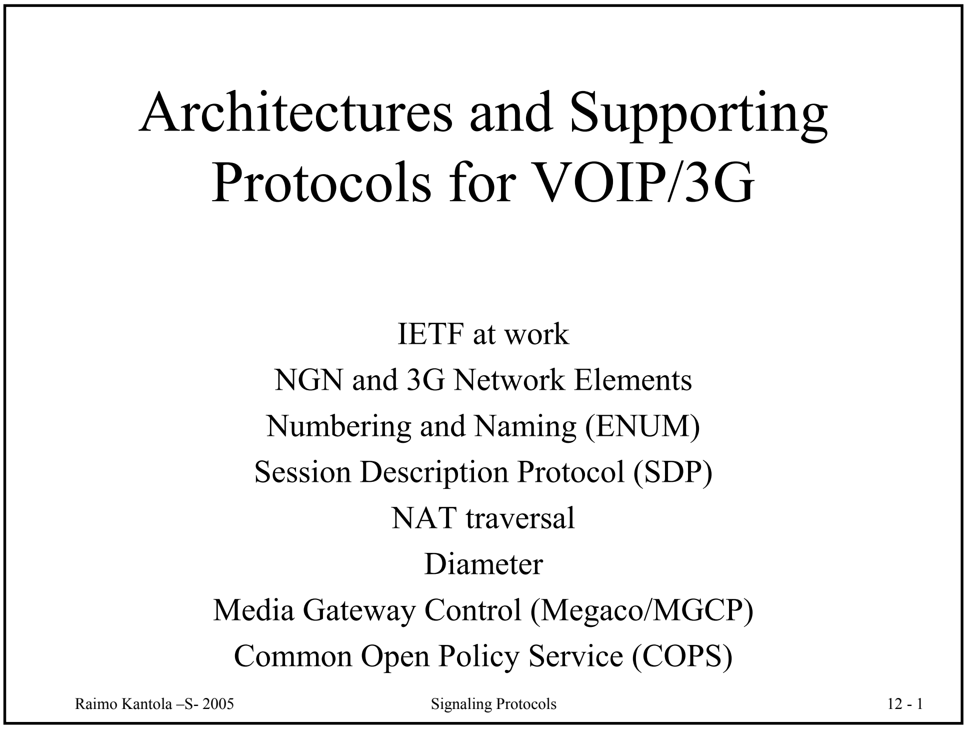
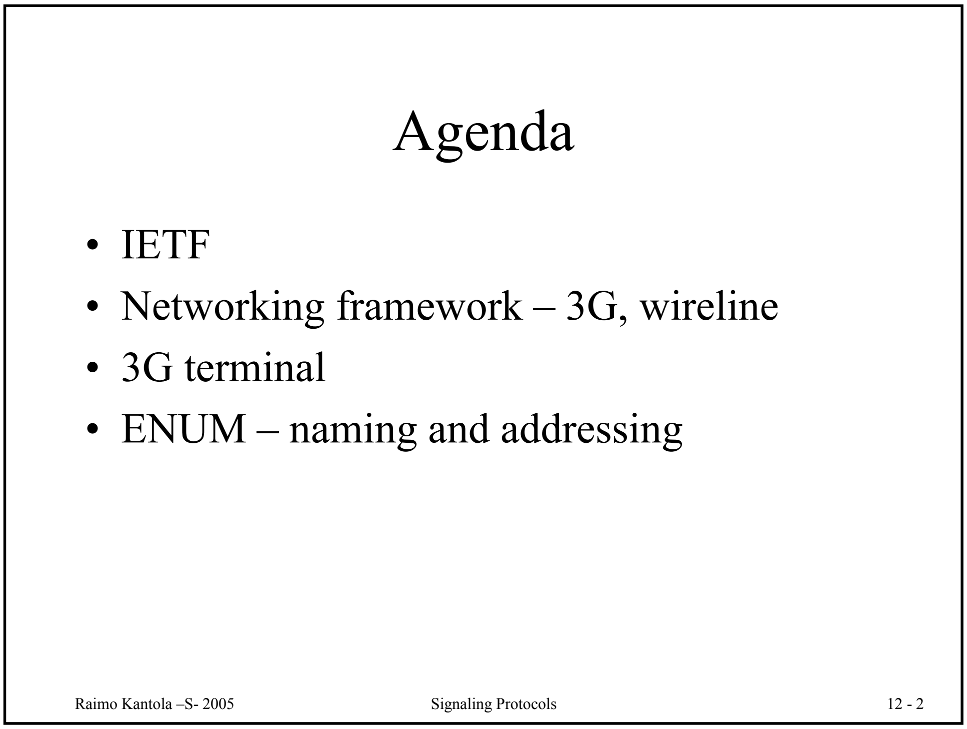


Architectures and Supporting Protocols for VOIP/3G

IETF at work
NGN and 3G Network Elements
Numbering and Naming (ENUM)
Session Description Protocol (SDP)
NAT traversal
Diameter
Media Gateway Control (Megaco/MGCP)
Common Open Policy Service (COPS)

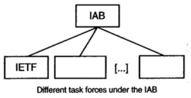


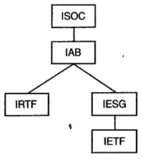
Agenda

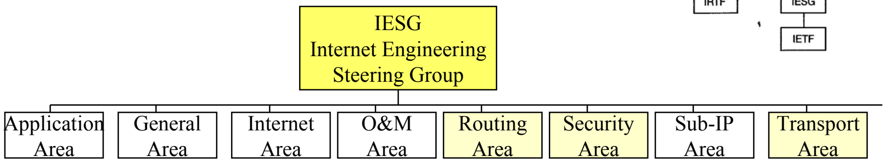
- IETF
- Networking framework – 3G, wireline
- 3G terminal
- ENUM – naming and addressing

IETF

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







Application Area: …
simple

O&M Area: aaa
dnsop

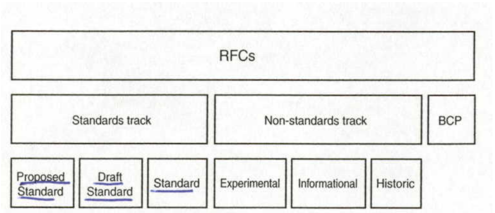
Routing Area: bgmp
idmr
idr
manet
mpls
ospf

Security Area: ipsec
smime
tls
…

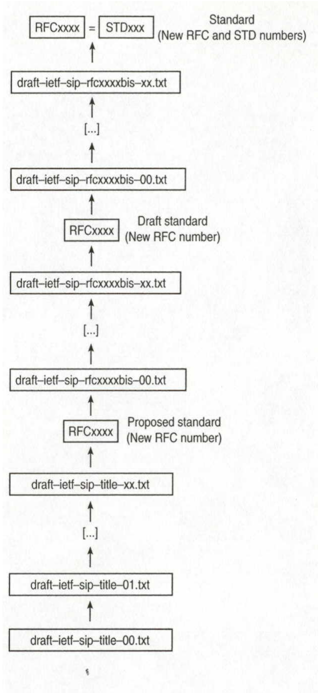
Transport Area: avt
enum
iptel
mmusic
sip
sipping
sigtran

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

IETF specifications



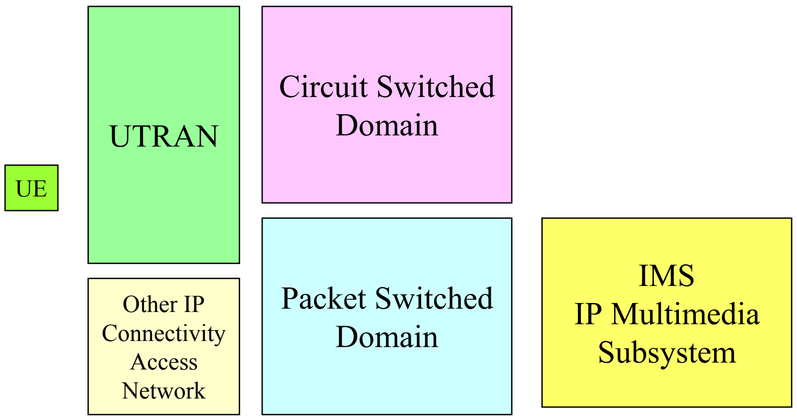
•Every standard follows the route Proposed standard-> Draft Standard-> Standard


RFCxxxx = STDxxx
Standard
(New RFC and STD numbers)
draft–ietf–sip–rfcxxxxbis–xx.txt
[...]
draft–ietf–sip–rfcxxxxbis–00.txt
RFCxxxx
Draft standard
(New RFC number)
draft–ietf–sip–rfcxxxxbis–xx.txt
[...]
draft–ietf–sip–rfcxxxxbis–00.txt
RFCxxxx
Proposed standard
(New RFC number)
draft–ietf–sip–title–xx.txt
[...]
draft–ietf–sip–title–01.txt
draft–ietf–sip–title–00.txt

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



UE

UTRAN

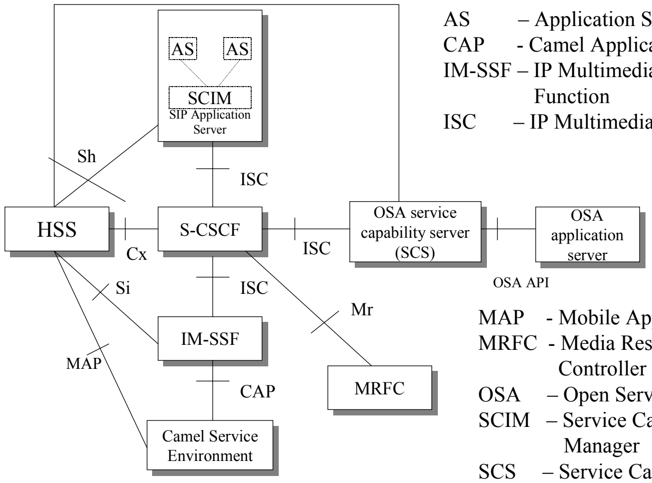
Other IP Connectivity Access Network

Circuit Switched Domain

Packet Switched Domain

IMS
IP Multimedia Subsystem

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

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

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?

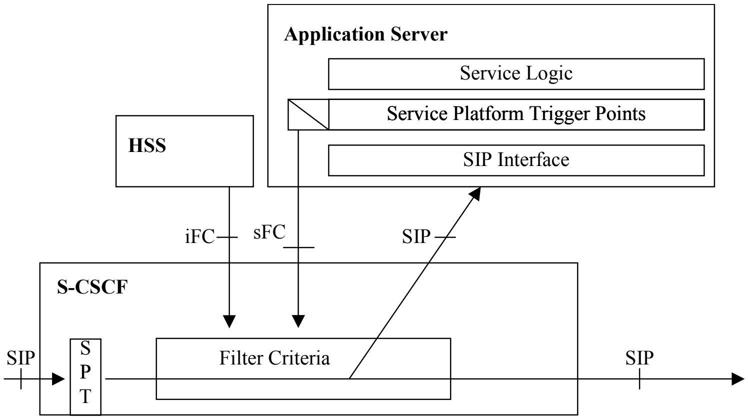
Q: Why should operators switch from circuit based voice services to IMS based voice services in 3G?

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 (from release 6)

3G Application Triggering

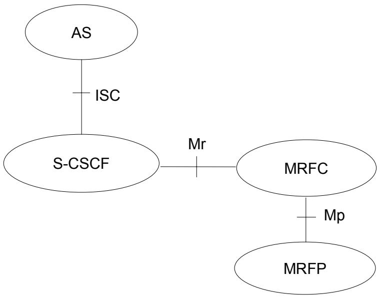


iFC – Initial Filter Criteria
sFC – Subsequent Filter Criteria
SPT – Service Point Trigger

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

sFC is considered historical (obsolete)

Media processing in 3G



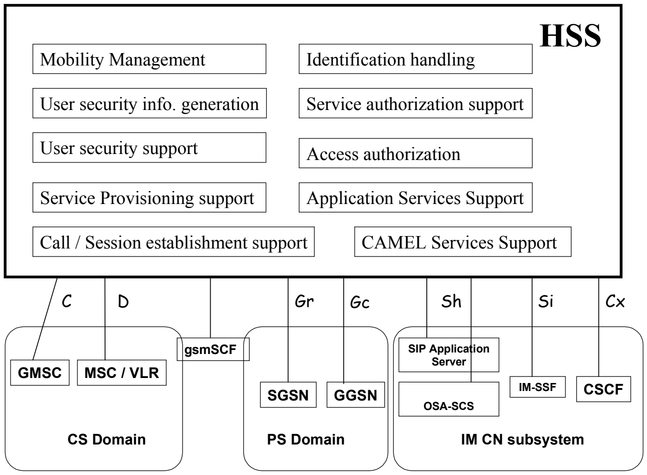
MRFC - Media Resource Function
Controller
MRFP – Media Resource Function
Processor

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

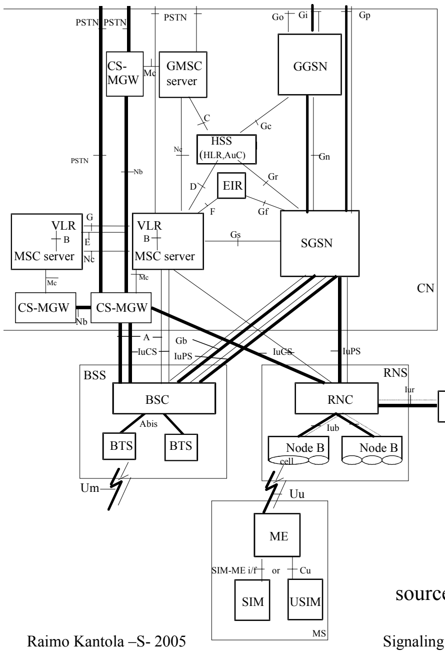
MRFC likely to have a general purpose processor,
MRFP has many DSPs – digital signal processors.

The role of HSS



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

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

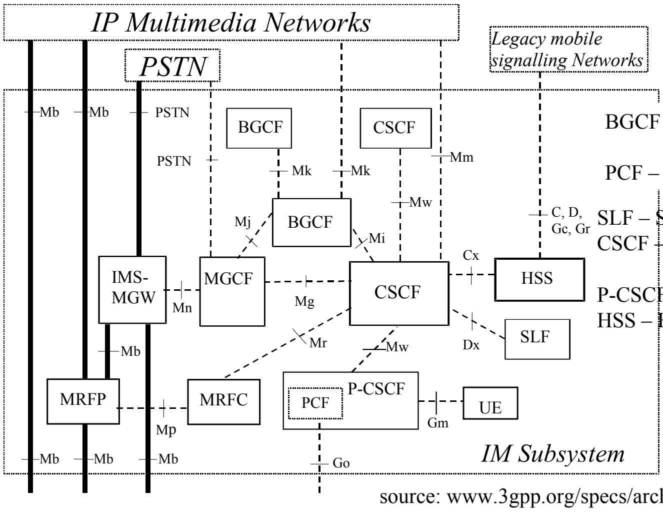
On CS side breakdown of MSC to Media Gateway and MSC server.

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

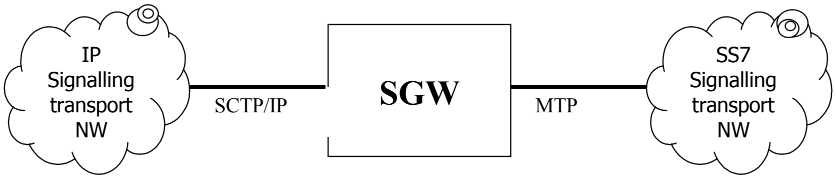
CSCF – Call Session Control Function

P-CSCF – Proxy CSCF

HSS – Home Subscriber Server

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

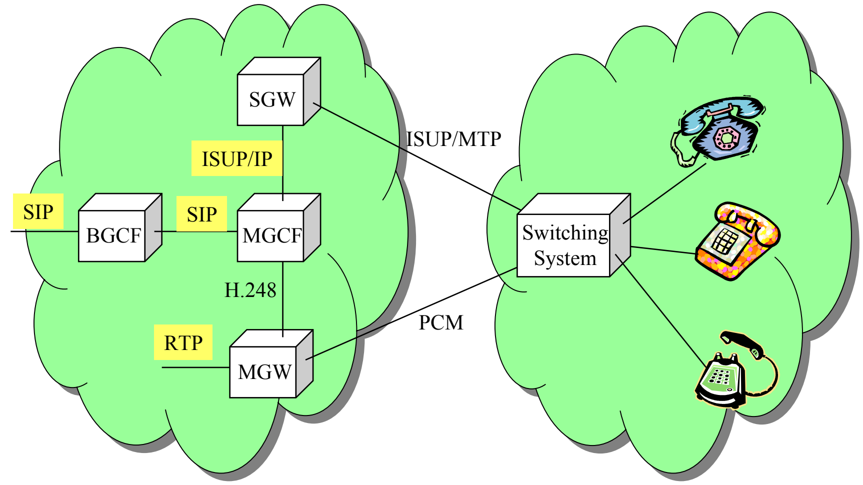
Signaling Gateway maps SS7 MTP to SCTP/IP transport



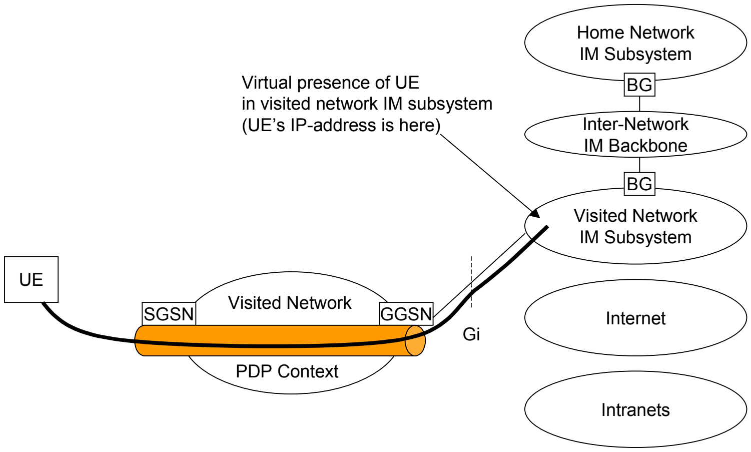
This allows to transfer signaling and service processing responsibility to IP based environment.

IMS Interworking with the PSTN

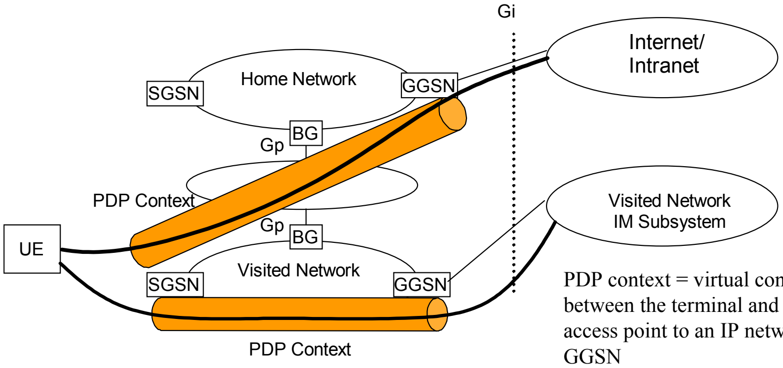
- IMS terminals must support CSN services due to Emergency Call requirements, so PSTN interworking can occur thru the CS domain. However, IMS Interworking with PSTN is also possible.



UE has a tunnel to visited IMS


Home Network IM Subsystem
BG
Inter-Network IM Backbone
BG
Visited Network IM Subsystem
Virtual presence of UE in visited network IM subsystem (UE's IP-address is here)
UE
SGSN
Visited Network
GGSN
PDP Context
Gi
Internet
Intranets

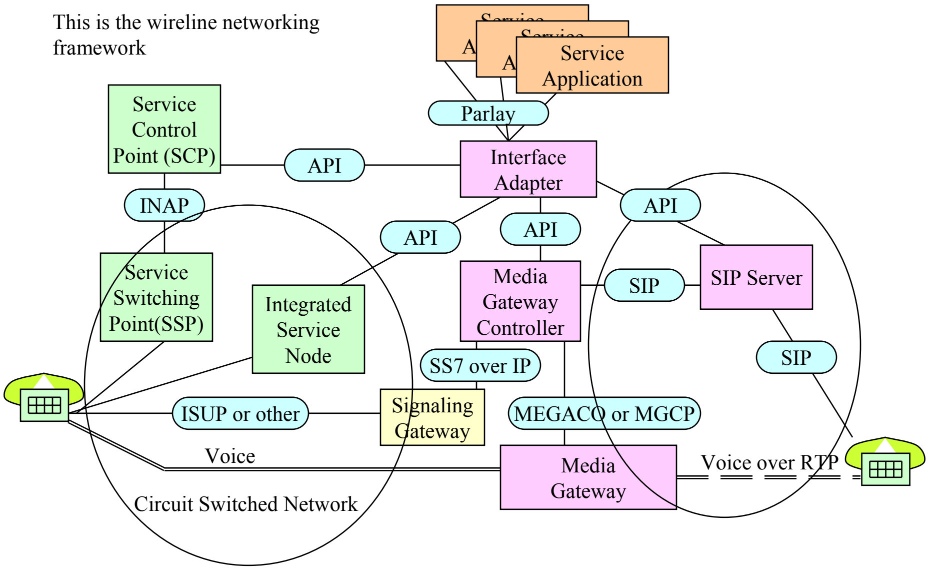
3G UE can use several services at the same time



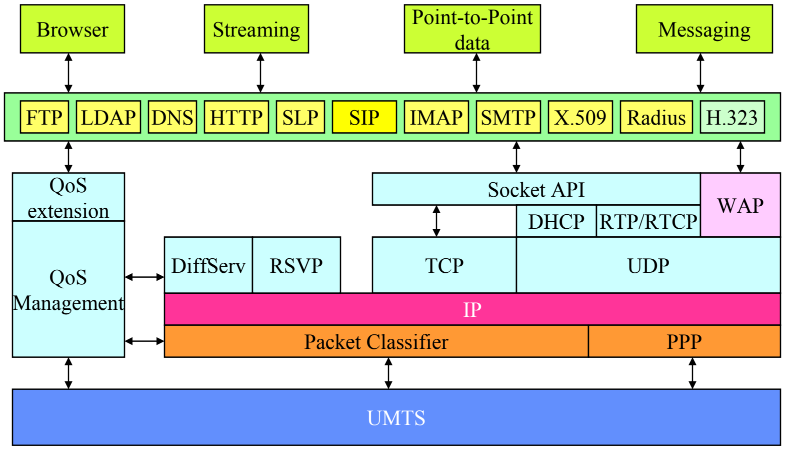
PDP context = virtual connection between the terminal and an access point to an IP network thru GGSN

ETSI SoftSwitch Architecture for NGN

This is the wireline networking framework

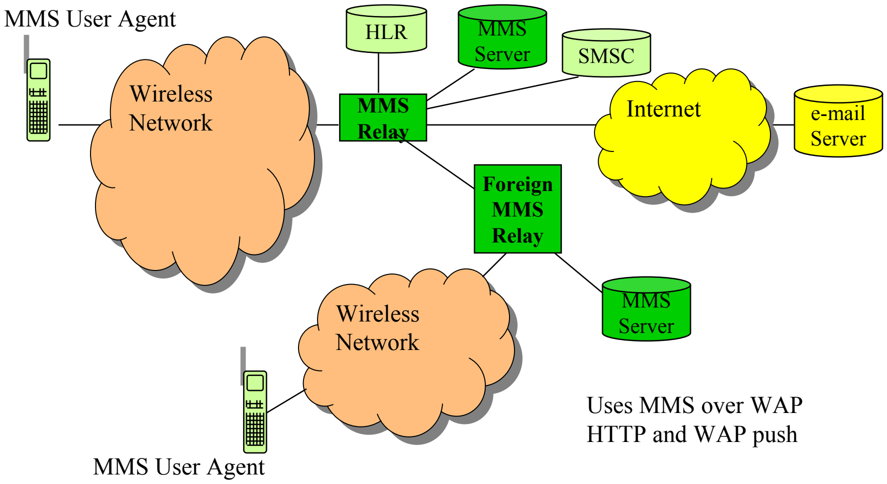


The UMTS terminal functional model



Browser
Streaming
Point-to-Point data
Messaging
FTP
LDAP
DNS
HTTP
SLP
SIP
IMAP
SMTP
X.509
Radius
H.323
QoS extension
QoS Management
Socket API
WAP
DHCP
RTP/RTCP
DiffServ
RSVP
TCP
UDP
IP
Packet Classifier
PPP
UMTS

The GPRS and 3G networks implement the Multimedia Messaging Service



MMS User Agent
Wireless Network
HLR
MMS Server
SMSC
MMS Relay
Internet
e-mail Server
Foreign MMS Relay
MMS Server
Wireless Network
MMS User Agent

Uses MMS over WAP
HTTP and WAP push

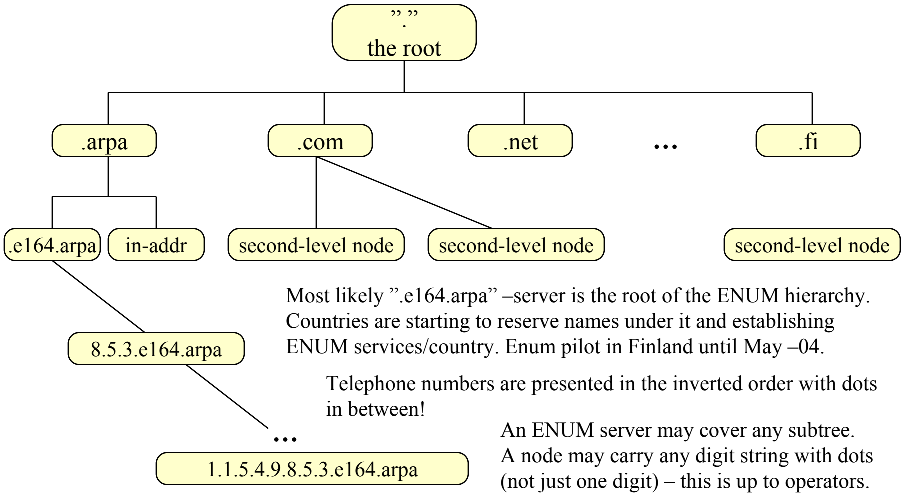
Supporting protocols for IP telephony – wired and wireless

- ENUM – addressing and naming
- Gateway control - Megaco
- Policy Control – COPS
- 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 until May –04.

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

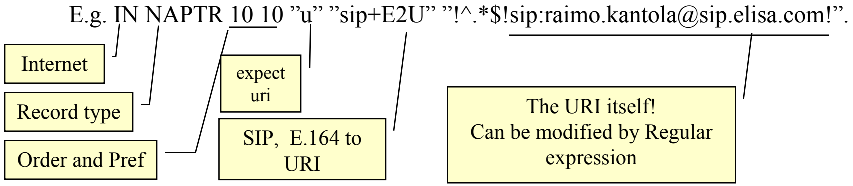
An ENUM server may cover any subtree. A node may carry any digit string with dots (not just one digit) – this is up to operators.

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!”.



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."

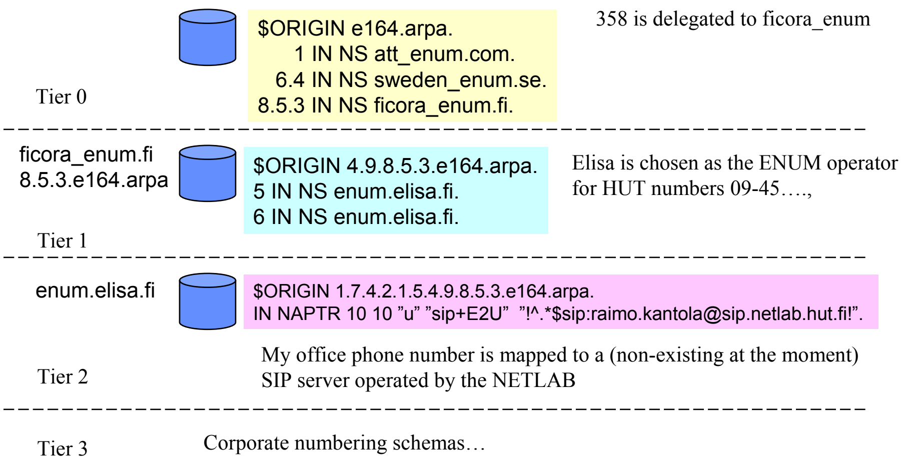
For this example telephone number we might get back the following NAPTR records:

```
$ORIGIN 2.1.2.1.5.5.5.0.7.7.1.e164.arpa.
 IN NAPTR 100 10 "u" "sip+E2U"  "!^.*$!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

This follows the ”US model” suggested by Tuomo Rostela for 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

Tier 1

ficora_enum.fi
8.5.3.e164.arpa

```
$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….,

Tier 2

enum.elisa.fi

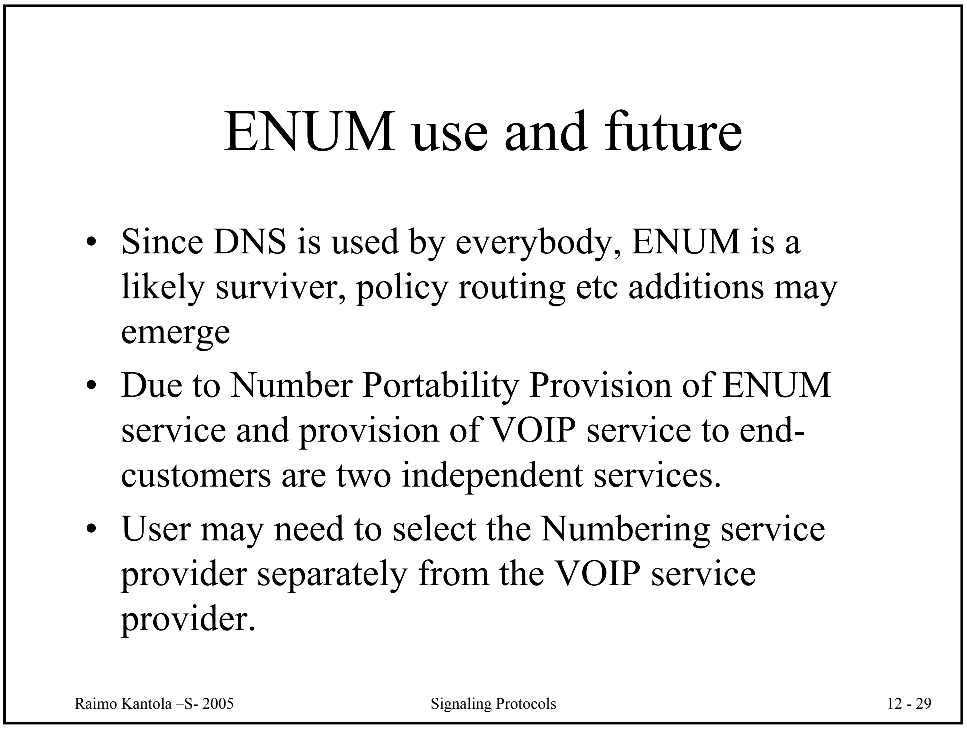
```
$ORIGIN 1.7.4.2.1.5.4.9.8.5.3.e164.arpa.
IN NAPTR 10 10 ”u” ”sip+E2U”  ”!^.*$sip:raimo.kantola@sip.netlab.hut.fi!”.
```

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

Tier 3

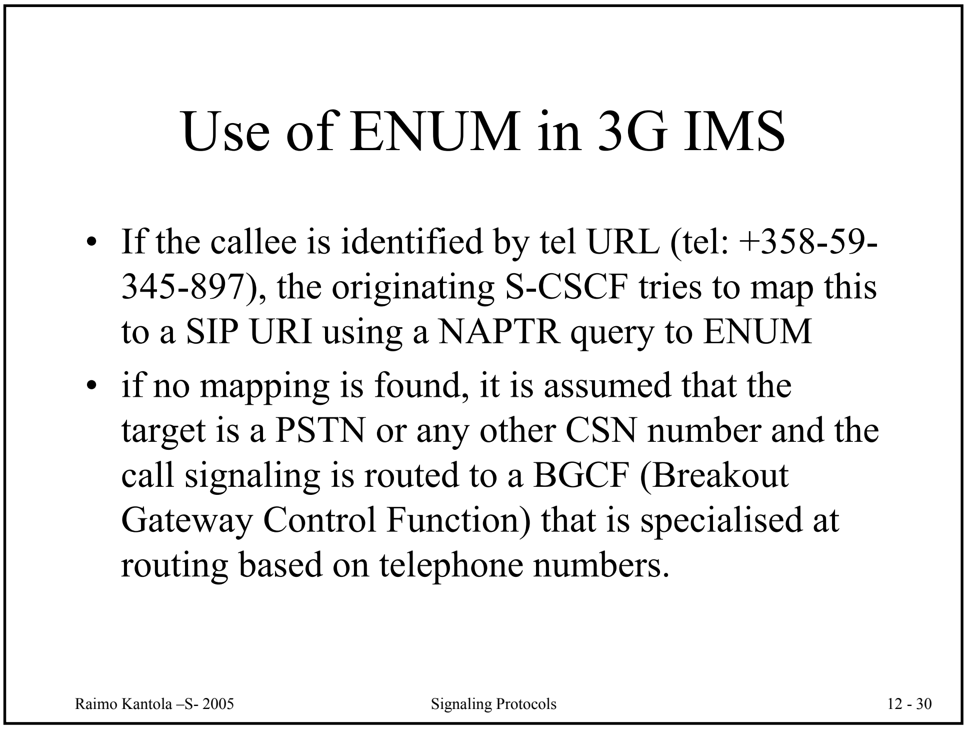
Corporate numbering schemas…

In Finnish ENUM pilot until 31.5.2004 only Tier 1 and Tier 2 present!



ENUM use and future

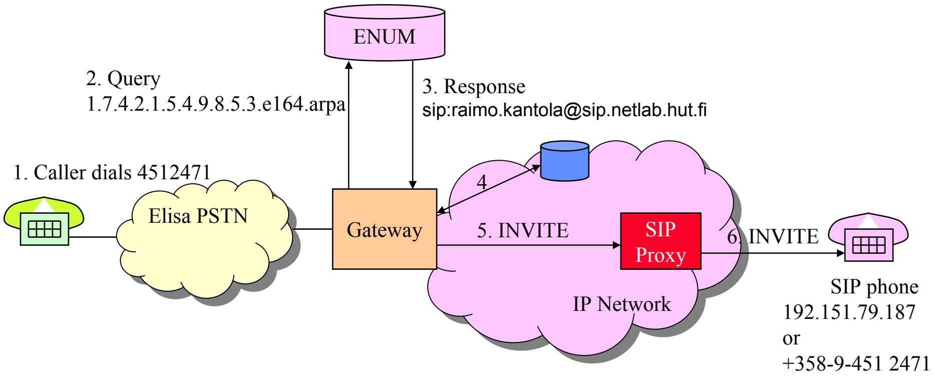
- Since DNS is used by everybody, ENUM is a likely surviver, policy routing etc additions may emerge
- Due to Number Portability Provision of ENUM service and provision of VOIP service to end-customers are two independent services.
- User may need to select the Numbering service provider separately from the VOIP service provider.



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
- 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



ENUM

2. Query
1.7.4.2.1.5.4.9.8.5.3.e164.arpa

3. Response
sip:raimo.kantola@sip.netlab.hut.fi

1. Caller dials 4512471

Elisa PSTN

Gateway

4

5. INVITE

SIP Proxy

6. INVITE

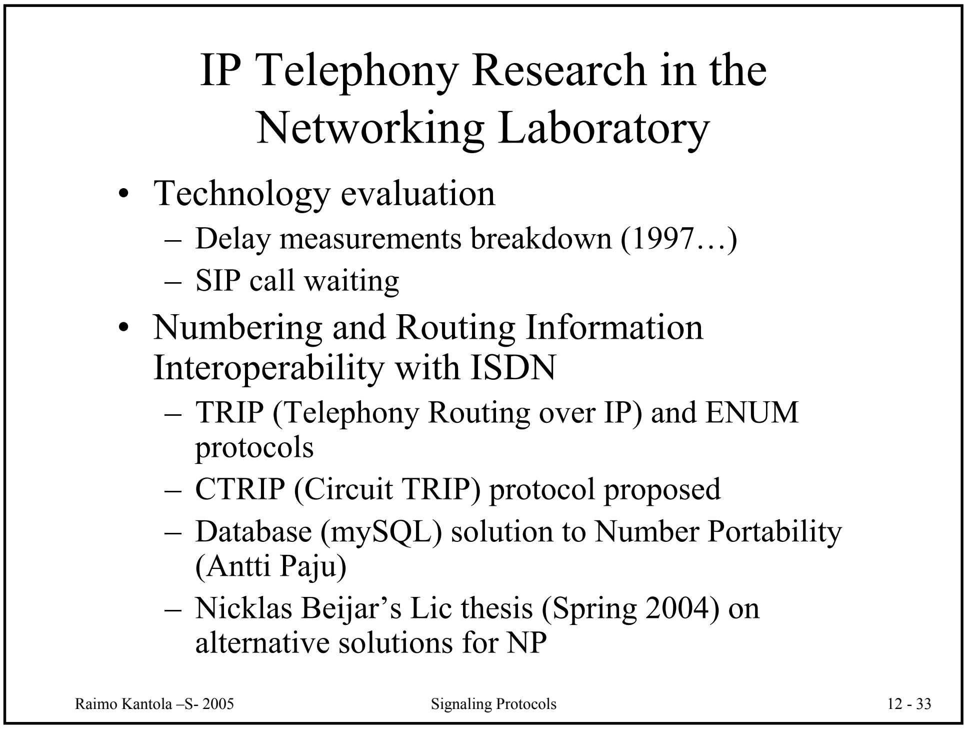
IP Network

SIP phone
192.151.79.187
or
+358-9-451 2471

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.

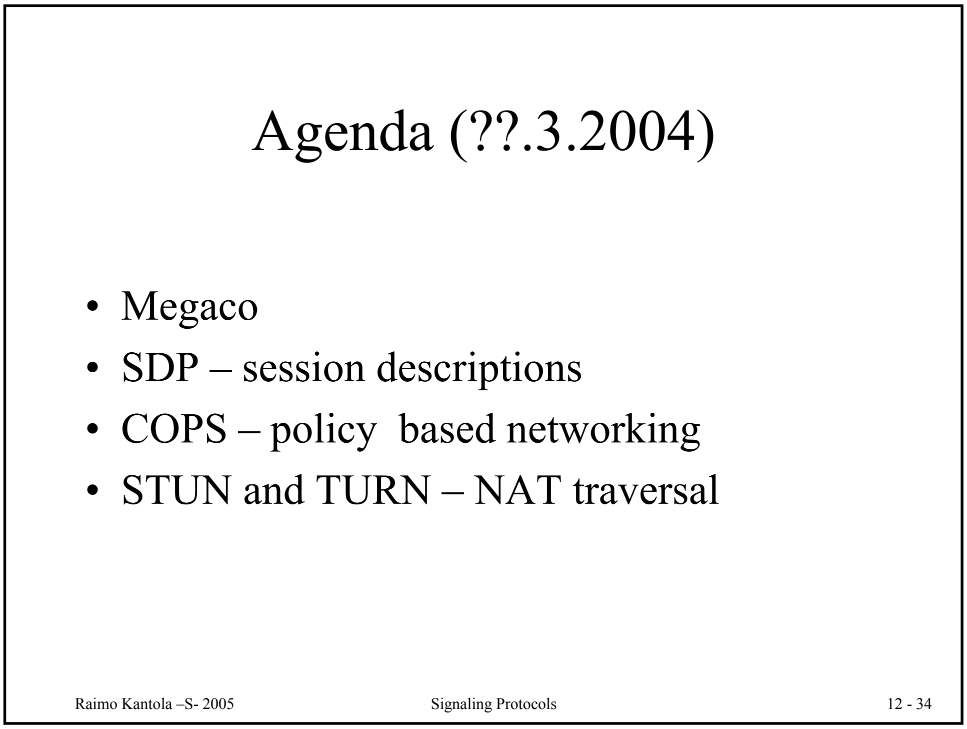
ENUM issues and problems

- Long chain of DNS servers results 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.
- Management of numbering data.
- 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 31.5.2004, after that commercial operation?



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



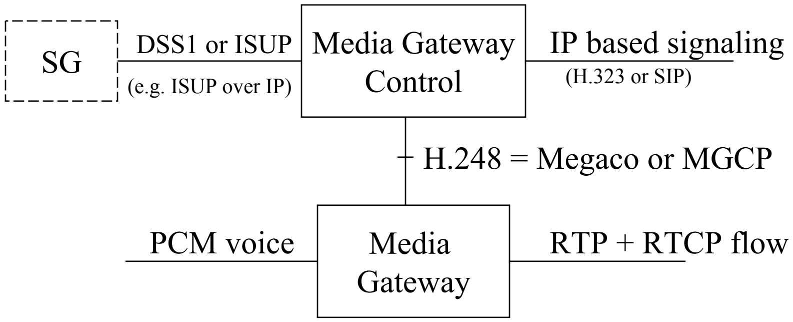
Agenda (??.3.2004)

- Megaco
- SDP – session descriptions
- COPS – policy based networking
- STUN and TURN – NAT traversal

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

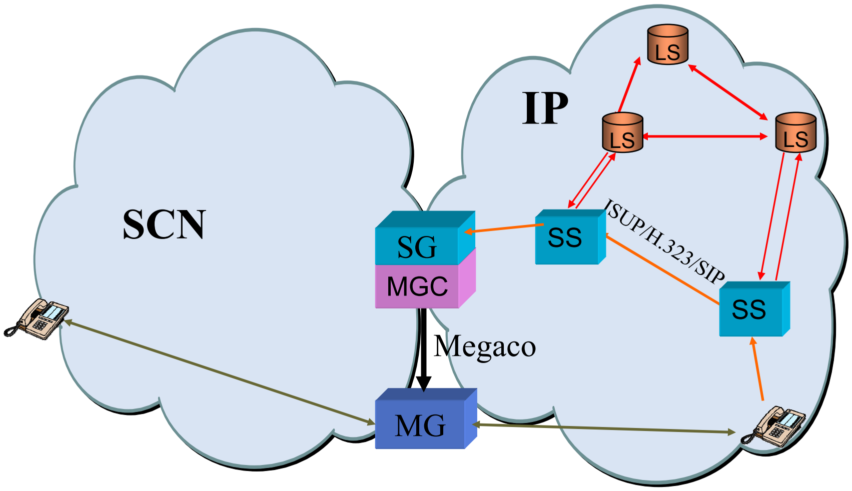


MG - Trunk gateway, residential gateway etc.
Many MGs can be controlled by one MGC, MGCs can be a mated pair --> higher availability performance.

Megaco functions

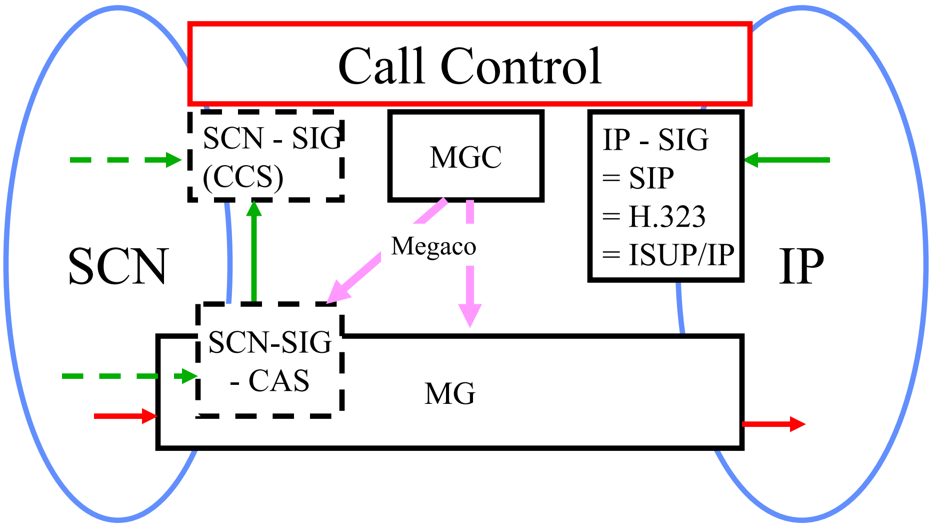
- Establishment of connections between terminations
  - PCM –timeslots for voice
  - ephemeral packet stream terminations: IP-address + source + dest UDP-port number
- Release of connections
- separation of signaling from voice band in case of CAS and analogue subsc signaling

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.

QoS – Integrated Serv. and DiffServ help resolving the QoS issue in VOIP and 3G IMS

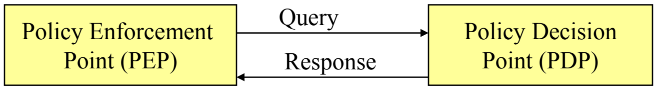
- Integrated Services
  - Different treatment to different flows
  - State info stored in network, routers examine packets!!!(not good)
  - Reservation merging
  - RSVP protocol – for reservation of resources
- DiffServ
  - Defines a small nrof traffic classes with different priority levels
  - Packets tagged with level tags at the beginning(ingress)
  - Routers just examine tags
  - Better scaling
  - Requires policy management: e.g. which packets to assign to which class.

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

Common Open Policy Service Protocol (COPS) can be used to exchange policy info



Policy Enforcement Point (PEP)

Query

Response

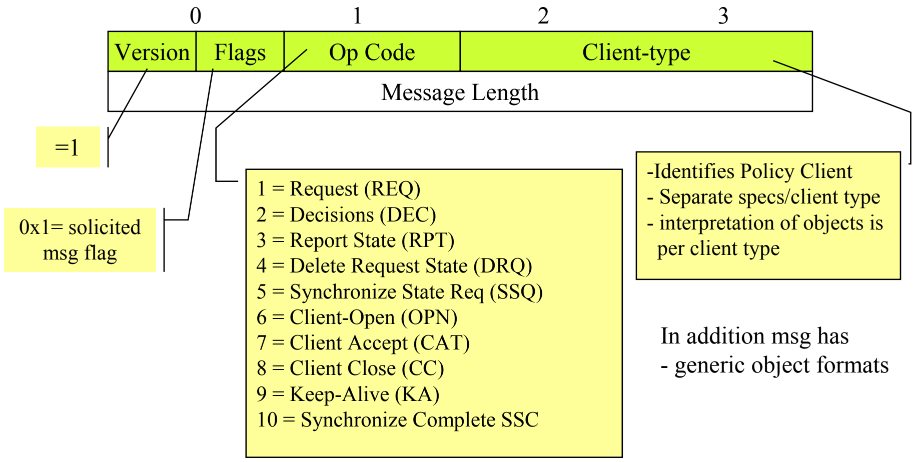
Policy Decision Point (PDP)

- Examples of PEPs are Network Address Translators (NAT), Firewalls, RSVP Routers, GGSN in 3G
- PEP sends requests, updates, deletes to PDP
- PDP returns decisions to PEP (can also overwrite its decision at any time)
- Uses TCP for transport, Extensible for different PEPs
- PEP and PDP share state
- In case of PDP failure, PEP can make local policy decisions

RFC 2748

COPS Common Header

RFC 2748 of Jan 2000



0		1	2	3
Version	Flags	Op Code	Client-type	
Message Length				

=1

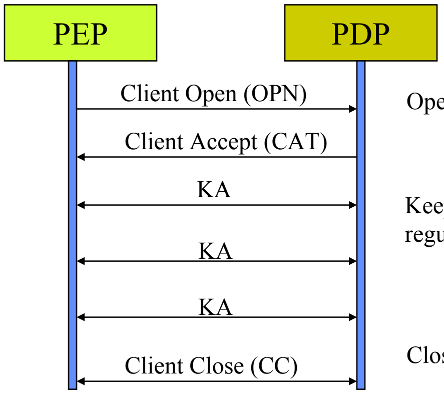
0x1= solicited msg flag

1 = Request (REQ)
2 = Decisions (DEC)
3 = Report State (RPT)
4 = Delete Request State (DRQ)
5 = Synchronize State Req (SSQ)
6 = Client-Open (OPN)
7 = Client Accept (CAT)
8 = Client Close (CC)
9 = Keep-Alive (KA)
10 = Synchronize Complete SSC

-Identifies Policy Client
- Separate specs/client type
- interpretation of objects is per client type

In addition msg has
- generic object formats

COPS maintains a TCP session

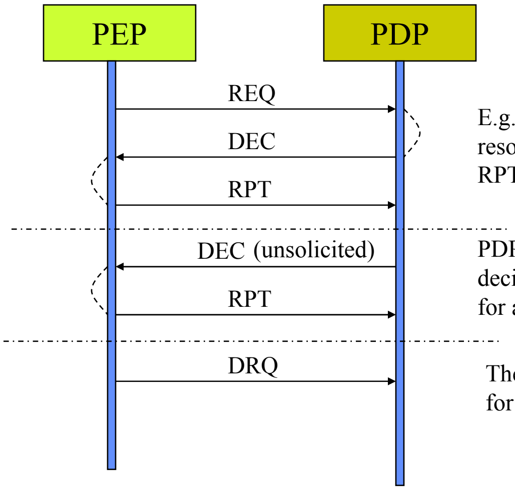


Opening a session establises a context

Keep-alive messages must be sent on regular intervals

Closing the session removes all state

PDP makes policy decisions on request or at any time

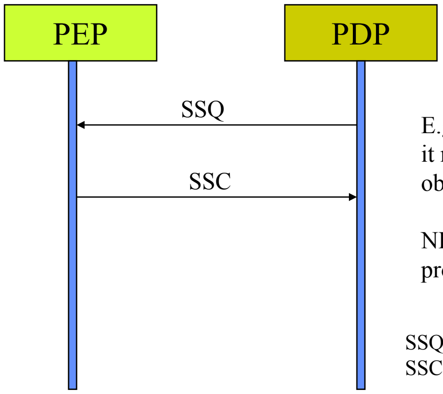


E.g. PEP may need to allocate some resourse – PDP makes the decision
RPT – reports the state change at PEP

PDP may at any time change its previous decision: e.g. default policy is overridden for a time. PEP must abide always!

There may be a need to remove state for a object: PDP needs to know.

PDP may need to synchronize its state with PEP



E.g. PDP has failed and after recovery it needs to restore the state of policy objects from the network (i.e. from PEPs)

NB: PEP does not change its state in this procedure!

SSQ – Synchronize State reQuest
SSC – SynchroniSe Complete

Use examples for COPS

- Wireline VOIP: COPS can be used to control a NAT+Firewall (PEP) from a Proxy Server (PDP).
    - Default policy is: all TCP/IP ports for media streams are closed (deny policy)
    - Per SIP session Proxy sends a DEC message to “open the gate” for bi-directional media flow.
    - When BYE is received, gate is again closed
- 3G IMS: to authorize resources for PDP contexts of media flows.

COPS can be used in two modes

- Outsourcing mode
  - PEP contacts the PDP every time a decision needs to be made
- Provisioning mode (COPS-PR)
  - RFC 3084
  - PEPs make local policy decision based on what the PDP has downloaded to the PEP
  - SPPI – Stucture of Policy Provisioning Information (RFC 3159) describes the PIB - Policy Information Base
- IMS uses both modes of COPS!
- Initial implementations of COPS are poor and buggy…

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 multicast group
- Mbone – part of Internet that supports 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.)

SDP can describe

- Session name and purpose
- Time(s) the session is active
  - start, stop time, repetition
- 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.

* = optional

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)

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

NAT Traversal

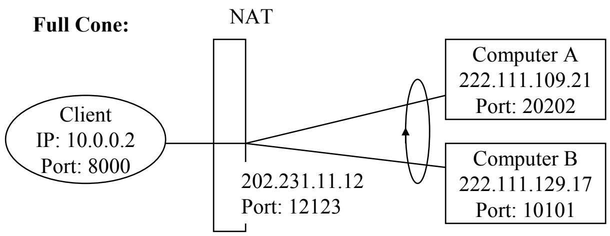
RFC 3489 Title: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network
Address Translators (NATs)
Author(s): J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy
Status: Standards Track Date: March 2003
See also: http://corp.deltathree.com/technology/nattraversalinsip.pdf
Traversal Using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

- For the purpose of IPv4 address saving, many users sit behind Network Address Translators.
- NATs are of 4 types: Full Cone, Restricted Cone, Port Restricted Cone and Symmetric.
- NAT address/port mappings will be dropped after some time of not seeing packets thru the mapping

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

NAT Types 1, 2, 3

Full Cone:

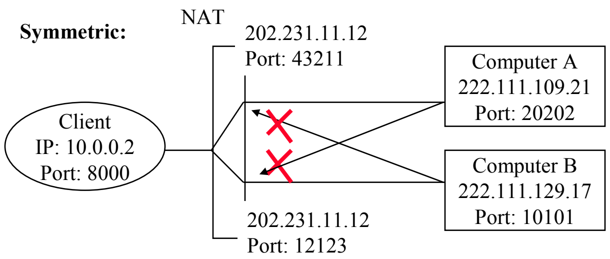


1. Client sends a msg to A
2. A responds to NAT address and port
3. Also B can send msgs to client

Restricted Cone: NAT will block messages from B until Client has sent a msg to B, After that both A and B will see the same mapping in NAT

Port Restricted Cone: NAT will block packets from all ports but the one to which Client has previously sent packets.

NAT type: Symmetric



NAT provides a different mapping for different destinations. Messages from Computer B to Cient will be blocked thru the mapping established for Computer A.

STUN does not allow incoming TCP connections to traverse thru NATs,
STUN does not allow incoming UDP packet thru Symmetric NATs.

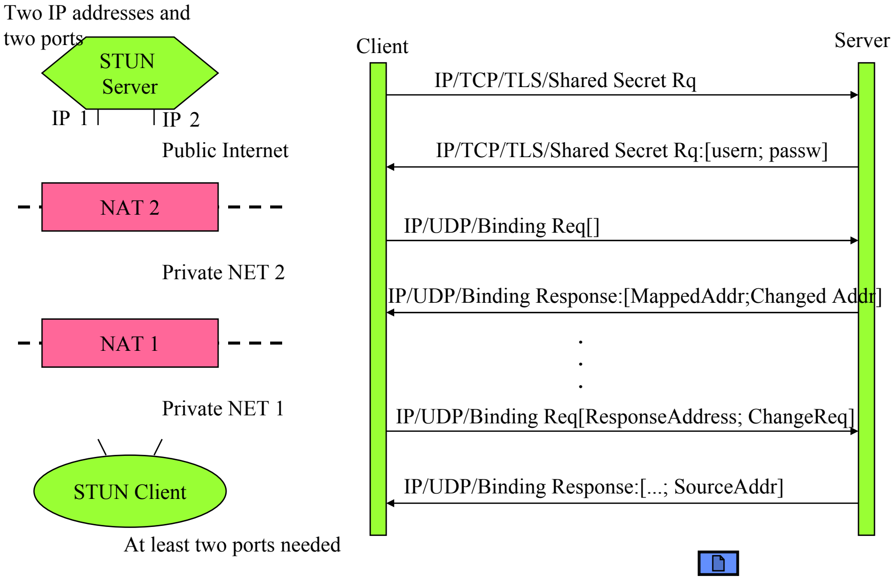
Symmetric NATs are common in large Enterprises.

STUN does not allow communication between two parties behind the same NAT using public Internet addresses.

Alternative approaches of NAT traversal

- Application Gateway: Application functions are embedded in the NAT. These functions rewrite parameters in Application protocol fields, e.g. in SIP messages.
- MIDCOM (RFC 3303) – a protocol is used to control the NAT by an Application proxy server. Requires changes to existing NATs. Requires a control relationship between the NAT and the proxy.
- STUN - allows entities behind a NAT to first discover the presence of a NAT and the type of NAT, and then to learn the addresses bindings allocated by the NAT. STUN requires no changes to NATs, and works with an arbitrary number of NATs in tandem between the application entity and the public Internet.

STUN model assumes nested NATs



Two IP addresses and two ports

STUN Server

IP 1

IP 2

Public Internet

NAT 2

Private NET 2

NAT 1

Private NET 1

STUN Client

At least two ports needed

Client

Server

IP/TCP/TLS/Shared Secret Rq

IP/TCP/TLS/Shared Secret Rq:[usern; passw]

IP/UDP/Binding Req[]

IP/UDP/Binding Response:[MappedAddr;Changed Addr]

.
.
.

IP/UDP/Binding Req[ResponseAddress; ChangeReq]

IP/UDP/Binding Response:[...; SourceAddr]

Types of NAT are discovered by sending responses from different source address and port

Flags	Source Address	Source Port	CHANGED-ADDRESS
none	Da	Dp	Ca:Cp
Change IP	Ca	Dp	Ca:Cp
Change port	Da	Cp	Ca:Cp
Change IP and Change port	Ca	Cp	Ca:Cp

Table 1: Impact of Flags on Packet Source and CHANGED-ADDRESS in Binding Respons

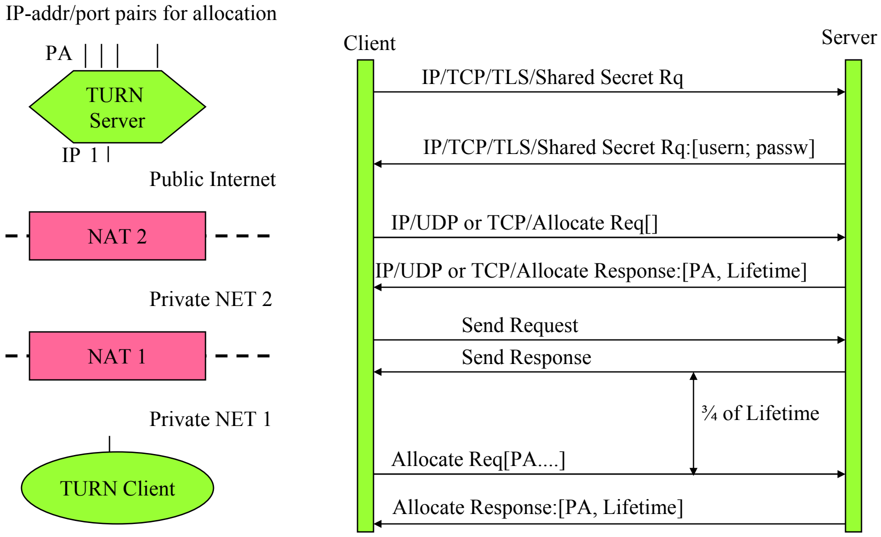
The full procedure of discovering the type of NAT and Firewall is in the RFC

STUN plays with the identity of the user: opens a door for inpersonation. Therefore, security, excluding man-in-the-middle attacks is crucial!
When a SIP application fills in SDP fields and some SIP fields, NAT traversal needs to be taken into account!

Traversal Using Relay NAT(TURN) helps with Symmetric NATs

- TURN allows for an element behind a NAT or firewall to receive incoming dat over TCP or UDP connections from a single Peer.
- TURN does not allow for users to run servers on well known ports if they are behind a NAT
- Based on draft: draft-rosenberg-midcom-turn-03.
- Technically TURN is an extension to STUN (protocol formats and attributes), TURN can be co-implemented with STUN. TURN-server+STUN-server and TURN-cliet + STUN-client
- a TURN server allocates a Public Internet IP-address/port pair (PA) to the Clie Relays messages sent to PA to the Client wrapped in TURN headers.

TURN model is similar to STUN



IP-addr/port pairs for allocation

PA

TURN Server

IP 1

Public Internet

NAT 2

Private NET 2

NAT 1

Private NET 1

TURN Client

Client

Server

IP/TCP/TLS/Shared Secret Rq

IP/TCP/TLS/Shared Secret Rq:[usern; passw]

IP/UDP or TCP/Allocate Req[]

IP/UDP or TCP/Allocate Response:[PA, Lifetime]

Send Request

Send Response

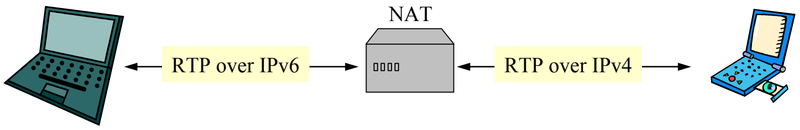
¾ of Lifetime

Allocate Req[PA....]

Allocate Response:[PA, Lifetime]

The whole thing of STUN and TURN becomes ICE = Interactive Connectivity Establishment.

NAT for Interworking IPv6/IPv4



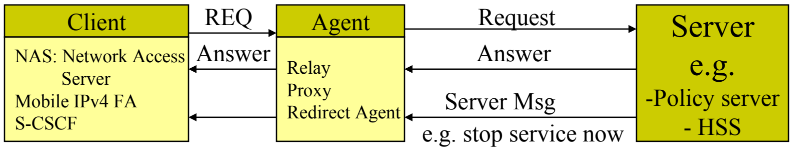
Alternative approaches:

1. Find a suitable NAT using ICE = STUN and TURN (slow)
2. Use ANAT SDP (alternative network address type semantics) to place both IPv4 and IPv6 addresses in an SDP offer (or an answer). As a result, if both endpoints happen to have IPv6 addresses, NAT is not used (complementary to approach 1)
3. Session Policies (”draft: Supporting Intermediary session policies in SIP): This essentially means that one of the CSCF proxies controls a NAT and provides the translation service for IMS terminals (seems like an efficient solution).

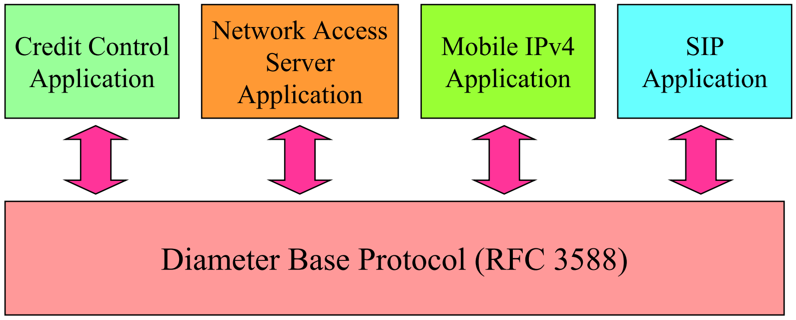
NB: for signaling interworking a proxy with a double IPv6/IPv4 stack is needed on the boundary. It needs to Record-Route to stay on the signaling path for all subsequent messages so that it can translate the underlaying transport protocol (IPv6/IPv4).

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
- Provides ***Authentication*** of users, ***Authorization*** and ***Accounting*** of use
- Carried over TCP or SCTP



Overall Diameter Architecture


Credit Control Application
Network Access Server Application
Mobile IPv4 Application
SIP Application
Diameter Base Protocol (RFC 3588)

Diameter documents

Internet-Drafts:
Diameter Mobile IPv4 Application (134692 bytes)
Diameter Network Access Server Application (197153 bytes)
Diameter Extensible Authentication Protocol (EAP) Application (89596 bytes)
GSMPv3 Base Specification (264992 bytes)
Diameter Credit-control Application (303309 bytes)
Diameter Session Initiation Protocol (SIP) Application (170592 bytes)

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)

Date: 29.12.2004, 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

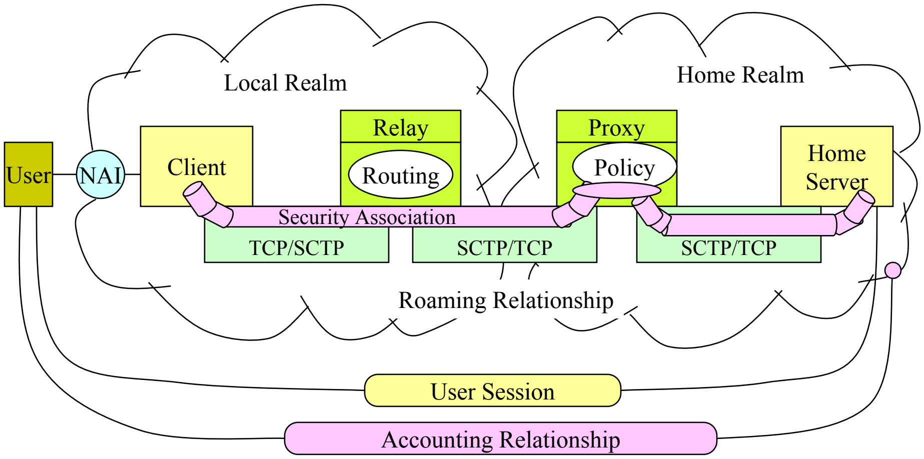
User Authentication

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.

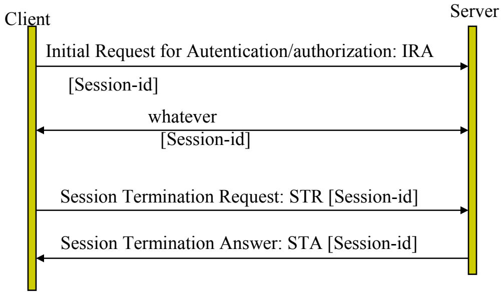
Security Association
A security association is an association between two endpoints in a Diameter session which allows the endpoints to communicate with integrity and confidentially, even in the presence of relays and/or proxies.

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


Client
Server
Initial Request for Autentication/authorization: IRA
[Session-id]
whatever
[Session-id]
Session Termination Request: STR [Session-id]
Session Termination Answer: STA [Session-id]

A diameter node has a peer table

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

origin host
-from capability
exchange:
CER/CEA

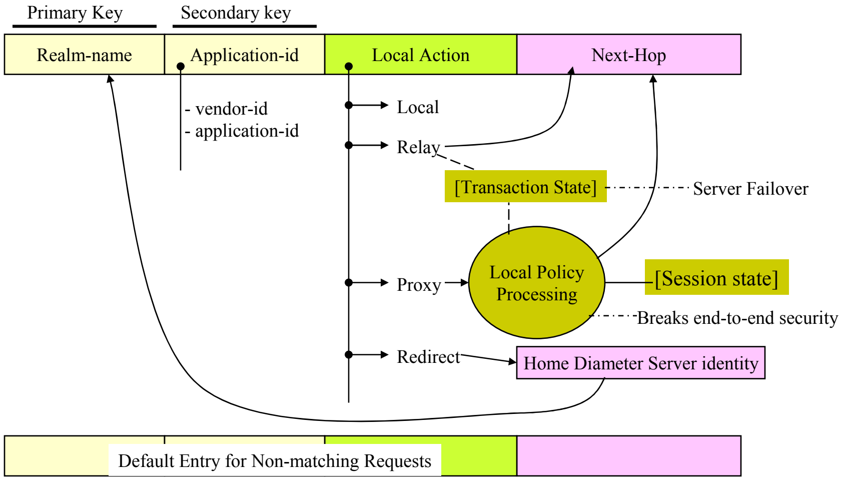
- Closed
- Wait-conn-ack
- wait-I-CEA
- wait-I-CEA/Elect
- wait-returns
- R-Open
- I- Open
- ….
- …
- Stop
- = state of the "dialog" with the peer

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

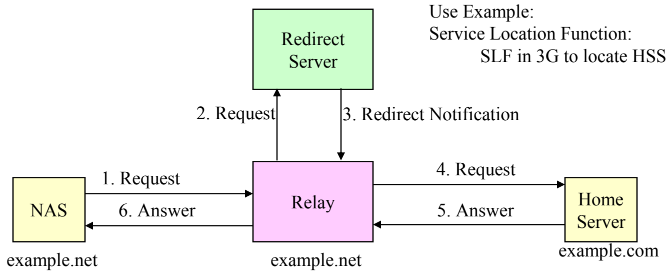
Realm Routing Table describes the actions of a Diameter Node



Primary Key
Secondary key
Realm-name
Application-id
Local Action
Next-Hop
- vendor-id
- application-id
Local
Relay
[Transaction State]
Server Failover
Proxy
Local Policy Processing
[Session state]
Breaks end-to-end security
Redirect
Home Diameter Server identity
Default Entry for Non-matching Requests

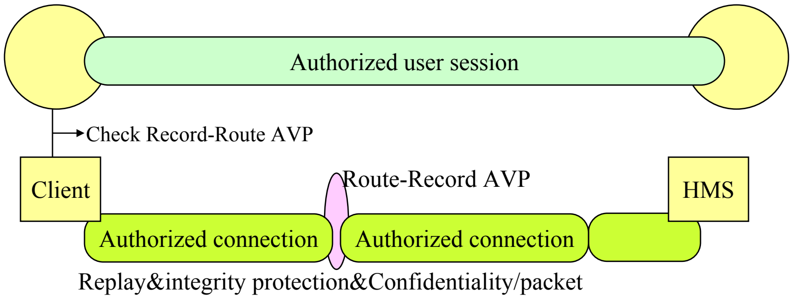
A node can act as proxy for some user connections and as a relay for others.
The Routing Table is configuration information.

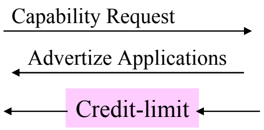
Redirect server helps to centralize Diameter request routing in a roaming consortium



Use Example:
Service Location Function:
SLF in 3G to locate HSS

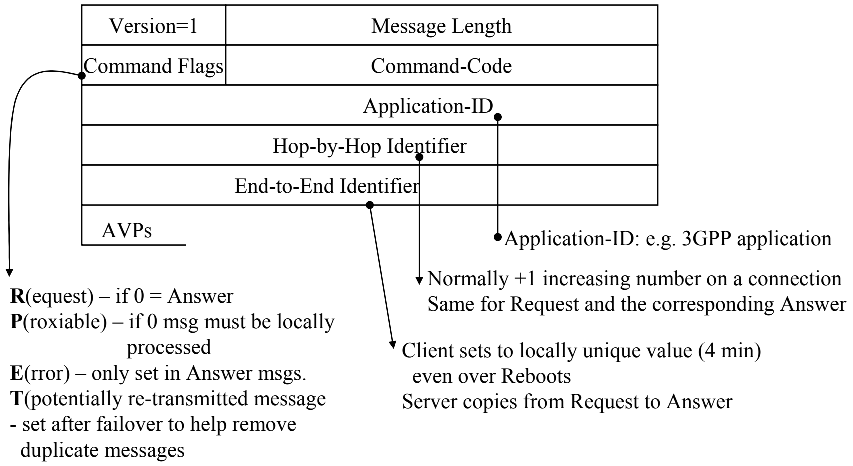
A node must watch over its peers to achieve security





- 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



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

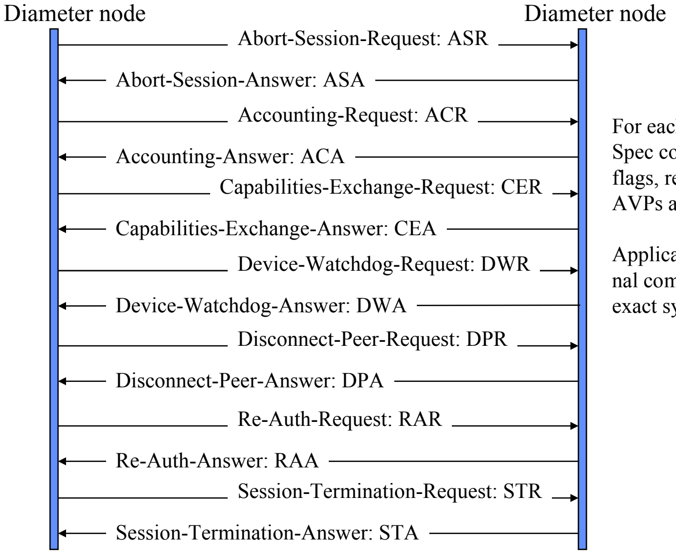
Application-ID: e.g. 3GPP application

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



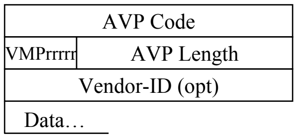
Diameter node
Diameter node
Abort-Session-Request: ASR
Abort-Session-Answer: ASA
Accounting-Request: ACR
Accounting-Answer: ACA
Capabilities-Exchange-Request: CER
Capabilities-Exchange-Answer: CEA
Device-Watchdog-Request: DWR
Device-Watchdog-Answer: DWA
Disconnect-Peer-Request: DPR
Disconnect-Peer-Answer: DPA
Re-Auth-Request: RAR
Re-Auth-Answer: RAA
Session-Termination-Request: STR
Session-Termination-Answer: STA

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.

Base protocol AVPs

AVPs have a common header



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

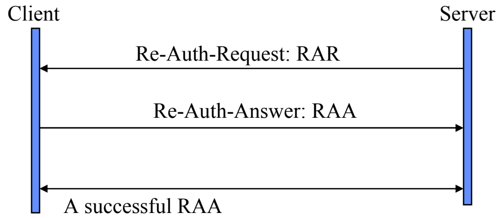
Radius is the current standard for AAA in the Internet. E.g. when an ISP uses accesses the Internet thru a modem line, the POP uses Radius to contact a DB in order to check access rights.
Radius problems are: vulnerability to certain attacks, limited set of attributes are supported and the architecture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

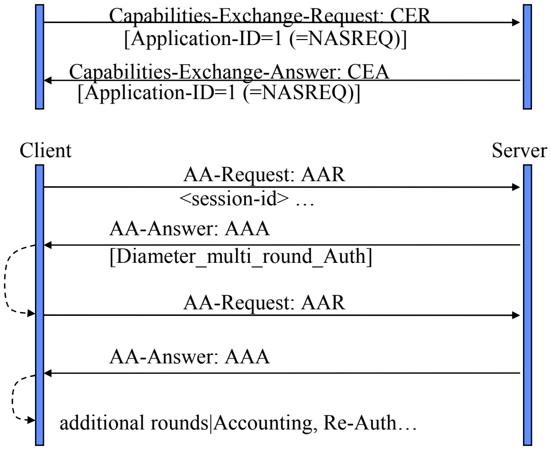


A successful RAA
must be followed by application specific
Authentication/authorization message

Use example: enforcing a credit limit on a user during a long telephone call.

NASREQ defines an authentication and authorization application

draft-ietf-aaa-diameter-nasreq-10.txt of Nov 2002.


Capabilities-Exchange-Request: CER
[Application-ID=1 (=NASREQ)]
Capabilities-Exchange-Answer: CEA
[Application-ID=1 (=NASREQ)]
Client
Server
AA-Request: AAR
<session-id> …
AA-Answer: AAA
[Diameter_multi_round_Auth]
AA-Request: AAR
AA-Answer: AAA
additional rounds|Accounting, Re-Auth…

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

Accounting is defined in BASE.

AAR and AAA have loads of AVPs!

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

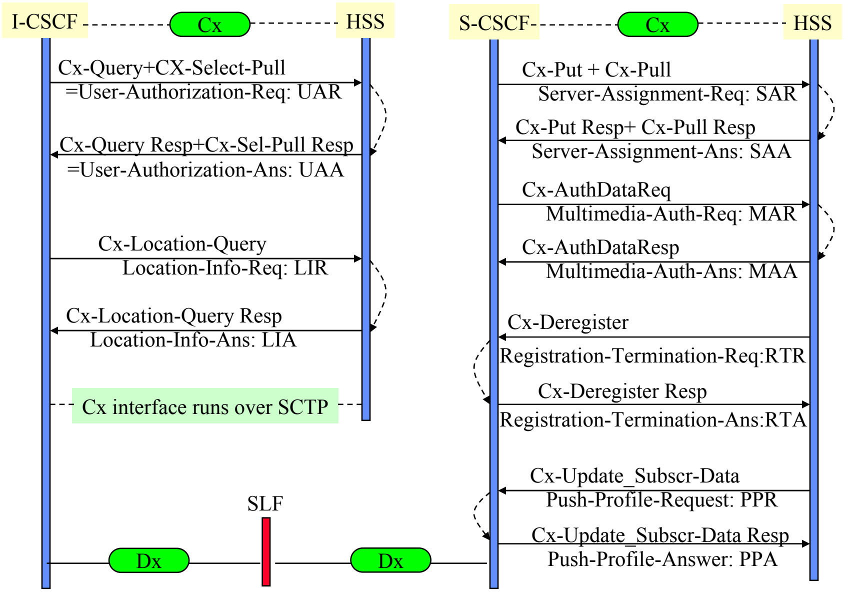
Source: http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-sip-app-05.txt

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

draft-ietf-aaa-diameter-cc-06.txt

3G IMS Diameter migrating to SIP Application



I-CSCF — Cx — HSS

Cx-Query+CX-Select-Pull
=User-Authorization-Req: UAR

Cx-Query Resp+Cx-Sel-Pull Resp
=User-Authorization-Ans: UAA

Cx-Location-Query
Location-Info-Req: LIR

Cx-Location-Query Resp
Location-Info-Ans: LIA

Cx interface runs over SCTP

Dx — SLF — Dx

S-CSCF — Cx — HSS

Cx-Put + Cx-Pull
Server-Assignment-Req: SAR

Cx-Put Resp+ Cx-Pull Resp
Server-Assignment-Ans: SAA

Cx-AuthDataReq
Multimedia-Auth-Req: MAR

Cx-AuthDataResp
Multimedia-Auth-Ans: MAA

Cx-Deregister
Registration-Termination-Req:RTR

Cx-Deregister Resp
Registration-Termination-Ans:RTA

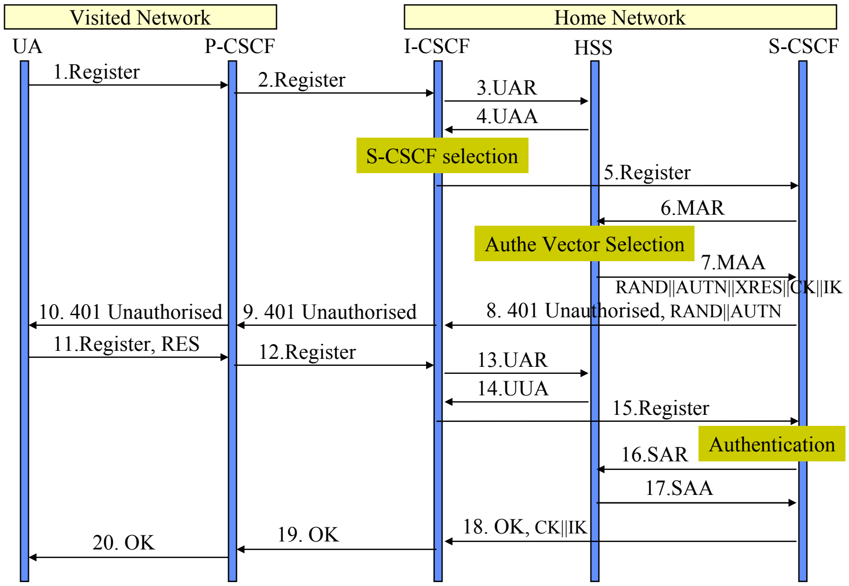
Cx-Update_Subscr-Data
Push-Profile-Request: PPR

Cx-Update_Subscr-Data Resp
Push-Profile-Answer: PPA

Use of Diameter in 3G IMS

- 3GPP has a Vendor-ID, 3GPP Multi Media Application is defined as a vendor specific application. Is expected to migrate to the future Diameter SIP Application when that becomes RFC.
- 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 cash 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.

Registration – user not registered



Visited Network

Home Network

UA

P-CSCF

I-CSCF

HSS

S-CSCF

1.Register

2.Register

3.UAR

4.UAA

S-CSCF selection

5.Register

6.MAR

Authe Vector Selection

7.MAA RAND||AUTN||XRES||CK||IK

8. 401 Unauthorised, RAND||AUTN

9. 401 Unauthorised

10. 401 Unauthorised

11.Register, RES

12.Register

13.UAR

14.UUA

15.Register

Authentication

16.SAR

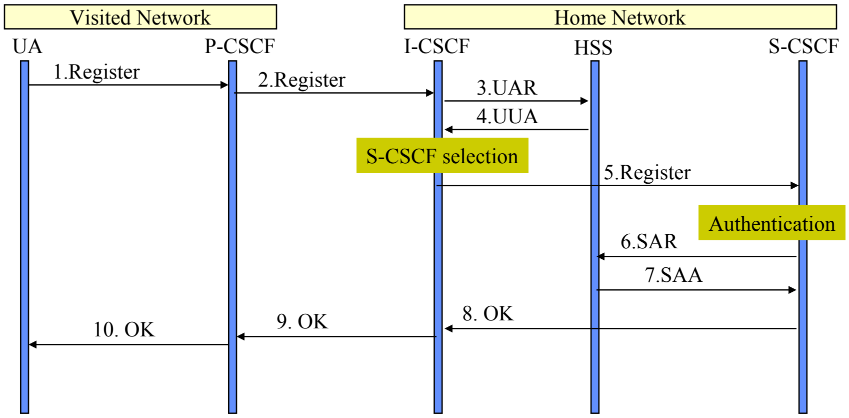
17.SAA

18. OK, CK||IK

19. OK

20. OK

Registration – user currently registered



Visited Network

Home Network

UA

P-CSCF

I-CSCF

HSS

S-CSCF

1.Register

2.Register

3.UAR

4.UUA

S-CSCF selection

5.Register

Authentication

6.SAR

7.SAA

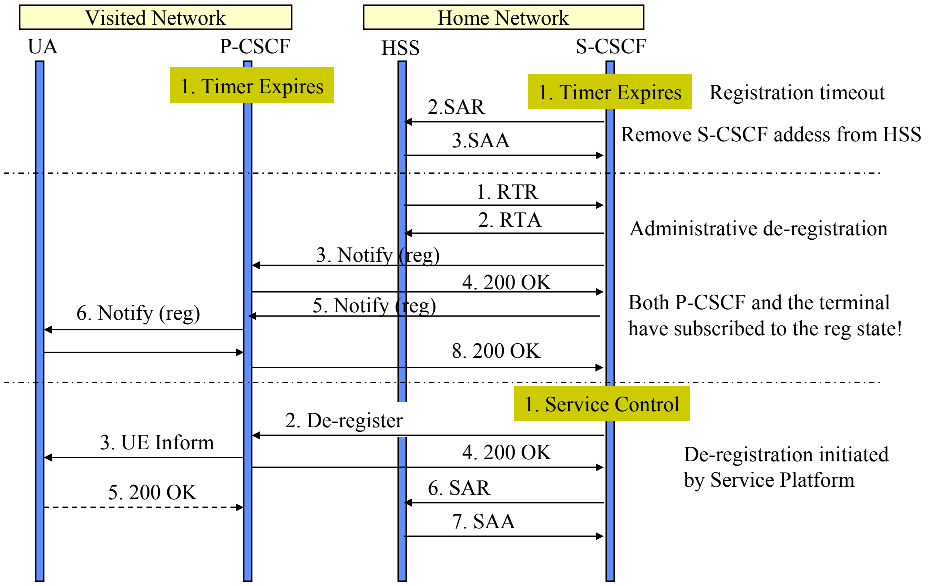
8. OK

9. OK

10. OK

- 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



Visited Network

Home Network

UA

P-CSCF

HSS

S-CSCF

1. Timer Expires

1. Timer Expires

Registration timeout

2.SAR

Remove S-CSCF addess from HSS

3.SAA

1. RTR

2. RTA

Administrative de-registration

3. Notify (reg)

4. 200 OK

5. Notify (reg)

6. Notify (reg)

Both P-CSCF and the terminal have subscribed to the reg state!

8. 200 OK

1. Service Control

2. De-register

3. UE Inform

4. 200 OK

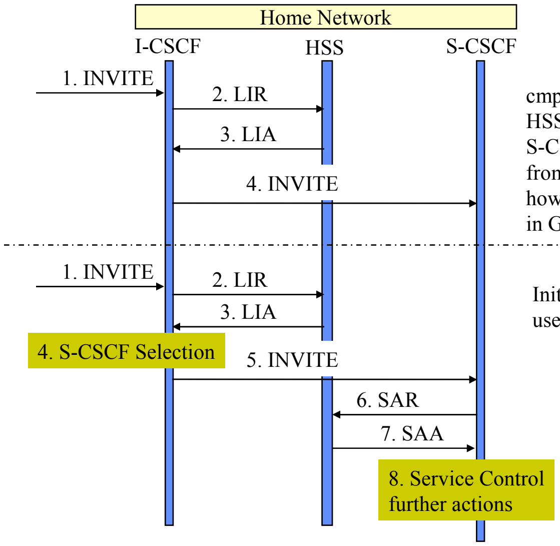
De-registration initiated by Service Platform

5. 200 OK

6. SAR

7. SAA

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.

Summary

- IP telephony requires many supporting protocols.
- Many IETF protocols overlap with GSM protocols (e.g. Diameter with MAP) in terms of functionality
- 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.