains an issue.

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 interfire 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

- 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 etc per service

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

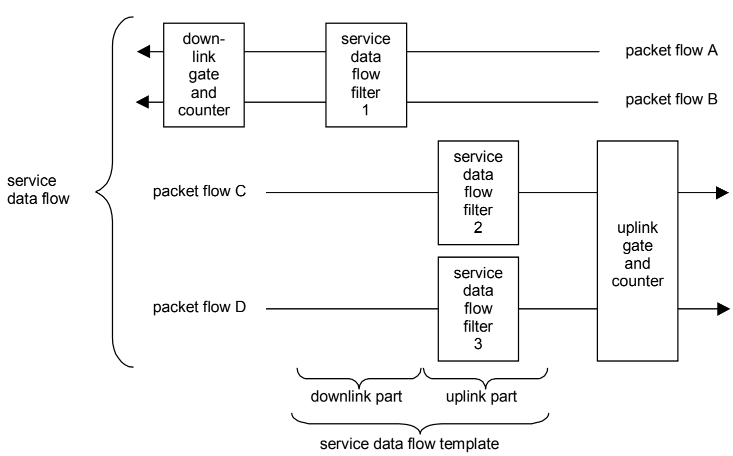
Service data flow: An aggregate set of packet flows.

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.

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

FBC	Flow Based Charging
IP-CAN	IP Connectivity Access Network
OFCS	Offline Charging System
OCS	Online Charging System
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDF	Policy Decision Function
PEP	Policy Enforcement Point
SBLP	Service Based Local Policy
SPR	Subscription Profile Repository

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.

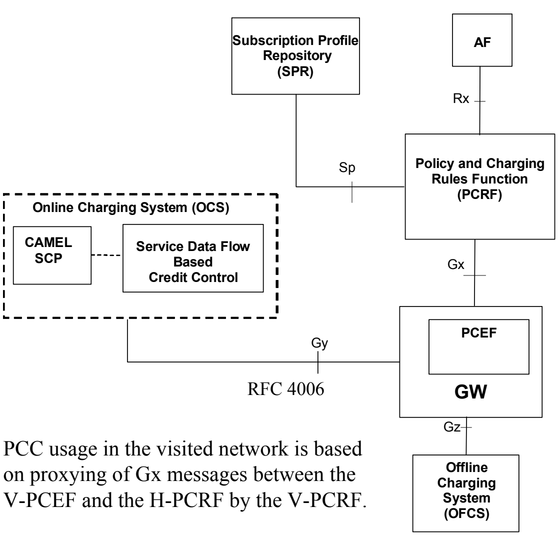
The PCC architecture allows the charging control to be applied on a per service data flow basis, independent of the policy control.

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.

PCC elements

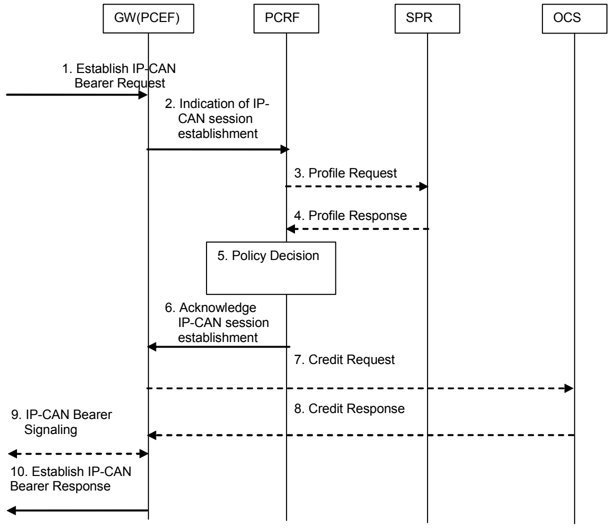


SPR example – HSS
AF example P-CSCF
PCEF example – GGSN
or PDG for WLAN access

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).

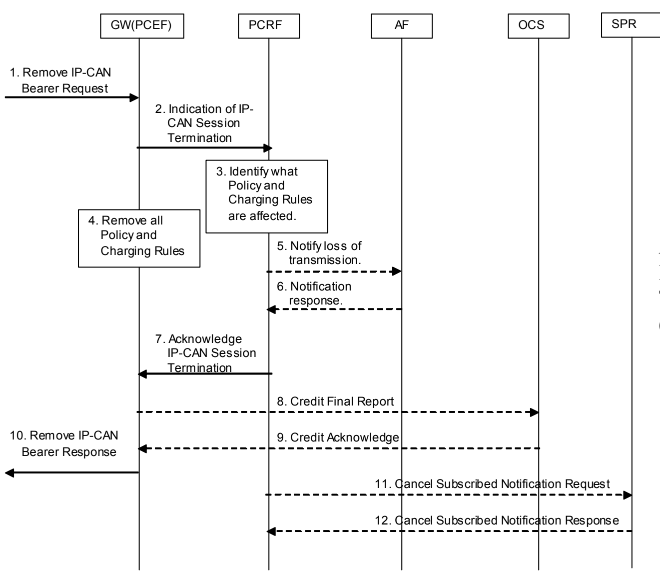
PCC usage in the visited network is based on proxying of Gx messages between the V-PCEF and the H-PCRF by the V-PCRF.

IP-CAN session establishment for PCC



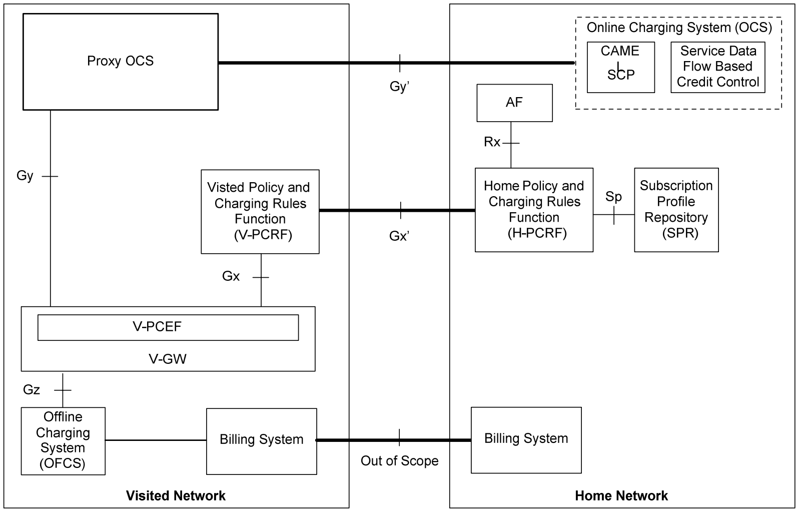
This is a logical Information flow that is used as a basis for protocol design

IP-CAN session termination for PCC

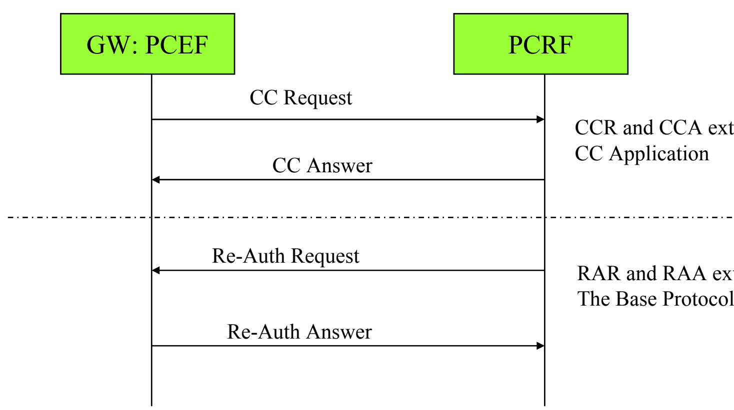


Also GW(PCEF) Initiated IP-CAN Session Termination is supported (not shown)

Proxying rules to visited network



Policy and Charging Control over Gx interface



CCR and CCA extended from CC Application

RAR and RAA extended from The Base Protocol

3GPP TS 29.212 V1.0.0 (2006-12)

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

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
  - 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?

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
- IETF development model is one protocol for one problem.
- Client-Server model is used whenever possible.
- The drive is towards providing PSTN like control over services and over what a user can do in the IP environment.
- Through access to the Internet, the open Internet model lives on.