IP Multimedia Subsystem

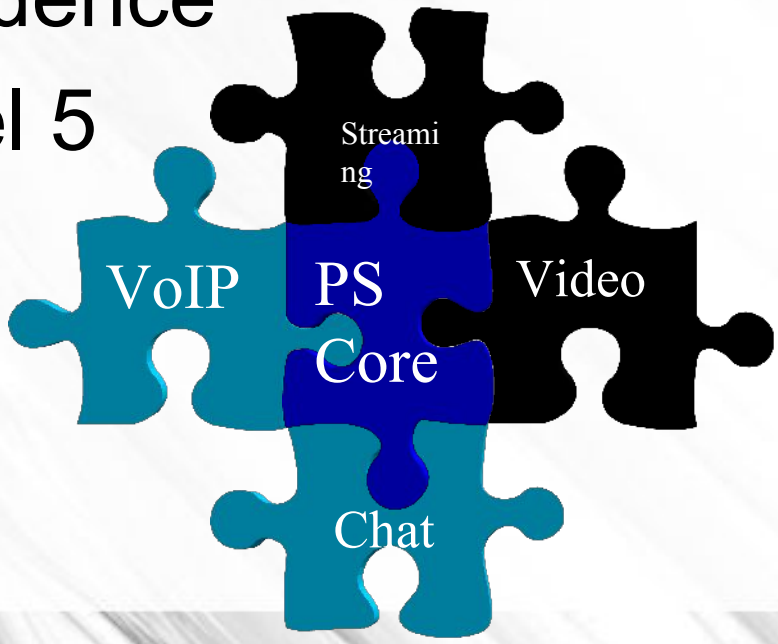
Nathan Bliss

Introduction

- Release 5 ->
- IMS is an IP based core network infrastructure enabling advanced service features involving rich multimedia content
- It is a move towards an all-packet-switched infrastructure

Overview

- IP connectivity & service control architecture for multimedia
- Access independence
- Introduced in Rel 5



Example Services

- VoIP (including PoC/PTT)
- Multiplayer Games
- Session-based peer-to-peer services
- Session-based content services (e.g. streaming)
- Event-based services (e.g.Email)

IPv6 and IPv4

- Interworking supported by 3GPP standards

QoS

- UE can negotiate:
  - Media type
  - Bit rate
  - Packet size

Charging/Billing

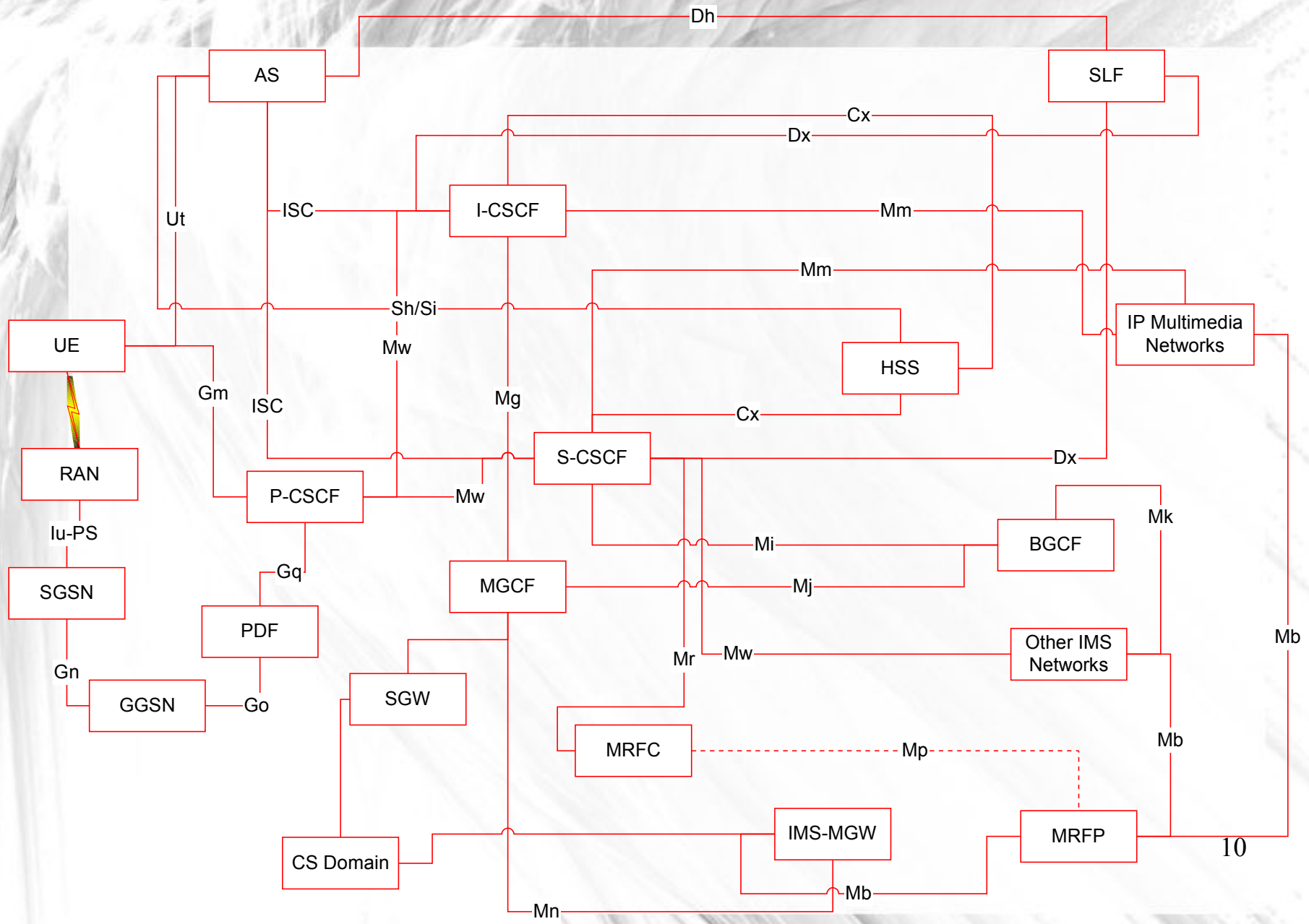
- Entities involved:
  - GGSN
  - IMS
  - Application Server

Service Control Model

- Home-based service control model
- Service development model based on standardising service capabilities, not actual services

Entities in the IMS Architecture

- The next few slides summarise the roles each entity plays in the IMS


Dh
AS
SLF
Cx
Dx
Ut
ISC
I-CSCF
Mm
Mm
Sh/Si
UE
Mw
IP Multimedia Networks
HSS
Gm
ISC
Mg
Cx
RAN
S-CSCF
Dx
P-CSCF
Mw
Mk
Iu-PS
Mi
BGCF
Gq
MGCF
Mj
SGSN
PDF
Mb
Mr
Mw
Other IMS Networks
Gn
SGW
GGSN
Go
MRFC
Mp
Mb
IMS-MGW
MRFP
CS Domain
Mb
Mn

Session Management & Routing

P-CSCF	Proxy Call Session Control Function
I-CSCF	Interrogating Call Session Control Function
S-CSCF	Serving Call Session Control Function

Databases

HSS	Home Subscriber Server
SLF	Subscription Locator Function

Services

AS	Application Server
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor

Interworking

BGCF	Breakout Gateway Control Function
MGCF	Media Gateway Control Function
IMS-MGW	IMS Media Gateway
SGW	Signalling Gateway

Policy Support

PDF	Policy Decision Function
SEG	Security Gateway
THIG	Topology Hiding Inter-network Gateway

Charging/Billing

OCS	Online Charging System
CDF	Charging Data Function
CGF	Charging Gateway Function
CTF	Charging Triggering Function
CRF	Charging Rule Function

P-CSCF

- First point of contact for the user of originating traffic
- Last point of contact before the user for terminating traffic

- Functions of P-CSCF:
  - Compression
  - IP Security Associations
  - Policy enforcement
  - Emergency call detection (ongoing in Rel. 7)

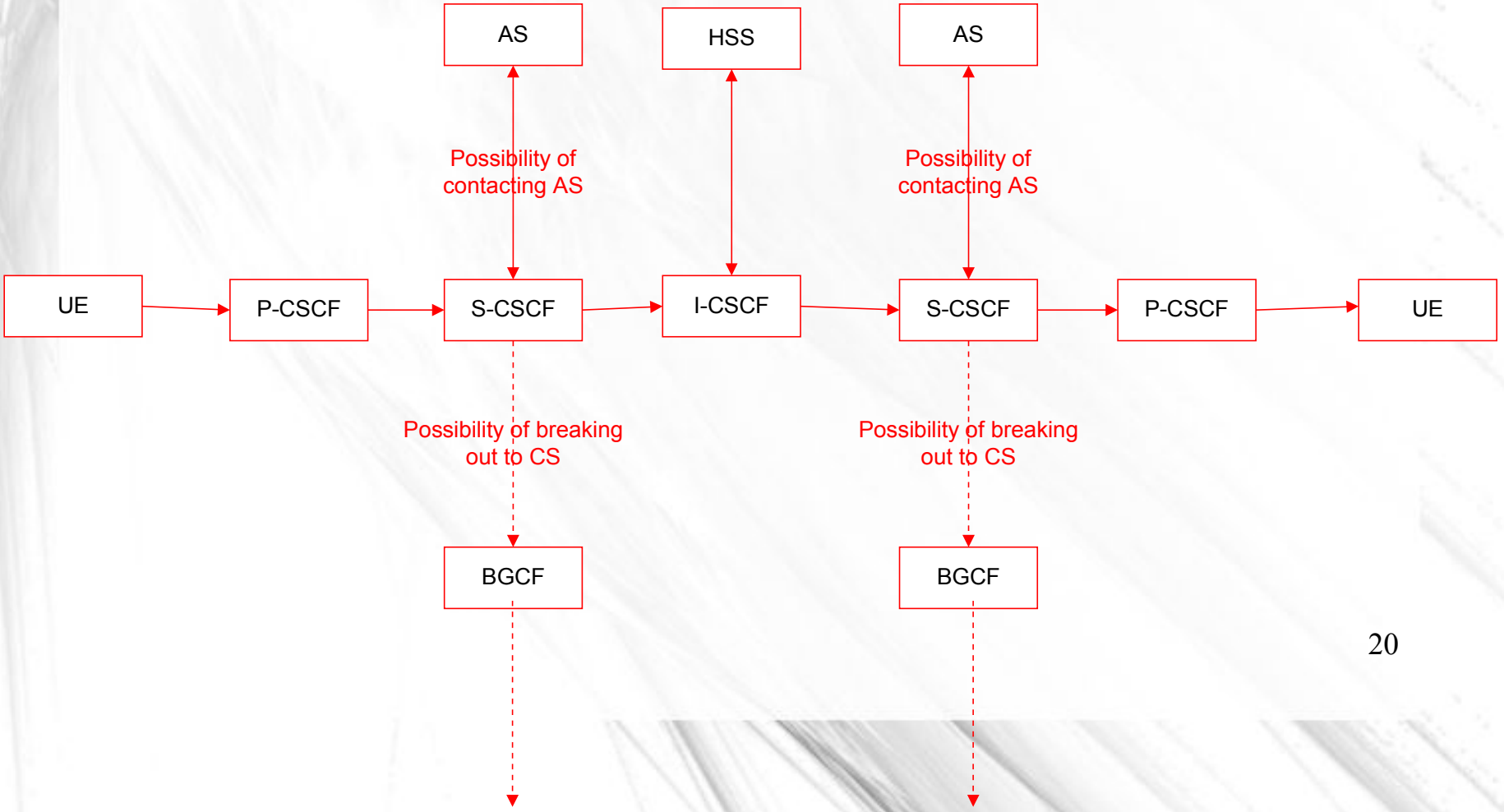
I-CSCF

- Contact point within an operator network for connections targeted to its subscribers
- Functions of I-CSCF:
  - Querying HSS for routing information
  - Assigning a S-CSCF
  - Routing incoming requests
  - THIG functionality (optional)

S-CSCF

- Handles registration
- Maintains session states
- Routing decisions
- Stores service profile
- Downloads security vectors from HSS
- Authenticates users
- Converts Tel URIs to SIP URIs when necessary

Basic CSCF Routing



HSS

- Release 5/6 HLR
- Storage of IMS Access Parameters
- User requirements for S-CSCF capabilities
- Functionality for CS, PS & IP Multimedia

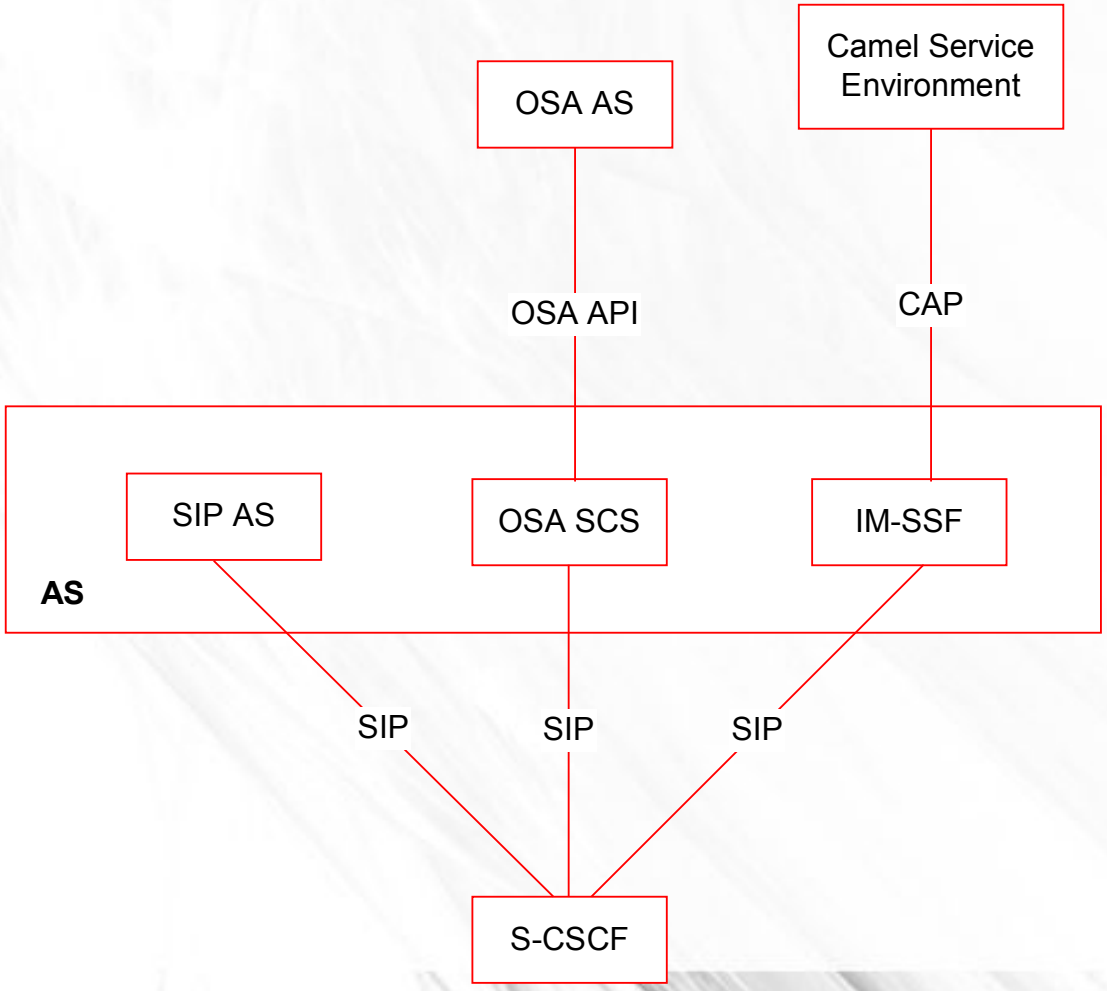
SLF

- HSS Locator
- Used in the case of multiple HSS nodes deployed within one PLMN

Application Servers

- Servers that host and execute services
  - e.g. Call Control, user interaction, etc
- Can be SIP-based
  - e.g. SIP App Servers used for PoC, streaming, etc

AS Types


OSA AS
Camel Service Environment
OSA API
CAP
SIP AS
OSA SCS
IM-SSF
AS
SIP
SIP
SIP
S-CSCF

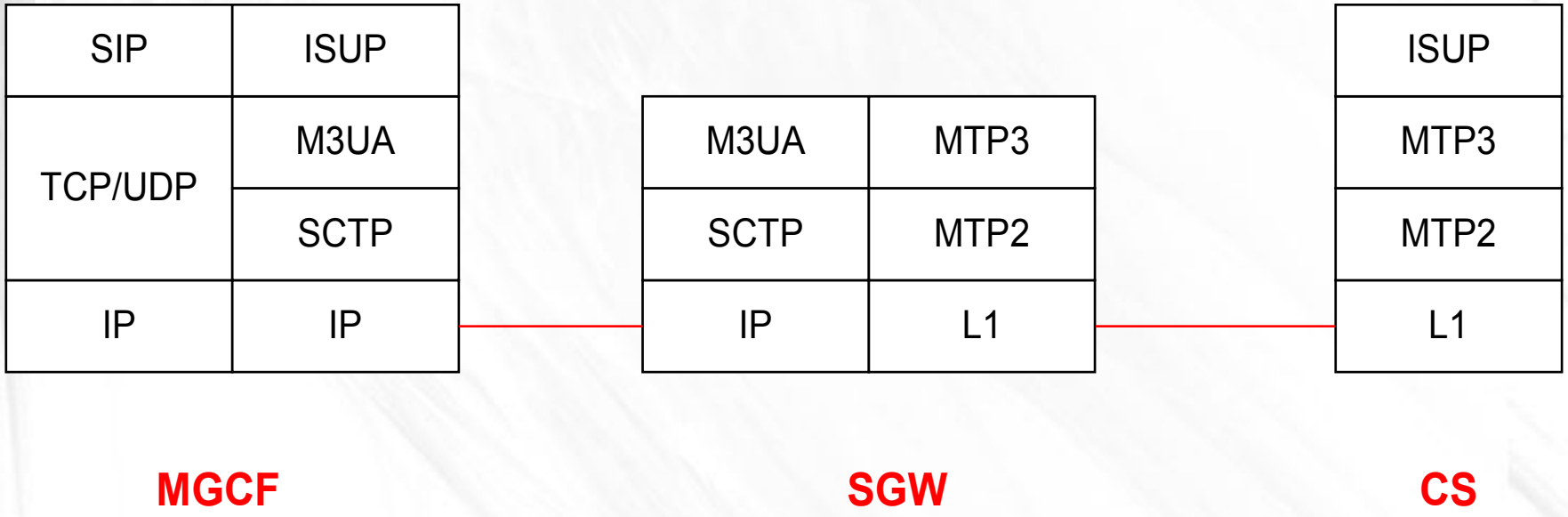
MRFC & MRFP

- Transcoding
- Mixing of media streams
- Announcements

BGCF

- This network entity is used where a SIP session is “broken out” to the Circuit-Switched domain
- Entails conversion between SIP and ISDN (ISUP) protocols
- Resulting ISUP request is then forwarded to the SGW

VoIP←→ISDN Signalling Conversion



IMS-MGW

- Controlled by MGCF
- Implements actual plane bearer switching functionality

PDF

- Authorisation
- Admission Control
- Releases Authorisation Tokens
- Maps SDP parameters to a specific PDP Context QoS

SEG

- Secures control-plane traffic between security domains
- Mandatory security features:
  - Confidentiality
  - Data Integrity
  - Authentication

THIG

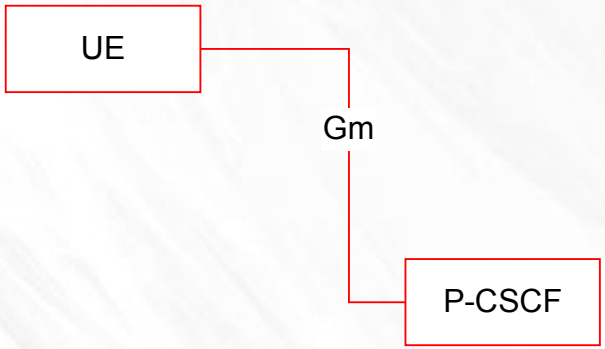
- Hides details of network beyond
- Must be placed in routing path if THIG features are desired
- Encrypts/decrypts headers which reveal topology information

IMS Reference Points

- The next few slides give a short summary of each of the IMS reference points
- Charging/billing is described separately

Gm Interface

- Connects UE to IMS (via P-CSCF)

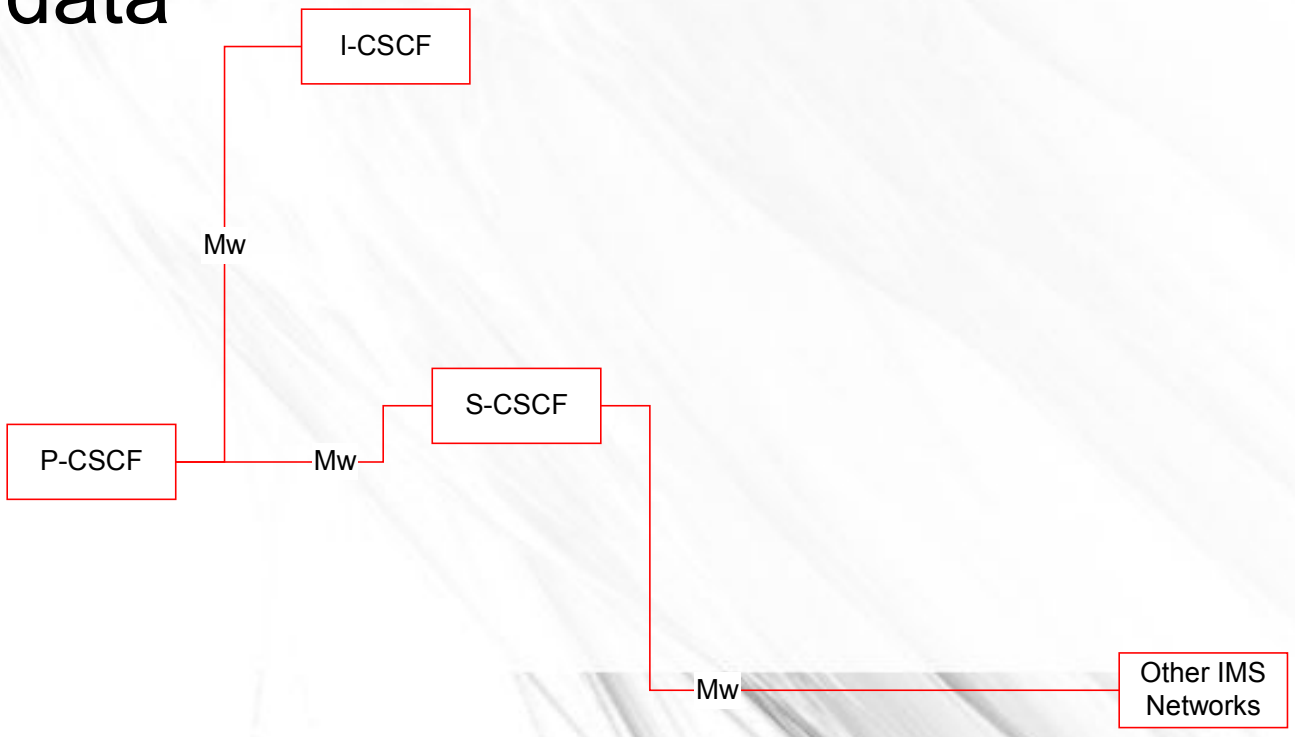


Gm Interface

- Used by UE for:
  - Sending of Registration Request with indication of supported security mechanisms
  - Exchange of parameters enabling mutual authentication
  - Negotiation of parameters for security association
  - Initiation of SIP compression
  - Reception of implicitly registered user identities
  - Establishment of session control procedures (dialog-based) or transaction procedures (e.g. Message)

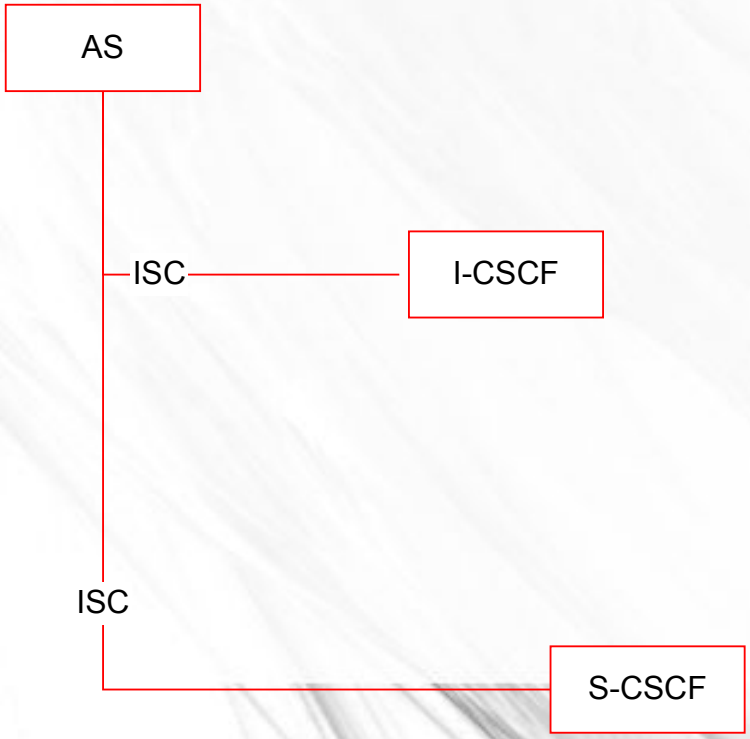
Mw Interface

- Links the different CSCFs together
- Also used to relay charging related data



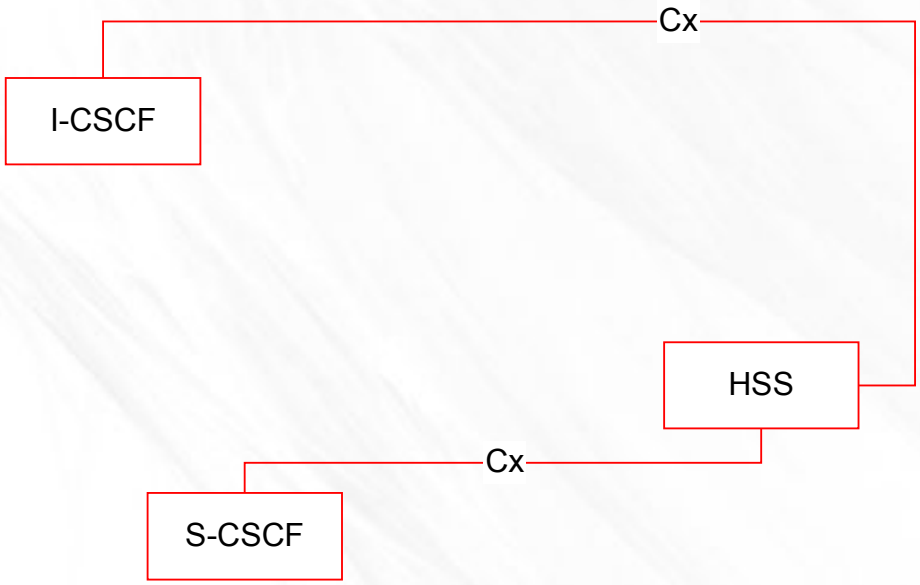
ISC Interface

- IMS Service Control
- SIP-based
- Used for service control between CSCF & AS



Cx Interface

- Links I-CSCF/S-CSCF to HSS



Cx Interface

- DIAMETER protocol
- Location management
- User Data Handling
- User Authentication

- The Cx Interface is described in more detail in the following slides…

Location Management

- Includes Registration/de-registration
- Includes location retrieval

❖ Message Sequence Chart

- Registration Termination Request (RTR/RTA) is initiated by HSS for de-registration
- Location Information Request (LIR/LIA) is used to query HSS for assigned S-CSCF for methods other than registration

User Profile Data Handling

- Push-Profile-Request (PPR/PPA) used by HSS to update S-CSCF with user profile data

Authentication

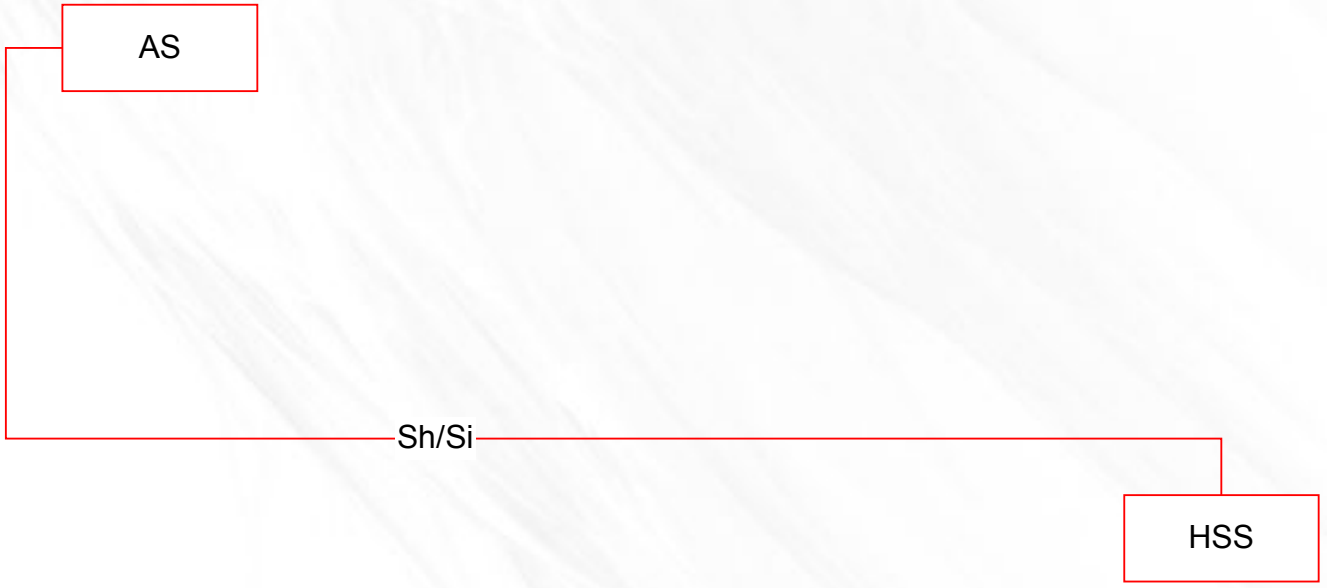
- Multimedia-Auth-Request (MAR/MAA) sent by S-CSCF to HSS
- MAA contains an Authentication Vector (Scheme, RAND, AUTN, XRES, IK, CK)

Dx Interface

- Interface between I-CSCF/S-CSCF & SLF
  - Used with multiple HSS nodes deployed in one PLMN

Sh & Si Interfaces

- Interface between HSS & AS



Sh Interface

- Example messages:
  - User-Data-Request (UDR)
  - User-Data-Answer (UDA)
  - Profile-Update-Request (PUR)
  - Profile-Update-Answer (PUA)
- DIAMETER
- HSS contains list of ASs permitted to retrieve/store data

Sh Interface

- Examples of data passed over Sh:
  - Name of S-CSCF serving user
  - Charging function addresses
  - Location data

Sh Interface

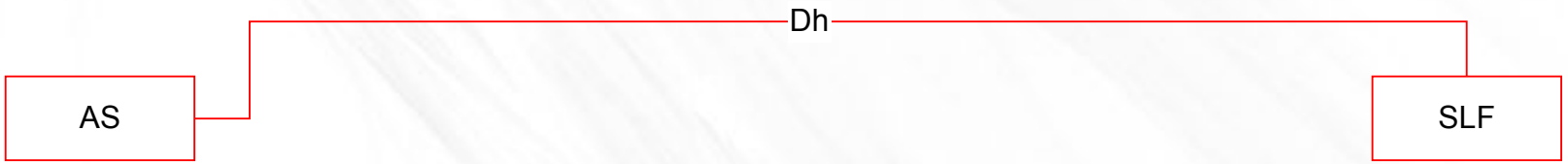
- Subscription/Notification:
  - Allows AS to receive notifications for changes to user data stored in the HSS
  - AS sends SNR (Subscribe-Notifications-Request)
  - HSS acknowledges subscription with SNA
  - HSS sends Push-Notification-Request (PNR) to AS to notify AS of changes (PNA acknowledges)

Si Interface

- Used between CAMEL AS (IM-SSF) & HSS
- Used for transport of CAMEL subscription data including triggers from HSS to IM-SSF

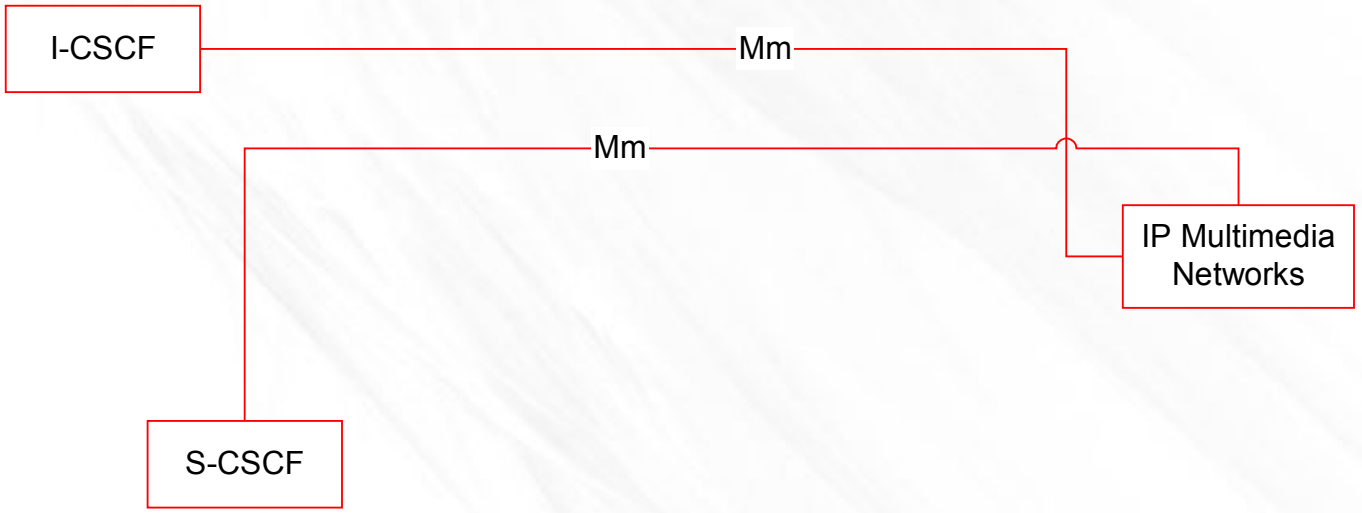
Dh Interface

- Interface between AS & SLF
- Introduced in Rel 6
- Used in conjunction with Sh interface
- DIAMETER



Mm Interface

- Interface between CSCFs and external IP multimedia networks

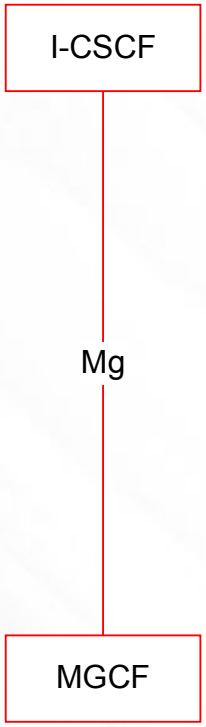


Mm Interface

- Allows I-CSCF to receive a session request from an external SIP server or SIP terminal
- Allows S-CSCF to forward requests to external multimedia IP networks

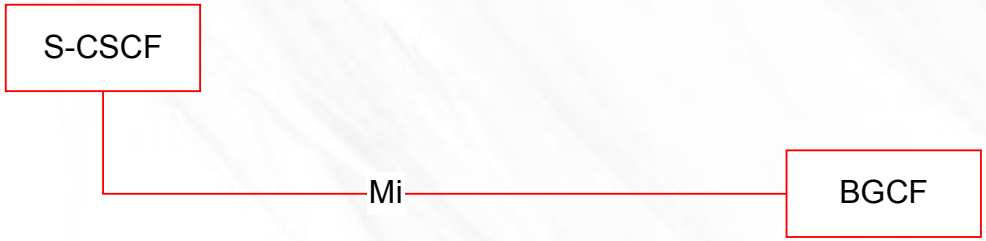
Mg Interface

- Interfaces the CS edge function (MGCF) to I-CSCF
- SIP-based



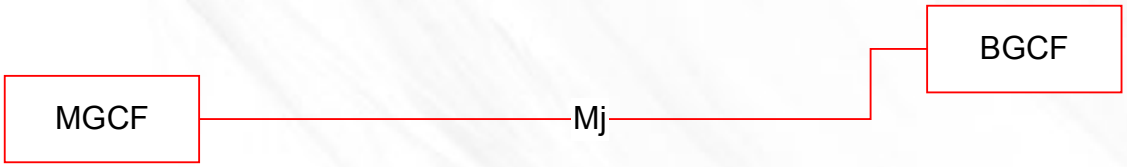
Mi Interface

- Interface between S-CSCF & BGCF
- SIP-based
- Used when S-CSCF determines that a request needs to be routed to the CS domain



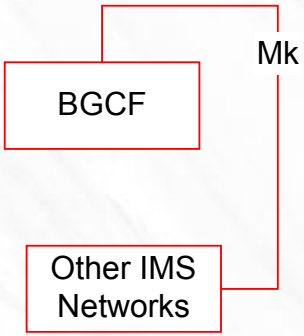
Mj Interface

- Interface between MGCF & BGCF
- SIP-based
- If breakout to CS domain occurs in same PLMN, BGCF forwards the session to MGCF via this interface



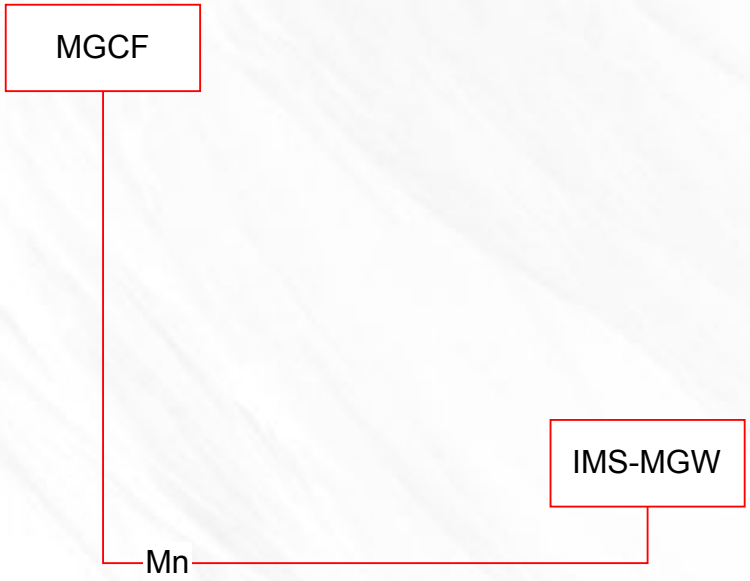
Mk Interface

- Used by BGCF to interface with another network's BGCF for breakout to CS domain in another network



Mn Interface

- Interface between MGCF & IMS-MGW

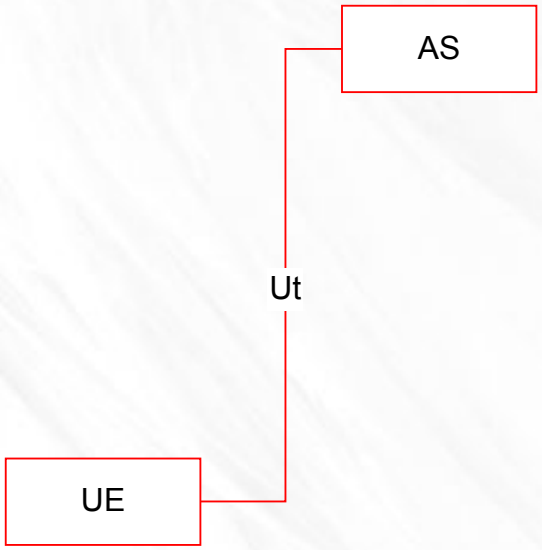


Mn Interface

- Based on H.248
- Controls user plane for user plane functions. e.g:
  - User bearer IP media connections
  - Invocation of echo cancellers
  - DTMF tones
  - Announcements

Ut Interface

- Interface between UE & AS



Ut Interface

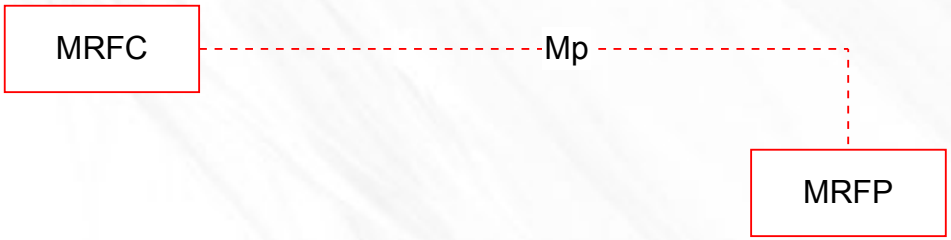
- Gives users HTTP access to web pages allowing them to configure profile & service options
- Standardized in Release 6

Mr Interface

- Interface between S-CSCF & MRFC
- Used to activate bearer related services such as the playing of an announcement

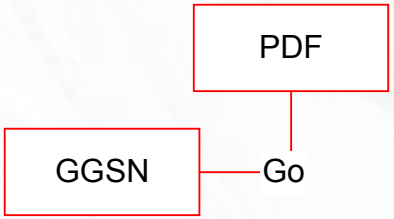
Mp Interface

- Allows MRFC to control MRFP
- H.248-based
- For control of media streams, such as creating connections for conference media



Go Interface

- Interface between GGSN & Policy Decision Function (PDF)

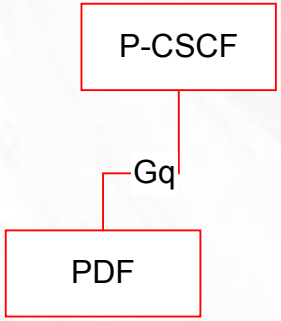


Go Interface

- Based on COPS (Common Open Policy Service) protocol
- Allows GGSN to implement the QoS negotiated at the IMS level by querying the Policy Decision Function
- Also used for charging correlation between IMS & PS RAB domains

Gq Interface

- Interface between P-CSCF & PDF



Gq Interface

- Transports policy setup information to the PDF
- Used to also deliver:
  - Authorisation token
  - Charging IDs
  - GGSN IP addresses

IMS Registration

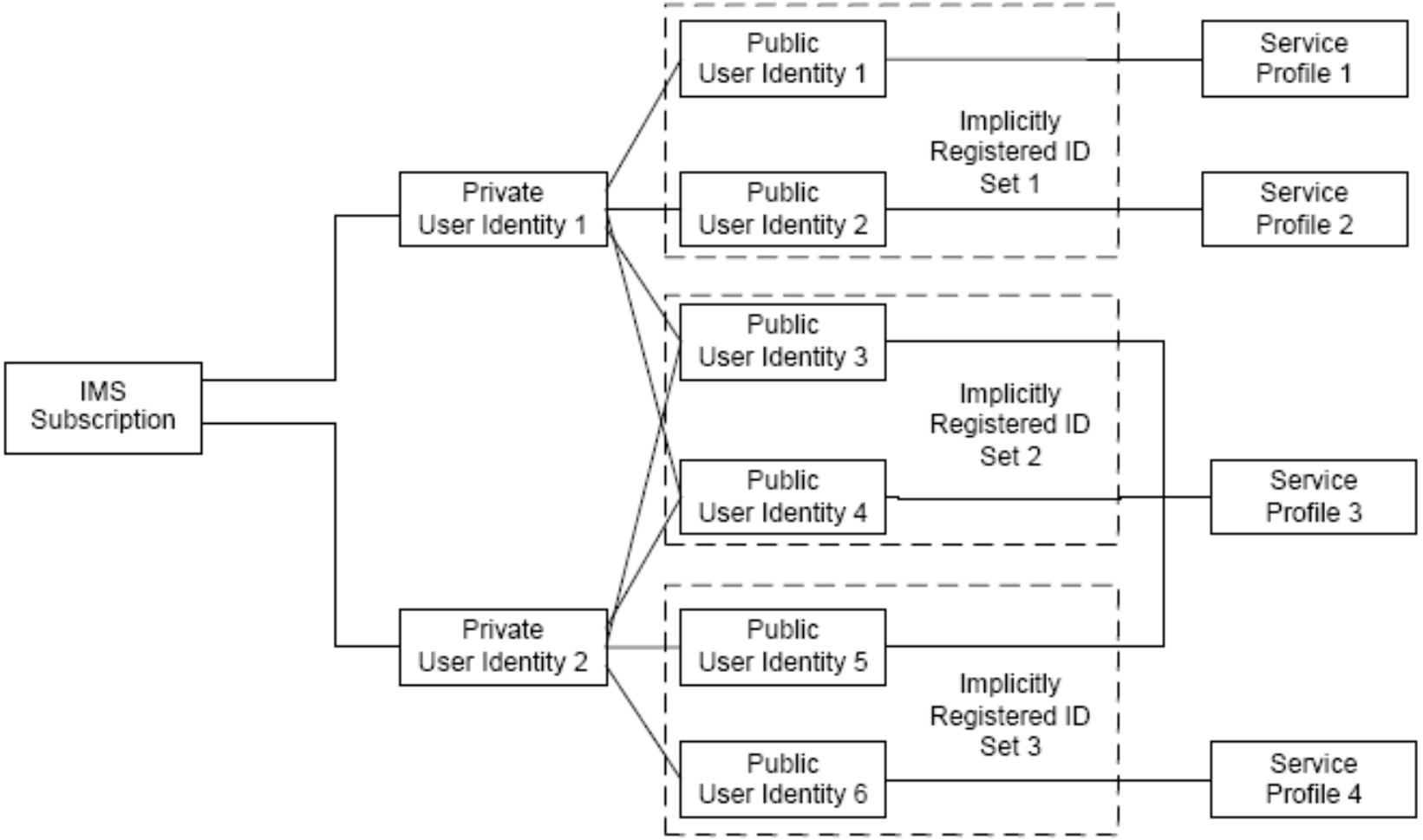
- Message Sequence Chart Part1
  - Part2

- UE must periodically refresh its registration
- S-CSCF will implicitly de-register UE when registration timer expires
- UE sets expiry timer to zero to de-register

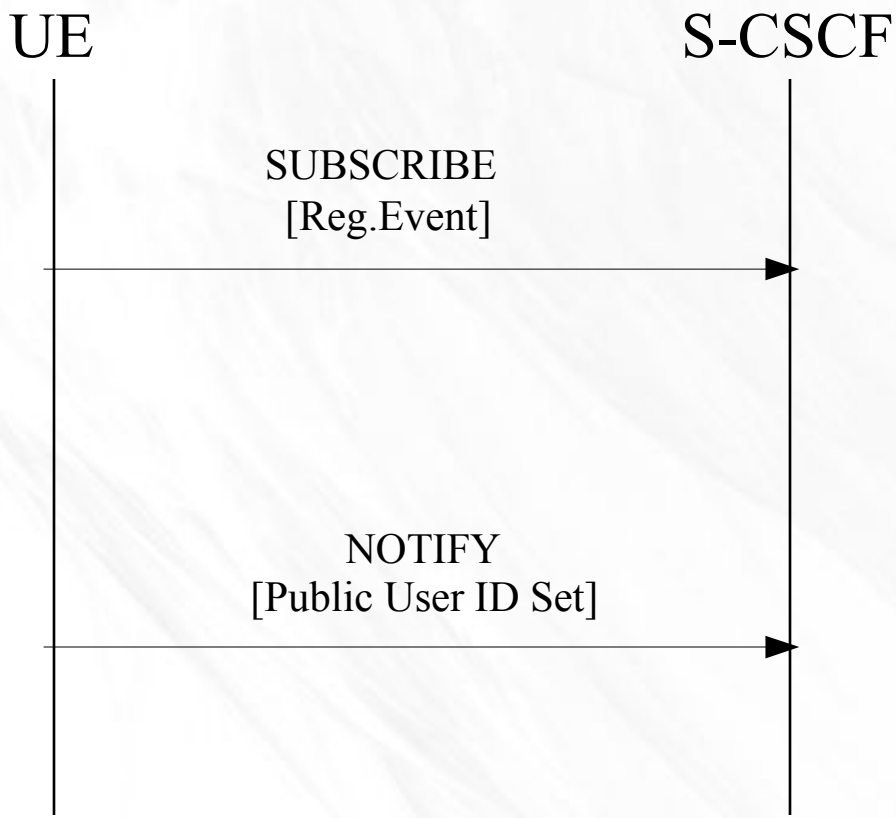
Implicit Registration

- 3GPP extension
- Allows a group of public user identities to be registered after one single explicit registration request containing one of the public user identities
- Same thing can apply to de-registration
- User IDs in implicit registration request can point to different service profiles

User Profile



User of SUBSCRIBE to fetch Public User ID Set



Session Initiation

IMS Session Establishment

- This message sequence chat gives the call flow for basic IMS session establishment

User Identities: Private User Identity

- Defined by HPLMN and stored in ISIM application & HSS
- Identifies user subscription in Registration Request
- Sent within all registration requests and stored by S-CSCF
- Cannot be modified by the user
- NOT used for SIP message routing

User Identities: Public User Identity

- Published and available to other users
- SIP-URI or tel-URI format
- At least one PuUID stored in ISIM
- Cannot be modified by UE
- Multiple PuUIDs can be registered
- Identifies an ID to be registered in a Registration Request and used for requesting contact with other parties

URI Examples

- SIP-URI:

  sip:user@ims.com

- tel-URI:

  +4915151454704

Mechanism for Legacy USIMs

- Derived from IMSI
- PrUID:

  <IMSI>@<MNC>.<MCC>.IMSI.3gppnetwork.org

- Temporary PuUID:

  sip:<IMSI>@<MNC>.<MCC>.IMSI.3gppnetwork.org

  - Used only by CSCF & HSS elements
  - Should be set to “barred”

- Implicitly registered PuUIDs used after initial registration

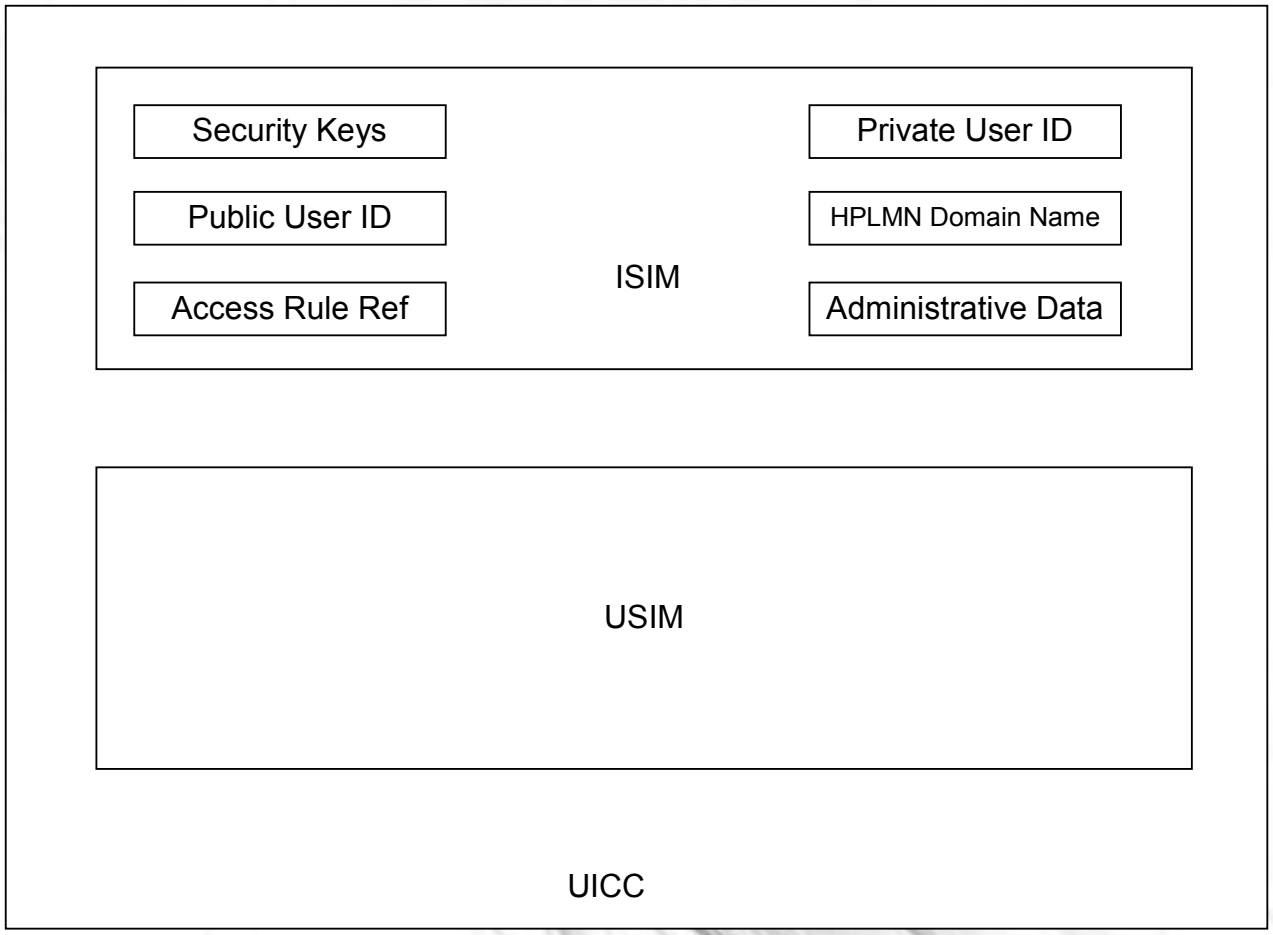
Public Service Identities

- Example: Used for a distribution list or conference
- Allows 1 SIP URI to identify a list or service

- SIP URIs can also be used for identifying network elements. e.g:

  sip:voda.scscf2@ims-network.com

ISIM, USIM & UICC



Sharing a Single User ID Between Multiple Devices

- Differentiation based on PrUID
- Note: IMS supports sequential forking & parallel forking

Proxy CSCF Discovery

- There are two Standardized mechanisms specified in 3GPP:

  GPRS Procedure

  - Data is contained in Protocol Configuration Options IE in PDP Context Messages
  - Release 6 & later GGSNs only

  DHCP/DNS Procedure

  - This is an access-independent method

S-CSCF Assignment

- Executed when a user registers
- Executed when an unregistered user receives a SIP request
- Executed during fault recovery

- I-CSCF receives S-CSCF capabilities from HSS for selection:

  Server-Capabilities Attrubute Value Pair (AVP)

  Selection algorithms are not standardized

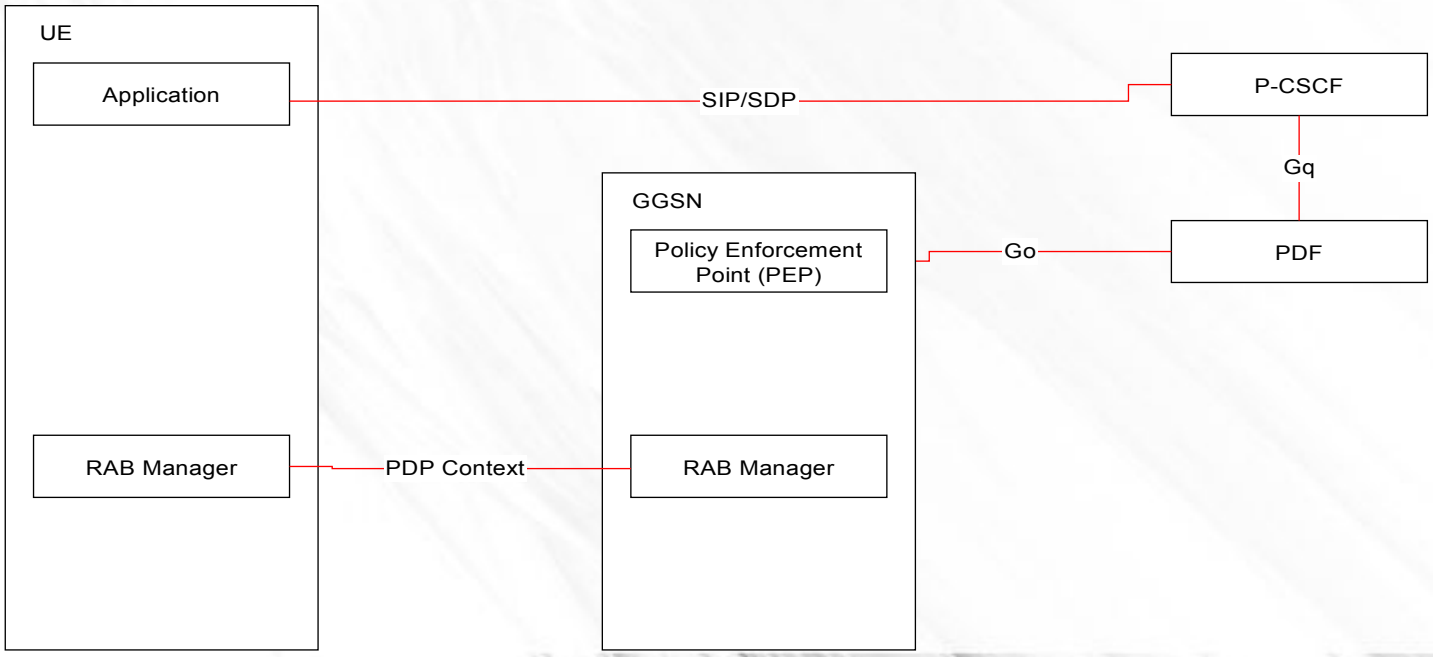
- Note: S-CSCF has option to maintain user profile after de-registration for optimisation purposes

AVP Types

- Mandatory
- Optional
- Server-Name (server SIP URI)

Control of Bearer Traffic

- Interaction between IMS & GGSN known as *"Session Based Local Policy"* (SBLP) control



PDF (Policy Decision Function)

- Fully integrated with P-CSCF in Release 5
- Allows and Provisions QoS attributes via the PDP Context

Policy Enforcement Point (PEP)

- GGSN function
- Enforces decisions made by the PDF

SBLP Functions

- Bearer Authorisation:
  - Involves PDF mapping SDP parameters to IP QoS parameters
- Authorisation Token:
  - Created in PDF
  - Delivered to UE, which then includes it in a PDP Context Activation Request
  - GGSN then uses this to identify authorising PDF
- Authorisation token & flow identifiers are inserted into TFT information element

SDP Example

```
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=inactive
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=inactive
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

Media Grouping

- GGSN can force UE to use separate PDP contexts for different media
- SDP component called "Single Reservation Flow" (SFR) is use for this purpose
- Release 6 adds capability to charge on an IP flow basis

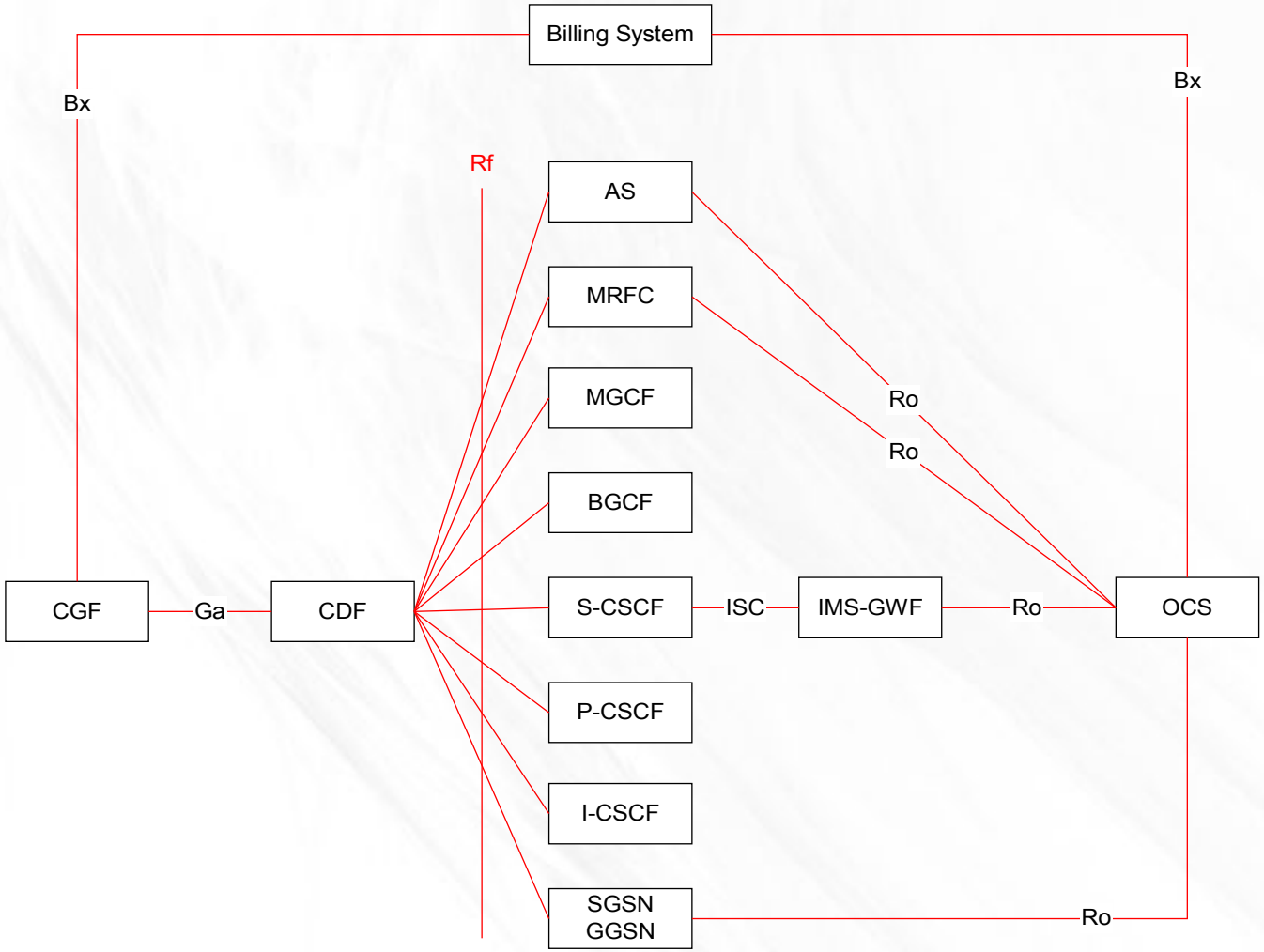
QoS Parameter Types

Traffic Class	Max DL rate
Guaranteed DL rate	Max UL rate
Guaranteed UL rate	Max SDU size
SDU format data	BER
SDU error ratio	Traffic-handling Priority
Delivery of errorneous SDUs	Allocation/Retention Priority
Transfer Delay	Delivery Order
Source statistics descriptor	

Maximum Allowed UMTS Traffic Class per Media Type

UMTS Traffic Class	Media Type (m-line in SDP)
Conversational	Bi-directional audio/video
Streaming	Uni-directional audio/video
Conversational	Application
Interactive	Data
Interactive	Control
Background	Others

IMS Charging Architecture



Offline Charging

- Based on trigger conditions, such as beginning and end of IMS sessions
- CDF is the central point in offline charging system
- DIAMETER Accounting Requests (ACRs) sent to CDF via Rf interface
- CGF is needed to consolidate data from (possibly) multiple CDFs
- Message Sequence Chart

Offline Charging Functions

- Charging Triggering Function (CTF):
  - Monitors SIP signalling
  - Detects trigger conditions
  - Extracts data from SIP signalling & assembles charging data
  - Sends charging data to CDF
- Charging Data Function (CDF):
  - Constructs CDRs
  - Delivers CDRs to CGF

Offline Charging Functions

- Charging Gateway Function (CGF):
  - Correlatation, consolidation, filtering functions & addition of operator-specific info
  - CDR error handling & storage
  - Processing of CDRs
  - Delivery of CDRs to billing system
- Billing System:
  - Creates the actual bill

Online Charging

- Direct Debiting:
  - IMS entity sends request to OCS which finds correct tariff & checks subscriber's credit (known as " Immediate Event Charging" in 3GPP terminology)
- Unit Reservation:
  - OCS reserves an amount from the subscriber's account which is consolidated at regular intervals (3GPP: " Session Charging")

Correlation of Charging Data

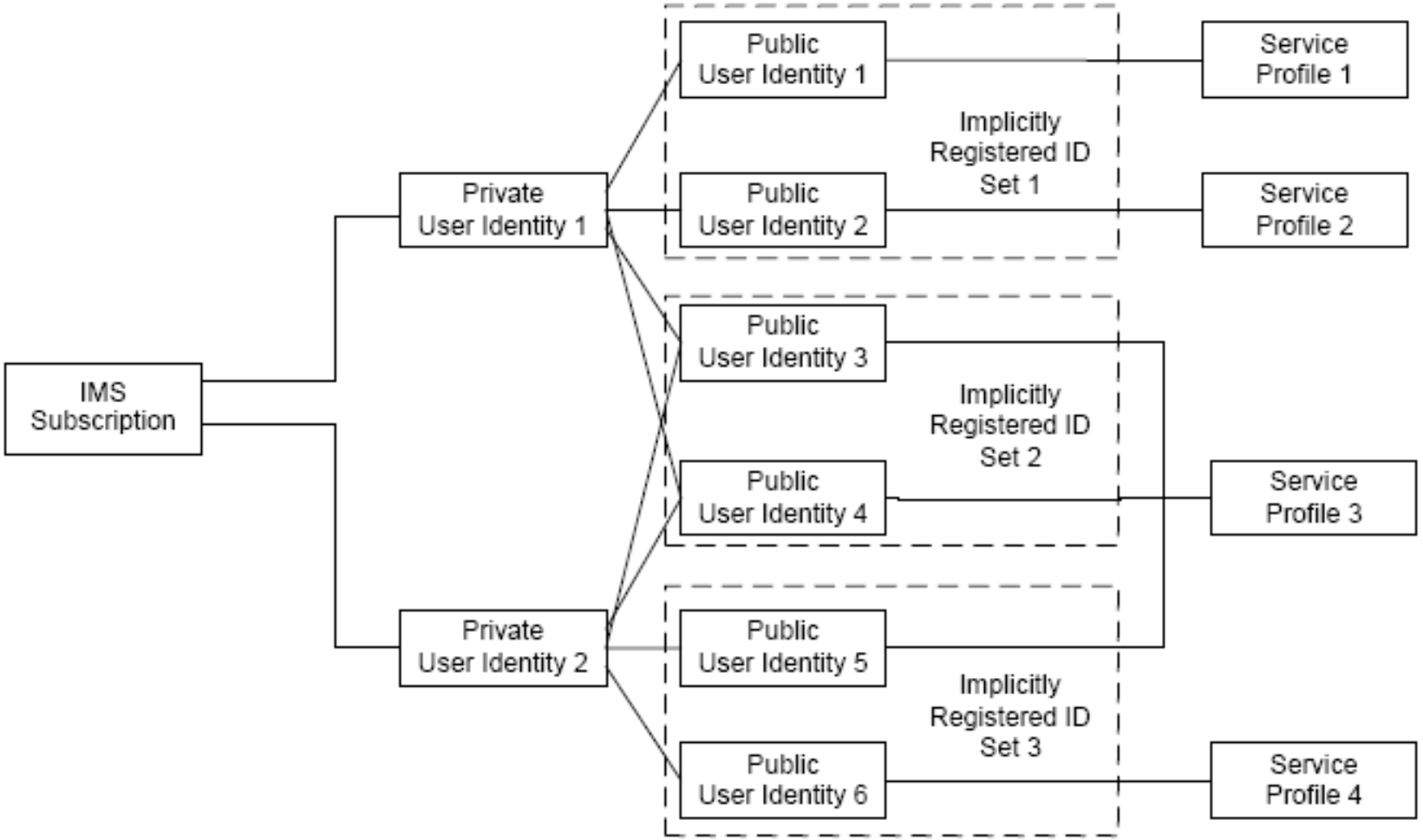
- IMS Charging Identifier (ICID)
- GPRS Charging Identifier (GCID)
  - Allows charging correlation between IMS & IP-CAN

Distribution of Charging Data

- COPS: Common Open Policy Service
- COPS-PR: Common Open Policy Service Usage for Policy PRovisioning

❖ Message Sequence Example
  - Part1
  - Part2

User Profile



User (Agent) Profile

- Contains at least 1 PrUID
- Contains at least 1 Service Profile
- May contain more than 1 PrUID

❖ See example file [UserProfile.htm]

Service Profile

- Sent from HSS to S-CSCF in SAA (Server Assignment Answer) & PPR (Push-Profile-Request)
- Carried in 1 DIAMETER AVP as an XML document
- Consists of 3 parts:
  - Public ID
  - Core network service authorisation (e.g. Permitted SDP parameters)
  - Initial Filter Criteria

Initial Filter Criteria

- Triggers onward routing of SIP message to Application Server
- Contains Trigger Points
  - Absence of a trigger point can be used for unconditional routing to Application Server
- Trigger Point contains one or more Service Point Triggers

Service Point Trigger

- Request URI (identifies a target resource)
- SIP Method (e.g. INVITE, MESSAGE)
- SIP Header
- Session Case
  - Originating, Terminating or Terminating-Unregistered
- Session Description
  - Can be used to match against SDP fields

Example of Initial Filter Criteria

Triggers for All Users

Del	RequestURI	Method	Header	Value	Session Case	Application Server URI
☐	*	INVITE	Accept-Contact	+g.poc.talkburst	ORIGINATING	sip:164.48.178.152:5080;lr
☐	*	PUBLISH	Event	poc-settings	TERMINATING	sip:164.48.178.152:5080;lr
☐	*	SUBSCRIBE	Event	conference	ORIGINATING	sip:164.48.178.152:5080;lr
☐	*	MESSAGE	Accept-Contact	+g.poc.talkburst	TERMINATING	sip:164.48.178.152:5080;lr
☐	*	MESSAGE	Accept-Contact	+g.poc.groupad	ORIGINATING	sip:164.48.178.152:5080;lr
☐	*	SUBSCRIBE	Event	presence.winfo	TERMINATING	sip:164.48.178.152:5080;lr
☐	*	SUBSCRIBE	Event	presence	TERMINATING	sip:164.48.178.152:5080;lr
☐	*	PUBLISH	Event	presence	TERMINATING	sip:164.48.178.152:5080;lr
☐	*	SUBSCRIBE	Event	presence	ORIGINATING	sip:164.48.178.152:5080;lr

Delete

CS Interworking

- Control Plane Interworking: MGCF
- User Plane Interworking: IMS-MGW

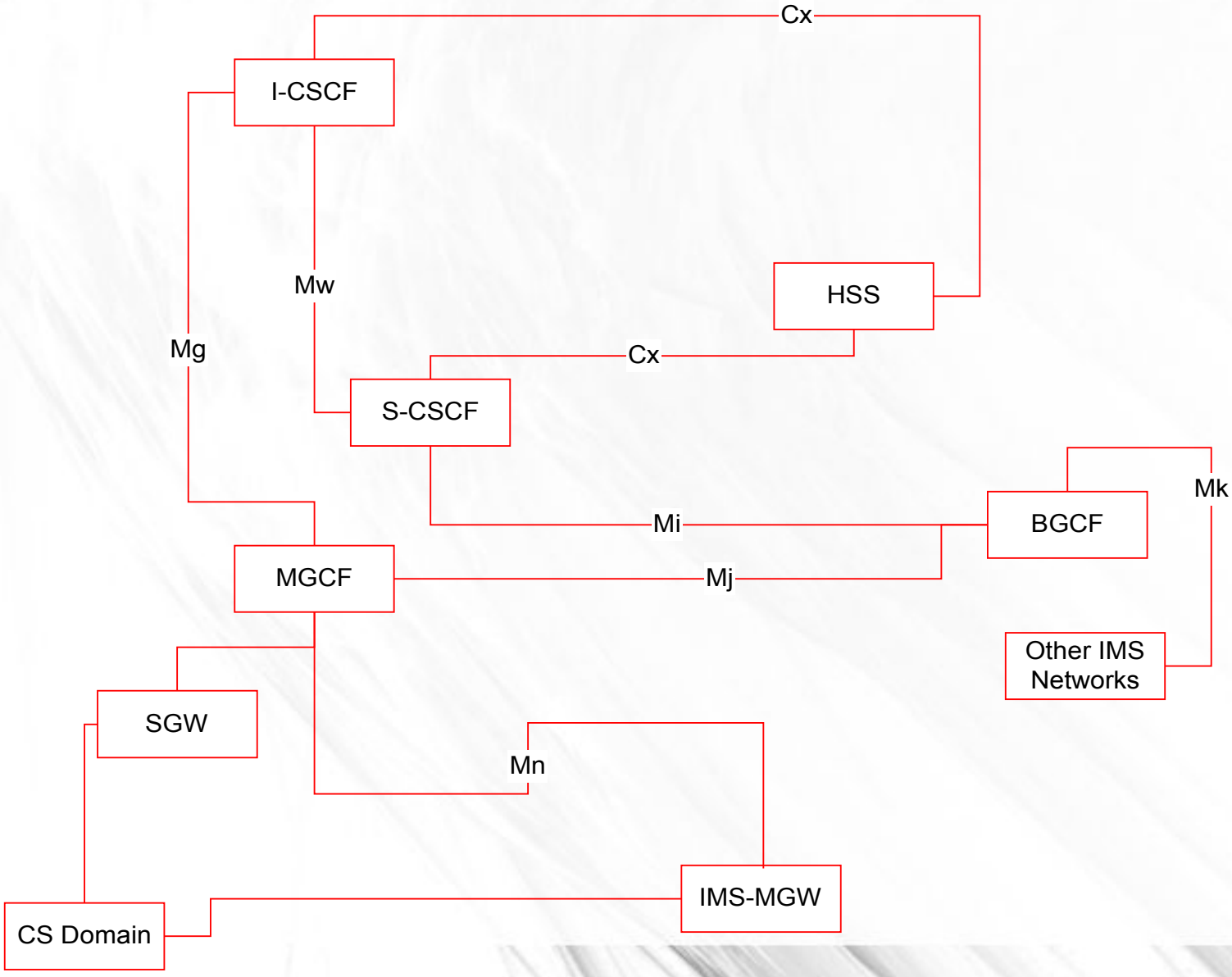
- IMS → CS

  MGCF converts between ISUP & SIP

- CS → IMS

  E.164 number is routed to MGCF

  MGCF converts E.164-formatted number to a SIP URI format


Cx
I-CSCF
Mw
HSS
Mg
Cx
S-CSCF
Mk
Mi
BGCF
MGCF
Mj
Other IMS Networks
SGW
Mn
IMS-MGW
CS Domain

Compression

- Support of SIP compression between the the UE & P-CSCF is mandatory

IPv4 ←→ Ipv6 Interworking

- The next few slides describe some of the issues and solutions for interworking between IP version 4 and IP version 6

Application Level Gateway (ALG)

- Translates IP addresses WITHIN SIP messages

- Advantages:
  - Allows interworking between IPv4 and IPv6
    - Also allows interworking with LANs behind NAT translators
- Disadvantages:
  - Can present security issues
  - Resource intensive

Dual Stack Operation

- System whereby dual stack hosts are utilised

- Advantages:

  Minimises need for ALGs

- Disadvantages:
  - Needs to support both ‘A’ & ‘AAAA’ DNS records for IPv4 & IPv6 respectively

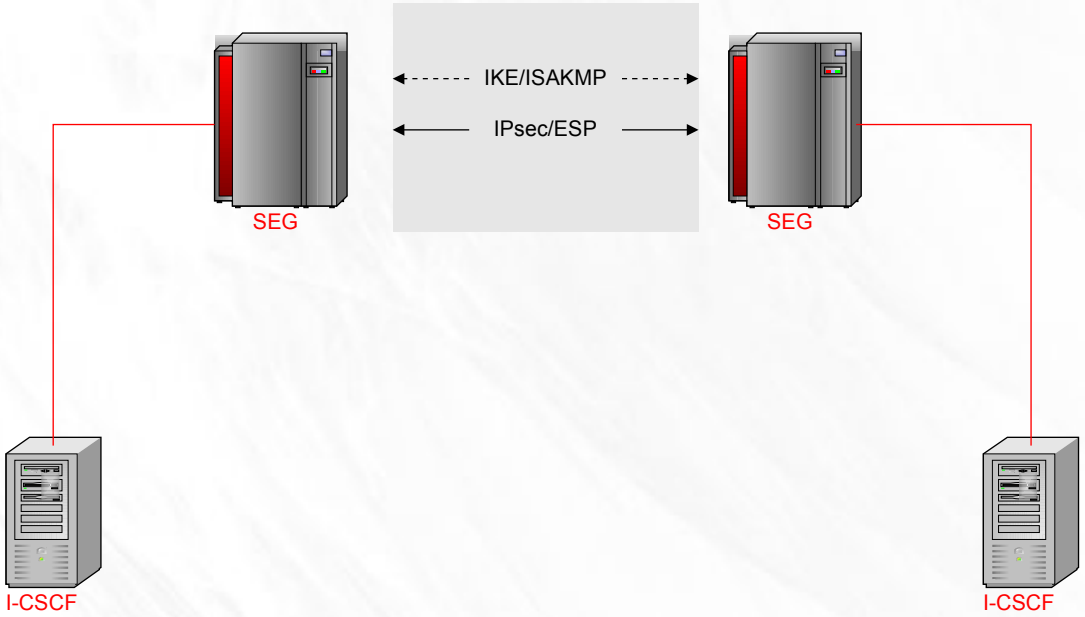
Tunnelling

- IPv6 packet is fully encapsulated within an IPv6 packet

IMS Security

- IMS security re-uses UMTS AKA parameters:
  - K
  - RAND
  - AUTN
  - SQN (Sequence Number)
  - AUTS (Synchronisation token generated by ISIM upon detection of sync failure)
  - RES
  - CK
  - IK

Security Domains



Security Domains

- IKE: Internet Key Exchange
- ISAKMP: Internet Security Association Key Management Protocol
- IPsec: IP Security
- ESP: Encapsulation Security Payload

- When defining Internet Security Domains, Confidentiality, Data Integrity & Authentication are mandatory features

- Security Protocols:
  - ESP, 3DES, MDS & SHA-1

Authentication & Security Agreement

- Authentication is based on the AKA protocol
- UE & P-CSCF exchange lists of supported security mechanisms. Highest commonly supported one is then used
- “Replay” is a feature used to prevent tampering of security agreement during transit (“bidding-down attack”):
  - [Reponse contains same suggested security parameters as the original request]
- Allows extendability whereby new security mechanisms can be added later

Confidentiality & Integrity Protection

- Mandatory in IMS access
- Ipsec
- AKA session keys are used as keys for ESP security associations
- IK is used as the Authentication Key
- CK is the derived Ciphering Key

IMS Presence

- Mechanism to publish a user's availability to other interested and authorised parties
- SIP has been extended with a "presence" event package
  - SIP PUBLISH
  - SIP NOTIFY

- Presentity:

  Entity providing information about its presence (to an Application Server)

- Watcher:

  Entity requesting information on a Presentity

- Presentity can set authorisation levels (using XCAP)

“winfo” Event Package

- Allows a user to subscribe to information regarding their “watchers”
  - Successful subscription to presence
  - Successful presence publication
- Note: Subscription can also be to a Resource List

Messaging

- Messaging Types:
  - Immediate (SIP Message)
    - Can also be sent to a List URL on an AS
  - Session-based
    - Can include other media types in addition to text
    - Uses “Message Session Relay Protocol” (MSRP)
    - Emulation of IRC (multi-party session)

Conferencing

- A Conferencing Server, after a SIP INVITE, can create a new instance of a conference & assign it a URI
- URI can then be globally published
- A SIP Event Package “conference” is used for notification of changes regarding participants
- A SIP SUBSCRIBE request can then be sent to the conference URI

Inviting Users to the Conference

- Method 1:

  REFER request sent to server

  Refer-To header contains conference URI

- Method 2:
  - *REFER* is sent to *Conference URI* & *User URI* is included in *Refer-To* header
  - Causes the ‘focal point’ to generate an INVITE request for the invited user

Example

- Referring a user to a conference
- Subscribing to a conference

- NOTIFY is a notification carrying the conference state at that point in time

Group Management

- Example: “Buddy List”
- Enables group data to be stored in the network
- Synchronises multiple devices holding the group data

Access Control List

- Mechanism to restrict contact and only allow contact from members of a specific group

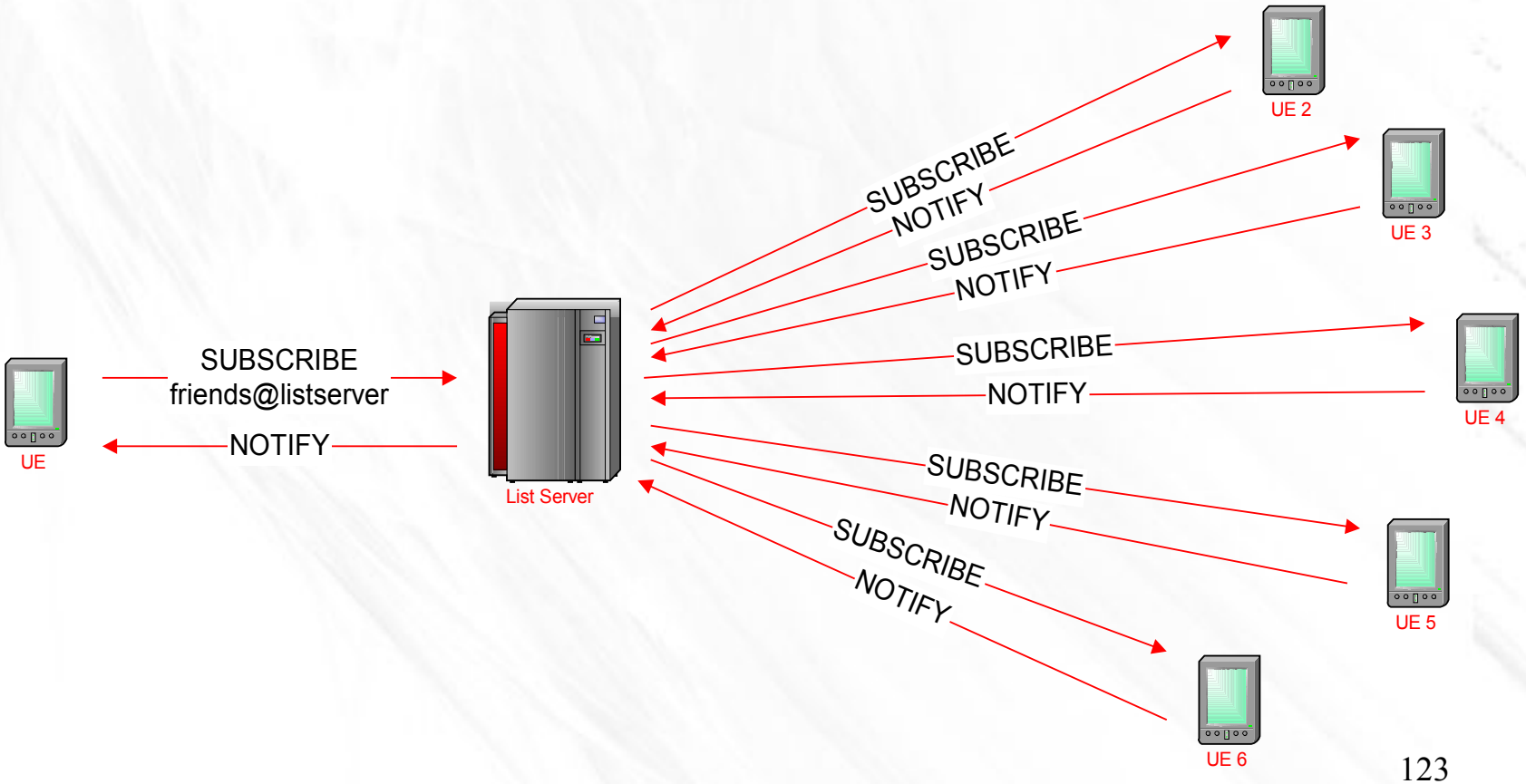
XDM

- XML Document Management
- XCAP (XML Configuration Access Protocol) is the OMA protocol used to manipulate and access XML documents between client & server
- XML schemas have been defined by the OMA (see file UserProfile.htm for example)

Aggregation of Group Data

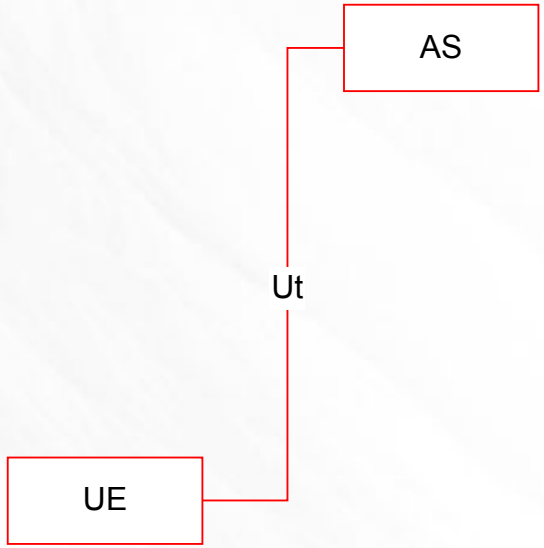
- Allows single SUBSCRIBE to deal with multiple resources
- URI points to a list of other URIs
- Uses “Resource List Server” (RLS)
- Tag “eventlist” is used

Resource List Server



Resource Lists

- The Ut interface is used to manipulate resource lists



IMS Registration Example

- Registration across Visitor PLMN
  - Message sequence chart Part 1
  - Message sequence chart Part 2

Transport Layer Protocols Used by SIP

- Default: UDP
- Greater than 1300 bytes: TCP

Headers

- *Via*

  An element adds its SIP Address to this header so that responses to the request are routed back to it

- *Route*

  Set to the SIP address of the next hop

- *Service-Route*

  Used by the S-CSCF to give the UE routing information to be used from that point onwards

- *Path*

  Used by the P-CSCF to store its address in an initial REGISTER request to ensure it remains in the routing path for future terminating requests

- *Record-Route*

  - Used by CSCFs to remain in the routing path for future originating requests

Examples: Register Request from UE to P-CSCF

```
REGISTER sip:registrar.home1.net SIP/2.0

Via: SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7

Max-Forwards: 70

P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-
3gpp=234151D0FCE11

From: <sip:user1_public1@home1.net>;tag=4fa3

To: <sip:user1_public1@home1.net>

Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000

Call-ID: apb03a0s09dkjdfglkj49111

Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net", nonce="",

uri="sip:registrar.home1.net", response=""

Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-
s=12345678; port-c=2468; ports=

1357

Require: sec-agree

Proxy-Require: sec-agree

CSeq: 1 REGISTER

Supported: path

Content-Length: 0
```

Examples: Register Request from P-CSCF to I-CSCF

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net", nonce="",
uri="sip:registrar.home1.net", response="", integrity-protected="no"
CSeq:
Supported:
Content-Length:
```

Examples: Register Request from I-CSCF to S-CSCF

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info:
Path:
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

Unauthorised Response from S-CSCF to I-CSCF

```
SIP/2.0 401 Unauthorized

Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1,
SIP/2.0/UDP

pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP

[5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7

From: <sip:user1_public1@home1.net>;tag=4fa3

To: <sip:user1_public1@home1.net>; tag=5ef4

Call-ID: apb03a0s09dkjdfglkj49111

WWW-Authenticate: Digest realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-
MD5, ik="00112233445566778899aabbccddeeff",

ck="ffeeddccbbaa11223344556677889900"

CSeq: 1 REGISTER

Content-Length: 0
```

Unauthorised Response from P-CSCF to UE

SIP/2.0 401 Unauthorized

Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7

From:

To:

Call-ID:

WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5

Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-c=8642;

port-s=7531

CSeq:

Content-Length:

2nd Register Request from UE

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1"
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-
c=2468; ports=
1357
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642;
port-s=7531
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 2 REGISTER
Supported: path
```

Authentication

- 3GPP AKA paremeters are mapped to HTTP Digest Authentication
- Algorithm value "AKAv1-MDS" distinguishes 3GPP AKA mechanism from other HTTP digest mechanisms
- PrUID is used by the S-CSCF to obtain the correct authentication vector
- Security Associations are established between UE & P-CSCF

Security Associations

- Characterised by:
  - Protected client ports
  - Protected server ports
- Ports are used as part of the address in SIP headers
- Default unprotected ports are used if protected ports have not been supplied
- When re-authentication takes place, UE & P-CSCF only change their protected client ports
- Server ports remain the same (otherwise, contact data would change, requiring re-authentication)

TCP

- Response is routed to the same port that the request was received from
- Due to the connection-oriented nature of TCP (with TCP, connection is setup in advance and that connection is then re-used until the TCP session is terminated)

SIP Security Agreement

- Provides extendability
- Currently only IPsec is used
- List of supported mechanisms in *401 Unauthorised* message contains weighted preferences

Security Negotiation Example

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net", nonce="",
uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678;
port-c=2468; ports=
1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

Security Negotiation Example

SIP/2.0 401 Unauthorized

Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7

From:

To:

Call-ID:

WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5

Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-c=8642;

port-s=7531

CSeq:

Content-Length:

Compression

- Mandatory support but NOT mandatory use
- “comp” added to headers to indicate support

Compression Header Example

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net", nonce="",
uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678;
port-c=2468; ports=
1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

User IDs: Private

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce="",
uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-
c=2468; ports=
1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

User IDs: Public

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce="",
uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-
c=2468; ports=
1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

Subscription to Registration State Info

- ***Event***: This field is populated with the value "reg" to specify the use of the registration state package
- Registration state info is returned in an XML form in a NOTIFY message
- Examples follow

SUBSCRIBE **sip:user1_public1@home1.net** SIP/2.0

Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7

Max-Forwards: 70

Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>,
<sip:orig@scscf1.home1.net;lr>

P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>

P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11

Privacy: none

From: <sip:user1_public1@home1.net>;tag=31415

To: <sip:user1_public@home1.net>

Call-ID: b89rjhnedlrfjflslj40a222

Require: sec-agree

Proxy-Require: sec-agree

CSeq: 61 SUBSCRIBE

Event: reg

Expires: 600000

Accept: application/reginfo+xml

Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-c=8642;

port-s=7531

Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

Content-Length: 0

```
NOTIFY sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
Max-Forwards: 70
Route: <sip:pcscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=31415
To: <sip:user1_public1@home1.net>;tag=151170
Call-ID:
CSeq: 42 NOTIFY
Subscription-State: active;expires=600000
Event: reg
Content-Type: application/reginfo+xml
Contact: <sip:scscf1.home1.net>
Content-Length: (...)
```

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo“ version="1" state="full">
     <registration aor="sip:user1_public1@home1.net" id="a7" state="active">
          <contact id="76" state="active" event="registered">
               <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
          </contact>
     </registration>
     <registration aor="sip:user1_public2@home1.net" id="a8" state="active">
          <contact id="77" state="active" event="created">
               <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
          </contact>
     </registration>
     <registration aor="tel:+358504821437" id="a9" state="active">
          <contact id="78" state="active" event="created">
               <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
          </contact>
     </registration>
</reginfo>
```

Sending Partial State Change Info

- State parameter is set to “partial” when a NOTIFY message contains only change information

Network Initiated Re-Authentication

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo“ version="1"
state="partial">
     <registration aor="sip:user1_public1@home1.net" id="as9"
     state="active">
          <contact id="76" state="active" event="shortened"
          expires="600">
               <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
          </contact>
     </registration>
</reginfo>
```

De-registration

```
REGISTER sip:registrar.home1.net SIP/2.0

Via: SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7

P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11

Max-Forwards: 70

From: <sip:user1_public1@home1.net>;tag=4fa3

To: <sip:user1_public1@home1.net>

Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=0

Call-ID: apb03a0s09dkjdfglkj49111

Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net",

nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,

uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1"

CSeq: 7 REGISTER

Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-
s=87654321; port-c=8642;

port-s=7531

Require: sec-agree

Proxy-Require: sec-agree

Supported: path

Content-Length: 0
```

Early IMS Security

- Where IDs have to be derived from USIM (not ISIM)
- Based on a simplified authentication mechanism involving MSISDN to IP Address checks done by the HSS

Asserted Identities

- P-Asserted-Identity & P-Preferred-Identity
  - Originating P-CSCF replaces ‘Preferred-ID’ with ‘Asserted-ID’
  - Asserted ID is guaranteed to be a registered & authenticated Public User ID of the originating party
  - S-CSCF can add an additional URI to ‘P-Asserted-Identity’ (e.g. tel URI)

Privacy Header

- Set to ‘ID’ to indicate privacy
- If terminating network is not within originating network’s trust domain, S-CSCF removes ‘P-Asserted-Identity’
- Otherwise, destination P-CSCF is trusted to remove the ‘P-Asserted-Identity’ in order to retain the requested privacy

P-Called-Party-ID

- Used to store a request URI after the original request URI is replaced by the S-CSCF with the actual IP address of the destination (‘From:’ & ‘To:’ can be set arbitrarily)
- Allows terminating party to determine which of their PuUIDs were used in the request

Provisional Responses

- 'Supported: 100rel' indicates support of reliably sent provisional responses (RFC 3262)
  - Mechanism allowing provisional responses to be sent reliably
  - Support is mandatory for IMS
  - 'PRACK' must be sent by receiver of provisional response
  - 'Require: 100rel' is used to prompt receiving terminal for PRACK request
  - 'RSeq' is used to distinguish between multiple provisional responses
  - Acknowledged provisional response is identified in 'RAck' header (includes RSeq & CSeq from provisional response)

Resource Reservation

- Resource reservation can happen in the send & receive directions at the originating end and also the send & receive directions at the remote end

❖ Message Sequence Chart

Preconditions

- SDP Preconditions Extension is specified in RFC 3312 (“qos” precondition type)
- Allows UE to delay completion of session establishment until resources have been reserved at both ends

❖ Example: See [SDP_Preconditions_Example.html]

Media Authorisation

- Authorisation Token (*P-Media-Authorisation*):
  - Included in INVITE
  - Included in '183 Session Progress'
  - UE then includes it in Activate PDP Context Request
- Note that any CSCF in the routing path could reject certain media types

IMS Session Setup Variations

- IMS Session Setup Without Resource Reservation
- Resource-based IMS Session Setup Without Preconditions:
  - 3GPP Rel 7
  - Optional simplified alternative to preconditions mechanism
  - Uses principle of setting media stream to "inactive" in SDP
  - re-INVITE is sent after resource reservation, now with media stream set to "active"

Communication with non-IMS UEs

- IMS UE to non-IMS Terminal
- non-IMS Terminal to IMS UE