3GPP TSG CN Plenary Meeting #14 **NP-010639**
Kyoto, Japan, 12th –14th December 2001

Source: **MCC**

Title: **All LSs sent from CN1 since TSG CN#13 meeting**

Agenda item: **6.1.1**

Document for: **INFORMATION**

Introduction:

This document contains **10 agreed** LSs sent from **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #14 for information only.

TDoc #	Status	Source	Tdoc Title	Type	Comments
N1-011428	AGREED	Xien Chen	LS out to SA2 on QoS call flows.	LS OUT	Related to N1-011357, N1-011381 and N1-011383. Revised from 1419
N1-011430	AGREED	Miguel Garcia	LS out to SA1, SA2, SA3, SA5, CN4 on usage of Private-ID.	LS OUT	Due to discussion on N1-011355. Revised from 1427
TDoc #	**Status**	**Source**	**Tdoc Title**	**Type**	**Comments**
N1-011594	AGREED	Inma C.	LS to SA1 on Multicall handover requirements	LS OUT	To: SA1, Linked to 1556 and 1581.
N1-011572	AGREED	Inma C.	LS to GERAN on WB-AMR Signalling	LS OUT	To: GERAN2, Linked to 1290
N1-011625	AGREED	Atle Monrad	Liaison Statement response on 'LS On the handling of the Protocol Configuration Options IE'	LS OUT	To: CN4, Linked to 1612
TDoc #	**Status**	**Source**	**Tdoc Title**	**Type**	**Comments**
N1-011763	AGREED	Keith Drage	Liaison statement to SA2 on configuration hiding for BGCF	LS OUT	LS based on N1-011651
N1-011768	AGREED	Duncan Mills	Response to LS on IMS identifiers and ISIM and USIM	LS OUT	Revised from N1-011748
TDoc #	**Status**	**Source**	**Tdoc Title**	**Type**	**Comments**
N1-012041	AGREED	Keith Drage	Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	LS OUT	Linked to 1942. To: S1 Cc: S2, S3 REVISED from 1963
N1-012044	AGREED	Roland Gruber	Liaison Statement on Addition of section " Conditions for IOV reset " to 09.95	LS OUT	To: GERAN, GERAN1
N1-012050	AGREED	Gabor Bajko	LS on Interworking between 3GPP UE (IPv6 only) and SIP device external to IMS (IPv4 only)'	LS OUT	To: SA2 Cc: CN3 REVISED from 2006

3GPP TSG-CN1 Meeting #19bis ***Tdoc N1-011428***
Sophia-Antipolis, 2.-4. Oct 2001

Title: **Liaison Statement on "The Integration of RSVP and SIP"**

Source: TSG_CN WG1

To: TSG_SA WG2

Contact Person:
Name: Xin Chen
E-mail Address: xchen2@lucent.com
Tel. Number: +44-1793-883137

Attachment: N1-011357, Combination of N1-011381 and N1-011383

---

1. Overall Description:

In CN1 19bis meeting, there were contributions to show two different ways of the integration of RSVP and SIP signalling to complete a QoS-Assured Precondition session establishment.

The major difference shown in the flows between the two approaches is when the originating UE sends the COMET to the terminating UE. Also note, in both approaches, it is assumed that GGSN is not RSVP aware.

In mobile originating procedure, the originating UE sends the COMET message to the terminating UE with the indication that the all QoS preconditions or part of the preconditions have been satisfied. In N1-011357, the COMETmessage is sent after local PDP Context has been activated successfully and RSVP procedures for both directions have been completed, in other words, the COMET is sent to confirm that all the preconditions have been achieved. In N1-011381, the COMET is sent immediately after the local PDP Context has been activated successfully and the originating UE finishes its own RSVP signalling successfully, in other words, to confirm that half of the preconditions have been achieved.

In mobile terminating procedure, corresponding to the case that COMET is sent after a the bi-directional QoS reservation has finished, the terminating UE will continue the SIP session establishment procedure by sending the 180 Ringing when it receives the COMET message from originating UE, as is also shown in N1-011357.

In the case that COMET message is sent after the unidirectional QoS reservation procedure has completed (originating UE → terminating UE), upon the terminating UE completing its own RSVP setup (terminating UE → originating UE), it combines the information received from the COMET sent by originating UE and gets the conclusion that all the preconditions are met, then it will continue the SIP session establishment by sending 180 Ringing to the originating UE, this terminating procedure is shown in N1-011383.

2. Actions:

To SA2 group

ACTION: During the discussion, no technical issues were raised concerning the applicability or compatibility of both solutions towards the usage of RSVP with the “many-folks” draft. There was discussion on whether RSVP from the terminal was something which was required for consideration within 3GPP Rel-5. Before deciding whether to accept those contributions or not, CN1 would kindly ask SA2 to respond to the following issues:

- Whether RSVP is still a valid option to be considered in 3GPP Rel 5?
- CN1 is interested to understand what SA2 was intending in regards to the QoS preconditions.
- Advise CN1 on SA2’s understanding of the applicability of the “many-folks” signalling regarding uni-directional and bi-directional QoS reservation indication.

The dates for the next CN1 meetings are:

- CN1#20 15th – 19th October 2001 Brighton, U.K.
- CN1#20bis 13th.--15th. Nov 2001 Seattle, USA

CN1 thanks S2 for any feedback that may be provided.

3GPP TSG-CN1 Meeting #19bis ***Tdoc N1-011357***
Sophia Antipolis, France, 2.- 4. October 2001

Source: Ericsson

Title: QoS flows: end-to-end RSVP, no SBLP

Agenda item: 8.8 IMS call initiation

Document for: APPROVAL

Introduction

As agreed in last CN1-CN3-CN4 joint meeting in Dresden, QoS end-to-end flows examples (MO and MT) shall be shown in 24.228. This contribution is attempting to give the example flows based on MO without Service-based Local Policy case.

This document presents an example of a realization that demonstrate the QoS interaction with the SIP signalling flows in the case that there is end-to-end RSVP, and the SIP signalling is used to convey the information on the successful completion of both the uplink and downlink streams.

This is a realization of 3G TS 23.207 v5.0.0, section 6.3.2. This contribution is in line with the approved CR to 23.228, S2-012332: *"A minimum requirement to meet the QoS preconditions defined for a media stream in a certain direction, is that a satisfactory PDP context is established at the local access for that direction"*.

Proposal

It is proposed to add a new clause in Annex A-X 7.y End-to-End QoS and Signalling Call flows. This clause contains two subclauses 7.y.3 Mobile Originating, without Service-Based Local Policy, with RSVP end-to-end, the COMET shows the bidirectional resource reservation and 7.y.4, Mobile Terminating, without Service-Based Local Policy, with RSVP end-to-end, the COMET shows the bidirectional resource reservation.

7.y End-to-End QoS and Signalling Call Flows

7.y.3 Mobile Originating, without Service-based Local Policy, RSVP end to end

The flows in Figure 7.y.3-1 show an example of the QoS interaction during a session setup. Because the S-CSCF is not involved in QoS interaction, it is not shown in the flow in the sake of clarity, but it is assumed that the S-CSCF is the next entity of the P-CSCF shown in this flow.

This example is appropriate for a SIP QoS Assured session . It is assumed that both the UAC and UAS have chosen to use RSVP as the additional QoS reservation protocol, which means both the UAC and UAS establish satisfactory PDP context on their respective accesses, and also perform a bidirectional ("sendrecv") resource reservation. The usage of RSVP is one of the possible mechanisms for satisfy the QoS requirements.

The diagrams show the alternative where the GGSN is not RSVP aware. However, the scenario where the GGSN is RSVP aware is also possible.

Note: The diagram is roaming independent. This diagram provides the flows for SIP session signalling, PDP context establishment, and resource reservation (RSVP).

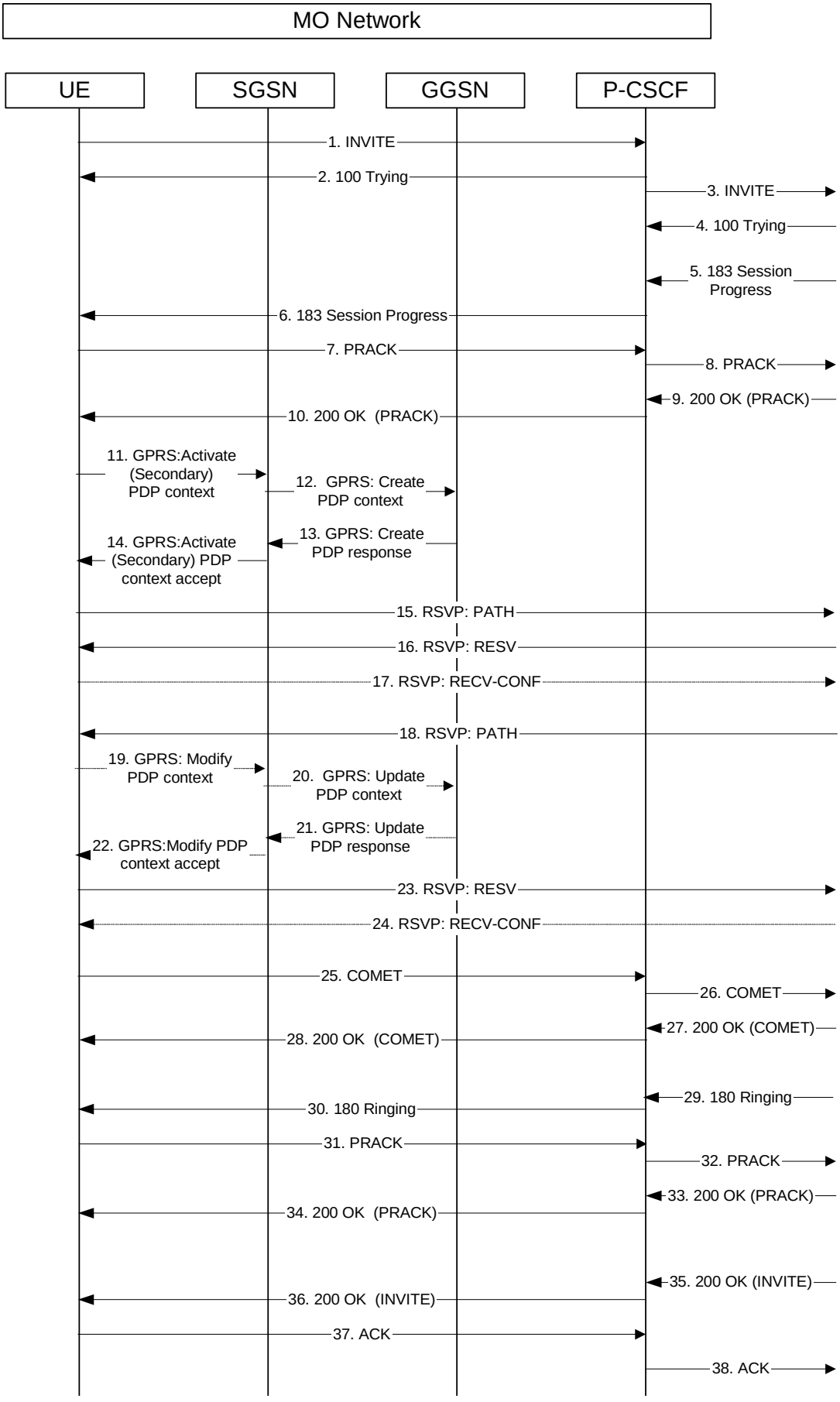


Figure 7.y.3-1 Interaction between SIP/SDP, GPRS and RSVP, Mobile origination

1. **INVITE (UE to P-CSCF) – see example in Table 7.y.3-1**

The originating UE determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. The UE also requires to establish preconditions QoS for both directions in QoS Assured mode. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

For this example, it is assumed that originating UE is capable of sending two simultaneous video streams, either H261 or MPV format, and two simultaneous audio streams, either AMR, G726-32, PCMU, or G728.

UE sends the INVITE request, containing an initial SDP, to the P-CSCF.

Table 7.y.3-1: INVITE (UE to P-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Supported: 100rel
Remote-Party-ID: “John Doe” <sip:user1_public1@home1.net>;privacy=off
Anonymity: Off
From: sip:user1_public1@home1.net;tag=171828
To: sip:user2_public1@home2.net
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Cseq: 127 INVITE
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 3400 RTP/AVP 98 99
a=rtpmap:98 H261
a=rtpmap:99:MPV
a=qos:mandatory sendrecv
m=video 3402 RTP/AVP 98 99
a=rtpmap:98 H261
a=rtpmap:99:MPV
a=qos:mandatory sendrecv
m=audio 3456 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
m=audio 3458 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
```

SDP The SDP contains the full set of codecs supported by UE#1. The originating UE requests also to establish preconditions in QoS Assured mode, but it does not request confirmation of the establishment of the QoS preconditions from the terminating side.

2. **100 Trying (P-CSCF to UE) – see example in Table 7.y.3-2**

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.y.3-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

3. **INVITE (P-CSCF to S-CSCF) – see example in Table 7.y.3-3**

The P-CSCF remembers (from the registration procedure) the request routing for this UE. This becomes the Request-URI in the request. This next hop is the S-CSCF within the home network of UE#1.

P-CSCF adds itself to the Record-Route header and Via header.

P-CSCF#1 examines the media parameters, and removes any choices that the network operator decides based on local policy, not to allow on the network.

For this example, assume the network operator disallows H261 video encoding.

The INVITE request is forwarded to the S-CSCF.

Table 7.y.3-3: INVITE (P-CSCF to S-CSCF)

```
INVITE sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf1.visited1.net
Route: sip:user2_public1@home2.net
Supported:
Remote-Party-ID:
Anonymity:
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 3400 RTP/AVP 99
a=rtpmap:99:MPV
a=qos:mandatory sendrecv
m=video 3402 RTP/AVP 99
a=rtpmap:99:MPV
a=qos:mandatory sendrecv
m=audio 3456 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
m=audio 3458 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
```

4. **100 Trying (S-CSCF to P-CSCF) – see example in Table 7.y.3-4**

S-CSCF responds to the INVITE request (3) with a 100 Trying provisional response.

Table 7.y.3-4: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

5. **183 Session Progress (S-CSCF to P-CSCF) – see example in Table 7.y.3-5**

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response, per the S-CSCF to S-CSCF procedures. The destination indicates that it supports "Precondition" and requests a confirm from the originating side for QoS reservation.

Table 7.y.3-5: 183 Session Progress (S-CSCF to P-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.visited2.net, sip:scscf2.home2.net, sip:scscf1.home1.net,
sip:pcscf1.visited1.net
Remote-Party-ID: “John Smith” <sip:user2_public1@home2.net>;privacy=off;screen=yes
Anonymity:
Require: 100rel
From:
To: sip:user2_public1@home2.net; tag=314159
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9021
Content-Disposition: precondition
Content-Type: application/sdp
Content-length: (…)

v=
o=- 2987933615 2987933615 IN IP6 5555::eee:fff:aaa:bbb
s=
c=IN IP6 5555::eee:fff:aaa:bbb
b=
t=
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 6543 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv confirm
m=audio 0 RTP/AVP 97 96 0 15
```

SDP The SDP contains the set of codecs supported by UE#2. UE#2 supports the preconditions and requests that UE#1 sends a confirmation when the preconditions are met in the originating side.

6. **183 Session Progress (P-CSCF to UE) – see example in Table 7.y.3-6**

P-CSCF forwards the 183 Session Progress response to the originating endpoint.

Table 7.y.3-6: 183 Session Progress (P-CSCF to UE)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Remote-Party-ID:
Anonymity:
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-Disposition:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
a=
m=
```

7. **PRACK (UE to P-CSCF) – see example in Table 7.y.3-7**

UE#1 determines which media flows should be used for this session, and which codecs should be used for each of those media flows. If there was any change in media flows, or if there was more than one choice of codec for a media flow, then UE#1 must include an SDP in the PRACK message sent to UE#2.

For this example, assume UE#1 chooses AMR as the codec to use for the single audio stream.

UE includes this information in the PRACK request to P-CSCF.

Editor's Note: The use of three-message codec negotiation (one round-trip to determine common capabilities, then originator picks the ones to use) is allowed by RFC2543, but will apparently not be supported by 2543bis. This inconsistency needs to be resolved.

Table 7.y.3-7: PRACK (UE to P-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: sip:user1_public1@home1.net;tag=171828
To: sip:user2_public1@home2.net;tag=314159
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Cseq: 128 PRACK
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Rack: 9021 127 INVITE
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:mandatory sendrecv
m=audio 0 RTP/AVP 97 96 0 15
```

SDP	The SDP contains a single codec (AMR). UE#1 still indicates the need to establish the preconditions. in QoS Assured mode.

8. **PRACK (P-CSCF to S-CSCF) – see example in Table 7.y.3-13**

P-CSCF adds the Route header corresponding to the session.

P-CSCF forwards the PRACK request to S-CSCF.

Table 7.y.3-8: PRACK (P-CSCF to S-CSCF)

```
PRACK sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.visited2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Contact:
Rack:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

9. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.y.3-9**

   S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.y.3-9: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

10. **200 OK (P-CSCF to UE) – see example in Table 7.y.3-10**

    P-CSCF forwards the 200 OK response to UE.

Table 7.y.3-10: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Length:
```

11. **GPRS: Active (Secondary) PDP Context (UE to SGSN)**

    The UE sends an Activate (Secondary) PDP Context message to the SGSN with the UMTS QoS parameters.

12. **GPRS: Create PDP Context (SGSN to GGSN)**

    The SGSN checks the user profile to authorize the requested QoS and also the available resource, if both are granted, it sends the corresponding Create PDP Context message to the GGSN.

13. **GPRS: Create PDP Context Resp (GGSN to SGSN)**

    The GGSN checks its own available resources; if enough resources are available it sends a Create PDP Context Response message back to SGSN.

14. **GPRS: Active PDP Context Accept (SGSN to UE)**

The SGSN sends an Activate PDP Context Accept message to UE.

Editor's Note: It is shall be possible that PDP Context activation starts immediately after flow 6 to save the time for call setup.

15. **RSVP: PATH (UE#1 to UE#2)**

After the PDP context establishment procedure is completed, UE#1 sends a RSVP PATH message to the UE#2.

16. **RSVP: RESV (UE#2 to UE#1)**

UE#2 answers with a RESV message to UE#1.

17. **RSVP: RESV-CONF (UE#1 to UE#2)**

UE#1 sends a RSVP RESV-CONF message to UE#2 if the RESV message (16) requested an optional confirmation.

18. **RSVP: PATH (UE#2 to UE#1)**

UE#2 sends an RSVP PATH message to UE#1. This message can arrive at any time. Particularly, it can arrive before the GPRS procedure to activate the (Secondary) PDP context has started (message 11).

19. **GPRS: Modify PDP Context (UE to SGSN)**

UE #1may send a Modify PDP Context message to the SGSN with the necessary modification to UMTS QoS parameters according to the received RSVP PATH message.

20. **GPRS: Update PDP Context (SGSN to GGSN)**

The SGSN checks the user profile to authorize the requested QoS (this check will happen only if a higher QoS is requested) and also the available resource, if both are granted; it sends the corresponding Update PDP Context message to the GGSN.

21. **GPRS: Update PDP Context Resp (GGSN to SGSN)**

The GGSN checks its available resource and accepts the PDP modification request, and sends a Update PDP Context Response message back to SGSN.

22. **GPRS: Modify PDP Context Accept (SGSN to UE)**

The SGSN sends a Modify PDP Context Accept message to UE.

Note: Steps 19 to 22 are optional. This procedure can happen if the existing PDP context doesn't conform the QoS requirement of the RSVP, but this is an implementation issue.

23. **RSVP: RESV (UE#1 to UE#2)**

UE#1 answers the RSVP path message with an RSVP RESV message to UE#2. This message cannot be sent until the PDP context has been establish (message 14 is received, and 22, if applicable).

24. **RSVP: RESV-CONF (UE#2 to UE#1)**

UE#2 sends a RSVP RESV-CONF message to UE#1 if the RESV message (23) requested an optional confirmation.

25. **COMET (UE to P-CSCF) – see example in Table 7.y.3-25**

When the UE#1 finishes the QoS reservation for both the uplink and downlink direction, it sends the COMET request to the terminating endpoint, via the signalling path established by the INVITE request. The request is sent first to P-CSCF. The message contains the successful indication of the established QoS path.

Note that this message must be sent once message 16 (RSVP RESV) is received for the uplink reservation and message 23 (RSVP RESV) is sent for the downlink reservation.

Table 7.y.3-25: COMET (UE to P-CSCF)

```
COMET sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: sip:user1_public1@home1.net;tag=171828
To: sip:user2_public1@home2.net;tag=314159
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Cseq: 129 COMET
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:success sendrecv
m=audio 0 RTP/AVP 97 96 0 15
```

SDP: The SDP indicates that the QoS resource reservation for both send and receive mode was successful at the originating side.

26. **COMET (P-CSCF to S-CSCF) – see example in Table 7.y.3-26**

P-CSCF forwards the COMET request to S-CSCF.

Table 7.y.3-26: COMET (P-CSCF to S-CSCF)

```
COMET sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.visited2.net, sip: [5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

27. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.y.3-27**

S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.y.3-27: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length: 0
```

28. **200 OK (P-CSCF to UE) – see example in Table 7.y.3-28**

P-CSCF forwards the 200 OK response to UE.

Table 7.y.3-28: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Length:
```

29. **180 Ringing (S-CSCF to P-CSCF) – see example in Table 7.y.3-29**

As the COMET is used to send confirmation of end-to-end QoS reservation in both directions, the destination endpoint determines that all the pre-conditions have been met. Then the destination continues with the session establishment by alerting the user and sending the 180 Ringing.

Table 7.y.3-29: 180 Ringing (S-CSCF to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.visited2.net, sip:scscf2.home2.net, sip:scscf1.home1.net,
sip:pcscf1.visited1.net
Remote-Party-ID: “John Smith” <sip:user2_public1@home2.net>;privacy=off;screen=yes
Anonymity:
Require: 100rel
From:
To:
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9022
Content-length: 0
```

30. **180 Ringing (P-CSCF to UE) – see example in Table 7.y.3-30**

S-CSCF forwards the 180 Ringing response to P-CSCF.

Table 7.y.3-30: 180 Ringing (S-CSCF to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Remote-Party-ID:
Anonymity:
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-length:
```

31. **PRACK (UE to P-CSCF) – see example in Table 7.y.3-31**

UE indicates to the originating subscriber that the destination is ringing. It responds to the 180 Ringing provisional response with a PRACK request.

Table 7.y.3-31: PRACK (UE to P-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: sip:user1_public1@home1.net;tag=171828
To: sip:user2_public1@home2.net;tag=314159
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Cseq: 130 PRACK
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Rack: 9022 127 INVITE
Content-length: 0
```

32. **PRACK (P-CSCF to S-CSCF) – see example in Table 7.y.3-32**

    P-CSCF adds a Route header, with the saved value from the previous response. P-CSCF identifies the proper saved value by the Request-URI.

    P-CSCF forwards the PRACK request to S-CSCF.

Table 7.y.3-32: PRACK (P-CSCF to S-CSCF)

```
PRACK sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.visited2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Contact:
Rack:
Content-length:
```

33. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.y.3-33**

    S-CSCF forwards the 200 OK response for PRACK to P-CSCF.

Table 7.y.3-33: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route:
From:
To:
Call-ID:
CSeq:
Content-Length:
```

34. **200 OK (P-CSCF to UE) – see example in Table 7.y.3-34**

    P-CSCF forwards the 200 OK response to UE.

Table 7.y.3-34: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Length:
```

35. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.y.3-35**

When the called party answers, the terminating endpoint sends a 200 OK final response to the INVITE request

Table 7.y.3-35: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Contact:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
b=
t=
m=
m=
m=audio 6543 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:success sendrev
m=
```

SDP: The SDP indicates that the QoS resource reservation for both send and receive mode was successful from the terminating endpoint side.

36. **200 OK (P-CSCF to UE) – see example in Table 7.y.3-36**

P-CSCF forwards the 200 OK final response to the session originator.

Table 7.y.3-36: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

37. **ACK (UE to P-CSCF) – see example in Table 7.y.3-37**

UE responds to the 200 OK with an ACK request sent to P-CSCF.

Table 7.y.3-37: ACK (UE to P-CSCF)

```
ACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: sip:user1_public1@home1.net;tag=171828
To: sip:user2_public1@home2.net;tag=314159
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Cseq: 127 PRACK
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Content-length: 0
```

38. **ACK (P-CSCF to S-CSCF) – see example in Table 7.y.3-38**

P-CSCF forwards the ACK request to S-CSCF.

Table 7.y.3-38: ACK (P-CSCF to S-CSCF)

```
ACK sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.visited2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Contact:
Content-length:
```

7.y.4 Mobile Termination, without Service-based Local Policy, RSVP end to end

The flows in Figure 7.y.4-1 show an example of the QoS interaction during a session setup. Because the S-CSCF is not involved in QoS interaction, it is not shown in the flow in the sake of clarity, but it is assumed that the S-CSCF is the next entity of the P-CSCF shown in this flow.

This example is appropriate for a SIP QoS Assured session . It is assumed in this example that both the UAC and UAS have chosen to use RSVP as the additional QoS reservation protocol, which means both the UAC and UAS establish satisfactory PDP context on their respective accesses, and also perform a bidirectional ("sendrecv") resource reservation.

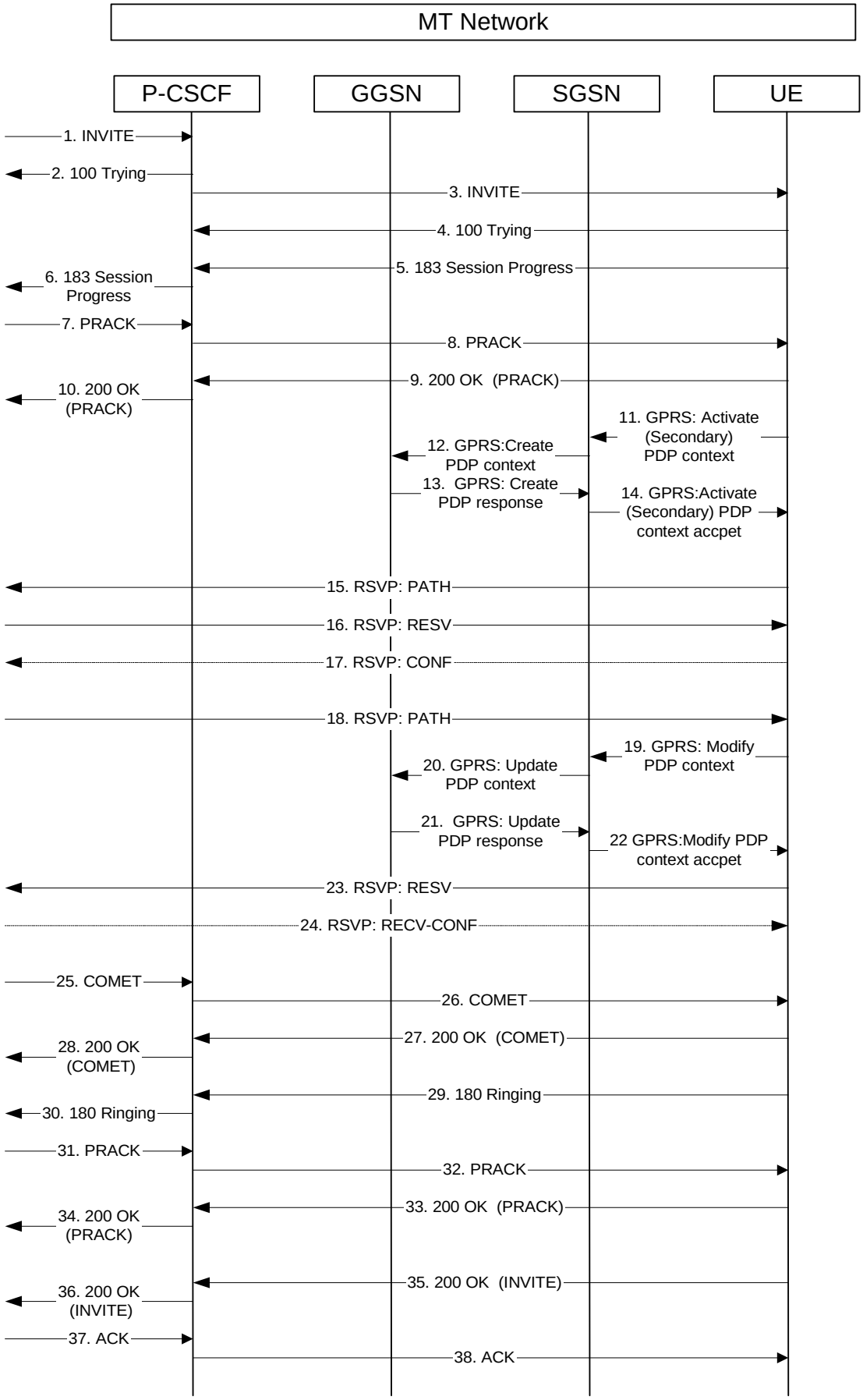


Figure 7.y.4-1 Interaction between SIP/SDP, GPRS and RSVP, Mobile termination

1. **INVITE (S-CSCF to P-CSCF) – see example in Table 7.y.4-1**

   S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF.

Table 7.y.4-1: INVITE (S-CSCF to P-CSCF)

```
INVITE sip:pcscf2.visited2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1. visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:user2_public1@home2.net
Record-Route: sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.visited1.net
Supported: 100rel
Remote-Party-ID: “John Doe” <sip:user1_public1@home1.net>;privacy=off
Anonymity: Off
From: sip:user1_public1@home1.net;tag=171828
To: sip:user2_public1@home2.net
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Cseq: 127 INVITE
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
m=audio 0 RTP/AVP 97 96 0 15
```

SDP The SDP requests to establish preconditions in QoS Assured mode, but it does not request confirmation of the QoS preconditions from the terminating side.

2. **100 Trying (P-CSCF to S-CSCF) – see example in Table 7.y.4-2**

   P-CSCF responds to the INVITE request with a 100 Trying provisional response.

Table 7.y.4-2: 100 Trying (P-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

3. **INVITE (P-CSCF to UE) – see example in Table 7.y.4-3**

   P-CSCF examines the media parameters, and removes any that the network operator decides, based on local policy, not to allow on the network.

   P-CSCF determines the UE address from the value of the Request-URI and forwards the INVITE request to the UE.

Table 7.y.4-3: INVITE (P-CSCF to UE)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
Supported:
Remote-Party-ID:
Anonymity:
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length:

v=
o=
s=
c=
t=
m=
m=
m=
a=
a=
a=
a=
m=
```

4. **100 Trying (UE to P-CSCF) – see example in Table 7.y.4-4**

   UE may optionally send a 100 Trying provisional response to P-CSCF.

Table 7.y.4-4: 100 Trying (UE to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

5. **183 Session Progress (UE to P-CSCF) – see example in Table 7.y.4-5**

   UE#2 determines the complete set of codecs that it is capable of supporting for this session. It determines the intersection with those appearing in the SDP in the INVITE request. For each media flow that is not supported, UE#2 inserts a SDP entry for media (m= line) with port=0. For each media flow that is supported, UE#2 inserts a SDP entry with an assigned port and with the codecs in common with those in the SDP from UE#1.

   For this example, assume UE#2 supports both AMR and G726, but not G728 (codec 15)

   UE responds with a 183 Session Progress response containing SDP back to the originator. This SDP may represent one or more media for a multimedia session. This response is sent to P-CSCF.

Table 7.y.4-5: 183 Session Progress (UE to P-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
Remote-Party-ID: “John Smith” <sip:user2_public1@home2.net>;privacy=off;screen=yes
Anonymity:
Require: 100rel
From:
To: sip:user2_public1@home2.net;tag=314159
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9021
Content-Disposition: precondition
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 6543 RTP/AVP 97 96
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:mandatory sendrecv confirm
a=rtpmap:96 G726-32/8000
m=audio 0 RTP/AVP 97 96 0 15
```

SDP The SDP contains the subset of codecs supported by UE#2. UE#2 supports the preconditions and requests that UE#1 sends a confirmation when the preconditions are met in the originating side.

6. **183 Session Progress (P-CSCF to S-CSCF) – see example in Table 7.y.4-6**

   P-CSCF forwards the 183 Session Progress response to S-CSCF.

Table 7.y.4-6: 183 Session Progress (P-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd])
Record-Route: sip:pcscf2.visited2.net,sip:scscf2.home2.net, sip:scscf1.home1.net,
sip:pcscf1.visited1.net
Remote-Party-ID:
Anonymity:
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-Disposition:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
a=
m=
```

7. **PRACK (S-CSCF to P-CSCF) – see example in Table 7.y.4-7**

   S-CSCF forwards the PRACK request to P-CSCF.

Table 7.y.4-7: PRACK (S-CSCF to P-CSCF)

```
PRACK sip:pcscf2.visited2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Contact:
Rack:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

8. **PRACK (P-CSCF to UE) – see example in Table 7.y.4-8**

   P-CSCF forwards the PRACK request to UE.

Table 7.y.4-8: PRACK (P-CSCF to UE)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
Cseq:
Contact:
Rack:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

9. **200 OK (UE to P-CSCF) – see example in Table 7.y.4-9**

   UE acknowledges the PRACK request with a 200 OK response.

Table 7.y.4-9: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

10. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.y.4-10**

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.y.4-10: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length:
```

11. **GPRS: Active (Secondary) PDP Context (UE to SGSN)**

    The UE sends an Activate (Secondary) PDP Context message to the SGSN with the UMTS QoS parameters.

12. **GPRS: Create PDP Context (SGSN to GGSN)**

    The SGSN checks the user profile to authorize the requested QoS and also the available resource, if both are granted, it sends the corresponding Create PDP Context message to the GGSN.

13. **GPRS: Create PDP Context Resp (GGSN to SGSN)**

    The GGSN checks its own available resources; if enough resources are available it sends a Create PDP Context Response message back to SGSN.

14. **GPRS: Active PDP Context Accept (SGSN to UE)**

    The SGSN sends an Activate PDP Context Accept message to UE.

    Editor's Note: It is shall be possible that PDP Context activation starts immediately after the reception of the PRACK for the 183 Session Progress, to save the time for call setup.

15. **RSVP: PATH (UE#2 to UE#1)**

    After the PDP context establishment procedure is completed, UE#2 sends a RSVP PATH message to the UE#1.

16. **RSVP: RESV (UE#1 to UE#2)**

    UE#1 answers with a RESV message to UE#2.

17. **RSVP: RESV-CONF (UE#2 to UE#1)**

    UE#2 sends a RSVP RESV-CONF message to UE#1 if the RESV message (16) requested an optional confirmation.

18. **RSVP: PATH (UE#1 to UE#2)**

    UE#1 sends an RSVP PATH message to UE#2. This message can arrive at any time. Particularly, it can arrive after message 9 and before the GPRS procedure to activate the (Secondary) PDP context has started (message 11).

19. **GPRS: Modify PDP Context (UE to SGSN)**

    UE #2may send a Modify PDP Context message to the SGSN with the necessary modification to UMTS QoS parameters according to the received RSVP PATH message.

20. **GPRS: Update PDP Context (SGSN to GGSN)**

    The SGSN checks the user profile to authorize the requested QoS (this check will happen only if a higher QoS is requested) and also the available resource, if both are granted; it sends the corresponding Update PDP Context message to the GGSN.

21. **GPRS: Update PDP Context Resp (GGSN to SGSN)**

    The GGSN checks its available resource and accepts the PDP modification request, and sends a Update PDP Context Response message back to SGSN.

22. **GPRS: Modify PDP Context Accept (SGSN to UE)**

    The SGSN sends a Modify PDP Context Accept message to UE.

    Note: Steps 19 to 22 are optional. This procedure can happen if the existing PDP context doesn't conform the QoS requirement of the RSVP, but this is an implementation issue.

23. **RSVP: RESV (UE#2 to UE#1)**

    UE#2 answers the RSVP path message with an RSVP RESV message to UE#1.

24. **RSVP: RESV-CONF (UE#1 to UE#2)**

    UE#1 sends a RSVP RESV-CONF message to UE#2 if the RESV message (23) requested an optional confirmation.

25. **COMET (S-CSCF to P-CSCF) – see example in Table 7.y.4-25**

    S-CSCF forwards the COMET request to P-CSCF. The SDP contains the indication that UE#1 has Assured QoS in for both the uplink and the downlink.

Table 7.y.4-25: COMET (S-CSCF to P-CSCF)

```
COMET sip:pcscf2.visited2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length:

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:success sendrecv
m=audio 0 RTP/AVP 97 96 0 15
```

SDP: The SDP indicates that the QoS resource reservation for both send and receive mode was successful at the originating side.

26. **COMET (P-CSCF to UE) – see example in Table 7.y.4-26**

    P-CSCF forwards the COMET request to UE.

Table 7.y.4-26: COMET (P-CSCF to UE)

```
COMET sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

27. **200 OK (UE to P-CSCF) – see example in Table 7.y.4-217**

UE acknowledges the COMET request with a 200 OK response.

Table 7.y.4-27: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

28. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.y.4-28**

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.y.4-28: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

From:
To:
Call-ID:
CSeq:
Content-length:
```

29. **180 Ringing (UE to P-CSCF) – see example in Table 7.y.4-29**

As the COMET is used to send confirmation of end-to-end QoS reservation in both directions, the destination endpoint determines that all the pre-conditions have been met. Then the destination continues with the session establishment by alerting the user and sending the 180 Ringing.

Table 7.y.4-29: 180 Ringing (UE to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
Require: 100rel
From:
To:
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9022
Content-length: 0
```

30. **180 Ringing (P-CSCF to S-CSCF) – see example in Table 7.y.4-30**

    P-CSCF forwards the 180 Ringing response to S-CSCF.

Table 7.y.4-30: 180 Ringing (P-CSCF to S-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.visited2.net,sip:scscf2.home2.net, sip:scscf1.home1.net,
sip:pcscf1.visited1.net
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-length:
```

31. **PRACK (S-CSCF to P-CSCF) – see example in Table 7.y.4-31**

    S-CSCF forwards the PRACK request to P-CSCF.

Table 7.y.4-31: PRACK (S-CSCF to P-CSCF)

```
PRACK sip:pcscf2.visited2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:

Rack:
Content-length:
```

32. **PRACK (P-CSCF to UE) – see example in Table 7.y.4-32**

    P-CSCF forwards the PRACK request to UE.

Table 7.y.4-32: PRACK (P-CSCF to UE)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
Cseq:
Rack:
Content-length:
```

33. **200 OK (UE to P-CSCF) – see example in Table 7.y.4-33**

    UE acknowledges the PRACK request with a 200 OK response.

Table 7.y.4-33: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

34. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.y.4-34**

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.y.4-34: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length:
```

35. **200 OK (UE to P-CSCF) – see example in Table 7.y.4-35**

When the called party answers the UE sends a 200 OK final response to the INVITE request (6) to P-CSCF, and starts the media flow(s) for this session.

Table 7.y.4-35: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
CSeq: 127 INVITE
Contact: sip:[5555::eee:fff:aaa:bbb]
Content-type: application/sdp
Content-length: (...)

v=
o=- 2987933615 2987933615 IN IP6 5555::eee:fff:aaa:bbb
s=
c=IN IP6 5555::eee:fff:aaa:bbb
b=
t=
m=
m=
m=audio 6543 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:success sendrev
m=
```

SDP: The SDP indicates that the QoS resource reservation for both send and receive mode was successful from the terminating endpoint side.

36. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.y.4-36**

P-CSCF indicates the resources reserved for this session should now be committed, and sends the 200 OK final response to S-CSCF.

Table 7.y.4-36: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.visited2.net, sip:scscf2.home2.net, sip:scscf1.home1.net,
sip:pcscf1.visited1.net
From:
To:
Call-ID:
CSeq:
Contact:
Content-type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
a=
m=
```

37. **ACK (S-CSCF to P-CSCF) – see example in Table 7.y.4-37**

S-CSCF forwards the ACK request to P-CSCF.

Table 7.y.4-37: ACK (S-CSCF to P-CSCF)

```
ACK sip:pcscf2.visited2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.visited1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Content-length: 0
```

38. **ACK (P-CSCF to UE) – see example in Table 7.y.4-38**

P-CSCF forwards the ACK request to UE.

Table 7.y.4-38: ACK (P-CSCF to UE)

```
ACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=token1
From:
To:
Call-ID:
Cseq:
Content-length:
```

3GPP TSG-CN1 Meeting #19bis ***Tdoc N1-011381***
Sophia-Antipolis, 2.-4. Oct 2001

Source:	**Lucent Technologies**
Title:	**CR to 24.228: QoS flows in Mobile Originating (GGSN is not RSVP aware)**
Agenda item:	**8.8**
Document for:	**APPROVAL / DISCUSSION**

Discussion

As agreed in last CN1-CN3-CN4 joint meeting in Dresden, QoS end-to-end flows examples (MO and MT) shall be shown in 24.228. This contribution is attempting to give the example flows based on MO without Service-based Local Policy and GGSN is RSVP non aware case.

Proposal

It is proposed that adding a new clause in Annex A-1 7.2.5

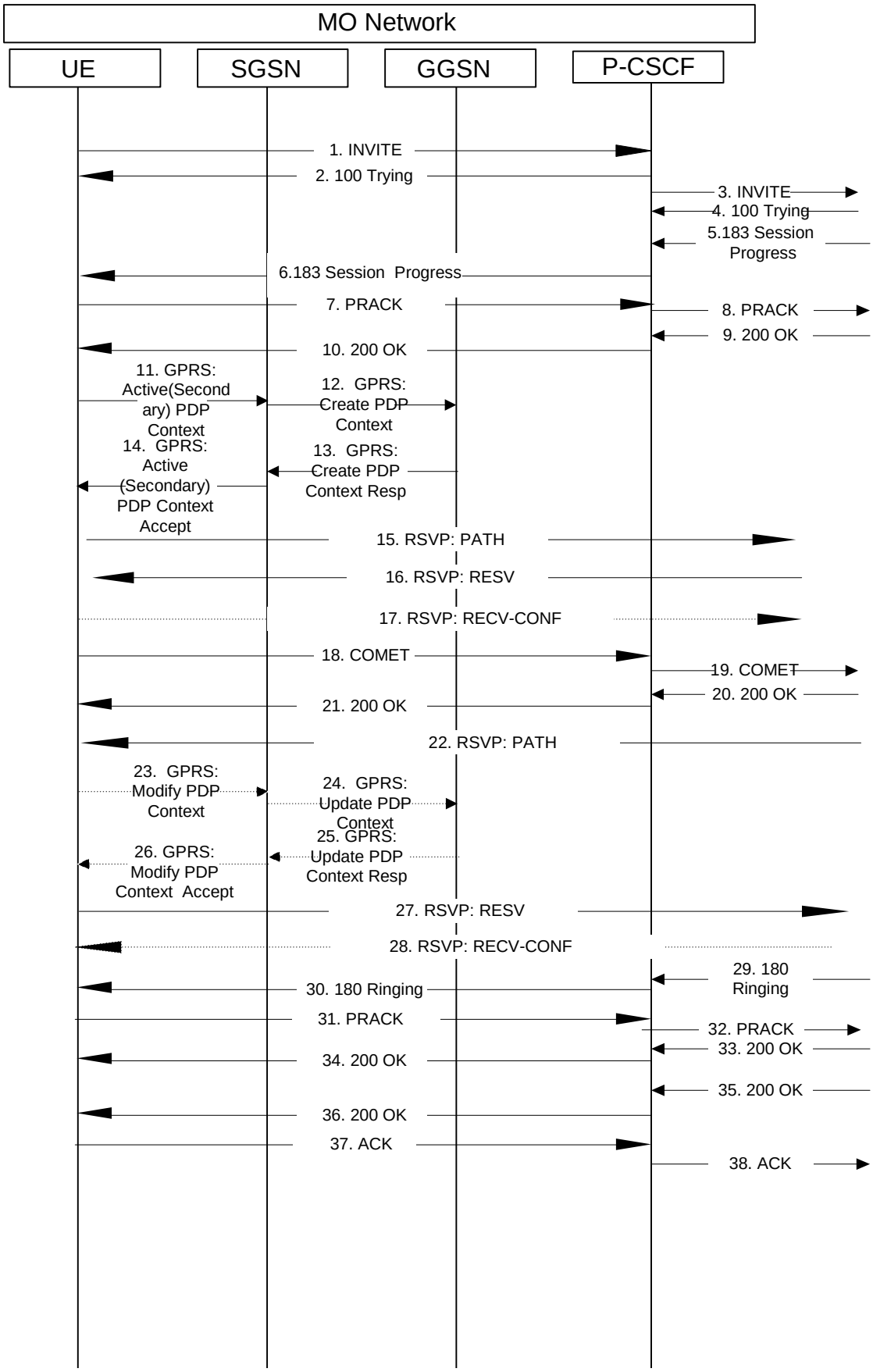
7.2.5 Mobile Originating with End-to-End-RSVP (without Service-based Local Policy, GGSN is not RSVP Aware)

All flows below show an example of QoS interaction during a session setup. Because the S-CSCF is not involved in QoS interaction, so it is not shown in the flow for simplify reason. This example is appropriate for a single-media session with QoS-Assured model. It is assumed in the example that both the UAC and UAS have chosen to use RSVP as the additional QoS reservation protocol which means both the UAC and UAS establishes satisfactory PDP contexts on their respective accesses, and also performs single-direction ("send") RSVP resource reservation.The usage of RSVP is one of the possible mechanisms for satisfy the QoS requirements, other mechanisms can also been used, etc. Diffserv.

Note: The diagrams in this subsection depict the case when the GGSN is not RSVP aware, however, the alternative of GGSN being RSVP aware is also possible.

Note: It is assumed that MO#2 is used in this flow

This diagram provides the flows for SIP session signalling, PDP context establishment, and resource reservation (RSVP).



1. **INVITE (UE to P-CSCF) – see example in Table 7.2.5-1**
UE#1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for

each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

For this example, assume UE#1 is capable of sending two simultaneous video streams, either H261 or MPV format, and two simultaneous audio streams, either AMR, G726-32, PCMU, or G728.

UE sends the INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism.

Editor's Note: Certain fields in the SDP carry no information. In particular the "o=", "s=" fields and "t=". These are, however, mandatory fields within SDP.Does 3GPP wish to define a non-standard version of SDP that removes these, and if so, how does this interwork with outside SIP networks that use standard SDP.

Table 7.2.5-1: INVITE (UE to P-CSCF)

```
INVITE sip:+1-212-555-2222@home2.net;user=phone SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Supported: 100rel
Remote-Party-ID: "John Doe" <tel:+1-212-555-1111>;privacy=off
Anonymity: Off
From: "Alien Blaster" <sip:B36(SHA-1(+1-212-555-1111; time=36123E5B; seq=72))@localhost>; tag=171828
To: sip:B36(SHA-1(+1-212-555-2222; time=36123E5B; seq=73))@localhost
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 127 INVITE
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 3400 RTP/AVP 98 99
a=qos:mandatory sendrecv
a=rtpmap:98 H261
a=rtpmap:99:MPV
m=video 3402 RTP/AVP 98 99
a=qos:mandatory sendrecv
a=rtpmap:98 H261
a=rtpmap:99:MPV
m=audio 3456 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
m=audio 3458 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
```

Request-URI: contains the keyed number from the user.

Via: contains the IP address or FQDN of the originating UE.

Remote-Party-ID: contains the public identity of the UE. The Display name is optional.

From:, To:, Call-ID: follow the recommendations of draft-ietf-sip-privacy-01, even though anonymity is not being requested for this session.

Cseq: a random starting number.

Contact: the IP address or FQDN of the originating UE.

SDP The SDP contains a set of codecs supported by UE#1 and desired by the user at UE#1 for this session.

2. **100 Trying (P-CSCF to UE) – see example in Table 7.2.5-2**

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.2.5-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

3. **INVITE (P-CSCF to S-CSCF) – see example in Table 7.2.5-3**

P-CSCF remembers (from the registration procedure) the request routing for this UE. This becomes the Request-URI header in the request. This next hop is the S-CSCF within the home network of UE#1.

P-CSCF adds itself to the Record-Route header and Via header.

P-CSCF#1 examines the media parameters, and removes any choices that the network operator decides based on local policy, not to allow on the network.

For this example, assume the network operator disallows H261 video encoding.

The INVITE request is forwarded to the S-CSCF.

Table 7.2.5-3: INVITE (P-CSCF to S-CSCF)

```
INVITE sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf1.home1.net
Route: sip:+1-212-555-2222@home2.net;user=phone
Supported:
Remote-Party-ID:
Anonymity:
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 3400 RTP/AVP 99
a=qos:mandatory sendrecv
a=rtpmap:99:MPV
m=video 3402 RTP/AVP 99
a=qos:mandatory sendrecv
a=rtpmap:99:MPV
m=audio 3456 RTP/AVP 97 96 0 15
a=qos:mandatory sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
m=audio 3458 RTP/AVP 97 96 0 15
a=qos:mandatory sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
```

Request-URI: is the first component in the remembered Path header from Registration.

Route: contains the remaining elements from the Path header from Registration, with the initial Request-URI (received from the UE) appended as the final component.

SDP The SDP contains the restricted set of codecs allowed by the network operator. The “m=” lines for the video media streams no longer list code 98 (H261).

Editor's Note: Modified text for this step is contained in Annex A.

4. **100 Trying (S-CSCF to P-CSCF) – see example in Table 7.2.5-4**

   S-CSCF responds to the INVITE request (3) with a 100 Trying provisional response.

Table 7.2.5-4: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

5. **183 Session Progress (S-CSCF to P-CSCF) – see example in Table 7.2.5-5**

   The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response (to 6), per the S-CSCF to S-CSCF procedures. The destination indicates that it supports "Precondition" and requests a confirmation from the originating side for QoS reservation.

Table 7.2.5-5: 183 Session Progress (S-CSCF to P-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.home2.net, sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.home1.net
Remote-Party-ID: "John Smith" <tel:+1-212-555-2222>;privacy=off;screen=yes
Anonymity: Off
Require: 100rel
From:
To: sip:B36(SHA-1(+1-212-555-2222; time=36123E5B; seq=73))@localhost; tag=314159
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9021
Content-Disposition: precondition
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::eee:fff:aaa:bbb
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 6544 RTP/AVP 97 96
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv confirm
m=audio 0 RTP/AVP 97 96 0 15
```

6. **183 Session Progress (P-CSCF to UE) – see example in Table 7.2.5-6**

   P-CSCF forwards the 183 Session Progress response to the originating endpoint.

Table 7.2.5-6: 183 Session Progress (P-CSCF to UE)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Remote-Party-ID:
Anonymity:
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-Disposition:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=a=
a=
a=
a=
m=
```

P-CSCF removes the Record-Route and Via headers, calculates the proper Route header to add to future requests, and saves that information without passing it to UE. The saved value of the Route header is:

```
Route: sip:scscf1.home1.net, sip:scscf2.home2.net, sip:pcscf2.home2.net
```

Editor's Note: Modified text for this step is contained in Annex A.

7. **PRACK (UE to P-CSCF) – see example in Table 7.2.5-7**

   UE#1 determines which media flows should be used for this session, and which codecs should be used for each of those media flows. If there was any change in media flows, or if there was more than one choice of codec for a media flow, then UE#1 must include an SDP in the PRACK message sent to UE#2.

   For this example, assume UE#1 chooses AMR as the codec to use for the single audio stream.

   UE includes this information in the PRACK request to P-CSCF.

Table 7.2.5-7: PRACK (UE to P-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: “Alien Blaster” <sip:B36(SHA-1(555-1111; time=36123E5B; seq=72))@localhost>;tag=171828
To: <sip:B36(SHA-1(555-2222; time=36123E5B; seq=73))@localhost>;tag=314159
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 128 PRACK

Rack: 9021 127 INVITE
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:mandatory sendrecv
m=audio 0 RTP/AVP 97 96 0 15
```

Request-URI: takes the value of the Contact header of the received 183 Session Progress response.

Via: takes the value of either the IP address of RQDN of the originating UE.

From:, To:, Call-ID: copied from the 183 Session Progress response so that they include any tag parameter.

Cseq: takes a higher value than that in the previous request.

The final selection of the media stream from the set of those supported by the terminating endpoint, given in the received 183 Session Progress response (14), is made by the originating UE and included in the SDP.

8. **PRACK (P-CSCF to S-CSCF) – see example in Table 7.2.5-8**

P-CSCF adds the Route header corresponding to the session. P-CSCF forwards the PRACK request to S-CSCF.

Table 7.2.5-8: PRACK (P-CSCF to S-CSCF)

```
PRACK sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.home2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Rack:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

Request-URI: the first component of the saved Route header.

Route: saved from the 183 Session Progress response (with first element moved to Request-URI) with the initial Request-URI (received from the UE) appended as the final component.

9. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.2.5-9**

   S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.2.5-9: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

From:
To:
Call-ID:
CSeq:

Content-Length:
```

10. **200 OK (P-CSCF to UE) – see example in Table 7.2.5-10**

    P-CSCF forwards the 200 OK response to UE.

Table 7.2.5-10: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:

Content-Length:
```

11. **GPRS: Active (Secondary) PDP Context (UE to SGSN)**

    The UE calculates the PDP Context QoS parameters needed for both downlink and uplink based on the SDP information. and sends an Activate (Secondary) PDP Context message to the SGSN with the those QoS parameters.

Editor's Note: In flow 11, the PDP Context QoS is based on the SDP parameters. The mapping between PDP Context and SDP is not standardized

12. **GPRS: Create PDP Context (SGSN to GGSN)**

    The SGSN checks the user profile to authorize the requested QoS and also the available resource, if both are granted, it sends the corresponding Create PDP Context message to the GGSN.

13. **GPRS: Create PDP Context Resp (GGSN to SGSN)**

    The GGSN authorizes the PDP context activation request according to the local operator's IP bearer resource based policy, the local operator's admission control function and the GPRS roaming agreements and sends a Create PDP Context Response message back to the SGSN.

14. **GPRS: Active PDP Context Accept (SGSN to UE)**

    The SGSN sends an Activate PDP Context Accept message to UE indicating the PDP Context has been activated and the QoS requirements have been authorized for both downlink and uplink

    Note: It is shall be possible that PDP Context activation starts immediately after flow 6 to save the time for call setup.

15. **RSVP: PATH (UE to Next Hop)**

    UE sends an RSVP PATH message to the next hop, through the GGSN with the QoS parameter required for its "send" direction. The GGSN does not process the RSVP PATH message

Editor's Note: The mapping between PDP Context and RSVP is not standardized

16. **RSVP: RESV (Terminating Side to UE)**

    The UE receives the RSVP RESV message in the downlink direction, through the GGSN. The GGSN does not process the RSVP RESV message. This message is originally sent by terminating UE to request the QoS reservation for the direction from originating UE to terminating UE.

17. **RSVP: RESV-CONF (UE to Next Hop)**

    The UE sends a RSVP RESV-CONF message to the next hop. The use of the RESV-CONF message is optional.

Editor's Note: The content of flow 11-17 is FFS.

18. **COMET (UE to P-CSCF) – see example in Table 7.2.5-18**

    At this point, the UE can determine that its end-to-end QoS for its "send" direction has been reserved successfully because it has used PDP Context Activation (secondary) procedure to guarantee the QoS from UE to GGSN and used RSVP to guarantee the QoS from GGSN to the terminating network. So when the UE finishes QoS reservation for its sending direction, it sends the COMET message with "a=qos:success sendonly " to the terminating endpoint to indicate this successful reservation for its "send" direction , via the signalling path established by the INVITE request.

Table 7.2.5-18: COMET (UE to P-CSCF)

```
COMET sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: "Alien Blaster" <sip:B36(SHA-1(555-1111; time=36123E5B; seq=72))@localhost>; tag=171828
To: <sip:B36(SHA-1(555-2222; time=36123E5B; seq=73))@localhost>;tag=314159
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 129 COMET
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:success sendonly
m=audio 0 RTP/AVP 97 96 0 15
```

Request-URI: takes the value of the Contact header of the received 183 Session Progress response.

Via: takes the value of either the IP address or FQDN of the originating UE.

From:, To:, Call-ID: copied from the 183 Session Progress response so that they include any tag parameters.

CSeq: takes a higher value than that in the previous request.

The SDP indicates that the resource reservation was successful.

19. **COMET (P-CSCF to S-CSCF) – see example in Table 7.2.5-19**

    P-CSCF forwards the COMET request to S-CSCF.

Table 7.2.5-19: COMET (P-CSCF to S-CSCF)

```
COMET sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.home2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

Request-URI: the first component of the saved Route header.

Route: saved from the 183 Session Progress response (with first element moved to Request-URI) with the initial Request-URI (received from the UE) appended as the final component.

20. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.2.5-20**

S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.2.5-20: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

From:
To:
Call-ID:
CSeq:

Content-Length:
```

21. **200 OK (P-CSCF to UE) – see example in Table 7.2.5-21**

P-CSCF forwards the 200 OK response to UE.

Table 7.2.5-21: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:

Content-Length:
```

22. **RSVP: PATH (Terminating Side to UE)**

At the mean time when the originating UE is reserving the QoS, the terminating UE is also using RSVP to reserve the QoS. The UE receives a RSVP PATH message in the downlink direction, through the GGSN. The GGSN does not process the RSVP PATH message. The message carries the QoS parameters for the terminating UE's "send" direction.

23. **GPRS: Modify PDP Context (UE to SGSN)**

    The UE may send a Modify PDP Context message to the SGSN with the necessary modification to PDP Context QoS parameters according to the received RSVP PATH message.

24. **GPRS: Update PDP Context (SGSN to GGSN)**

    The SGSN checks the user profile to authorize the requested QoS (this check will happen only if a higher QoS is requested) and also the available resource, if both are granted; it sends the corresponding Update PDP Context message to the GGSN.

25. **GPRS: Update PDP Context Resp (GGSN to SGSN)**

    The GGSN authorizes the PDP context modification according to the local operator's IP bearer resource based policy, the local operator's admission control function and the GPRS roaming agreements and sends an Update PDP Context Response message back to the SGSN.

26. **GPRS: Modify PDP Context Accept (SGSN to UE)**

    The SGSN sends a Modify PDP Context Accept message to UE.

    Note: Steps 23 to 26 are optional. This procedure can happen if the existing PDP context doesn't conform the QoS requirement of the RSVP, but this is an implementation issue. This procedure if it is successful will only modify the downlink PDP Context QoS parameters. If this procedure fails, the existing PDP Context is still valid.

27. **RSVP: RESV (UE to Next Hop)**

    UE sends the RSVP RESV message to the next hop to reserve the QoS for its "receive direction"., through the GGSN. The GGSN does not process the RSVP RESV message.

28. **RSVP: RESV-CONF (Terminating Side to UE)**

    The terminating UE sends RESV-CONF message to confirm that the QoS reservation has finished. The use of the RESV-CONF message is optional.

Editor's Note: The sequence of the RSVP messages exchanged by UAs are independent, this diagram just shows one possible sequence. For example, flow 15 is earlier than flow 22 in this call flows, but the reverse sequence is also possible.

Editor's Note: The content of the flow 22-28 is FFS

29. **180 Ringing (S-CSCF to P-CSCF) – see example in Table 7.2.5-29**

After the terminating UE successfully reserves the QoS for its "send" direction, and based on the confirmation (COMET) sent by originating party, the terminating UE can determine that all the pre-condition has been met (both directioin QoS has been reserved). Then it starts continue with the session transaction which is here to perform alerting.

Table 7.2.5-29: 180 Ringing (S-CSCF to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

Record-Route: sip:pcscf2.home2.net, sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.home1.net
Require: 100rel
From:
To:
Call-ID:
CSeq:
Contact: sip: [5555::eee:fff:aaa:bbb]
RSeq: 9022
Content-length: 0
```

30. **180 Ringing (P-CSCF to UE) – see example in Table 7.2.5-30**

S-CSCF forwards the 180 Ringing response to P-CSCF.

Table 7.2.5-30: 180 Ringing (S-CSCF to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-length:
```

Editor's Note: Additional QoS interactions to handle one-way media at this point (e.g. for PSTN ringback and announcements) is for further study.

31. **PRACK (UE to P-CSCF) – see example in Table 7.2.5-31**

UE indicates to the originating subscriber that the destination is ringing. It responds to the 180 Ringing provisional response (29) with a PRACK request.

Table 7.2.5-31: PRACK (UE to P-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: "Alien Blaster" <sip:B36(SHA-1(555-1111; time=36123E5B; seq=72))@localhost>;tag=171828
To: <sip:B36(SHA-1(555-2222; time=36123E5B; seq=73))@localhost>;tag=314159
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 130 PRACK

Rack: 9022 127 INVITE
Content-length: 0
```

Request-URI: takes the value of the Contact header of the 180 Ringing response.

Via: **takes the value of either the IP address or FQDN of the UE.**

From:, To:, Call-ID: copied from the 180 Ringing response so that they include any revised tag parameters.

Cseq: takes a higher value than in the previous request.

32. **PRACK (P-CSCF to S-CSCF) – see example in Table 7.2.5-32**

P-CSCF adds the Route header corresponding to the session.

P-CSCF forwards the PRACK request to S-CSCF.

Table 7.2.5-32: PRACK (P-CSCF to S-CSCF)

```
PRACK sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.home2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:

Rack:
Content-length:
```

33. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.2.5-33**

S-CSCF forwards the 200 OK response for PRACK to P-CSCF.

Table 7.2.5-33: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

From:
To:
Call-ID:
CSeq:
Content-Length:
```

34. **200 OK (P-CSCF to UE) – see example in Table 7.2.5-34**

P-CSCF forwards the 200 OK response to UE.

Table 7.2.5-34: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:

Content-Length:
```

35. **200 OK (S-CSCF to P-CSCF) – see example in Table 7.2.5-35**

When the called party answers, the terminating endpoint sends a 200 OK final response to the INVITE request

Table 7.2.5-35: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route:
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

36. **200 OK (P-CSCF to UE) – see example in Table 7.2.5-36**

P-CSCF indicates the resources reserved for this session should now be committed, and forwards the 200 OK final response to the session originator. UE can start the media flow(s) for this session.

Table 7.2.5-36: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

P-CSCF removes the Record-Route headers, calculates the proper Route header to add to future requests, and saves that information without passing it to UE.

37. **ACK (UE to P-CSCF) – see example in Table 7.2.5-43**

UE starts the media flow for this session, and responds to the 200 OK with an ACK request sent to P-CSCF.

Table 7.2.5-37: ACK (UE to P-CSCF)

```
ACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: “Alien Blaster” <sip:B36(SHA-1(555-1111; time=36123E5B; seq=72))@localhost>;tag=171828
To: <sip:B36(SHA-1(555-2222; time=36123E5B; seq=73))@localhost>;tag=314159
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 127 ACK

Content-length: 0
```

Cseq: is required to be the same value as Cseq contained in original INVITE request [3]

38. **ACK (P-CSCF to S-CSCF) – see example in Table 7.2.5-44**

P-CSCF forwards the ACK request to S-CSCF.

Table 7.2.5-38: ACK (P-CSCF to S-CSCF)

```
ACK sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:scscf2.home2.net, sip:pcscf2.home2.net, sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:

Content-length:
```

Request-URI: the first component of the saved Route header.

Route: saved from the 200 OK response (with first element moved to Request-URI) with the initial Request-URI (received from the UE) appended as the final component.

3GPP TSG-CN1 Meeting #19bis ***Tdoc N1-011383***
Sophia-Antipolis, 2.-4. Oct 2001

Source:	**Lucent Technologies**
Title:	**CR to 24.228: QoS flows in Mobile Terminating (GGSN is Not RSVP aware)**
Agenda item:	**8.8**
Document for:	**APPROVAL / DISCUSSION**

Discussion

As agreed in last CN1-CN3-CN4 joint meeting in Dresden, QoS end-to-end flows examples (MO and MT) shall be shown in 24.228. This contribution is attempting to give the example flows based on MT without Service-based Local Policy case.

Proposal

It is proposed that adding a new clause in Annex A-1 7.4.5 Mobile Terminating End-to-End QoS Flows and 7.4.5.1 Mobile Terminating with End-to-end RSVP (Without Service-Based Local Policy, GGSN is not RSVP aware)

7.4.5 Mobile Terminating End-to-End QoS and Signalling Call Flows

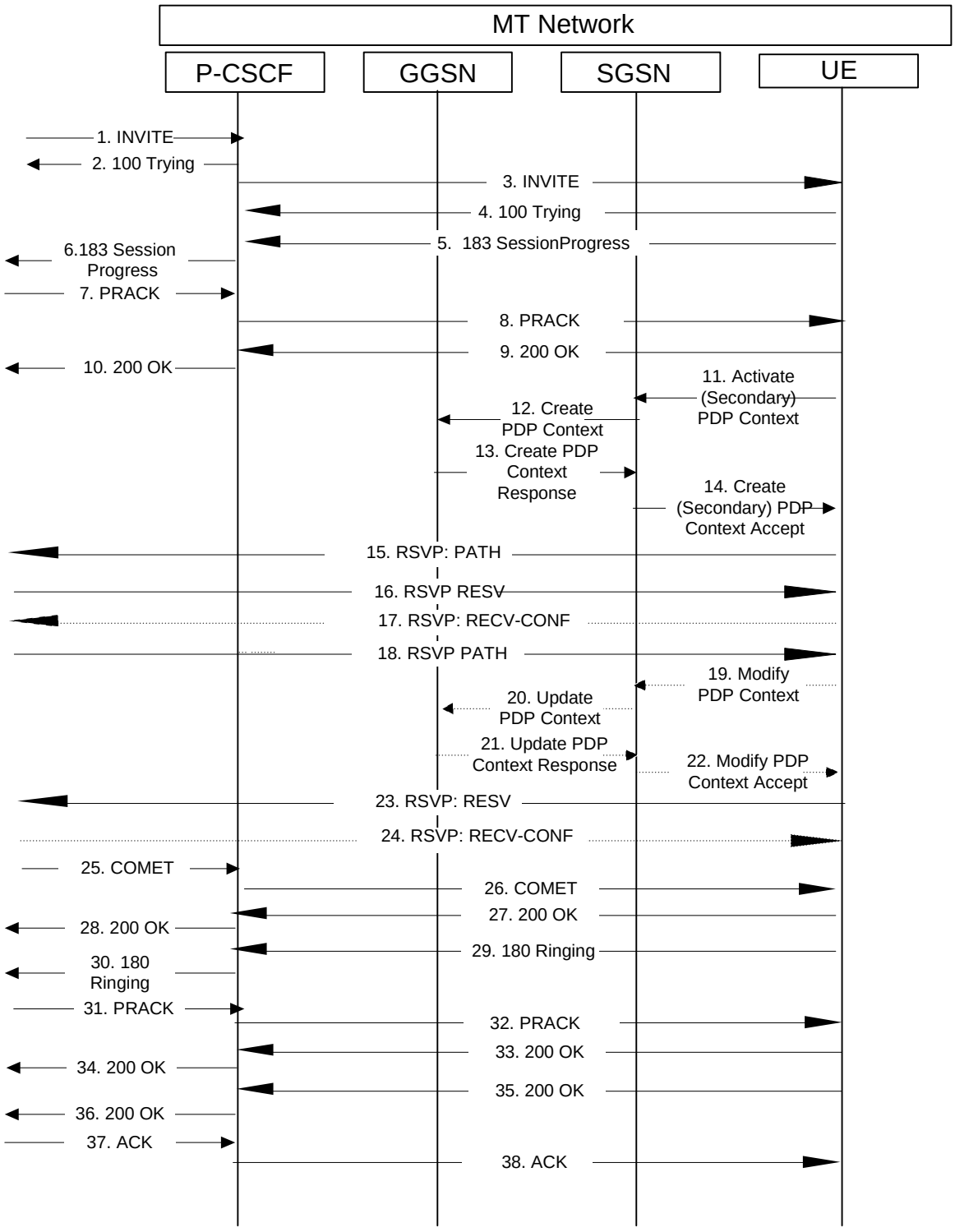
7.4.5.1 Mobile Terminating with End-to-End-RSVP (without Service-based Local Policy, GGSN is not RSVP Aware)

All flows below show an example of QoS interaction during a session setup. Because the S-CSCF is not involved in QoS interaction, so it is not shown in the flow for simplify reason. This example is appropriate for a single-media session with QoS-Assured model. It is assumed in the example that both the UAC and UAS have chosen to use RSVP as the additional QoS reservation protocol which means both the UAC and UAS establishes satisfactory PDP contexts on their respective accesses, and also performs single-direction ("send") RSVP resource reservation.The usage of RSVP is one of the possible mechanisms for satisfy the QoS requirements, other mechanisms can also been used, etc. Diffserv.

Note: The diagrams in this subsection depict the case when the GGSN is not RSVP aware, however, the alternative of GGSN being RSVP aware is also possible.

Note: It is assumed that MT#2 is used in this flow

This diagram provides the flows for SIP session signalling, PDP context establishment, and resource reservation (RSVP).


MT Network
P-CSCF
GGSN
SGSN
UE
1. INVITE
2. 100 Trying
3. INVITE
4. 100 Trying
5. 183 SessionProgress
6.183 Session Progress
7. PRACK
8. PRACK
9. 200 OK
10. 200 OK
11. Activate (Secondary) PDP Context
12. Create PDP Context
13. Create PDP Context Response
14. Create (Secondary) PDP Context Accept
15. RSVP: PATH
16. RSVP RESV
17. RSVP: RECV-CONF
18. RSVP PATH
19. Modify PDP Context
20. Update PDP Context
21. Update PDP Context Response
22. Modify PDP Context Accept
23. RSVP: RESV
24. RSVP: RECV-CONF
25. COMET
26. COMET
27. 200 OK
28. 200 OK
29. 180 Ringing
30. 180 Ringing
31. PRACK
32. PRACK
33. 200 OK
34. 200 OK
35. 200 OK
36. 200 OK
37. ACK
38. ACK

1. **INVITE (S-CSCF to P-CSCF) – see example in Table 7.4.5.1-1**

   S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE request to the P-CSCF.

Table 7.4.5.1-1: INVITE (S-CSCF to P-CSCF)

```
INVITE sip: pcscf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net SIP/2.0/UDP  scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:+1-212-555-2222@home2.net;user=phone
Record-Route: sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.home1.net
Supported:
Remote-Party-ID:
Anonymity:
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97 96 0 15
a=qos:mandatory sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
m=audio 0 RTP/AVP 97 96 0 15
```

Request-URI: built from the registration information

Via:, Record-Route: S-CSCF adds itself in the Record-Route and Via headers.

SDP The SDP contains the restricted set of codecs allowed by the network operator. The "m=" lines for the second audio stream shows a port number zero, which removes it from the negotiation.

2. **100 Trying (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-2**

   P-CSCF responds to the INVITE request (4) with a 100 Trying provisional response.

Table 7.4.5.1-2: 100 Trying (P-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

3. **INVITE (P-CSCF to UE) – see example in Table 7.4.5.1-3**

   P-CSCF examines the media parameters, and removes any that the network operator decides not to allow on the network.

   For this example, assume the network operator does not allow 64 kb/s audio, so the PCMU codec is removed.

   P-CSCF determines the UE address from the value of the Request-URI (which was previously returned by P-CSCF as a contact header value in the registration procedure), and forwards the INVITE request to the UE.

Table 7.4.5.1-3: INVITE (P-CSCF to UE)

```
INVITE sip:+1-212-555-2222@home2.net;user=phone SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1

Supported:
Remote-Party-ID:
Anonymity:
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-length:

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97 96 15
a=qos:mandatory sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
m=audio 0 RTP/AVP 97 96 0 15
```

P-CSCF removes the Record-Route and Via headers, calculates the proper Route header to add to future requests, and saves that information without passing it to UE. The saved value of the Route header is:

```
Route: sip:scscf2.home2.net, sip:scscf1.home1.net,
     sip:pcscf1.home1.net
```

Via: P-CSCF removes the Via headers, and generates a locally unique token to identify the saves values. It inserts this as a branch value on its Via header.

SDP The SDP contains the restricted set of codecs allowed by the network operator. The "m=" lines for the first audio stream no longer contains codec "0" (PCMU), which removes it from the negotiation.

Editor's Note: Modified text for this step is contained in Annex A.

4. **100 Trying (UE to P-CSCF) – see example in Table 7.4.5.1-4**

   UE may optionally send a 100 Trying provisional response to P-CSCF.

Table 7.4.5.1-4: 100 Trying (UE to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

5. **183 Session Progress (UE to P-CSCF) – see example in Table 7.4.5.1-5**

   UE#2 determines the complete set of codecs that it is capable of supporting for this session. It determines the intersection with those appearing in the SDP in the INVITE request. For each media flow that is not supported, UE#2 inserts a SDP entry for media (m= line) with port=0. For each media flow that is supported, UE#2 inserts a SDP entry with an assigned port and with the codecs in common with those in the SDP from UE#1.

   For this example, assume UE#2 supports both AMR and G726, but not G728 (code 15)

UE responds with a 183 Session Progress response containing SDP back to the originator. This SDP may represent one or more media for a multimedia session. This response is sent to P-CSCF.

Table 7.4.5.1-5: 183 Session Progress (UE to P-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
Remote-Party-ID: “John Smith” <tel:+1-212-555-2222>;privacy=off
Anonymity: Off
Require: 100rel
From:
To: sip:B36(SHA-1(+1-212-555-2222; time=36123E5B; seq=73))@localhost; tag=314159
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9021
Content-Disposition: precondition
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::eee:fff:aaa:bbb
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 6544 RTP/AVP 97 96
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:mandatory sendrecv confirm
a=rtpmap:96 G726-32/8000
m=audio 0 RTP/AVP 97 96 0 15
```

Remote-Party-ID: identifies the answering subscriber. It contains the public identifier URL, and the name of the answering party.

To: A tag is added to the To header.

Contact: identifies the IP address or FQDN of the UE.

SDP The SDP contains the subset of codecs supported by UE. It requests a confirmation of the QoS preconditions for establishing the session

6. **183 Session Progress (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-6**

P-CSCF forwards the 183 Session Progress response to S-CSCF.

Table 7.4.5.1-10: 183 Session Progress (P-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd])
Record-Route: sip:pcscf2.home2.net, sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.home1.net
Remote-Party-ID:
Anonymity:
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-Disposition:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
a=
m=
```

P-CSCF restores the Via headers and Record-Route headers from the branch value in its Via.

7. **PRACK (S-CSCF to P-CSCF) – see example in Table 7.4.5.1-7**

   S-CSCF forwards the PRACK request to P-CSCF.

Table 7.4.5.1-7: PRACK (S-CSCF to P-CSCF)

```
PRACK sip:pcscf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From: “Alien Blaster” <sip:B36(SHA-1(555-1111; time=36123E5B; seq=72))@localhost>;tag=171828
To: <sip:B36(SHA-1(555-2222; time=36123E5B; seq=73))@localhost>;tag=314159
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 128 PRACK

Rack: 9021 127 INVITE
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m=video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:mandatory sendrecv
m=audio 0 RTP/AVP 97 96 0 15
```

8. **PRACK (P-CSCF to UE) – see example in Table 7.4.5.1-8**

   P-CSCF forwards the PRACK request to UE.

Table 7.4.5.1-8: PRACK (P-CSCF to UE)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
Cseq:

Rack:
Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

Via: P-CSCF removes the Via headers, and generates a locally unique token to identify the saved values. It inserts this as a branch value on its Via header.

9. **200 OK (UE to P-CSCF) – see example in Table 7.4.5.1-9**

   UE acknowledges the PRACK request (14) with a 200 OK response.

Table 7.4.5.1-9: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

10. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-10**

    P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.5.1-10: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-length:
```

11. **GPRS: Active (Secondary) PDP Context (UE to SGSN)**

    After receiving the PRACK, the UE will stop the SIP transaction until end-to-end QoS for both directions have been achieved. The UE calculates the PDP Context QoS parameters needed for both downlink and uplink based on the SDP information in that PRACK and sends an Activate (Secondary) PDP Context message to the SGSN with the those QoS parameters.

Editor's Note: In flow 11, the PDP Context QoS is based on the SDP parameters. The mapping between PDP Context and SDP is not standardized

12. **GPRS: Create PDP Context (SGSN to GGSN)**

The SGSN checks the user profile to authorize the requested QoS and also the available resource, if both are granted, it sends the corresponding Create PDP Context message to the GGSN.

13. **GPRS: Create PDP Context Resp (GGSN to SGSN)**

    The GGSN authorizes the PDP context activation request according to the local operator's IP bearer resource based policy, the local operator's admission control function and the GPRS roaming agreements and sends a Create PDP Context Response message back to the SGSN.

14. **GPRS: Active PDP Context Accept (SGSN to UE)**

    The SGSN sends an Activate PDP Context Accept message to UE indicating the PDP Context has been activated and the QoS requirements have been authorized for both downlink and uplink

15. **RSVP: PATH (UE to Next Hop)**

    UE sends an RSVP PATH message to the next hop, through the GGSN with the QoS parameter required for its "send" direction. The GGSN does not process the RSVP PATH message

Editor's Note: The mapping between PDP Context and RSVP is not standardized

16. **RSVP: RESV (Originating Side to UE)**

    The UE receives the RSVP RESV message in the downlink direction, through the GGSN. The GGSN does not process the RSVP RESV message. This message is originally sent by originating side UE to request the QoS reservation for the direction from terminating UE to originating UE.

17. **RSVP: RESV-CONF (UE to Next Hop)**

    The UE sends a RSVP RESV-CONF message to the next hop. The use of the RESV-CONF message is optional.

18. **RSVP: PATH (Originating Side to UE)**

    At the mean time when the terminating UE is reserving the QoS, the originating UE is also using RSVP to reserve the QoS. The UE receives a RSVP PATH message in the downlink direction, through the GGSN. The GGSN does not process the RSVP PATH message. The message carries the QoS parameters for the originating UE's "send" direction.

Editor's Note: The sequence of the RSVP messages exchanged by UAs are independent, this diagram just shows one possible sequence. For example, flow 15 happens earlier than flow 18 in this call flows, but the reverse sequence is also possible.

19. **GPRS: Modify PDP Context (UE to SGSN)**

    The UE may send a Modify PDP Context message to the SGSN with the necessary modification to PDP Context QoS parameters according to the received RSVP PATH message.

20. **GPRS: Update PDP Context (SGSN to GGSN)**

    The SGSN checks the user profile to authorize the requested QoS (this check will happen only if a higher QoS is requested) and also the available resource, if both are granted; it sends the corresponding Update PDP Context message to the GGSN.

21. **GPRS: Update PDP Context Resp (GGSN to SGSN)**

    The GGSN authorizes the PDP context modification according to the local operator's IP bearer resource based policy, the local operator's admission control function and the GPRS roaming agreements and sends an Update PDP Context Response message back to the SGSN.

22. **GPRS: Modify PDP Context Accept (SGSN to UE)**

    The SGSN sends a Modify PDP Context Accept message to UE.

    Note: Steps 19 to 22 are optional. This procedure can happen if the existing PDP context doesn't conform the QoS requirement of the RSVP, but this is an implementation issue. This procedure if it is

successful will only modify the downlink PDP Context QoS parameters. If this procedure fails, the existing PDP Context is still valid.

23. **RSVP: RESV (UE to Next Hop)**

    UE sends the RSVP RESV message to the next hop to reserve the QoS for its "receive direction" through the GGSN. The GGSN does not process the RSVP RESV message.

24. **RSVP: RESV-CONF (Terminating Side to UE)**

    The originating UE sends RESV-CONF message to confirm that the QoS reservation has finished. The use of the RESV-CONF message is optional.

Editor's Note: The content of the flow 11-24 is FFS

25. **COMET (S-CSCF to P-CSCF) – see example in Table 7.4.5.1-25**

    After the originating side UE receives the RSVP: RESV message or RECV-CONF message, it know its "send" direction QoS has been reserved, it will immediately send COMET message to the terminating UE.

    Note: In this call flows, the terminating UE finishes its RSVP signalling earlier than originating UE. But it is also possible that this sequence can be reversed. It is worth mention here that the COMET shall be sent right after originating UE finishes its RSVP signalling and this is independent with the sequence of the RSVP signalling of either UAs.

    S-CSCF forwards the COMET request to P-CSCF.

Table 7.4.5.1-25: COMET (S-CSCF to P-CSCF)

```
COMET sip:pcscf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From: "Alien Blaster" <sip:B36(SHA-1(555-1111; time=36123E5B; seq=72))@localhost>;tag=171828
To: <sip:B36(SHA-1(555-2222; time=36123E5B; seq=73))@localhost>;tag=314159
Call-ID: B36(SHA-1(555-1111;time=36123E5B;seq=72))@localhost
Cseq: 129 COMET

Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c= IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 0 RTP/AVP 99
m-video 0 RTP/AVP 99
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=qos:success sendonly
m=audio 0 RTP/AVP 97 96 0 15
```

26. **COMET (P-CSCF to UE) – see example in Table 7.4.5.1-26**

    P-CSCF forwards the COMET request to UE.

Table 7.4.5.1-26: COMET (P-CSCF to UE)

```
COMET sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
Cseq:

Content-Type:
Content-length:

v=
o=
s=
c=
b=
t=
m=
m=
m=
a=
a=
a=
m=
```

Via: P-CSCF removes the Via headers, and generates a locally unique token to identify the saved values. It inserts this as a branch value on its Via header.

27. **200 OK (UE to P-CSCF) – see example in Table 7.4.5.1-27**

UE acknowledges the COMET request (21) with a 200 OK response.

Table 7.4.5.1-27: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

28. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-28**

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.5.1-28: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

From:
To:
Call-ID:
CSeq:
Content-length: 0
```

29. **180 Ringing (UE to P-CSCF) – see example in Table 7.4.5.1-29**

Before proceeding with session establishment, the UE waits for two events. First, the resource reservation initiated in step #11 to 16 must complete successfully. Second, the resource reservation initiated by the originating endpoint must complete successfully (which is indicated by message #26 received by UE). The UE may now immediately accept the session (and proceed with step #35), or alert the destination subscriber of an incoming session attempt; if the latter it indicates this to the calling party by a 180 Ringing provisional response sent to P-CSCF.

Table 7.4.5.1-29: 180 Ringing (UE to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
Require: 100rel
From:
To:
Call-ID:
CSeq:
Contact: sip:[5555::eee:fff:aaa:bbb]
RSeq: 9022
Content-length: 0
```

30. **180 Ringing (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-30**

    P-CSCF forwards the 180 Ringing response to S-CSCF.

Table 7.4.5.1-30: 180 Ringing (P-CSCF to S-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2_1.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.home2.net, sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.home1.net
Require:
From:
To:
Call-ID:
CSeq:
Contact:
RSeq:
Content-length:
```

31. **PRACK (S-CSCF to P-CSCF) – see example in Table 7.4.5.1-31**

    S-CSCF forwards the PRACK request to P-CSCF.

Table 7.4.5.1-31: PRACK (S-CSCF to P-CSCF)

```
PRACK sip:pcscf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Route: sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:

Rack:
Content-length:
```

32. **PRACK (P-CSCF to UE) – see example in Table 7.4.5.1-32**

    P-CSCF forwards the PRACK request to UE.

Table 7.4.5.1-32: PRACK (P-CSCF to UE)

```
PRACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
Cseq:

Rack:
Content-length:
```

Via: P-CSCF removes the Via headers, and generates a locally unique token to identify the saved values. It inserts this as a branch value on its Via header.

33. **200 OK (UE to P-CSCF) – see example in Table 7.4.5.1-33**

UE acknowledges the PRACK request (31) with a 200 OK response.

Table 7.4.5.1-33: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
CSeq:
Content-length: 0
```

34. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-34**

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.5.1-34: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

From:
To:
Call-ID:
CSeq:
Content-length:
```

35. **200 OK (UE to P-CSCF) – see example in Table 7.4.5.1-35**

When the called party answers, the UE sends a 200 OK final response to the INVITE request (6) to P-CSCF, and starts the media flow(s) for this session.

Table 7.4.5.1-35: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
CSeq: 127 INVITE
Contact: sip:[5555::eee:fff:aaa:bbb]
Content-length: 0
```

36. **200 OK (P-CSCF to S-CSCF) – see example in Table 7.4.5.1-36**

P-CSCF indicates the resources reserved for this session should now be committed, and sends the 200 OK final response to S-CSCF.

Table 7.4.5.1-37: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP icscf2.home2.net, SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip:pcscf2.home2.net, sip:scscf2.home2.net, sip:scscf1.home1.net, sip:pcscf1.home1.net
From:
To:
Call-ID:
CSeq:
Contact:
Content-length:
```

37. **ACK (S-CSCF to P-CSCF) – see example in Table 7.4.5.1-37**

S-CSCF forwards the ACK request to P-CSCF.

Table 7.4.5.1-37: ACK (S-CSCF to P-CSCF)

```
ACK sip:pcscf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]

Route: sip:[5555::eee:fff:aaa:bbb]
From:
To:
Call-ID:
Cseq:

Content-length:
```

38. **ACK (P-CSCF to UE) – see example in Table 7.4.5.1-38**

    P-CSCF forwards the ACK request to UE.

Table 7.4.5.1-38: ACK (P-CSCF to UE)

```
ACK sip:[5555::eee:fff:aaa:bbb] SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net;branch=token1
From:
To:
Call-ID:
Cseq:

Content-length:
```

Via: P-CSCF removes the Via headers, and generates a locally unique token to identify the saved values. It inserts this as a branch value on its Via header.

3GPP TSG-CN1 Meeting #19bis ***Tdoc N1-011430***
Sophia Antipolis, France, 2.- 4. October 2001

Title: **Liaison Statement on Usage of Private ID**
Source: **CN1**
To: **CN4, SA1, SA2, SA3, SA5**
Cc: **-**

Contact Person:
Name: Miguel A. Garcia
E-mail Address: Miguel.A.Garcia@ericsson.com

Attachments: **N1-011355**

---

1. Overall Description:

Currently CN1 assumes that the private user ID is carried in the From header value of the SIP REGISTER message. This assumption is based on the syntax of a third party registration according to the draft-ietf-sip-rfc2543bis-04 draft. While true third party registration is precluded from release 5, it may be desirable to obtain such a capability in future releases. It is not yet clear whether the above usage would preclude future third party registration.

CN1 has received the attached contribution N1-011355 which proposes that the private user ID is instead of the From: header transported in the user ID field of an authentication protocol within the Authentication header. This can be viewed as moving the private user ID from a mandatory field available in the Initial message from the UE (Register) and to another (optional) field which may not always be visible at intermediate SIP nodes (e.g. P-CSCF). From the SIP protocol perspective, 3GPP mandates information elements that are optional in SIP, but this is already applied to other information elements. However, 3GPP can not mandate the behaviour of non-3GPP SIP clients. The motivation is:

1. To allow the possibility of 3rd Party Registration. This allows a different entity or user in the network to perform SIP Registration on behalf of another user. A typical example of third party registration is when a secretary registers his boss to the network. The working assumption solution adopted for Release 5 is aligned with the standard SIP behaviour for SIP third party registrations and uses the From field to contain the private identity to identify the user performing the SIP registration. In first party registrations the To: and From: headers should contain the same identity (i.e. identify the same user). In third party registrations the To: and From field contain different identities.
2. To provide an access to IMS from non-3GPP networks, Private Identity needs to be provided to the 3GPP network (P-CSCF, S-CSCF). The current IMS SIP third party registration mechanism may create complications in enabling standard off-the-shelf SIP clients to register with the IMS using the same registration procedures as in Rel 5, as non-3GPP SIP clients normally perform first party registration and may not be configurable to perform third party registrations.
3. In the case of a decomposed TE/MT scenario, the current IMS registration mechanism may create complications for a standard SIP User Agent running in the TE to register to the network, as non-3GPP SIP User Agents are not aware of Private Identity and perform first party registrations and may not be configurable to perform third party registrations.

During the discussion of the attached contribution, the Stage 2 TS 23.228 description on Private Identity was considered and some questions were raised regarding the standardization impacts on other working groups and on service requirements for SIP 3rd Party Registrations, use of the Private Identity in charging records and any security aspects.

2. Actions:

To SA1:

1. To clarify if there is a need to support third party SIP registration for IMS i.e. to allow SIP Registration other than the subscriber. CN1 believes that this capability is not needed for Release 5.

2. CN1 will be interested to know if the 3rd party registration requirement will be required in subsequent releases.

To SA2:

It is believed that IMS stage 2 TS23.228 implies that that 3rd party registration not required.

1. To confirm that the 3rd Party SIP Registration capability is not required for Release 5.
2. CN1 will be interested to know if the 3rd party registration requirement will be required in subsequent releases
3. To identify what other usages of the private user identity exist outside those mentioned in stage 2.
4. To identify which entities require access to the private user identity in order to carry out these functions. In particular, does the functionality of the P-CSCF depend on knowledge of the private user identity.

To SA3:

1. To verify whether it is acceptable to transport the private user identifier in the optional (from the SIP perspective) Authentication header value of the REGISTER message instead of the mandatory (from the SIP perspective) From header value. This will effectively mandate the Authorization header in 3GPP-IMS UEs.
2. Does SA3 foresee any additional security issues with the proposed approach?
3. To respond regarding whether there is an impact to the date when the specification/documentation containing the Authentication Protocol and header details including the transport of the Private User ID would be available for Rel 5 if the approach contained in N1-011355 was adopted by CN1.

To SA2/SA5:

1. The P-CSCF may use the Private Identity for charging and it this is included in the CDR generated by P-CSCF. Currently the P-CSCF has access to the private identity carried in the FROM field. To confirm that the Private Identity should be available at the P-CSCF

2. To verify whether the attached contribution contradicts any charging assumptions.

To CN4:

1. To verify whether it is acceptable to transport the private user identifier in the Authentication header value of the REGISTER message instead of the From header value.
2. To confirm that Private Identity is required to be available in the S-SCSF before the UE has been authenticated.

3. Date of Next CN1 Meetings:

CN1_20	15th - 19th October 2001	Brighton, UK
CN1_20bis	13th – 15th November 2001	Seattle, US

3GPP TSG-CN1 Meeting #19bis ***Tdoc N1-011355***
Sophia Antipolis, France, 2.- 4. October 2001

Source: Ericsson

Title: Usage of the Private ID in registration scenarios

Agenda item: 8.4 IMS registration

Document for: APPROVAL

Introduction

The current flows in 24.228 v1.4.0 shows the registration procedure in sections 6 and 16. The use of the public and private user IDs constitute a third party registration, even when the case is a first party registration.

Ericsson demonstrates in this contribution thatthere is no reason to do third party registrations for first party ones.

Discussion

The current flows in 24.228 v1.4.0 shows the registration procedures in sections 6 and 16. When a user wants to register a public ID, the SIP User Agent populates the From: header with the private user ID, and the To: header with the public user ID. This effectively, from the SIP point of view, constitutes a third party registration.

Third party registrations in SIP are defined as those which a third party entity registers a user on his/her behalf. In the call flows in sections 6 and 16 in 24.228, all the registrations are third party ones. A regular SIP registrar will consider that the private user ID is trying to register another user: the public user ID.

Third party registrations, as 24.228 shows, have the following problems:

1. It is not aligned with the standard SIP behaviour for first party registrations. In first party registrations the To: and From: headers should be the same identity.

2. As the IMS is an access independent network, access must be granted from non 3GPP access networks. The third party registration mechanism precludes standard off-the-shelf SIP clients to register the IMS, as regular SIP clients perform first party registration and cannot be configured to perform third party registrations.

3. In the case of a decomposed TE/MT scenario, it prevents also a standard client running in the TE to register to the network, as regular SIP clients perform first party registrations and cannot be configured to perform third party registrations

TS 23.228 v5.1.0 states in section 4.3.3.1, the following, regarding the private user identity:

Every IM CN subsystem subscriber shall have a private user identity. The private identity is assigned by the home network operator, and used, for example, for Registration, Authorisation, Administration, and Accounting purposes. This identity shall take the form of a Network Access Identifier (NAI) as defined in RFC 2486 [14]. It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

- *The Private User Identity is not used for routing of SIP messages.*

- *The Private User Identity shall be contained in all Registration requests, (including Re-registration and De-registration requests) passed from the UE to the home network.*

- *The Private User Identity shall be securely stored on the USIM (it shall not be possible for the UE to modify the Private User Identity)*

- *The Private User Identity is a unique global identity defined by the Home Network Operator, which may be used within the home network to uniquely identify the user from a network perspective.*
- *The Private User Identity shall be permanently allocated to a user (it is not a dynamic identity), and is valid for the duration of the user's subscription with the home network.*
- *The Private User Identity is used to identify the user's information (for example authentication information) stored within the HSS (for use for example during Registration).*
- *The Private User Identity may be present in charging records based on operator policies.*
- *The Private User Identity identifies the subscription (e.g. IM service capability) not the user.*
- *The Private User Identity is authenticated only during registration of the subscriber, (including re-registration and de-registration).*
- *The HSS and S-CSCF need to obtain and store the Private User Identity.*

An analysis of 24.228 has revealed that the private ID is only used at registration time for purpose of authenticating the user. There is no substantial reason to transport the private user ID in the From header. It seems more natural that the private user ID, which is used to authenticate the user, is conveyed in an authentication header.

SIP already has developped the *Authorization* header. The main purpose of the *Authorization* value field is, according to rfc2543bis [4], to convey the credentials containing the authentication information of the user agent for the realm of the resource being requested. Therefore, it seems natural, to place the private user ID in the Authorization header.

TS 24.228 v1.4.0 does not show any authentication examples at the moment. However, the current assumption in S3 is to use the Extensible Authentication Protocol [1] as the authentication protocol within SIP. The EAP packet includes a user ID field, that in the case of 3GPP, should carry the private user ID. The EAP packet is base64 encoded and included in an Authorization header. An example of an EAP packet included in the Authentication header of SIP looks like:

```
Authorization: eap eap-p=AQAAEwFqYXJpQGFya2tvLmNvbQ==
```

The base64 string above encodes an EAP packet which includes a private user ID in the user ID field.

The current proposal of carrying the private user ID in the user ID field of the authentication protocol does not depend on the actual authentication protocol. The proposed changes are in line with the current assumption in S3 that EAP [1] is the protocol used to authenticate users. EAP may be used in HTTP and SIP, as defined in [2] and can reuse the existing AKA mechanisms, as described in [3]. Typically all authentication protocols contain a field to supply the user ID, independent of the actual protocol. In the case of SIP, this is also true when the authentication mechanism is HTTP Basic or HTTP Digest.

Proposal

Ericsson proposes to align the registration with standard SIP procedures according to the following principles:

1. The From: header is populated with the public user ID, the same one that is in the To: header
2. The private user ID is conveyed in the user ID field of the authentication protocol (independently of the actual authentication protocol). The authentication protocol s carried in SIP in the Authentication header.

Note that the proposed solution meets the requirement to carry the private user ID at registration time and does not depend on the actual authentication protocol.

********** FIRST PROPOSED CHANGE **********

6 Signalling flows for REGISTER (non hiding)

6.1 Introduction

6.2 Registration signalling: user not registered

Figure 6.2-1 shows the registration signalling flow for the scenario when the user is not registered. For the purpose of this registration signalling flow, the subscriber is considered to be roaming. In this signalling flow, the home network does not have network configuration hiding active.

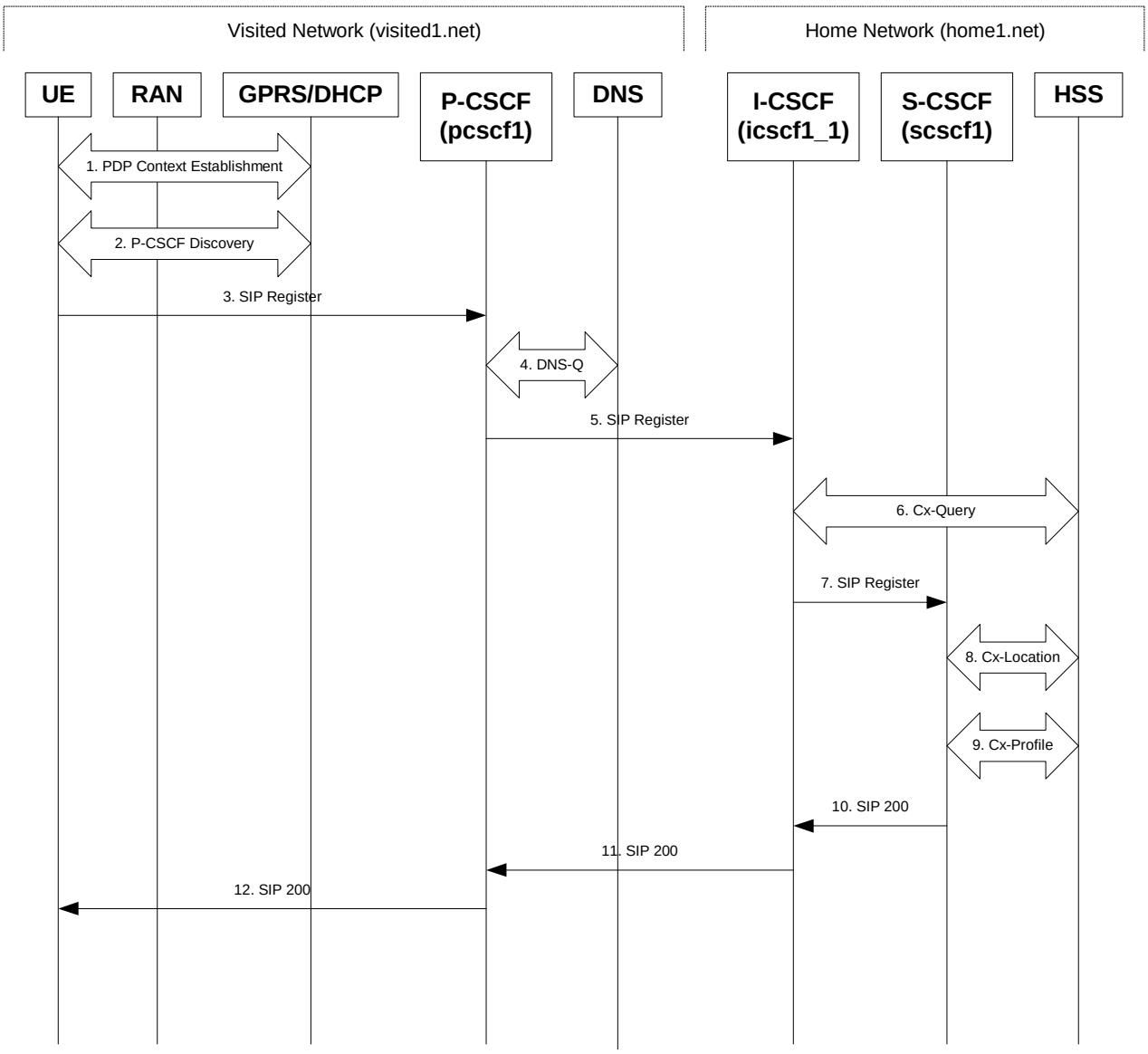


Figure 6.2-1: Registration signalling: user not registered

1. **GPRS Attach / PDP Context Establishment (UE to GPRS)**

   This signalling flow is shown to indicate the GPRS Attach and PDP Context Activation procedures that must be completed prior to application registration. When complete, the UE will have acquired an IP address (provided by the GGSN) which serves as the host address for the duration of the PDP context.

2. **CSCF Discovery (UE to GPRS/ DHCP)**

This signalling flow is the procedure to discover the Proxy CSCF in the visited IM CN subsystem.

The UE should be able to obtain the IP address of the P-CSCF during the PDP Context Activation procedure. At the PDP Context Activation time, the IP address of the P-CSCF shall be conveyed to the UE in the Activate PDP Context Accept message. The UEs that do not support DHCP shall use this P-CSCF discovery procedure.

Additionally, the UEs that incorporate the DNS and DHCP client software that supports DHCP extensions (specified in draft-ietf-sip-dhcp-03.txt) may employ the DHCP mechanism to discover the P-CSCF in the visited IM CN subsystem. When allocating an IP address to the UE, the DHCP server may provide the UE with the fully-qualified domain name (FQDN) of the P-CSCF and the address of the DNS server in the visited IM CN subsystem. Subsequently, the DNS client in the UE will utilise the provided FQDN and perform an address-record lookup (i.e. type A DNS access) to obtain the IP address of the P-CSCF in the visited IM CN subsystem.

NOTE: A UE may be roaming within the home network.

Editor's Note: IANA Considerations - Currently the IANA has not assigned an "DHCP option number" for the *SIP Servers DHCP Option* defined in the draft-ietf-sip-dhcp-03.txt. Therefore, the DHCP alternative can not be currently implemented.
[19 Jul. 2001]
This draft is currently with the IESG and approval is expected. It is therefore reasonable to expect publication by year end. It is also standards track so normative references could be made. It is also reasonable to expect the necessary IANA registration to occur in that timeframe.

Editor's Note: Second approach needs further study on the interactions with the restrictions on the Signalling PDP Context, TS 23.228 subclause 4.2.6.

3. **SIP REGISTER request (UE to P-CSCF) – see example in Table 6.2-3**

The purpose of this request is to register the user's SIP URI with a S-CSCF in the home network. This request is routed to the P-CSCF because it is the only SIP server known to the UE. In the following SIP request, the Contact field contains the user's host address.

The P-CSCF will perform two actions, binding and forwarding. The binding is between the User's SIP address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which was acquired during PDP context activation process.

Table 6.2-3 SIP REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <Sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 1 REGISTER
Expires: 7200
Content-Length: 0
```

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routeing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Via: IPv6 PDP address of the SIP session allocated during the PDP Context Activation process.

From: This indicates the SIP public identity of the user ~~(stored in the USIM)~~ originating the REGISTER request. The public identity of the user may be obtained from the USIM. ~~In SIP, this can be a third-party.~~

~~Editor's note: One proposal is: "This is a natural place for the private user identity or NAI for the subscriber. Forming a SIP URL from the NAI is a simple matter of prepending "sip:". For example, if the subscriber's NAI is 19725835472@operator.com, then the From: header would be sip:19725835472@operator.com." Alternatively it could be the SIP-URL of the party registering.~~

To: This indicates the SIP public identity of the user ~~identifier~~ being registered. This is the identity by which other parties know this subscriber. It ~~is~~ may be obtained from the USIM.

~~Editor's note: One proposed additional text: "In this case, this is the public user identity for the subscriber."~~

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary point of contact for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF.

Editor's note: It is for further study whether this information is stored in the HSS and the S-CSCF for the subscriber in order to support multiple registrations.

Call Id: Call Identifier for this Registration generated as per [3]

Authorization: It carries authentication information. The private user ID is carried in the user ID field of the authenticaion protocol.

Cseq: Cseq for this Registration generated as per [3]

Upon receiving this request the P-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

4. **DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

The P-CSCF sends the REGISTRATION request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTRATION request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTRATION request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 6.2-4a DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=_sip.udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

The DNS records are retrieved according to RFC2782 [4].

Table 6.2-4b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=_sip.udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net           0 IN SRV 1 10 5060 icscf1_1.home1.net
                                        0 IN SRV 1  0 5060 icscf7_1.home1.net

icscf1_1.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_1.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC2782 [4] is used to select the I-CSCF (i.e., the icscf1_1.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e., 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTRATION request to this IP address (i.e., 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

5. **SIP REGISTER request (P-CSCF to I-CSCF) – see example in Table 6.2-5**

Since this P-CSCF is a stateful proxy, it is required to be in the path for all Mobile Originated and Mobile Terminated requests for this user. To ensure this, the P-CSCF has to put itself into the path for future requests. One solution of achieving this is to have the P-CSCF as the contact point for this user at the home registrar.

To do this the P-CSCF creates a temporary SIP URI for the user called user1%40home1.net@pcscf1.visited1.net. As part of its internal registration procedure the P-CSCF binds the temporary SIP URI to the user's SIP URI which was also bound to the IP address of the UE as shown in signalling flow 3. The P-CSCF then forwards the REGISTER request for user1_public1@home1.net, to the home registrar, using a contact address of user1_public1%40home1.net@pcscf1.visited1.net.

This signalling flow shows the SIP REGISTER being forward from the P-CSCF to the I-CSCF in the home domain.

Table 6.2-5 SIP REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From:
To:
Contact: <sip:user1_public1%40home1.net@pcscf1.visited1.net>
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require, Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

6. **Cx-Query**

   The I-CSCF requests information related to the required S-CSCF capabilities from the HSS. The HSS provides the I-CSCF with either the S-CSCF address for the subscriber (if the subscriber is currently registered) or the S-CSCF required capabilities (if the subscriber is not currently registered.) Since the subscriber is not registered in this case, the HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

7. **SIP REGISTER request (I-CSCF to S-CSCF) – see example in Table 6.2-7**

   I-CSCF does not modify the Path header.

   This signalling flow forwards the SIP REGISTER from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 6.2-7 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

Upon receiving this request the S-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

8. **Cx-Location**

   The S-CSCF shall send its location information to the HSS. The HSS stores the S-CSCF name for that subscriber. The HSS sends a response to the S-CSCF to acknowledge the sending of location information.

9. **Cx-Profile**

   The S-CSCF shall send the subscriber's identity to the HSS in order to be able to download the subscriber profile to the S-CSCF. The HSS returns the subscriber's profile to the S-CSCF. The S-CSCF shall store the subscriber profile for that indicated user.

10. **SIP 200 OK response (S-CSCF to I-CSCF) – see example in Table 6.2-10**

    The S-CSCF sends acknowledgment to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.2-10 SIP 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:pcscf1.visited1.net>
From:
To: <sip:user1_public1@home1.net>;tag=7899
Call-ID:
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires:
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

11. **SIP 200 OK response (I-CSCF to P-CSCF) – see example in Table 6.2-11**

    The I-CSCF forwards acknowledgment from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.2-11 SIP 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

12. **SIP 200 OK response (P-CSCF to UE) – see example in Table 6.2-12**

    The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgment from the I-CSCF to the UE indicating that Registration was successful.

Table 6.2-12 SIP 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

********** NEXT PROPOSED CHANGE **********

6.3 Registration signalling: re-registration – user currently registered

For the purpose of the re-registration signalling flow shown in figure 6.3-1, the subscriber is considered to be roaming. In this signalling flow, the home network does not have network configuration hiding active.

This signalling flow assumes:

1. That the same PDP Context allocated during the initial registration scenario is still used for re-registration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 is completed first.

Editor's Note: If the same PDP-Context is not available, is it guaranteed that the UE will get back the same IP address at this point? If this is not possible, would there be a problem with the binding in the P-CSCF (user_public1@home1.net and [5555::aaa:bbb:ccc:ddd])?

2. The DHCP procedure employed for P-CSCF discovery is not needed.

3. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

Periodic application level re-registration is initiated by the UE either in response to the expiration of the existing registration information or in response to a change in the registration status of the UE. Re-registration follows the same path as described in subclause 16.2.

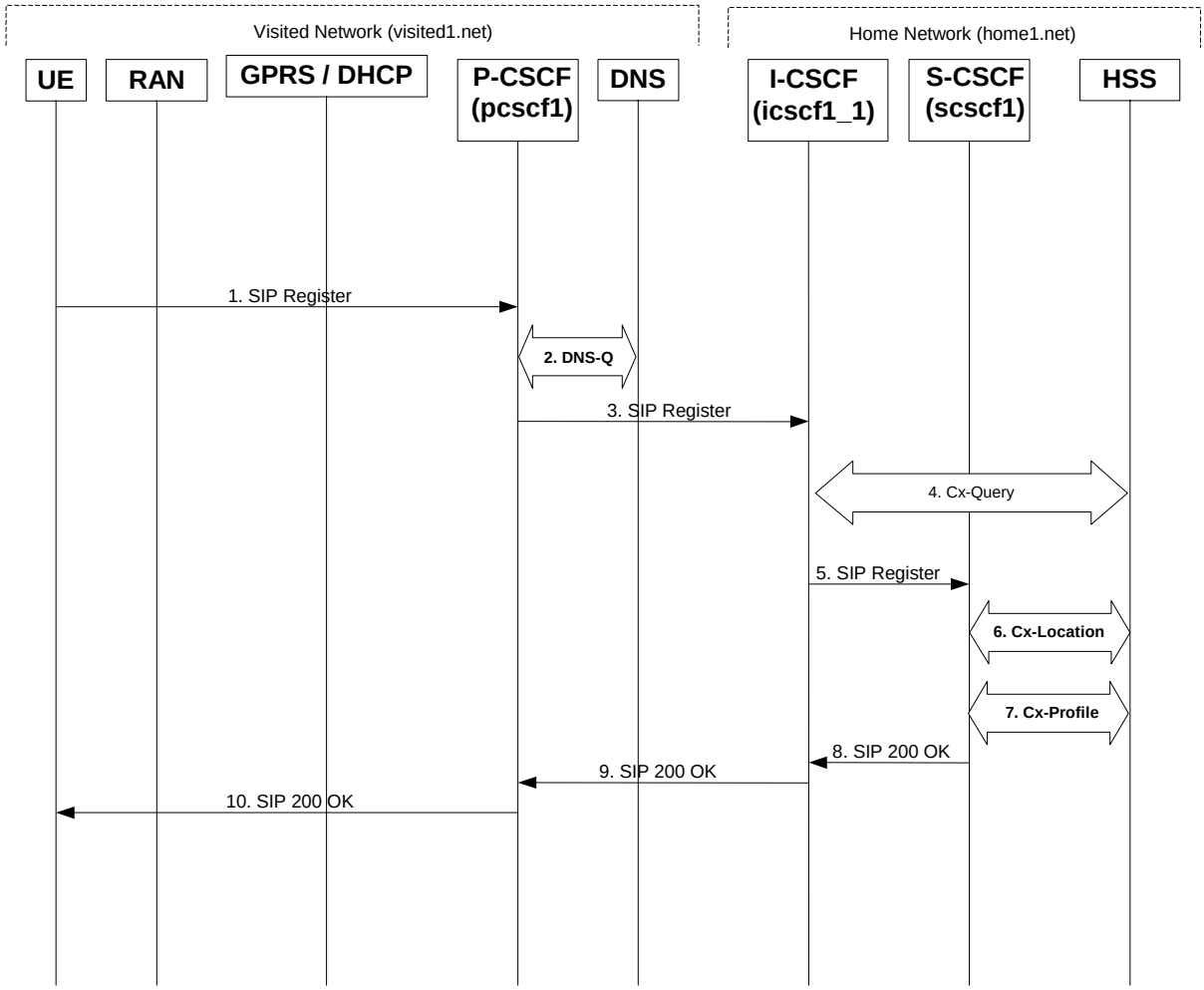


Figure 6.3-1: Re-registration when UE roaming

1. **SIP REGISTER request (UE to P-CSCF) – see example in Table 6.3-1**

   The registration expires in the UE. The UE re-registers by sending a new REGISTER request. This request is sent to the same P-CSCF with which the UE initially registered. The P-CSCF maintains the same binding between the User's SIP public address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which it established during the original registration.

Table 6.3-1 SIP REGISTER (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: ~~<sip:user_private@home1.net>~~ <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 7 REGISTER
Expires: 7200
Content-Length: 0
```

The header field usage is the same as for the initial registration scenario:

From: This indicates the ~~private~~ SIP public identity of the user ~~(stored in the USIM)~~ originating the REGISTER request. The public identity of the user may be obtained from the USIM.

To: This indicates ~~the target of the REGISTER request~~SIP public identity of the user being registered. ~~The target is the public identity that is being registered.~~ This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF.

Editor's note: It is for further study whether this information is stored in the HSS and the S-CSCF for the subscriber in order to support multiple registrations.

Authorization: It carries authentication information. The private user ID is carried in the user ID field of the authentication protocol.

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routeing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Upon receiving this request the P-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

2. **DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI. The DNS provides the P-CSCF with an address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

3. **SIP REGISTER request (P-CSCF to I-CSCF) – see example in Table 6.3-3**

This signalling flow shows the SIP Register request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 6.3-3 SIP REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require, Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

4. **Cx-Query**

The I-CSCF requests information related to the required S-CSCF capabilities from the HSS. The HSS shall determine that the user is currently registered, and send an indication of current S-CSCF to the I-CSCF. Hence, the S-CSCF selection procedure is not needed.

5. **SIP REGISTER request (I-CSCF to S-CSCF) – see example in Table 6.3-5**

This signalling flow forwards the SIP REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 6.3-5 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip: pcscf1.visited1.net>
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

Upon receiving this request the S-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

6. **Cx-Location**

   The S-CSCF shall send its location information to the HSS. The HSS stores the S-CSCF name for that subscriber. The HSS sends a response to the S-CSCF to acknowledge the sending of location information.

   If the S-CSCF can detect that this is a reregistration, then this flow need not be performed, and the currently saved information is used instead.

7. **Cx-Profile**

   The S-CSCF shall send the subscriber's identity to the HSS in order to be able to download the subscriber profile to the S-CSCF. The HSS returns the subscriber's profile to the S-CSCF. The S-CSCF shall store the subscriber profile for that indicated user.

   If the S-CSCF can detect that this is a reregistration, then this flow need not be performed, and the currently saved information is used instead.

8. **SIP 200 OK response (S-CSCF to I-CSCF) – see example in Table 6.3-8**

   The S-CSCF sends acknowledgment to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.3-8 SIP 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip: scscf1.home1.net>, <sip: pcscf1.visited1.net>
From:
To: <sip:user1_public1@home1.net>;tag=7899
Call-ID:
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires:
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

9. **SIP 200 OK response (I-CSCF to P-CSCF) – see example in Table 6.3-9**

   The I-CSCF forwards acknowledgment from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.3-9 SIP 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net, <sip: pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

10. **SIP 200 OK response (P-CSCF to UE) – see example in Table 6.3-10**

    The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgment from the I-CSCF to the UE indicating that Registration was successful.

Table 6.3-10 SIP 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

********** NEXT PROPOSED CHANGE **********

6.8 Registration error conditions.

6.8.1 Re-registration – failure of re-registration

This signalling flow (see figure 6.8.1-1) is a continuation of the signalling flow in subsubclause 16.3 “Registration Signalling: Re-Registration – User Currently Registered” after reception of signalling flow 4. This signalling flow shows the recovery after a failure of the S-CSCF that had been assigned to the subscriber in a previous registration.

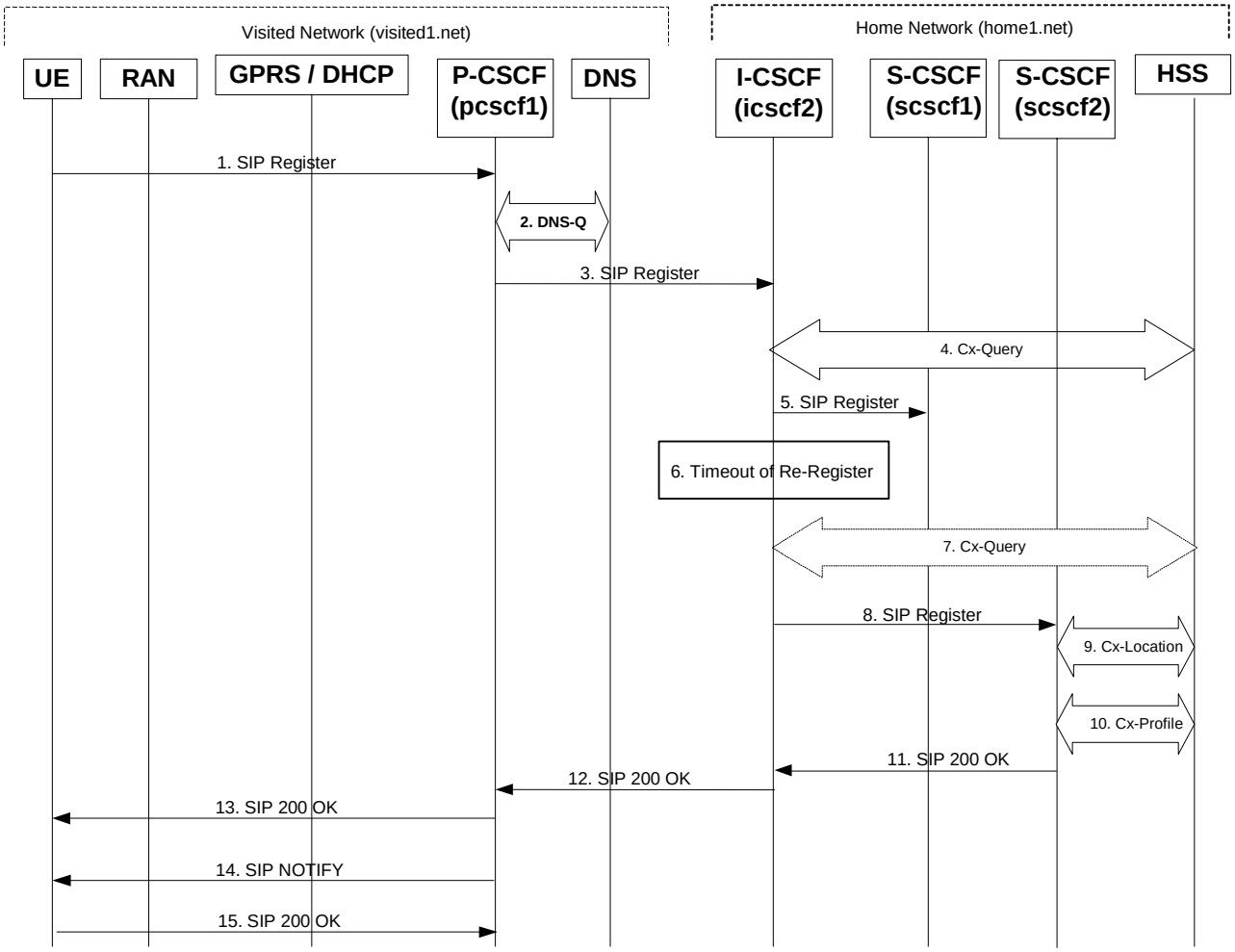


Figure 6.8.1-1: Failure of previous S-CSCF during re-registration

Steps 1 through 4 are the same as the signalling flow in subclause 16.3.

5 **SIP REGISTER (I-CSCF to S-CSCF) – see example in Table 6.8.1-5**

This signalling flow forwards the SIP REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

I-CSCF adds a proper I-CSCF name to the Path header.

Table 6.8.1-5 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From: <sip:user1_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:user1%40home1.net@pcscf.visited1.net>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 10 REGISTER
Expires: 7200
Content-Length: 0
```

6 **Timeout of Re-Register**

The I-CSCF times out, waiting for the response from the S-CSCF.

Editor's Note: The value of the timer in this particular instance is FFS. Clearly the value of the timers in the P-CSCF and UE waiting for the response must be considered when choosing this value.

7 **Cx-Query (Optional)**

The I-CSCF informs the HSS that the S-CSCF for the subscriber is unreachable and requests information related to the required S-CSCF capabilities from the HSS, The HSS sends the capability information required for S-CSCF selection. The I-CSCF uses this information to select a suitable S-CSCF.

This step is optional. Depending on implementation, sufficient information may be available to the I-CSCF from Step 4, to allow the I-CSCF select an alternate S-CSCF. Alternative mechanisms (for example a CSCF management plane) would be used to enable the HSS learn of S-CSCF failure. In addition, the HSS will learn about the assignment of a new S-CSCF in Step 9.

8 **SIP REGISTER (I-CSCF to S-CSCF) – see example in Table 6.8.1-8**

This signalling flow forwards the SIP REGISTER request from the I-CSCF to the newly selected S-CSCF. The Request-URI is changed to the address of the new S-CSCF.

Table 6.8.1-8 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf2.home1.net SIP/2.0
Via:
Via:
Via:
Path:
Path:
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

The remaining steps (9-15) are the same as in the normal re-registration case (steps 6-12 in subclause 16.3)

********** NEXT PROPOSED CHANGE **********

16 Signalling flows for REGISTER (hiding)

16.1 Introduction (see 6.1)

16.2 Registration signalling: user not registered

Figure 16.2-1 shows the registration signalling flow for the scenario when the user is not registered. For the purpose of this signalling flow, the subscriber is considered to be roaming. In this signalling flow, the home network has network configuration hiding active.

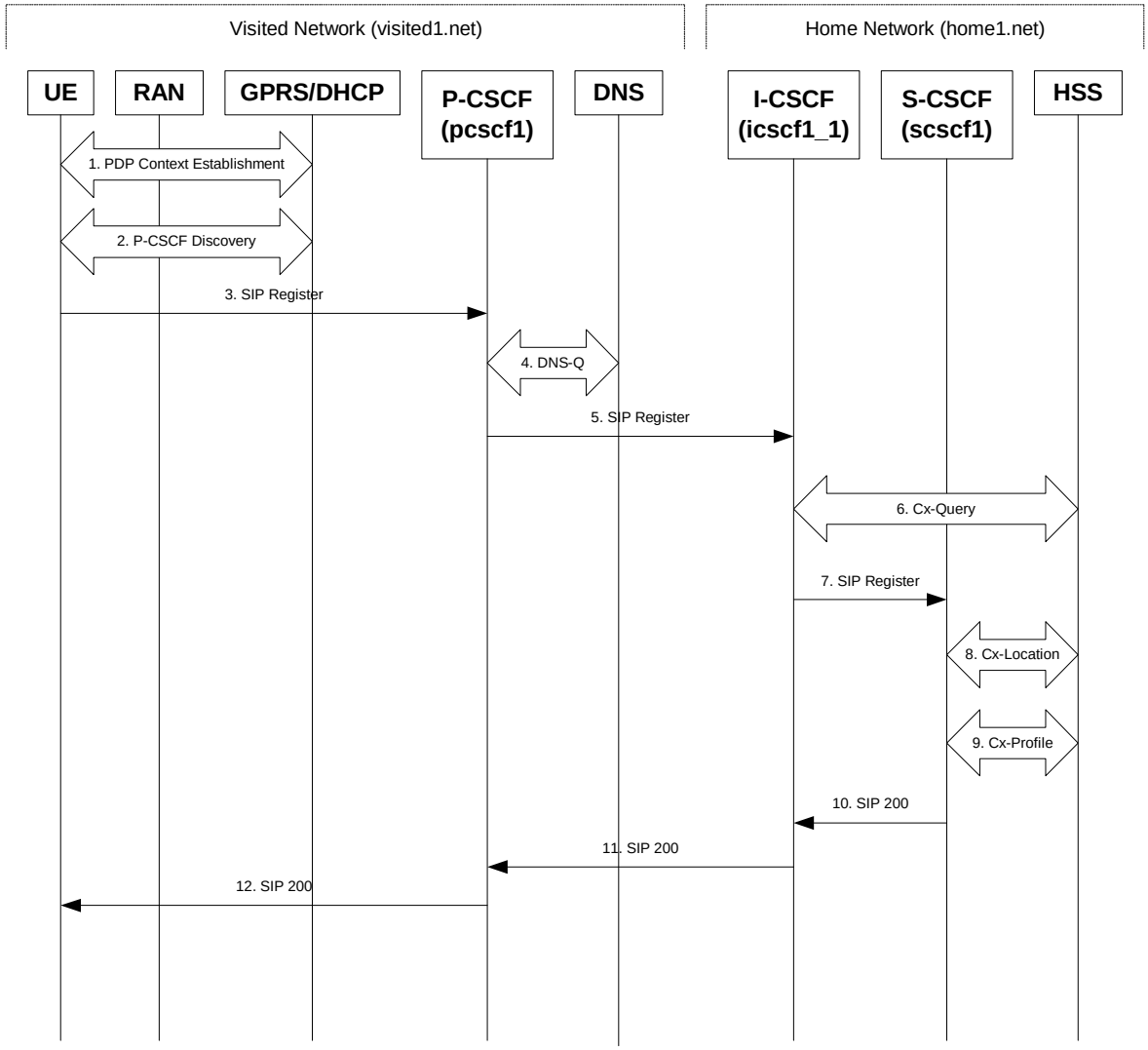


Figure 16.2-1: Registration when UE roaming

1. **GPRS Attach / PDP Context Establishment (UE to GPRS)**

   This signalling flow is shown to indicate the GPRS Attach and PDP Context Activation procedures that must be completed prior to application registration. When complete, the UE will have acquired an IP address (provided by the GGSN) which serves as the host address for the duration of the PDP context.

2. P-**CSCF Discovery (UE to GPRS/ DHCP)**

   This signalling flow is the procedure to discover the Proxy CSCF in the visited IM CN subsystem.

   The UE should be able to obtain the IP address of the P-CSCF during the PDP Context Activation procedure. At the PDP Context Activation time, the IP address of the P-CSCF shall be conveyed to the UE in the Activate PDP Context Accept message. The UEs that do not support DHCP shall use this P-CSCF discovery procedure.

   Additionally, the UEs that incorporate the DNS and DHCP client software that supports DHCP extensions (specified in draft-ietf-sip-dhcp-03.txt) may employ the DHCP mechanism to discover the P-CSCF in the visited IM CN subsystem. When allocating an IP address to the UE, the DHCP server may provide the UE with the fully-qualified domain name (FQDN) of the P-CSCF and the address of the DNS server in the visited IM CN subsystem. Subsequently, the DNS client in the UE will utilise the provided FQDN and perform an address-record lookup (i.e. type A DNS access) to obtain the IP address of the P-CSCF in the visited IM CN subsystem.

   NOTE: A UE may be roaming within the home network.

Editor's Note: IANA Considerations - Currently the IANA has not assigned an "DHCP option number" for the *SIP Servers DHCP Option* defined in the draft-ietf-sip-dhcp-03.txt. Therefore, the DHCP alternative can not be currently implemented.
[19 Jul. 2001]
This draft is currently with the IESG and approval is expected. It is therefore reasonable to expect publication by year end. It is also standards track so normative references could be made. It is also reasonable to expect the necessary IANA registration to occur in that timeframe.

Editor's Note: Second approach needs further study on the interactions with the restrictions on the Signalling PDP Context, TS 23.228 subclause 4.2.6.

3. **SIP REGISTER request (UE to P-CSCF) – see example in Table 16.2-3**

The purpose of this request is to register the user's SIP URI with a S-CSCF in the home network. This request is routed to the P-CSCF because it is the only SIP server known to the UE. In the following SIP request, the Contact field contains the user's host address.

The P-CSCF will perform two actions, binding and forwarding. The binding is between the User's SIP address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which was acquired during PDP context activation process.

Table 16.2-3 SIP REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <Sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 1 REGISTER
Expires: 7200
Content-Length: 0
```

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routeing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Via: IPv6 PDP address of the SIP session allocated during the PDP Context Activation process.

From: This indicates the SIP public identity of the user ~~(stored in the USIM)~~ originating the REGISTER request. The public identity of the user may be obtained from the USIM .~~In SIP, this can be a third-party.~~

~~Editor's note: One proposal is: "This is a natural place for the private user identity or NAI for the subscriber. Forming a SIP URL from the NAI is a simple matter of prepending "sip:". For example, if the subscriber's NAI is 19725835472@operator.com, then the From: header would be sip:19725835472@operator.com." Alternatively it could be the SIP-URL of the party registering.~~

To: This indicates the SIP public identity of the user ~~identifier~~ being registered. This is the identity by which other parties know this subscriber. It ~~is~~ may be obtained from the USIM.

Editor's note: One proposed additional text: "In this case, this is the public user identity for the subscriber."

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary point of contact for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF.

Editor's note: It is for further study whether this information is stored in the HSS and the S-CSCF for the subscriber in order to support multiple registrations.

Call Id: Call Identifier for this Registration generated as per [3]

Authorization: It carries authentication information. The private user ID is carried in the user ID field of the authentication protocol.

Cseq: Cseq for this Registration generated as per [3]

Upon receiving this request the P-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

4. **DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

The P-CSCF sends the REGISTRATION request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTRATION request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTRATION request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 16.2-4a DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=_sip.udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

The DNS records are retrieved according to RFC2782 [4].

Table 16.2-4b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=_sip.udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net           0 IN SRV 1 10 5060 icscf1_1.home1.com
                                        0 IN SRV 1  0 5060 icscf7_1.home1.com

icscf1_1.home1.net                      0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_1.home1.net                      0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC2782 [4] is used to select the I-CSCF (i.e. the icscf1_1.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e., 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTRATION request to this IP address (i.e., 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

5. **SIP REGISTER request (P-CSCF to I-CSCF) – see example in Table 16.2-5**

Since this P-CSCF is a stateful proxy, it is required to be in the path for all Mobile Originated and Mobile Terminated requests for this user. To ensure this, the P-CSCF has to put itself into the path for future requests. One solution of achieving this is to have the P-CSCF as the contact point for this user at the home registrar.

To do this the P-CSCF creates a temporary SIP URI for the user called user1%40home1.net@pcscf1.visited1.net. As part of its internal registration procedure the P-CSCF binds the temporary SIP URI to the user's SIP URI which was also bound to the IP address of the UE as shown in signalling flow 3. The P-CSCF then forwards the REGISTER request for user1_public1@home1.net, to the home registrar, using a contact address of user1_public1%40home1.net@pcscf1.visited1.net.

This signalling flow shows the SIP REGISTER being forward from the P-CSCF to the I-CSCF in the home domain.

Table 16.2-5 SIP REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From:
To:
Contact: <sip:user1%40home1.net@pcscf1.visited1.net>
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require, Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

6. **Cx-Query**

   The I-CSCF requests information related to the required S-CSCF capabilities from the HSS. The HSS provides the I-CSCF with either the S-CSCF address for the subscriber (if the subscriber is currently registered) or the S-CSCF required capabilities (if the subscriber is not currently registered.) Since the subscriber is not registered in this case, the HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

7. **SIP REGISTER request (I-CSCF to S-CSCF) – see example in Table 16.2-7**

   I-CSCF adds a proper I-CSCF name to the Path header.

   This signalling flow forwards the SIP REGISTER from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 16.2-7 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
       [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

Upon receiving this request the S-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

8. **Cx-Location**

   The S-CSCF shall send its location information to the HSS. The HSS stores the S-CSCF name for that subscriber. The HSS sends a response to the S-CSCF to acknowledge the sending of location information.

9. **Cx-Profile**

The S-CSCF shall send the subscriber's identity to the HSS in order to be able to download the subscriber profile to the S-CSCF. The HSS returns the subscriber's profile to the S-CSCF. The S-CSCF shall store the subscriber profile for that indicated user.

10. **SIP 200 OK response (S-CSCF to I-CSCF) – see example in Table 16.2-10**

The S-CSCF sends acknowledgment to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.2-10 SIP 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires:
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

11. **SIP 200 OK response (I-CSCF to P-CSCF) – see example in Table 16.2-11**

The I-CSCF translates the S-CSCF name in the Path header. The I-CSCF forwards acknowledgment from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.2-11 SIP 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:token(scscf1.home1.net)>, <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

12. **SIP 200 OK response (P-CSCF to UE) – see example in Table 16.2-12**

The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgment from the I-CSCF to the UE indicating that Registration was successful.

Table 16.2-12 SIP 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

********** NEXT PROPOSED CHANGE **********

16.3 Registration signalling: re-registration – user currently registered

For the purpose of the re-registration signalling flow shown in figure 16.3-1, the subscriber is considered to be roaming. In this signalling flow, the home network has network configuration hiding active.

This signalling flow assumes :

1. That the same PDP Context allocated during the initial registration scenario is still used for re-registration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 is completed first.

Editor's Note: If the same PDP-Context is not available, is it guaranteed that the UE will get back the same IP address at this point? If this is not possible, would there be a problem with the binding in the P-CSCF (user_public1@home1.net and [5555::aaa:bbb:ccc:ddd])?2. The DHCP procedure employed for P-CSCF discovery is not needed.

3. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

Periodic application level re-registration is initiated by the UE either in response to the expiration of the existing registration information or in response to a change in the registration status of the UE. Re-registration follows the same path as described in subclause 16.2.

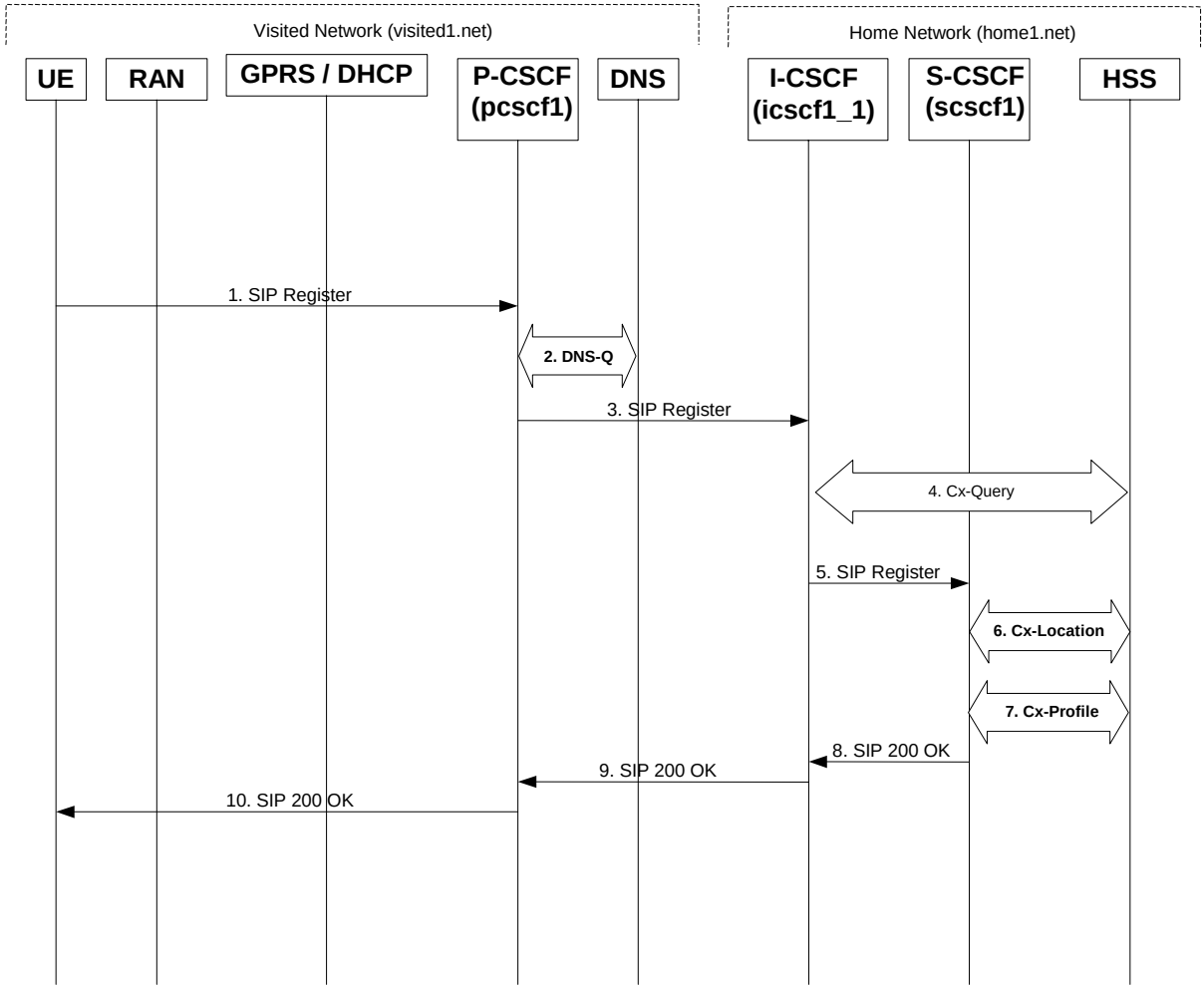


Figure 16.3-1: Re-registration when UE roaming

1. **SIP REGISTER request (UE to P-CSCF) – see example in Table 16.3-1**

The registration expires in the UE. The UE re-registers by sending a new REGISTER request. This request is sent to the same P-CSCF with which the UE initially registered. The P-CSCF maintains the same binding between the User's SIP public address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which it established during the original registration.

Table 16.3-1 SIP REGISTER (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <Sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 7 REGISTER
Expires: 7200
Content-Length: 0
```

The header field usage is the same as for the initial registration scenario:

From: This indicates the ~~private~~ SIP public identity of the user ~~(stored in the USIM)~~ originating the REGISTER request. The public identity of the user may be obtained from the USIM.

To: This indicates ~~the target of the REGISTER request~~ SIP public identity of the user being registered. ~~The target is the public identity that is being registered.~~ This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF.

Editor's note: It is for further study whether this information is stored in the HSS and the S-CSCF for the subscriber in order to support multiple registrations.

Authorization: It carries authentication information. The private user ID is carried in the user ID field of the authentication protocol.

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routeing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Upon receiving this request the P-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

2. **DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI. The DNS provides the P-CSCF with an address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

3. **SIP REGISTER request (P-CSCF to I-CSCF) – see example in Table 16.3-3**

This signalling flow shows the SIP Register request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 16.3-3 SIP REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From:
To:
Contact: <sip:user1%40home1.net@pcscf1.visited1.net>
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require, Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

4. **Cx-Query**

   The I-CSCF requests information related to the required S-CSCF capabilities from the HSS. The HSS shall determine that the user is currently registered, and send an indication of current S-CSCF to the I-CSCF. Hence, the S-CSCF selection procedure is not needed.

5. **SIP REGISTER request (I-CSCF to S-CSCF) – see example in Table 16.3-5**

   This signalling flow forwards the SIP REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

   I-CSCF adds a proper I-CSCF name to the Path header.

Table 16.3-5 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_1.home1.net>, <sip: pcscf1.visited1.net>
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

Upon receiving this request the S-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

6. **Cx-Location**

   The S-CSCF shall send its location information to the HSS. The HSS stores the S-CSCF name for that subscriber. The HSS sends a response to the S-CSCF to acknowledge the sending of location information.

   If the S-CSCF can detect that this is a reregistration, then this flow need not be performed, and the currently saved information is used instead.

7. **Cx-Profile**

The S-CSCF shall send the subscriber's identity to the HSS in order to be able to download the subscriber profile to the S-CSCF. The HSS returns the subscriber's profile to the S-CSCF. The S-CSCF shall store the subscriber profile for that indicated user.

If the S-CSCF can detect that this is a reregistration, then this flow need not be performed, and the currently saved information is used instead.

8. **SIP 200 OK response (S-CSCF to I-CSCF) – see example in Table 16.3-8**

   The S-CSCF sends acknowledgment to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.3-8 SIP 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip: scscf1.home1.net>, <sip: icscf1_1.home1.net>, <sip: pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires:
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

9. **SIP 200 OK response (I-CSCF to P-CSCF) – see example in Table 16.3-9**

   The I-CSCF translates the S-CSCF name in the Path header. The I-CSCF forwards acknowledgment from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.3-9 SIP 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:token(scscf1.home1.net)>, <sip: icscf1_1.home1.net>, <sip: pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

10. **SIP 200 OK response (P-CSCF to UE) – see example in Table 16.3-10**

    The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgment from the I-CSCF to the UE indicating that Registration was successful.

Table 16.3-10 SIP 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

********** NEXT PROPOSED CHANGE **********

16.4 Registration signalling: mobile initiated deregistration

Figure 16.4-1 shows a signalling flow for mobile initiated deregistration. For the purposes of this deregistration signalling flow, the subscriber is considered to be roaming. In this signalling flow, the home network has configuration hiding active.

This signalling flow assumes:

1. That the same PDP Context allocated during the initial registration scenario is still used for deregistration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 must first be completed.

Editor's Note: If the same PDP-Context is not available, is it guaranteed that the UE will get back the same IP address at this point? If this is not possible, would there be a problem with the binding in the P-CSCF (user_public1@home1.net and [5555::aaa:bbb:ccc:ddd])?

2. The procedure employed for P-CSCF discovery is not needed.

3. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

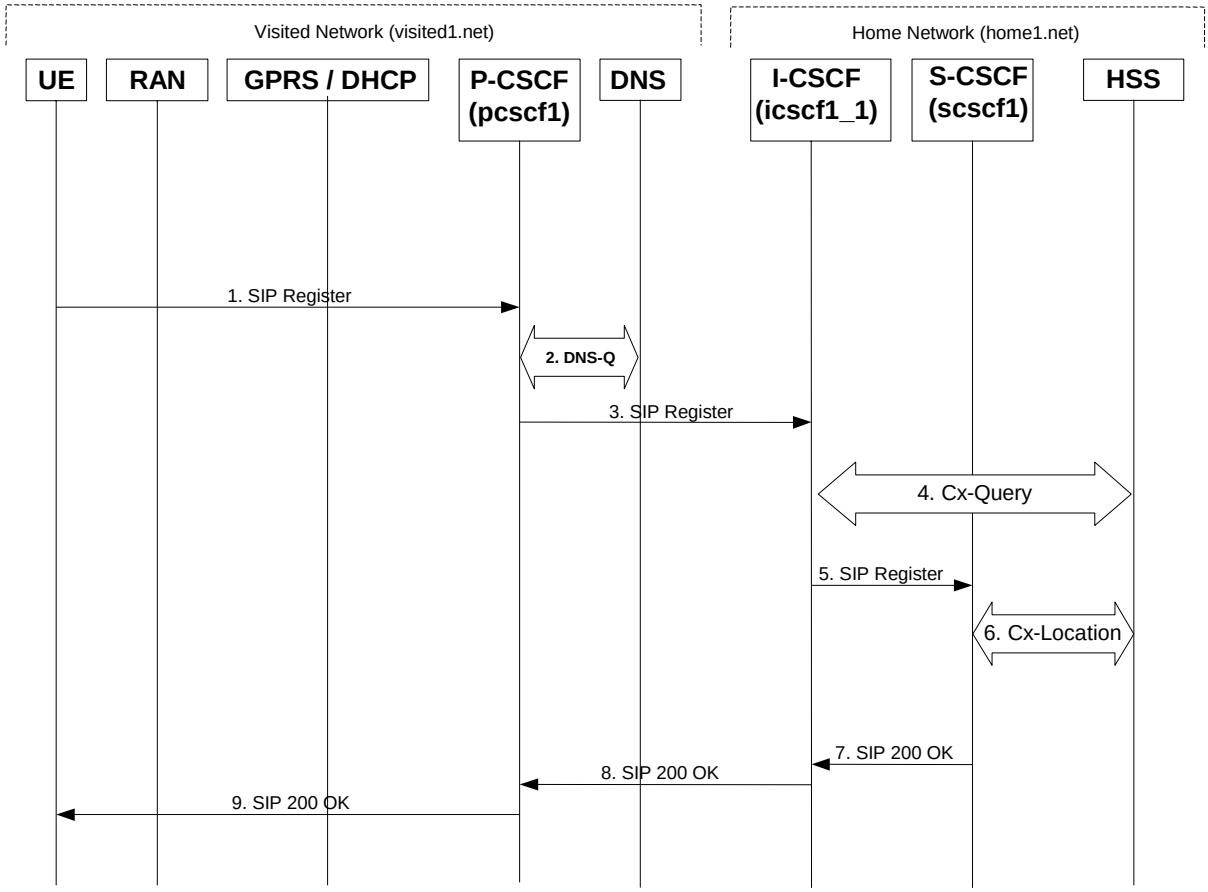


Figure 16.4-1: Registration signalling: mobile initiated deregistration

1. **SIP REGISTER request (UE to P-CSCF) – see example in Table 16.4-1**

   The UE intends to de-register itself. It does so by sending a new REGISTER request. This request looks similar as in re-register case, but the Expires header contains zero. This request is sent to the same P-CSCF with which the UE initially registered.

Table 16.4-1 SIP REGISTER (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <Sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 7 REGISTER
Expires: 0
Content-Length: 0
```

The header field usage is the same as for the initial registration scenario:

From: This indicates the private SIP public identity of the user (stored in the USIM) originating the REGISTER request. The public identity of the user may be obtained from the USIM.

To: This indicates the target of the REGISTER requestSIP public identity of the user. The target is the public identity that is being de-registered. This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being de-registered.

Authorization: It carries authentication information. The private user ID is carried in the user ID field of the authentication protocol.

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Expires: The 0 value indicates the registration is being cancelled.

Upon receiving this request the P-CSCF will reset the SIP registration timer for this UE to 0.

2. **DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI. The DNS provides the P-CSCF with an address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

3. **SIP REGISTER request (P-CSCF to I-CSCF) – see example in Table 16.4-3**

This signalling flow shows the SIP Register request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 16.4-3 SIP REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require, Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

4. **Cx-Query**

   The I-CSCF requests information related to the required S-CSCF capabilities from the HSS. The HSS shall determine that the user is currently registered, and send an indication of current S-CSCF to the I-CSCF. Hence, the S-CSCF selection procedure is not needed.

5. **SIP REGISTER (I-CSCF to S-CSCF) – see example in Table 16.4-5**

   I-CSCF adds a proper I-CSCF name to the Path header.

   This signalling flow forwards the SIP REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 16.4-5 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_1.home1.net> <sip:pcscf1.visited1.net>
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

   Upon receiving this request the S-CSCF will reset the SIP registration timer for this UE to 0.

6. **Cx-Location**

   The S-CSCF shall notify the HSS to clear its location information for that subscriber. The HSS deletes the S-CSCF name for that subscriber. The HSS sends a response to the S-CSCF to acknowledge the clearing of location information.

7. **SIP 200 OK (S-CSCF to I-CSCF) – see example in Table 16.4-7**

   The S-CSCF sends acknowledgment to the I-CSCF indicating that deregistration was successful. This request will traverse the path that the REGISTER request took as described in the Via list. The S-CSCF clears its information for that subscriber.

Table 16.4-7 SIP 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
From: <sip:user1_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>;tag=7899
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
CSeq: 3 REGISTER
Date: Wed, 11 July 2001 08:49:37 GMT
Expires: 0
Content-Length: 0
```

Path: The S-CSCF inserts its own name to the front of the list.

8. **SIP 200 OK (I-CSCF to P-CSCF) – see example in Table 16.4-8**

   The I-CSCF forwards acknowledgment from the S-CSCF to the P-CSCF indicating that deregistration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.4-8 SIP 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:token(scscf1.home1.net)>, <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

9. **SIP 200 OK (P-CSCF to UE) – see example in Table 16.4-9**

   The P-CSCF forwards the acknowledgment from the I-CSCF to the UE indicating that deregistration was successful. The P-CSCF clears its information for that subscriber after sending the acknowledgment to the UE.

Table 16.4-9 SIP 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Date:
Expires:
Content-Length:
```

********** NEXT PROPOSED CHANGE **********

Annex A-8: Proposed additions to clauses 6, 16

6.8 Error handling: Registration signalling

6.8.1 Re-registration: failure of re-registration

This signalling flow is a continuation of the signalling flow in subclause 16.3 “Registration Signalling: Re-Registration – User Currently Registered” after reception of signalling flow 4. This signalling flow shows the recovery after a failure of the S-CSCF that had been assigned to the subscriber in a previous registration.

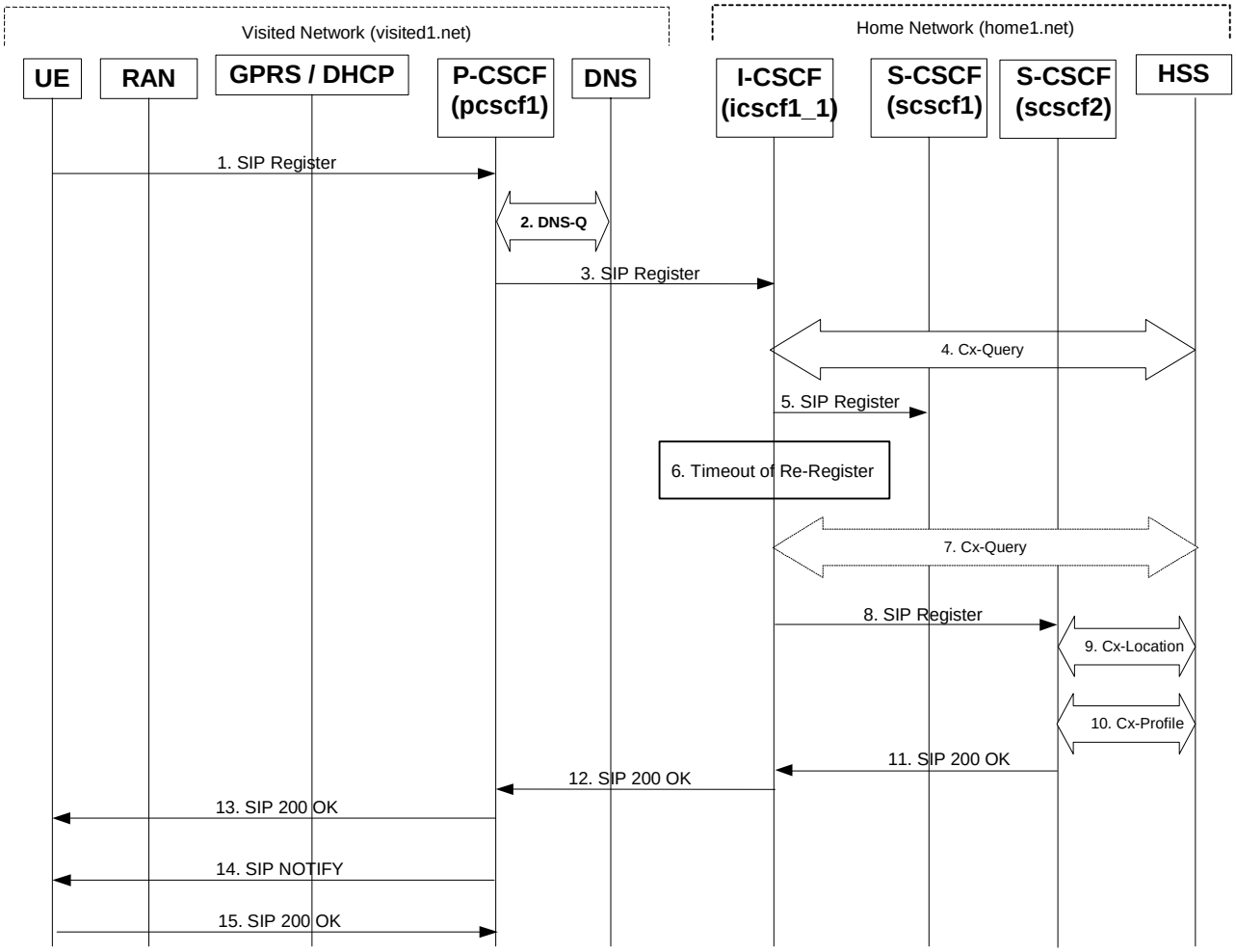


Figure 6.8.1-1: Failure of previous S-CSCF during re-registration

Steps 1 through 4 are the same as the signalling flow in subclause 16.3 “Registration Signalling: Re-Registration – User Currently Registered”

5 **SIP REGISTER (I-CSCF to S-CSCF) – see example in Table 6.8.1-5**

This signalling flow forwards the SIP REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

I-CSCF adds a proper I-CSCF name to the Path header.

Table 6.8.1-5 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_1.home1.net, SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_1.home1.net>, <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From: <sip:user1_private@home1.net> <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:user1%40home1.net@pcscf.visited1.net>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
Authorization:
CSeq: 10 REGISTER
Expires: 7200
Content-Length: 0
```

6 **Timeout of Re-Register**

The I-CSCF times out, waiting for the response from the S-CSCF.

Editor's Note: The value of the timer in this particular instance is FFS. Clearly the value of the timers in the P-CSCF and UE waiting for the response must be considered when choosing this value.

Editor's note: "Whether it is appropriate or not to send the Register request to S-CSCF2 when I-CSCF times out waiting for a response from S-CSCF1 is FFS. While doing a new HSS query or performing a new S-CSCF selection the UE might time out and resend the Register request.

If this step is found to be not a problem for the UE, then the issue of having one subscriber registered to only one S-CSCF must be clarified."

7 **Cx-Query (Optional)**

The I-CSCF informs the HSS that the S-CSCF for the subscriber is unreachable and requests information related to the required S-CSCF capabilities from the HSS, The HSS sends the capability information required for S-CSCF selection. The I-CSCF uses this information to select a suitable S-CSCF.

This step is optional. Depending on implementation, sufficient information may be available to the I-CSCF from Step 4, to allow the I-CSCF select an alternate S-CSCF. Alternative mechanisms (for example a CSCF management plane) would be used to enable the HSS learn of S-CSCF failure. In addition, the HSS will learn about the assignment of a new S-CSCF in Step 9.

8 **SIP REGISTER (I-CSCF to S-CSCF) – see example in Table 6.8.1-8**

This signalling flow forwards the SIP REGISTER request from the I-CSCF to the newly selected S-CSCF. The Request-URI is changed to the address of the new S-CSCF.

Table 6.8.1-8 SIP REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip: scscf2.home1.net SIP/2.0
Via:
Via:
Via:
Path:
Path:
Proxy-require:
Require:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

The remaining steps (9-15) are the same as in the normal re-registration case (steps 6-12 in subclause 16.3)

********** END OF PROPOSED CHANGES **********

References

1. L. Blunk, J. Vollbrecht: "PPP Extensible Authentication Protocol (EAP)", RFC 2284.
2. V. Torvinen, J. Arkko, A. Niemi, "HTTP Authentication with EAP", draft-torvinen-http-eap-00.txt, work in progress.
3. J. Arkko, H. Haverinen, "EAP AKA authentication", draft-arkko-pppext-eap-aka-00.txt, work in progress.
4. Handley, Schulzrinne, Schooler, Rosenberg: "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-04.txt, work in progress.

3GPP TSG-CN1 Meeting #20 ***Tdoc N1-011572***
Brighton, England, 15.-19. October 2001

Title: **LS to GERAN on WB-AMR Signalling**
Source: CN1
To: GERAN2
Cc:

Contact Person:
Name: **Inmaculada Carrión**
Tel. Number: +358503806481
E-mail Address: inmaculada.carrion-rodrigo@nokia.com

Attachments: N1-010628 [CR to TS 24.008 v 5.1.0]

---

1. Overall Description:

TSG CN1 thanks TSG GERAN for their liasion in N1-010290, and agrees that currently TS 24.008 does not cover the case when WB-AMR service is provided via the A-interface.

TSG CN1 discussed the problem and agreed to provide necessary signalling solutions for WB-AMR via A-interface. The attached CR under Tdoc N1-010628 was discussed during the meeting and the principle agreed. A modified version of this document will be submited in the next CN1 meeting in Cancun.

2. Actions:

No action required.

3. Date of Next CN1 Meetings:

CN1_21	26th – 30th November 2001	Cancun, Mexico.

3GPP TSG-CN1 Meeting #20 ***Tdoc N1-010628***
Brighton, England, 15.-19. October 2001

CR-Form-v4

CHANGE REQUEST

⌘ **24.008** **CR** **504** ⌘ ev **2** ⌘ Current version: **5.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Use Supported Codecs IE for all codec types
Source:	⌘	Nokia
Work item code:	⌘	AMR-WB
Date:	⌘	19.10.2001
Category:	⌘	**B**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘ In CN1#17, Tdoc N1-010818, it was proposed the following:

3GTS 24.008 is modified in Release 5 to indicate that all new codec types defined by SA4 from Release 5 onwards shall be indicated via the Supported Codecs IE and no longer shall new codepoints be added to Octet 3a of Bearer Characteristics.

An MSC that supports the new codec types (from Release 5 onwards) would check Octet 3a in BC IE for GSM codecs up to Rel4 and then Supported Codecs IE for any new codec types supported for GSM (listed with Radio Access Type – GSM) and all codec types for UMTS.

The MS supporting new codec types (from Release 5 onwards) shall indicate all codecs for GSM in Supported Codecs IE . However, also in BC IE the MS indicates the speech codecs up to version 3.

The MSC supporting new codec types (from Release 5 onwards) would check. If the Supported Codecs IE does not contain list for GSM then the Octet 3a in BC IE is used for GSM codecs. If the list of GSM codecs are received in the Supported Codecs IE then Octet 3a etc. are ignored. This behaviour ensures the backward compatibility in case of Release 5 mobile station and pre-Release 5 core network.

However the related CR was never implemented to 24.008 that currently reads:

10.5.4.32 Supported codec list

…

Speech codec information belonging to a GSM radio access shall not be conveyed by this information element, but by the *Bearer Capability* information element.

…

In order to allow less processing in the MSCs it is proposed to complement the

	solution in Tdoc N1-010818 by indicating in Supported Codec List also the GSM codecs up to Rel4 which are part of BC IE.
Summary of change: ⌘	Chapters 5.2.1, 5.2.1.2, 5.2.1.11, 5.2.2.3.1, 5.2.2.3.2, 5.2.3.3, 5.3.4.3.2, 9.3.2.6, 9.3.8.1, 9.2.8.3, 9.3.17b.2, 9.3.17b.4, 9.3.23.1.16, 10.5.4.5, 10.5.4.32
Consequences if not approved: ⌘	24.008 does not cover the case when WB-AMR service is provided via the A-interface. WB-AMR service is not applicable to the GERAN system with A-interface support.

Clauses affected:	⌘	10.5.4.32		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******First Modified Section ******

5.2.1 Mobile originating call establishment

The call control entity of the mobile station initiates establishment of a CC connection by requesting the MM sublayer to establish a mobile originating MM connection and entering the "MM connection pending" state. There are two kinds of a mobile originating call: basic call and emergency call. The request to establish an MM connection shall contain a parameter to specify whether the call is a basic or an emergency call. This information may lead to specific qualities of services to be provided by the MM sublayers. Timer T303 is started when the CM SERVICE REQUEST message is sent.

For mobile stations supporting eMLPP basic calls may optionally have an associated priority level as defined in 3GPP TS 23.067. This information may also lead to specified qualities of service to be provided by the MM sublayers.

While being in the "MM connection pending" state, the call entity of the mobile station may cancel the call prior to sending the first call control message according to the rules given in section 4.5.1.7.

The mobile station supporting multicall that is initiating an emergency call shall release one or more existing call to ensure the emergency call can be established if the multicall supported information stored in the mobile station described in section 5.2.1.2 and 5.2.2.1 indicates the network doesn't support multicall and some ongoing calls exists.

Having entered the "MM connection pending" state, upon MM connection establishment, the call control entity of the mobile station sends a setup message to its peer entity. This setup message is

- a SETUP message, if the call to be established is a basic call, and
- an EMERGENCY SETUP message, if the call to be established is an emergency call.

For UMTS speech calls no UMTS speech versions shall be included in *bearer capability IE*. For a ME which supports GSM and UMTS and supports more than GSM speech version 1 then speech versions for GSM shall be included in *Bearer Capability* IE and in *Supported Codec List* IE (see 10.5.4.32). For a UMTS established call these GSM speech versions shall be used by the network for handover to GSM. A ME which supports UMTS codecs different from the UMTS AMR codec shall include a list of supported codecs in *Supported Codec List* IE. Otherwise default UMTS AMR (see Chapter 5.2.1.11) speech version shall be assumed by the network.

For a GSM established call the list shall be used by the network for handover to UMTS.

The mobile station then enters the "call initiated" state. Timer T303 is not stopped.

The setup message shall contain all the information required by the network to process the call. In particular, the SETUP message shall contain the called party address information. If the mobile station supports multicall, it shall include the Stream Identifier (SI) information element. For the first call i.e. when there are no other ongoing calls the SI value shall be 1.

If timer T303 elapses in the "MM connection pending" state, the MM connection in progress shall be aborted and the user shall be informed about the rejection of the call.

******Next Modified Section ******

5.2.1.2 Receipt of a setup message

In the "null" or "recall present" states, upon receipt of a setup message (a SETUP message or an EMERGENCY SETUP message, see section 5.2.1.1), the call control entity of the network enters the "call initiated" state. It shall then analyse the call information contained in the setup message.

In UMTS, network shall include the SI received in the SETUP message into the RABid and send it back to the mobile station. For RABid see 3GPP TS 25.413. If the network receives the SETUP message with no SI, the network shall set the SI value to 1.

i) If, following the receipt of the setup message, the call control entity of the network determines that the call information received from the mobile station is invalid (e.g. invalid number), then the network shall initiate call clearing as defined in section 5.4 with one of the following cause values:

   # 1 "unassigned (unallocated) number"

   # 3 "no route to destination"

   # 22 "number changed"

   # 28 "invalid number format (incomplete number)"

ii) If, following the receipt of the setup message, the call control entity of the network determines that a requested service is not authorized or is not available, it shall initiate call clearing in accordance with section 5.4.2 with one of the following cause values:

   # 8 "operator determined barring",

   # 57 "bearer capability not authorized",

   # 58 "bearer capability not presently available",

   # 63 "service or option not available, unspecified", or

   # 65 "bearer service not implemented".

iii) Otherwise, the call control entity of the network shall either:

   - send a CALL PROCEEDING message to its peer entity to indicate that the call is being processed; and enter the "mobile originating call proceeding" state.

   - or: send an ALERTING message to its peer entity to indicate that alerting has been started at the called user side; and enter the "call received" state.

   - or: send a CONNECT message to its peer entity to indicate that the call has been accepted at the called user side; and enter the "connect request" state.

   The call control entity of the network may insert bearer capability information element(s) in the CALL PROCEEDING message to select options presented by the mobile station in the Bearer Capability information element(s) of the SETUP message. The bearer capability information element(s) shall contain the same parameters as received in the SETUP except those presenting a choice. Where choices were offered, appropriate parameters indicating the results of those choices shall be included.

   The CALL_PROCEEDING message shall also contain the priority of the call in the case where the network supports eMLPP. Mobile stations supporting eMLPP shall indicate this priority level to higher sublayers and store this information for the duration of the call for further action. Mobile stations not supporting eMLPP shall ignore this information element if provided in a CALL PROCEEDING message.

NOTE: If the network supports only R98 or older versions of this protocol and the priority is not included in the CALL PROCEEDING message, this does not imply that the network does not support eMLPP.

- The CALL_PROCEEDING message shall contain the multicall supported information in the network call control capabilities in the case where the network supports multicall and there are no other ongoing calls to the MS. Mobile stations supporting multicall shall store this information until the call control state for all calls returns to null. Mobile stations not supporting multicall shall ignore this information if provided in a CALL PROCEEDING message. If the multicall supported information is not sent in the CALL_PROCEEDING message, the mobile station supporting multicall shall regard that the network doesn't support multicall.

The call control entity of the network having entered the "mobile originating call proceeding" state, the network may initiate the assignment of a traffic channel according to section 5.2.1.9 (early assignment).

For UMTS speech calls no UMTS speech versions shall be included in *Bearer Capability IE;* if the SETUP includes a list of supported codecs in *Supported Codec List IE* then the network shall use this list to select the required codec type, see Chapter 5.2.1.11. Otherwise the default UMTS AMR (see Chapter 5.2.1.11) speech version shall be assumed.

For a GSM established call the list shall be used by the network for handover to UMTS.

GSM speech versions received ~~by the network~~ in *Bearer Capability* IE shall be used by~~ a network which supports up GSM speech version 3 or below the network~~ for GSM call establishment and handover to GSM. For GSM speech calls where no speech versions are included in *Bearer Capability IE* the network shall assume GSM speech version 1.

GSM speech versions received in *Supported Codec List* IE (see 10.5.4.32) by a network which supports up GSM speech version 3 or above shall be used for GSM call establishment and handover to GSM. For GSM speech calls where no speech versions are included in *Supported Codec List* IE the network~~ shall use GSM speech versions received in *Bearer Capability* IE.

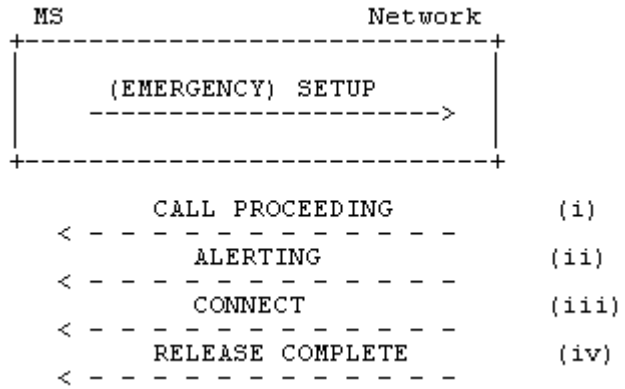


Figure 5.2/3GPP TS 24.008 Mobile originated call initiation and possible subsequent responses.

******Next Modified Section ******

5.2.1.11 Speech Codec Selection

The network can receive *Supported Codec List* IE in call establishment messages from the ME to inform the network of the codec types that it supports.

If the network does not receive *Supported Codec List IE* then default UMTS AMR speech version shall be assumed for UMTS calls, and GSM speech versions received in *Bearer Capability* shall be assumed for GSM calls..

The default UMTS AMR speech version for "R99 UMTS only" terminals is UMTS_AMR. The default UMTS AMR speech version for terminals supporting GSM & UMTS radio accesses and all terminals from Release 4 onwards is UMTS_AMR_2. For further details see 3G TS 26.103.

Note: 'UMTS_AMR_2' is fully backward compatible with 'UMTS_AMR', therefore if the UE supports 'UMTS_AMR_2' and the network is R99 and assumes 'UMTS_AMR' then no interworking problems will occur.

The network shall determine the default UMTS AMR speech version by the following:

i) If no GSM Speech Version codepoints are received neither in *Supported Codec List* IE nor in octet 3a etc. of the *Bearer Capabilities* IE then a "UMTS only" terminal is assumed and the default UMTS AMR speech version shall be UMTS_AMR.

ii) If at least one GSM Speech Version codepoint is received in *Supported Codec List* IE or in octet 3a etc. of the *Bearer Capabilities* IE then a terminal supporting GSM and UMTS is assumed and the default UMTS AMR speech version shall be UMTS_AMR_2.

If the *Supported Codec List* IE is received, the network shall select a codec from the list of codecs and indicate this to the ME via RANAP and RRC protocol in NAS Synchronisation Indicator IE. See 3GPP TS 25.413 and 3GPP TS 25.331.

Coding of the codec type (CoID) shall be, as defined in 3GPP 3GPP TS 26.103.

The network shall determine the preference for the selected codec type; codec type prioritisation is not provided by the ME.

The ME shall activate the codec type received in the NAS Synchronisation Indicator IE.

If the mobile station does not receive the NAS Synchronisation Indicator IE (RRC protocol) then it shall assume default UMTS AMR speech version.

For adaptive multirate codec types no indication of subsets of modes is supported in this protocol, from the ME or to the ME. It is a pre-condition that the support of such codec types by the ME implicitly includes all modes defined for that codec type.

******Next Modified Section ******

5.2.2.3.1 Response to SETUP

Having entered the "call present state" the call control entity of the mobile station shall - with the exception of the cases described below - acknowledge the SETUP message by a CALL CONFIRMED message, and enter the "mobile terminating call confirmed" state.

If the mobile station supports multicall, it shall include the Stream Identifier (SI) information element in the CALL CONFIRMED message.

- If the mobile station is located in the network supporting multicall, it shall never include the SI that is in use and shall include with either of the following two values:
- SI="no bearer"
- SI=new value (not used by any of the existing bearers)

If the mobile station supporting multicall is located in the network not supporting multicall, it shall include the SI with value 1.

The call control entity of the mobile station may include in the CALL CONFIRMED message to the network one or two bearer capability information elements to the network, either preselected in the mobile station or corresponding to a service dependent directory number (see 3GPP TS 29.007). The mobile station may also include one or two bearer capabilities in the CALL CONFIRMED message to define the radio channel requirements~~. For UMTS speech calls no UMTS speech versions shall be included in *bearer capability IE*~~.

For a ME which supports ~~GSM and UMTS and~~ supports more than GSM speech version 1 ~~then~~ GSM speech versions up to GSMspeech version 3 for GSM shall be included in both Supported Codec List IE (see 10.5.4.32) and *Bearer Capability* IE. Additionally, if the MS supports any other GSM speech versions, those speech versions shall be included in *Supported Codec List* IE. ~~For a UMTS established call these GSM speech versions shall be used by the network for handover to GSM.~~

A ME which supports UMTS codecs different from the UMTS AMR codec shall include the supported codecs in *Supported Codec List* IE in the CALL CONFIRMED message, otherwise default UMTS AMR (see Chapter 5.2.1.11) speech version shall be assumed by the network. In any case the rules specified in section 9.3.2.2 shall be followed. No UMTS speech versions shall be included in B*earer Capability* IE.

For a UMTS established call GSM speech versions shall be used by the network for handover to GSM.

NOTE: The possibility of alternative responses (e.g., in connection with supplementary services) is for further study.

A busy MS which satisfies the compatibility requirements indicated in the SETUP message shall respond either with a CALL CONFIRMED message if the call setup is allowed to continue or a RELEASE COMPLETE message if the call setup is not allowed to continue, both with cause #17 "user busy".

If the mobile user wishes to refuse the call, a RELEASE COMPLETE message shall be sent with the cause #21 "call rejected".

In the cases where the mobile station responds to a SETUP message with RELEASE COMPLETE message the mobile station shall release the MM connection and enter the "null" state after sending the RELEASE COMPLETE message.

The network shall process the RELEASE COMPLETE message in accordance with section 5.4.

****Next Modified Section ****

5.2.2.3.2 Receipt of CALL CONFIRMED and ALERTING by the network

The call control entity of the network in the "call present" state, shall, upon receipt of a CALL CONFIRMED message: stop timer T303, start timer T310 and enter the "mobile terminating call confirmed" state.

In UMTS, network shall include the SI received in the CALL CONFIRMED message into the RABid and send it back to the mobile station. For RABid see 3GPP TS 25.413. If the network receives the CALL CONFIRMED message with no SI, the network shall set the SI value to 1.

For UMTS speech calls no UMTS speech versions shall be included in *bearer capability IE;* if the CALL CONFIRMED message includes a list of supported codecs in *Supported Codec List IE* then the network shall use this list to select the required codec type, see Chapter 5.2.1.11. If no *Supported Codec List IE* is received by the network then default UMTS AMR (see Chapter 5.2.1.11) speech version shall be assumed.

GSM speech versions received by the network in *Bearer Capability* IE and *Supported Codec List* IE (see 10.5.4.32) Sshall be used by the network for GSM call establishment and handover to GSM. For GSM speech calls where no speech versions are included in *bearer capability IE* the network shall assume GSM speech version 1.

The call control entity of the mobile station having entered the "mobile terminating call confirmed" state, if the call is accepted at the called user side, the mobile station proceeds as described in 5.2.2.5. Otherwise, if the signal information element was present in the SETUP message user alerting is initiated at the mobile station side; if the signal information element was not present in the SETUP message, user alerting is initiated when an appropriate channel is available.

Here, initiation of user alerting means:

- the generation of an appropriate tone or indication at the mobile station; and
- sending of an ALERTING message by the call control entity of the MS to its peer entity in the network and entering the "call received" state.

The call control entity of the network in the "mobile terminated call confirmed" state shall, upon receipt of an ALERTING message: send a corresponding ALERTING indication to the calling user; stop timer T310; start timer T301, and enter the "call received" state.

In the "mobile terminating call confirmed" state or the "call received" state, if the user of a mobile station is User Determined User Busy then a DISCONNECT message shall be sent with cause #17 "user busy". In the "mobile terminating call confirmed" state, if the user of a mobile station wishes to reject the call then a DISCONNECT message shall be sent with cause #21 "call rejected".

******Next Modified Section ******

5.2.3.3 CC-Establishment confirmation

The call control entity of the network in the "CC-establishment present" state, shall, upon receipt of a CC-ESTABLISHMENT CONFIRMED message, stop timer T333 and enter the "CC-establishment confirmed" state.

In the "CC-establishment confirmed" state, the network sends a RECALL message. This message initiates user alerting and also shall include the Facility IE (providing additional information to be presented to the user for notification). The network starts timer T334 and enters the 'recall present' state.

Upon reception of the RECALL message the Mobile station stops T335 and enters the "recall present" state.

Additionally, for UMTS speech calls a ME which supports more than UMTS AMR codec shall include the list of supported codecs in *Supported Codec List* IE in the ESTABLISHMENT-CONFIRMED message.

For GSM speech calls a ME which supports more than GSM speech version 1 versions up to version 3 shall be included in both Supported Codec List IE (see 10.5.4.32) and *Bearer Capability* IE in the ESTABLISHMENT CONFIRMED message. In addition to that if the MS supports any other GSM speech versions, those speech versions shall be included in *Supported Codec List* IE in the ESTABLISHMENT CONFIRMED message.

If a *Supported Codec List* IE is received the network shall use the codec list for codec selection. See 5.2.1.11. If no *Supported Codec List*IE is received by the network then default UMTS AMR (See Chapter 5.2.1.11) speech version shall be assumed for UMTS, and the network shall determine the supported GSM speech versions from the *Bearer Capability* IE.~~,~~

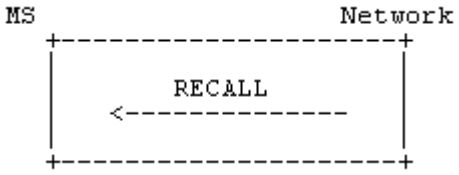


Figure 5.7b/3GPP TS 24.008 Recall

******Next Modified Section ******

5.3.4.3.2 Successful completion of in-call modification

If the destination network/mobile station receives a MODIFY message with a new mode which is already the actual one of the call the network/mobile station shall remain in the "active" state; send a MODIFY COMPLETE message with the actual mode; and shall not initiate anything else.

If the requested mode is a speech mode and the call is UMTS then if the ME supports UMTS codecs different from the UMTS AMR codec (*Supported Codec List* IE received by the network) then the network shall select a codec from this list, otherwise default UMTS AMR (see Chapter 5.2.1.11) speech version shall be assumed. If a codec is selected other than default AMR, the network shall send the selected codec type to the ME via RANAP NAS Synchronisation Indicator IE (see 5.2.1.11),.

If the requested mode is speech and the call is GSM then if GSM speech versions are included in either *Supported Codec ListIE* or in *Bearer Capability IE* then the network shall use these speech versions, if none are included then GSM speech version 1 shall be assumed.

If the requested mode is not the actual one and can be supported by the destination interface it shall change the channel configuration, if required, and step on to any internal resources necessary to support the next call mode. If the requested mode is a data or facsimile mode, it shall also perform the appropriate means to take the direction of the data call into account. After successful change of the channel configuration it shall start sending user information according to the next call mode and start interpreting received user channel information according to the next call mode; send a MODIFY COMPLETE message with the new call mode included and enter the "active" state (mobile station or network side). If the MODIFY message had contained a *reverse call setup direction* IE, the same IE shall be included in the MODIFY COMPLETE message.

In case of an alternate speech/facsimile group 3 service (refer to section 5.3.4) the old resources may still be kept reserved.

Upon receipt of the MODIFY COMPLETE message the originating side shall: initiate the alternation to those resources necessary to support the next call mode; stop timer T323; and enter the "active" state (mobile station or network side). The reaction of the originating side if it had included a reverse call setup direction IE in the MODIFY message, but the destination side did not include the IE in the MODIFY COMPLETE message is implementation dependent.

******Next Modified Section ******

9.3.2.6 Supported Codecs

This information element shall be included by the ME for UMTS speech calls for a ME which supports UMTS codecs different from the UMTS AMR codec. For GSM calls a ME which supports more than GSM speech version 1 shall include the list of supported codecs in *Supported Codec List* IE. If this information element is not included then the network shall use GSM speech versions received in *Bearer Capability* for GSM calls.

******Next Modified Section ******

9.3.8.1 Bearer capability

If the element is not included, the network shall by default assume speech and select full rate speech version 1. If this information element is included, it shall indicate speech, the appropriate speech version(s) and have the appropriate value of radio channel requirement field.

This information element shall be included by an ME supporting CTM text telephony.

For UMTS speech if no *Supported Codec List* IE is included then the network shall assume default UMTS AMR (see chapter 5.2.1.11) speech version ~~shall be assumed by the network~~for UMTS and determine supported GSM speech versions from *Bearer Capability* IE..

For GSM speech if no *Supported Codec List* IE is included then the network shall use GSM speech versions received in *Bearer Capability* for GSM calls.

******Next Modified Section ******

9.3.8.3 Supported Codecs

This information element shall be included by the mobile station for UMTS speech calls for a ME which supports UMTS codecs different from the UMTS AMR codec. If this information element is not included then the network shall assume default UMTS AMR (see chapter 5.2.1.11) speech codec.
For GSM calls a ME which supports more than GSM speech version 1 shall include the list of supported codecs in *Supported Codec List* IE. If this information element is not included then the network shall use GSM speech versions received in *Bearer Capability* for GSM calls.

******Next Modified Section ******

9.3.17b.2 Bearer capability 1 and bearer capability 2

If, in any subsequent SETUP message to be sent on this transaction the *bearer capability 1* information element is to be followed by the *bearer capability 2* IE, then the *bearer capability 2* IE shall be included in this message.

For UMTS speech if no *Supported Codec List* IE is included then the default UMTS AMR (see chapter 5.2.1.11) speech version shall be assumed by the network.

For GSM speech if no *Supported Codec List* IE is included then the network shall use GSM speech versions received in *Bearer Capability* for GSM calls.

******Next Modified Section ******

9.3.17b.4 Supported Codecs

This information element shall be included by the mobile station for UMTS speech calls for a ME which supports UMTS codecs different from the UMTS AMR codec.

For GSM calls a ME which supports more than GSM speech version 1 shall include the list of supported codecs in *Supported Codec List* IE. If this information element is not included then the network shall use GSM speech versions received in *Bearer Capability* for GSM calls.

******Next Modified Section ******

9.3.23.2.16 Supported Codecs

This information element shall be included by the mobile station for UMTS speech calls for a ME which supports UMTS codecs different from the UMTS AMR codec.

For GSM calls a ME which supports more than GSM speech version 1 shall include the list of supported codecs in *Supported Codec List* IE. If this information element is not included then the network shall use GSM speech versions received in *Bearer Capability* for GSM calls.

******Last Modified Section ******

10.5.4.32 Supported codec list

The purpose of the *Supported Codec List* information element is to provide the network with information about the speech codecs supported by the mobile.

The *Supported Codec List* information element is coded as shown in figure 10.5.118c/3GPP TS 24.008.

The *Supported Codec List* information element is a type 4 information element with a minimum length of 5 octets and a maximum length of m+3 octets.

Speech codec information belonging to GSM and UMTS radio access shall be conveyed by this information element.

3GPP TSG-CN1 Meeting #20 ***Tdoc N1-011594***
Brighton, England, 15.-19. October 2001

Title: **LS to SA1 on Multicall handover requirements**
Source: CN1
To: SA1
Cc:

Contact Person:
Name: **Inmaculada Carrión**
Tel. Number: +358503806481
E-mail Address: inmaculada.carrion-rodrigo@nokia.com

Attachments: N1-011556 [CR to TS 23.009 v 3.7.0]., N1-011581 [CR to TS 22.129 v 3.5.0]

---

1. Overall Description:

TSG CN1 finally reached an agreement on a compromised solution to solves the current problem on Bearer selection of calls part of a Multicall. The attached CRs were discussed during the meeting, the CR under CN1 responsabilitiy was conditionally agreed provided that SA1 can also agree the CR to 22.129 or some revision of it.

In a new attempt to implement a consistent set of specifications, the following was agreed during the meeting:

- to specify in TS 23.009 that during RAB assignment and relocation request a 3G_MSC-A supporting multicall may assign priorities. The management of priority levels is Implementation dependent, under operator control. and

- a proposal to relax the requirements in TS 22.129 so that they apply only to InterSystem handover; in case of IntraUMTS relocations the criteria are operator dependant

There were some concerns on the two different behaviours that the network should apply regarding the emergency call selection when performing a relocation (operator configuration), and an InterSystem UMTS to GSM handover (as currently specified in TS 22.129 3.5.0). This should be taken into account when discussing the attached CR to 22.129.

The attached CR on 23.009 (under Tdoc N1-011556) was conditionally approved by CN1 upon decision of SA1 on the other attached CR against 22.129 (under Tdoc N1-011581).

2. Actions:

To SA1 group.

ACTION: CN1 asks SA1 group to discuss the CR under Tdoc N1-011581, modify it if necessary and approve some version of it. CN1 would also ask SA1 group to inform us on the outcome of the discussion by next CN1 meeting CN1#21..

3. Date of Next CN1 Meetings:

CN1_21	26th – 30th November 2001	Cancun, Mexico.

3GPP TSG-CN1 Meeting #20 ***Tdoc N1-011556***
Brighton, England, 15.-19. October 2001

CR-Form-v4

CHANGE REQUEST

⌘ **23.009** **CR** **054** ⌘ ev **-** ⌘ Current version: **3.8.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Multicall bearer selection
Source:	⌘	Nokia
Work item code:	⌘	Multicall
Date:	⌘	10.10.01
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘

The current version of TS 22.129 specifies selection criteria for the network which shall be used in case of handover of a multicall when it is not be possible to handover all bearers belonging to the multicall:

5.4 Handover of a Multicall

...

It shall be possible to handover all the calls in a multicall configuration.. If the target cell is not able to accommodate all the calls in a multicall configuration, then the calls that are handed over shall be selected in following order:

i. The call of teleservice emergency call

ii. The call of teleservice telephony

iii. The call of any other type

Calls that cannot be handed over will be released.

If no single call can be selected according to the above criteria, handover shall be rejected.

CN1 was not able to agree on a solution implementing these requirements in the stage 2 specification of the handover procedures (TS 23.009), neither by discussion, nor by a formal vote.

In a new attempt to get a consistent set of specifications, it is proposed:
- to relax the requirements in TS 22.129 so that they apply only to InterSystem handover; in case of IntraUMTS relocations the criteria are operator dependant; and
- to specify in TS 23.009 that during RAB assignment and relocation request a 3G_MSC-A supporting multicall may assign priorities. The management of priority levels is Implementation dependent, under operator control.

Summary of change:	⌘	Text added to role of 3G_MSC-A and 3G_MSC-B
Consequences if not approved:	⌘	Inconsistency between the requirements (TS 22.129) and the stage 2 specification (TS 23.009). Furthermore inconsistent behaviour in different handover scenarios, as different selection criteria may be applied by 3G_MSC-A and 3G_MSC- B, when selecting which bearers of a multicall will be handed over.

Clauses affected:	⌘	4.3.1 and 4.4.1			
Other specs affected:	⌘	**X**	Other core specifications	⌘	22.129
			Test specifications		
			O&M Specifications		
Other comments:	⌘	This CR depends on acceptance of the CR to TS 22.129, which changes the requirements for multicall handover.			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.3 3G_MSC-A

For roles and functional composition of the 3G_MSC-A working as pure GSM MSC, please see previous clause ("MSC-A").

4.3.1 Role of 3G_MSC-A

In the Intra-3G_MSC handover/relocation case, the 3G_MSC-A (simply termed 3G_MSC) controls the call, the mobility management and the radio resources before, during and after an Intra-3G_MSC handover/relocation. When RANAP or BSSMAP procedures have to be performed, they are initiated and driven by 3G_MSC-A.

In the case of intra-MSC handover of a speech call, 3G_MSC-A controls the transcoder in the core network. The 3G_MSC-A determines if a transcoder is required to be inserted or released in the CN.

In the case of Inter-3G_MSC relocation, 3G_MSC-A links out the transcoder.

In the Inter-3G_MSC relocation case, 3G_MSC-A is the 3G_MSC that controls the call and the mobility management of the UE during the call, before, during and after a basic or subsequent relocation. When RANAP procedures related to dedicated resources have to be performed towards the UE, they are initiated and driven by 3G_MSC-A. The 3G_MSC-A - 3G_MSC-B interface works as a 3G_MSC - RNS interface for the RANAP procedures. The Direct Transfer signalling is relayed transparently by 3G_MSC-B between 3G_MSC-A and the UE.

During a basic relocation, 3G_MSC-A initiates and controls all the relocation procedure, from its initiation (reception of Relocation Required from RNS-A on Iu-interface) until its completion (reception of Relocation Complete from 3G_MSC-B on E-interface).

During a subsequent relocation back to 3G_MSC-A, 3G_MSC-A acts as an RNS towards 3G_MSC-B, which controls the relocation procedure until the termination in 3G_MSC-A of the handover radio resources allocation (sending of the Relocation Request Acknowledge to 3G_MSC-B from 3G_MSC-A). Then all relocation related messages shall terminate at 3G_MSC-A (e.g. Relocation Detect/Complete from RNS-B, Relocation Cancel from RNS-A).

During a subsequent relocation to a third 3G_MSC, 3G_MSC-A works towards 3G_MSC-B' as described above in the basic relocation paragraph and towards 3G_MSC-B as described above in subsequent relocation paragraph.

In the Inter-System, inter-3G_MSC handover case, 3G_MSC-A is the 3G_MSC which controls the call and the mobility management of the UE/MS during the call, before, during and after a basic or subsequent inter-system handover. When BSSAP procedures related to dedicated resources have to be performed towards the UE/MS, they are initiated and driven by 3G_MSC-A. The 3G_MSC-A – MSC-B interface works as a 3G_MSC – BSS interface for a subset of BSSMAP procedures. These BSSMAP procedures described in 3GPP TS 09 08 [7] are those related to dedicated resources. The DTAP signalling is relayed transparently by MSC-B between 3G_MSC-A and the UE/MS.

During a basic inter-system UMTS to GSM handover, 3G_MSC-A initiates and controls all the handover procedure, from its initiation (reception of Relocation Required from RNS-A on Iu-interface) until its completion (reception of Handover Complete from MSC-B on E-interface).

During a subsequent inter-system UMTS to GSM handover back to 3G_MSC-A, 3G_MSC-A acts as a BSS towards 3G_MSC-B, which controls the handover procedure until the termination in 3G_MSC-A of the handover radio resources allocation (sending of the Handover Request Acknowledge to 3G_MSC-B from 3G_MSC-A). Then all handover related messages shall terminate at 3G_MSC-A (e.g. Handover Detect/Complete from BSS-B, Relocation Cancel from RNS-A).

During a subsequent inter-system UMTS to GSM handover to a third 3G_MSC, 3G_MSC-A works towards MSC-B' as described above in the basic inter-system handover paragraph and towards 3G_MSC-B as described above in subsequent inter-system handover paragraph.

During a basic inter-system GSM to UMTS handover, 3G_MSC-A initiates and controls all the handover procedure, from its initiation (reception of Handover Required from BSS-A on A-interface) until its completion (reception of Handover Complete from 3G_MSC-B on E-interface).

During a subsequent inter-system GSM to UMTS handover back to 3G_MSC-A, 3G_MSC-A acts as an RNS towards MSC-B, which controls the handover procedure until the termination in 3G_MSC-A of the handover radio resources allocation (sending of the Handover Request Acknowledge to MSC-B from 3G_MSC-A). Then all handover related

messages shall terminate at 3G_MSC-A (e.g. Relocation Detect/Complete from RNS-B, Handover Failure from BSS-A).

During a subsequent inter-system GSM to UMTS handover to a third 3G_MSC, 3G_MSC-A works towards 3G_MSC-B' as described above in the basic inter-system handover paragraph and towards MSC-B as described above in subsequent inter-system handover paragraph.

3G_MSC-A may assign a priority level defined as RAB parameter in 3GPP TS 25.413 [11] for each bearer. In case of relocation of a multicall configuration the 3G_MSC-B or the target RNC shall select the bearers to be handed over according to the priority level, if the target cell is not able to accommodate all bearers. If a selection has to be made between bearers of the same priority level, then the selection criteria are implementation dependent.

If 3G_MSC-A supports the optional supplementary service Multicall (See 3GPP TS 23.135) and UE is engaged with multiple bearers the following description applies;

- In the Intra-3G_MSC relocation case, the 3G-MSC-A tries to relocate all bearers to a new RNS.
- In the basic relocation case, the 3G-MSC-A tries to relocate all bearers to 3G_MSC-B. If 3G_MSC-A receives an indication that the 3G_MSC-B does not support multiple bearers, then 3G_MSC-A shall be able to select one bearer to be handed over according to the 3GPP TS 22.129 [9] ~~priority level defined as RAB parameters in 3GPP TS 25.413~~ and tries again to relocate the selected bearer.
- In the subsequent relocation to a third 3G_MSC-B' case, the 3G-MSC-A tries to relocate all bearers to 3G_MSC-B'. If 3G_MSC-A receives an indication that the 3G_MSC-B' does not support multiple bearers, then 3G_MSC-A shall be able to select one bearer to be handed over according to 3GPP TS 22.129 [9] ~~the priority level defined as RAB parameters in 3GPP TS 25.413 [11]~~ and tries again to relocate the selected bearer.
- In the Intra-3G_MSC inter-system UMTS to GSM handover case and the basic inter-system UMTS to GSM handover case, the 3G_MSC-A shall be able to select one bearer to be handed over according 3GPP TS 22.129 [9] ~~to the priority level defined as RAB parameters in 3GPP TS 25.413 [11]~~ and tries to handover the selected bearer.
- In all cases described above, 3G_MSC-A shall release some calls which has been carried by the bearers failed to set up in new RNS or the bearers not to be handed over.

********** NEXT MODIFIED SECTION **********

4.4 3G_MSC-B

For roles and functional composition of the 3G_MSC-B working as pure GSM MSC, please see previous clause ("MSC-B").

4.4.1 Role of 3G_MSC-B

...

If 3G_MSC-B does not support the optional supplementary service Mutlicall (See 3GPP TS 23.135) and 3G_MSC-A requests to relocate multiple bearers, 3G_MSC-B shall indicate that it does not support multiple bearers to 3G_MSC-A.

If 3G_MSC-B supports the optional supplementary service Multicall (See 3GPP TS 23.135) and UE is engaged with multiple bearers the following description applies;

- In the basic relocation case, the 3G_MSC-B shall be able to allocate a~~n~~ Handover Number for each bearer. The 3G_-MSC-B shall also be able to select some bearers to be handed over according to the priority level defined as RAB parameters in 3GPP TS 25.413 [11] so that the number of bearers will fulfill the maximum number of

bearers supported by the 3G_MSC-B. If a selection has to be made between bearers of the same priority level, then the selection criteria are implementation dependent.

- In the Intra-3G_MSC relocation case, the 3G_ -MSC-B tries to relocate all bearers to a new RNS.
- In the subsequent relocation back to the 3G_MSC-A or to a third 3G_MSC-B' case, the 3G_ -MSC-B tries to request to the 3G_MSC-A to relocate all bearers to the 3G_MSC-A or to the 3G_MSC-B'.
- In the Intra-3G_MSC inter-system UMTS to GSM handover case and the subsequent inter-system UMTS to GSM handover back to the 3G_MSC-A or to a third MSC-B' case, the 3G_MSC-B shall be able to select one bearer to be handed over according to 3GPP TS 22.129 [9] ~~the priority level defined as RAB parameters in 3GPP TS 25.413 [11~~] and tries to handover the selected bearer.

3GPP TSG-CN1 Meeting #20
Brighton, England, 15.-19. October 2001

Tdoc N1-011581

3GPP TSG-SA1 Meeting # *??*

Tdoc ??

CR-Form-v4

CHANGE REQUEST

⌘ **22.129** **CR** ?? ⌘ ev **-** ⌘ Current version: **3.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Bearer selection criteria of calls in a multicall
Source:	⌘	Nokia
Work item code:	⌘	Multicall
Date:	⌘	11.09.01
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘ The current version of TS 22.129 specifies selection criteria for the network which shall be used in case of handover of a multicall when it is not be possible to handover all bearers belonging to the multicall:

5.4 Handover of a Multicall

...

It shall be possible to handover all the calls in a multicall configuration.. If the target cell is not able to accommodate all the calls in a multicall configuration, then the calls that are handed over shall be selected in following order:

i. The call of teleservice emergency call

ii. The call of teleservice telephony

iii. The call of any other type

Calls that cannot be handed over will be released.

If no single call can be selected according to the above criteria, handover shall be rejected.

CN1 was not able to agree on a solution implementing these requirements in the stage 2 specification of the handover procedures (TS 23.009), neither by discussion, nor by a formal vote.

In a new attempt to get a consistent set of specifications, it is proposed:
- to relax the requirements in TS 22.129 so that they apply only to InterSystem

		handover; in case of IntraUMTS relocations the criteria are operator dependant; and - to specify in TS 23.009 that during RAB assignment and relocation request a 3G_MSC-A supporting multicall may assign priorities. The management of priority levels is Implementation dependent, under operator control.
Summary of change:	⌘	
Consequences if not approved:	⌘	Inconsistency between the requirements (TS 22.129) and the stage 2 specification (TS 23.009).

Clauses affected:	⌘	5.4			
Other specs affected:	⌘	X	Other core specifications	⌘	23.009
			Test specifications		
			O&M Specifications		
Other comments:	⌘	This CR is a precondition for the acceptance of the CR to TS 23.009.			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.4 Handover of a Multicall

The handover event can trigger changes to individual calls in any multicall scenario.

It shall be possible to handover all the calls in a multicall configuration.

If the target system is UMTS and the target cell is not able to accommodate all the calls in a multicall configuration, then the calls that are handed over are selected according to operator preferences.

~~It shall be possible to handover all the calls in a multicall configuration..~~ If the target ~~cell is not able to accommodate all the calls in a multicall configuration~~ system is GSM, then the call~~s~~ that is~~are~~ handed over shall be selected in following order:

i. The call of teleservice emergency call

ii. The call of teleservice telephony

iii. The calls of any other type according to operator preferences.

Calls that cannot be handed over will be released.

~~If no single call can be selected according to the above criteria, handover shall be rejected.~~

A change in the availability of suitable radio resources may also occur for other reasons in addition to handover.

3GPP TSG-CN1 Meeting #20 ***Tdoc N1-011625***
Brighton, England, 15th – 19th October 2001

Title: Liaison Statement response on 'LS On the handling of the Protocol Configuration Options IE'

Source: CN1

To: CN4

Cc:

Contact Person:
Name: Atle Monrad
Tel. Number: +47 372 93 665
E-mail Address: Atle.Monrad@eto.ericsson.se

Attachments: none

---

1. Overall Description:

CN1 thanks CN4 for their LS N4-011217 'LS On the handling of the Protocol Configuration Options IE'.

In this Liaison, CN4 informs CN1 about ongoing discussions concerning the Protocol configuration options IE available in a number of session management messages, and asks for CN1s opinion in the matter.

CN1 has discussed the issue identified by CN4 and has reached the following conclusion:

1. By definition, the PCO IE is a 'container' sent between UE and GGSN transparently to the SGSN. It is CN1's understanding that, the SGSN shall treat this IE conditionally: if it is received, then it shall be transmitted without any modifications.

2. It was also identified that, TS 24.008 does not mandate a PCO IE in the Active PDP Context Response/Reject messages when the MS includes a PCO IE in the Activate PDP Context Request message. Therefore, it's up to the GGSN to decide whether it has to send a PCO IE back to the mobile or not.

2. Actions:

To CN4 group.

ACTION: CN1 recommends CN4 to continue their work taking into account this answer from CN1.

In case CN4 experience interworking problems between the UE and GGSN or between the UE and external PDN due to the Protocol configuration options information element, CN1 would like to be informed and determine if 24.008 needs clarifications.

3. Date of Next CN1 Meeting:

CN1 #21 26th -30th of November 2001, Cancun

3GPP TSG-CN1 Meeting #20bis ***Tdoc N1-011763***

Seattle, Washington, USA, 13.-15. November 2001

Title: Liaison Statement on configuration hiding between S-CSCF and MGCF

Source: CN1

To: SA2

Cc:

Contact Person:

Name: **Keith Drage**

Tel. Number: +44 7799658151

E-mail Address: drage@lucent.com

Attachments: None

---

1. Overall Description:

CN1 is writing SIP procedural text for the THIG function. TS 23.228 describes that the configuration of the network, in particular the number of S-CSCFs needs to be hidden. The S-CSCF and MGCF may be in different networks, and thus hiding should appear between these two entities.

The only functionality that describes provision of the THIG function at the moment is the I-CSCF. Reading TS 23.002 and TS 23.228 it is apparently not possible to insert an I-CSCF between S-CSCF and MGCF.

The BGCF does appear between these two entities. The BGCF has no description for providing THIG.

2. Actions:

To SA2 group.

ACTION: CN1 asks SA2 whether configuration hiding of S-CSCFs is required between S-CSCF and MGCF when they are in different networks, and which entity provides that functionality. Appropriate clarifications are requested in TS 23.228.

3. Date of Next CN1 Meetings:

CN1_21	26th – 30th November 2001	Cancun, Mexico.
CN1_SIPadhoc	14th – 18th January 2002	Phoenix, USA

3GPP TSG-CN1 Meeting #20bis ***Tdoc N1-011768***
Seattle, Washington, USA, 13.-15. November 2001

Title: LS on IMS identifiers
Source: CN1
To: SA2, T3, SA3, SA1, T2
Cc: EP SCP
Response to: LS (S2-013067) on IMS identifiers and ISIM and USIM from SA2

Contact Person:
Name: Duncan Mills
Tel. Number: +44 1635 676074
E-mail Address: duncan.mills@vf.vodafone.co.uk

Attachments: None

CN1 received and discussed the LS from SA2 in Tdoc N1-011728 (S2-013067) and understands the potential advantage of being able to, for instance, re-use the current USIM for IMS service. In order to progress the study in SA2 as to the feasibility of this, CN1 is pleased to provide SA2 with the information requested in the LS:

The SIP protocol requires various different inputs at the mobile terminal. Such inputs to the protocol could be from one of three sources:

- Fields stored in the UICC;
- fields stored in the mobile equipment (including those allocated by the network, e.g. IP address, system information, etc); or
- fields entered by the user.

At the present point in time CN1 can list the various inputs to SIP that it has specified in 24.228 and 24.229, but for some fields, cannot categorically say from which source that input is taken. The following is a list of inputs and the current assumption/best guess at from where the value of each field is obtained (It should be noted that this list is by no means exhaustive, but it does try to detail the more important inputs to SIP):

Private User Identity – *it is assumed that this is* ***stored on the UICC****, although for access independence it may be possible for the operator to provide the user with some other means of entering the private ID.*

Public User Identity – *it is assumed that (as per 23.228) at least one public identity will be* ***stored on the UICC****. It is CN1's opinion that public IDs could also be stored in the user equipment or be entered by the user.*

Alias – *CN1 assumes that it may be possible for the user to enter an alias e.g. to be displayed as a CLI or dial-back number.*

Cell ID – *This field shall only be obtained from the user equipment.*

Visited Network Identifier – *The assumption is that this field will be inserted by the P-CSCF.*

Home Network Domain – *It is assumed that this field will be* ***stored on the UICC****.*

Event packages – *It may be necessary for a terminal to have access to certain events to which it must subscribe. It is currently assumed that this information will be stored in the user equipment*

Security Keys/Algorithms – *CN1 has not yet considered where this information will be stored and awaits input from SA3, although it is envisaged that* ***the UICC may be impacted****.*

CN1 can also inform SA2 that interested delegates are happy to engage in a joint discussion with SA2 on this matter, at the co-located meetings in Cancun, 26th – 30th November 2001.

3GPP TSG-CN1 Meeting #21 ***Tdoc N1-012041***

Cancun, Mexico, 26.- 30. November 2001 **was *Tdoc N1-011963***

Title: Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem

Source: CN1

To: TSG_SA WG1

Cc: TSG_SA WG2, TSG_SA WG3

Response to: LS (S1-011190 → N1-011942) on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem from TSG SA WG1.

Contact Person:
Name: Keith Drage
Tel. Number: +44 1793 776249
E-mail Address: drage@lucent.com

Attachments: None

---

1. Overall Description:

In their incoming liaison statement, SA1 asked:

> **SA1** has received and reviewed CN1's liaison N1-011313. **SA1 reasserts the importance of user privacy and anonymity and prefers that the use of IPv6 not reveal additional information about the user's location**, e.g., that the user may be in a location other than his home PLMN.
>
> At the same time, SA1 does not have a good feel for just how serious a problem this is for user security, or how much complexity it would add to the specifications. SA1 does believe that this requirement is not mandatory for Release 5, especially if it threatens the timeliness of the Release 5 schedule. At the same time, if the complexity of adding this in Release 6, if required, were significantly greater than starting with it in Release 5, then SA1 would reconsider the advisability of its inclusion as a service requirement.
>
> SA1 would like specific feedback from CN1 on these complexity concerns.

CN1 identifies that there are a number of architectural solutions that would resolve this problem, each with their own problems of complexity and compatibility. These solutions would each require further investigation within both SA2 and CN1 before adoption. These are not in any order of precedence.

1. Where either the UA or the home network on behalf of the user may require privacy or anonymity, then provide the GGSN in the home network. This would result in the user always having an IPv6 address allocated by the home network, and therefore when the user roamed, there would be no change in IPv6 address for that user, and therefore no indication of change in location. This is a valid option within Release 5, and is determined by information placed in the USIM by the network operator. It is not envisaged that it would be feasible to change to a home network GGSN on a per-call basis. This solution provides a certain degree of privacy (e.g., still the IPv6 address may reveal the location of the user within a certain geographical area within the operator's network). This mechanism has the disadvantage that all the bearer paths also get routed via the home network, rather than being transferred directly between the two roaming networks.
2. Use a protocol such as mobile IP. This can be regarded as impractical given the decision to base the IP transport on GPRS.
3. Provide an anonymiser function. This entity acts as a network address translator, and needs to exist on both the signalling path and on the bearer path. Such functionality is not intended to be specified by IETF for IPv6. Based on S-CSCF decision, this could be inserted in similar manner to that currently being investigated for the MRFC / MRFP. However, it does not exist in the SA2 architecture at this point, and therefore it is not feasible to include in Release 5. This entity could be in the home network, or any other network, but presumably would have to be in the home network to give location privacy, unless some means of allocating addresses to the anonymiser itself is defined that does not identify the location of the

anonymiser. This mechanism therefore has the disadvantage that all the bearer paths also get routed via the home network, rather than being transferred directly between the two roaming networks.

2. Actions:

For information, answer to a request.

3. Date of Next CN1 Meetings:

CN1_SIP-adhoc	14th – 18th January 2002	Phoenix, USA.
CN1_22	28th Jan.– 1st February 2002	Sophia Antipolis, France
CN1_22bis	19th – 21st February 2002	?

3GPP TSG-CN1 Meeting #21 ***Tdoc N1-012044***

Cancun, Mexico, 26.- 30. November 2001

Title: Liaison Statement on Addition of section " Conditions for IOV reset " to 09.95

Source: TSG CN1

To: TSG GERAN, TSG GERAN-WG1

Cc:

Response to: -

Contact Person:

Name: Roland Gruber

Tel. Number: +49 89 722 46392

E-mail Address: roland.gruber@mch.siemens.de

Attachments: N1-011959, N1-011960: *09.95 CRs " Conditions for IOV reset "* for endorsement
N1-011969, N1-011847: *04.64 CRs " Conditions for IOV reset "* for information

---

1. Overall Description:

During the Cn1#21 meeting it was spotted, that two different mobile LLC implementations have been identified for a GPRS R97 mobile for the case that the same authentication triplets were used twice by the network. In consequence the ciphered data could not be de-ciphered by the receiver.

2. Actions:

To TSG GERAN, TSG GERAN-WG1**group.**

ACTION:
TSG CN1 has agreed CRs on 09.95 for R97 and R98, in order to publish the problem and propose a solution. As 09.95 is under the responsibility of TSG GERAN respectively TSG GERAN-WG1 TSG CN1 would like to ask TSG GERAN to endorse the attached CRs and to assign CR numbers.

3. Date of Next CN1 Meetings:

CN1_SIP-adhoc	14th – 18th January 2002	Phoenix, USA.
CN1_22	28th Jan.– 1st February 2002	Sophia Antipolis, France
CN1_22bis	19th – 21st February 2002	?

CR-Form-v3

CHANGE REQUEST

⌘ **09.95** **CR** **A00?** ⌘ rev **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network X

Title:	⌘	Conditions for IOV reset
Source:	⌘	Siemens AG
Work item code:	⌘	GPRS
Date:	⌘	30th Nov. 2001
Category:	⌘	**A**
Release:	⌘	R98

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	IOT tests showed, that the term "change of Kc" was interpreted different by some manufactures, in case the same triplet were used twice subsequently by the network.
Summary of change:	⌘	The problem of unsyncron LLC peer entities is described and as solution the usage of the explixit IOV assignemnt via a XID exchange is proposed.
Consequences if not approved:	⌘	No solution for the case of different MS and SGSN implementation with the consequence that the ciphered data could not be de-ciphered by the receiver.

Clauses affected:	⌘	5.4 (new)
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

.

5.4 Conditions for IOV reset

5.4.1 Justification

It was found that the term "change of Kc" used in 3GPP TS 04.64 sec. 8.9.2 was interpreted differently.

Two different mobile implementations have been identified for a GPRS R98 mobile for the case that the same authentification triplets were used twice by the network:

a) the MS does not reset the IOV value to its default value, but keeps the current value;

b) the MS resets the IOV value to its default value.

5.4.2 Solution

TSG-CN1 Meeting #21has agreed that only the behaviour described in 5.4.1 a) is correct and has clarified this behaviour in the corresponding CR 04.64 A155.

5.4.3 Implementation requirements

All new GPRS mobiles shall support the correct behaviour of the IOV handling descibed above within four months of the relevant specification (04.64 v7.4.0) being published by 3GPP.

5.4.4 Support of Legacy mobiles

After the assignment of the same Kc value, in order to avoid different IOV values in the SGSN and the legacy mobile station, the SGSN may negotiate a random IOV value, after the authentification procedure is completed.

CR-Form-v3

CHANGE REQUEST

⌘ **09.95** **CR** **A00?** ⌘ rev **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network X

Title:	⌘	Conditions for IOV reset
Source:	⌘	Siemens AG
Work item code:	⌘	GPRS
Date:	⌘	30th Nov. 2001
Category:	⌘	**F**
Release:	⌘	R97

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	IOT tests showed, that the term "change of Kc" was interpreted different by some manufactures, in case the same triplet were used twice subsequently by the network.
Summary of change:	⌘	The problem of unsyncron LLC peer entities is described and as solution the usage of the explixit IOV assignemnt via a XID exchange is proposed.
Consequences if not approved:	⌘	No solution for the case of different MS and SGSN implementation with the consequence that the ciphered data could not be de-ciphered by the receiver.

Clauses affected:	⌘	5.4 (new)
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

.

5.4 Conditions for IOV reset

5.4.1 Justification

It was found that the term "change of Kc" used in 3GPP TS 04.64 sec. 8.9.2 was interpreted differently.

Two different mobile implementations have been identified for a GPRS R97 mobile for the case that the same authentification triplets were used twice by the network:

a) the MS does not reset the IOV value to its default value, but keeps the current value;

b) the MS resets the IOV value to its default value.

5.4.2 Solution

TSG-CN1 Meeting #21has agreed that only the behaviour described in 5.4.1 a) is correct and has clarified this behaviour in the corresponding CR 04.64 A154.

5.4.3 Implementation requirements

All new GPRS mobiles shall support the correct behaviour of the IOV handling descibed above within four months of the relevant specification (04.64 v6.10.0) being published by 3GPP.

5.4.4 Support of Legacy mobiles

After the assignment of the same Kc value, in order to avoid different IOV values in the SGSN and the legacy mobile station, the SGSN may negotiate a random IOV value, after the authentification procedure is completed.

3GPP TSG-CN1 Meeting #21 ***Tdoc N1-011847***

Cancun, Mexico, 26 – 30 November 2001

CR-Form-v4

CHANGE REQUEST

⌘ **04.64** **CR** **A155** ⌘ ev ⌘ Current version: **7.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Conditions for IOV reset
Source:	⌘	Siemens AG
Work item code:	⌘	GPRS
Date:	⌘	29.11.01
Category:	⌘	**A**
Release:	⌘	R98

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	IOT tests showed, that the term "change of Kc" was interpreted different by some manufactures, in case the same triplet were used twice subsequently by the network.
Summary of change:	⌘	It is clarified that the conditions to reset the IOV value to is set to default is only applicable, if the value of the Kc is different.
Consequences if not approved:	⌘	Different MS and SGSN implementation with the consequence that the ciphered data could not be de-ciphered by the receiver.

Clauses affected:	⌘	8.9.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

8.9.2 Input Offset Value (IOV)

The Input Offset Value (IOV) is an LLC layer parameter used for ciphering. IOV is a random 32 bit value, generated by the SGSN. See also annex A.

The value for IOV can be different for I frames and UI frames. IOV-UI is IOV for UI frames. IOV-I is IOV for I frames.

The default values of IOV are given in **Error! Reference source not found.**. The following rules apply to default IOV values:

- After a change of Kc to a different value, negotiation of IOV-I may be omitted and the default value applied. If ABM is re-established for an LLE, and Kc is not changed to a different value since ABM was last (re-)established for this LLE, then a random IOV-I value shall be negotiated.
- After a change of Kc to a different value, negotiation of IOV-UI may be omitted and the default value applied. If the unconfirmed send state variable V(U) is reset for an LLE, and Kc is not changed to a different value since V(U) was last reset for this LLE, then a random IOV-UI value shall be negotiated.

3GPP TSG-CN1 Meeting #21

Tdoc N1-011969
revised Tdoc N1-011846

Cancun, Mexico, 26 – 30 November 2001

CR-Form-v4

CHANGE REQUEST

⌘ **04.64** **CR** **A154** ⌘ ev **1** ⌘ Current version: **6.9.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Conditions for IOV reset
Source:	⌘	Siemens AG
Work item code:	⌘	GPRS
Date:	⌘	29.11.01
Category:	⌘	**F**
Release:	⌘	R97

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	IOT tests showed, that the term "change of Kc" was interpreted different by some manufactures, in case the same triplet were used twice subsequently by the network.
Summary of change:	⌘	It is clarified that the conditions to reset the IOV value to is set to default is only applicable, if the value of the Kc is different.
Consequences if not approved:	⌘	Different MS and SGSN implementation with the consequence that the ciphered data could not be de-ciphered by the receiver.

Clauses affected:	⌘	8.9.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

8.9.2 Input Offset Value (IOV)

The Input Offset Value (IOV) is an LLC layer parameter used for ciphering. IOV is a random 32 bit value, generated by the SGSN. See also annex A.

The value for IOV can be different for I frames and UI frames. IOV-UI is IOV for UI frames. IOV-I is IOV for I frames.

The default values of IOV are given in Table 9. The following rules apply to default IOV values:

- After a change of Kc to a different value, negotiation of IOV-I may be omitted and the default value applied. If ABM is re-established for an LLE, and Kc is not changed to a different value since ABM was last (re-)established for this LLE, then a random IOV-I value shall be negotiated.

- After a change of Kc to a different value, negotiation of IOV-UI may be omitted and the default value applied. If the unconfirmed send state variable V(U) is reset for an LLE, and Kc is not changed to a different value since V(U) was last reset for this LLE, then a random IOV-UI value shall be negotiated.

3GPP TSG-CN1 Meeting #21 ***Tdoc N1-012050***

Cancun, Mexico, 26.- 30. November 2001

Title: **LS on Interworking between 3GPP UE (IPv6 only) and SIP device external to IMS (IPv4 only)'**

Source: **TSG CN WG1**

To: **TSG SA WG2**

cc: **TSG CN WG3**

Date: **30 November 2001**

Contact Person:
Name: **Gábor Bajkó *(Nokia)***
E-mail Address: **Gabor.Bajko@nokia.com**
Tel. Number: **+36 20 9849259**

Attachement: N1-011884, N3-010572

---

1. Overall Description:

TSG CN WG3 and TSG CN WG1 have started to work out solutions for the interworking scenarios between an IMS UE (only mandated to support IPv6) and SIP terminals external to the IMS network (having support for IPv4 only). The WGs have made efforts to find solutions which have less impact to the architecture.

The solution outlined below has been endorsed by TSG CN WG3 and added to the informative annex of TS 29.162:

- There is a need for a NAT-PT device that is able to translate the IP headers between different IP protocols and able to provide IPv4 addresses from its pool for temporary use, when requested
- There is a need for a new functionality in IMS for IPv4/IPv6 interworking purposes on SIP control plane
- There is a need for a control protocol between the network element providing the new functionality and the NAT-PT for the purpose of communication between the two entities. A suitable protocol candidate is e.g. MEGACO.
- There is a need to support DNS ALG functionality in the IMS local name server

As the solution has architectural impacts, TSG CN WG1 has noted the proposed solution and would like to kindly ask TSG SA WG2's opinion in this matter.

2. Actions:

TSG SA WG2 is kindly asked to provide an architectural solution to the problem above, noting the described solution.

3. Date of Next TSG CN WG1 Meetings:

CN1 SIP ad-hoc	14 – 18 January 2002	Phoenix, USA.
CN1 #22	28 Jan. – 1 Feb 2002	Sophia Antipolis, France.

Date of Next TSG CN WG3 Meeting:

CN3 #21	28 Jan. – 1 Feb 2002	Sophia Antipolis, France.

3GPP TSG-CN-WG1, Meeting #21
26-30 November 2001,
Cancun, MX

Tdoc N1-011884

Agenda Item: 8.3

WI / Topic: Interworking

Source: Nokia

Title: Interworking between 3GPP UE (IPv6 only) and external SIP device (IPv4 only)'
Effected Specifications / Releases: 24.229, CN3 TSs

Document for: Discussion

Date: 2001-11-20

---

1 Problem statement

In 3GPP Rel5 the terminals shall use IPv6 (exclusively) when communicating with IMS.

As the timeframe for changing/upgrading the current IPv4 devices on the Internet to IPv6 is difficult to foresee, it is assumed that there will be a need for a session between a SIP-client using IPv4 (sitting on the Internet or a corporate network) and a 3G mobile terminal using IPv6, and for such a call to succeed the network needs to provide support for complex translation mechanisms.

The interworking is not limited to simple IP protocol translation (between v4 and v6) since applications like SIP include transport addresses (IP address and port number) in the packet payload to establish new media or data connections.

SIP is a protocol used for the initiation, modification, and termination of sessions. As a core part of its functionality, SIP carries the ports, IP addresses and domain names needed to describe the sessions it controls. There are three issues to be considered when setting up and controlling multimedia sessions with SIP through NAT-like devices:

- conveying the SIP messages themselves through these devices and assure that subsequent requests are correctly routed on the same path as the initial requests were routed.
- conveying the SIP-initiated media session streams through these devices.

2 IPv4/IPv6 translation mechanisms/protocols made available by the IETF community

In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic.

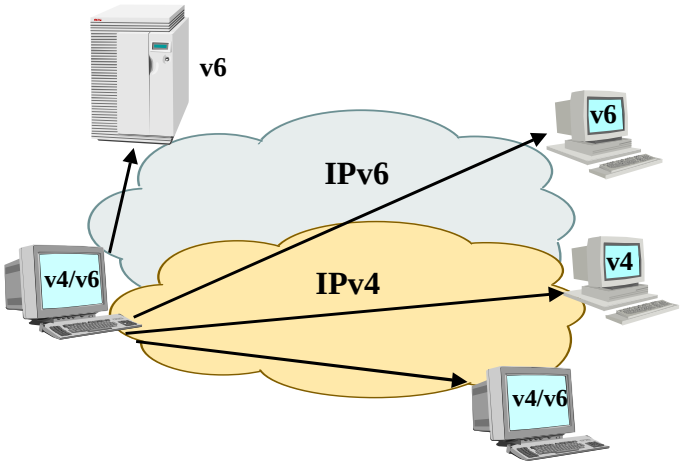
Once the IP addresses of the end points have been determined, appropriate routing mechanisms are necessary to send IP packets back and forth. If both the sender and the recipient have standard IPv6 addresses and direct connections to an IPv6 backbone, routing is

straightforward. If they can reach each other only over an IPv4 network, IPv4 encapsulation is necessary while traversing the IPv4 part of the network. If each end-host supports a different version of IP, then a protocol translator or gateway is needed between them.

IPv6 hosts and routers will need to retain backward compatibility with IPv4 devices for an extended time period (possibly years or even indefinitely) and will probably have the option of retaining their IPv4 addressing. To accomplish these goals, IPv6 transition relies on several special functions that have been built into the IPv6 standards work, including dual-stack hosts and routers; transition mechanisms which temporarily assign an IPv4 address to an IPv6 host; tunnelling IPv6 via IPv4 or convert between IPv6/IPv4 headers.

2.1. Dual stack hosts

Dual stack hosts have both protocol stacks and have an IPv4 address and at least one globally routable IPv6 address.



Once a few nodes have been converted to IPv6, there is the strong possibility that these nodes will require continued interaction with existing IPv4 nodes. This is accomplished with the dual-stack IPv4/IPv6 approach. When running a dual IPv4/IPv6 stack, a host can access both IPv4 and IPv6 resources. Routers running both protocols can forward traffic for both IPv4 and IPv6 end nodes. Dual Stack machines can use totally independent IPv4 and IPv6 addresses, or they can be configured with **an IPv6 address that is IPv4 compatible**.

2.1.1. IPv4 compatible IPv6 addresses

The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that utilize this technique are assigned special IPv6 unicast addresses that carry an IPv4 address in the low-order 32-bits. This type of address is termed as “IPv4 - compatible IPv6 address”:

80 bits	16 bits	32 bits
Network prefix	0000	IPv4 address

A second type of IPv6 address which holds an embedded IPv4 address is also defined. This address is used to represent the addresses of IPv4-only nodes (those nodes, which do not have a dual protocol stack and do not support IPv6) as IPv6 addresses. This type of address is termed as "IPv4 - mapped IPv6 address":

80 bits	16 bits	32 bits
Network prefix	FFFF	IPv4 address

A third type of IPv6 address which holds an embedded IPv4 address is utilized by some transition mechanisms. The “IPv4 - translated” address is used by an IPv6-enabled node when addressing an IPv4 node through an IPv6 - IPv4 protocol translator.

64 bits	16 bits	16 bits	32 bits
Network prefix	FFFF	0000	IPv4 address

2.2. IPv6 over IPv4 tunnelling

In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic. Tunneling provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic.
To be able to carry an IPv6 packet over an IPv4 backbone, an IPv4 header is added to the packet.
The value of the protocol field in the appended IPv4 header will be set to 41, to point that the packet contain an encapsulated packet.

There are two tunneling techniques:
- **automatic**: the encapsulating node determines the endpoint of the tunnel using dynamic routing
- **configured**: the encapsulating node determines the endpoint of the tunnel from an explicit configuration

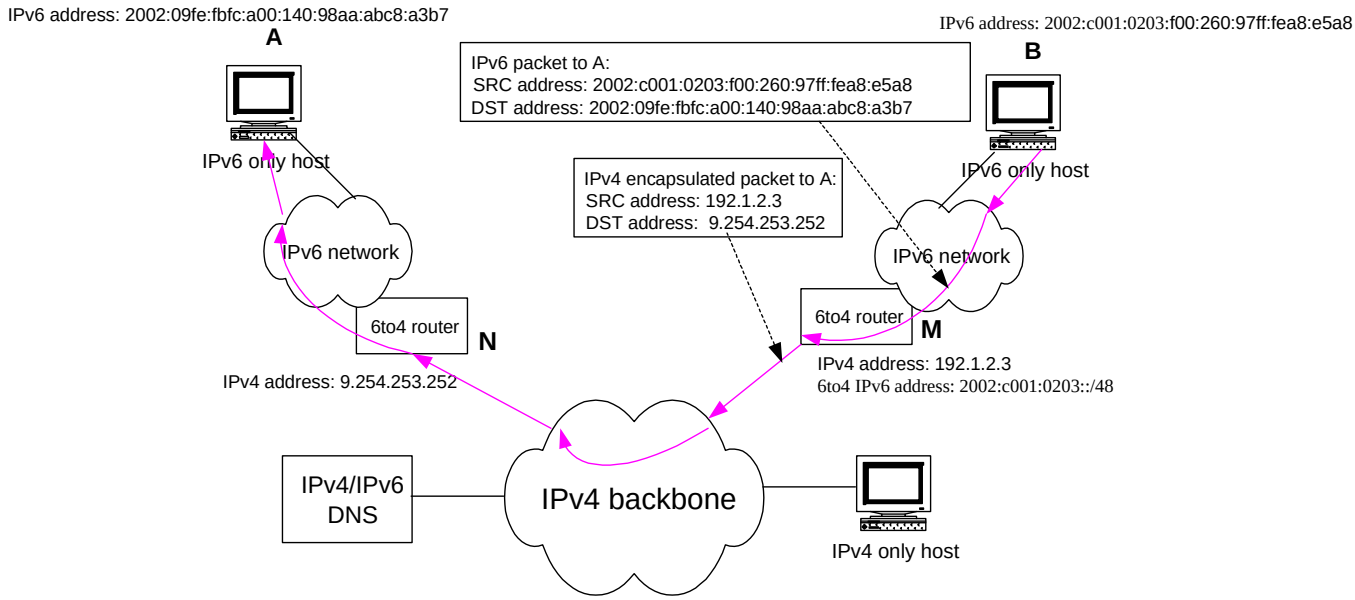
The underlying mechanism is the same in both tunneling techniques:
- the encapsulating node (tunnel entry point) creates an encapsulating IPv4 header and transmits the encapsulated packet.
- the exit node of the tunnel (the decapsulating node) receives the encapsulated packet, removes the IPv4 header and processes the resulted IPv6 packet

Tunneling techniques are usually classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel.
Tunneling can be done in a variety of ways:
- Host-to-Host: Ipv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves
- Router-to-Host: IPv6/IPv4 routers can tunnel IPv6 packets to their final destination
- Router-to-Router: IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves

- Host-to-Router: IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure

If the tunnel endpoint is the destination itself, the tunnel endpoint can be determined from the destination IPv6 address of the packet - the packet can be encapsulated automatically – this is called **automatic tunneling**
If the tunnel endpoint is an intermediate router which must decapsulate the IPv6 packet and forward to its final destination, the tunnel endpoint must be determined from configuration – this is called **configured tunneling**

2.2.1 Example of automatic encapsulation

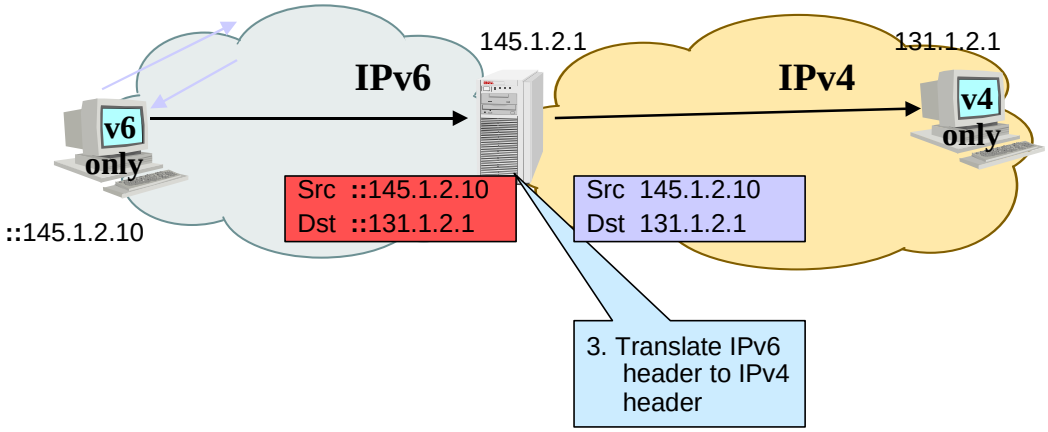


In the figure above an IPv6-only node **B** having a 64-bit interface identifier "260:97ff:fea8:e5a8" and a 16-bit site-level aggregator "f00" is connected to the IPv4 Internet via a dual stack 6to4 router **M**.. **M** has a publicly routable IPv4 address ”192.1.2.3" or ”c001:0203" in hexadecimal notation. The 6to4 address of **B** (a valid IPv6 address in fact) is "2002:c001:0203:f00:260:97ff:fea8:e5a8”. Similarly, the IPv6 only node **A** is connected to the IPv4 Internet via the dual stack 6to4 router **N**, which has a publicly routable IPv4 address “9.254.251.252” or “09fe:fbfc”. The 6to4 address of **A** is “2002:09fe:fbfc:a00:140:98aa:abc8:a3b7”.
When a sending host or router (such as **B** or **M**) sees a packet with the destination address of **A**, it first extracts the embedded IPv4 address (in this case ”09fe:fbfc"), and encapsulates the IPv6 packet in an IPv4 packet destined for this embedded address. When the 6to4 router **N** receives this packet, it decapsulates it, and forwards it to **A** using native IPv6 routing within the IPv6 stub network.
This mechanism is an alternative solution for automatic encapsulation. Nodes wishing to communicate using 6to4 addresses must satisfy the following restrictions:
• each 6to4 router must have at least one publicly routable IPv4 address. The so called "6to4" automatic encapsulation mechanism reduces this requirement to just a single publicly routable IPv4 address per site.
each node behind a 6to4 router with the “a.b.c.d” IPv4 address must have an IPv6 address of 2002:ab:cd:SLA:I_faceID, with SLA and I_faceID of the site.

2.3. Protocol Translators

2.3.1. Stateless IP and ICMP translation mechanism

The temporary IPv4 address will be used as an IPv4-translated IPv6 address and the packets will travel through a stateless IP/ICMP translator that will translate the packet headers between IPv4 and IPv6 and translate the addresses in those headers between IPv4 addresses on one side and IPv4-translated IPv6 addresses or IPv4-mapped IPv6 addresses on the other side.
When the IPv4-to-IPv6 translator receives an IPv4 datagram addressed to a destination that lies outside of the attached IPv4 island, it translates the IPv4 header of that packet into an IPv6 header. It then forwards the packet based on the IPv6 destination address. The original IPv4 header on the packet is removed and replaced by an IPv6 header. For ICMP messages all packets need to have the Type value translated and for ICMP error messages the included IP header also needs translation.
When the IPv6-to-IPv4 translator receives an IPv6 datagram addressed to an IPv4-mapped IPv6 address, it translates the IPv6 header of that packet into an IPv4 header. It then forwards the packet based on the IPv4 destination address. The original IPv6 header on the packet is removed and replaced by an IPv4 header. For ICMP messages all packets need to have the Type value translated and for ICMP error messages the included IP header also needs translation.

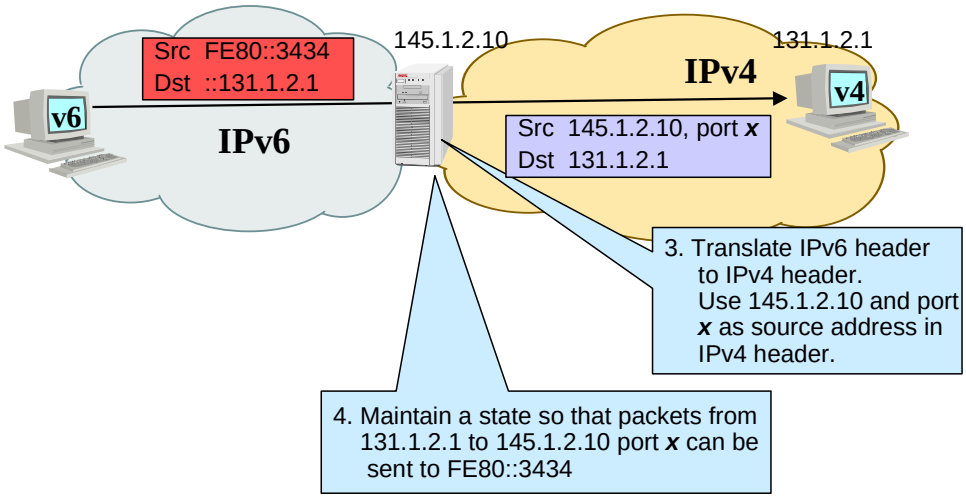


The SIIT specification does not cover how an IPv6 node can acquire a temporary IPv4 address from the pool of IPv4 addresses and how such a temporary address be registered in the DNS.

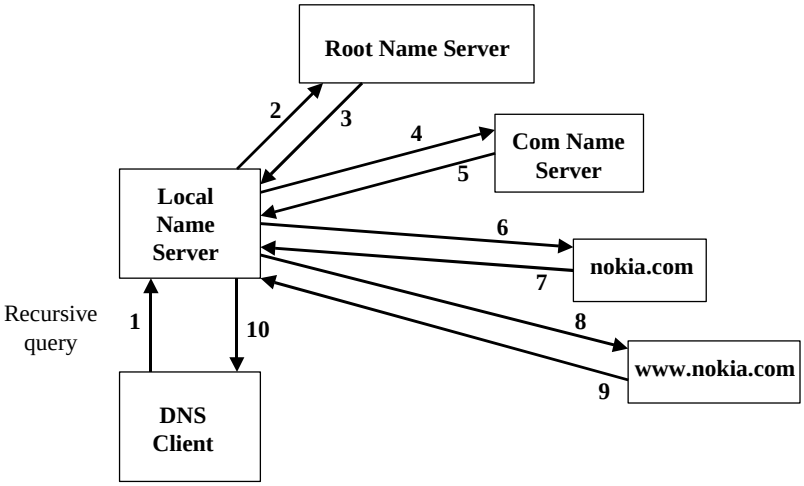
2.3.2. Network Address and Protocol Translator

NAT-PT is an IPv4-to-IPv6 transition mechanism which attempts to provide transparent routing to end-nodes in IPv6 realm trying to communicate with end-nodes in IPv4 realm and vice versa. This is achieved using a combination of Network Address Translation and Protocol Translation. This mechanism does not mandate dual stack in end nodes and does not have any special routing requirement neither requires tunneling support. This mechanism is based on NAT-like address translation and IP header conversion as described in [SIIT].

NAT-PT uses a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries. The IPv4 addresses are assumed to be globally unique. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing for the datagrams traversing between address realms. This requires no changes to end nodes and IP packet routing is completely transparent to end nodes. It does, however, require NAT-PT to track the sessions it supports and mandates that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router.



3 DNS Translation



The figure above shows how a recursive DNS query is made. In case the DNS Client has IPv6 protocol stack only, it will make a DNS query to find out the IP address of www.nokia.com , asking for a AAAA or A6 type record entry. In case the local name server does not receive a valid IPv6 address in response 9 (as www.nokia.com does not have an IPv6 address configured), the local name server will need to make a new DNS query for type A record. Before delivering the IPv4 address to the client, it has to translate it to an IPv6 address (IPv4 mapped IPv6), as the DNS client is IPv6 only. This functionality of the local name server is called DNS ALG (Application Level Gateway).

4 Interworking on SIP control plane

An example of SIP request is shown below:

```
INVITE sip:user2@home1.net
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip: pcscf1.visited1.net
Route: sip: icscf1@home1.net
Supported: 100rel
From: sip: user1@home1.net
To: sip: user2@home1.net
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Contact: Blaster@home1.net
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 3400 RTP/AVP 98 99
a=qos:mandatory sendrecv
a=rtpmap:98 H261
a=rtpmap:99:MPV
m=video 3402 RTP/AVP 98 99
a=rtpmap:98 H261
a=rtpmap:99:MPV
a=qos:mandatory sendrecv
m=audio 3456 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
m=audio 3458 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
```

The headers in **bold** are part of the SIP message, the rest is the SDP payload. The headers in **red** are used for routing the SIP requests and their responses. The address found in the Contact: header is used for sending subsequent request to.

Before delivering the message to the recipient, the S-CSCF shall recognize whether the final destination of the message (as far as could be seen from the DNS query – at DNS Zone level) is an IPv6 host or an IPv4 host.

There are two possible cases:

1) S-CSCF is dual stack
2) S-CSCF has IPv6 stack only

1) In case S-CSCF is dual stack, it shall:

- send the message out using the protocol version which corresponds to the one used by the destination (as published at the DNS Zone level) in case it is a one-shot message (no response is coming to it). In all other cases it shall:

- insert its own IP address into headers like Via, Record Route, Path, etc. which are used for routing. The version of IP address shall be the same as the version of IP the first hop outside the domain of the S-CSCF uses.

- in case the Contact: header field contains an IP address of which the protocol version is different than the one of the destination (at DNS Zone level), then change the address to its own address (protocol version to match to the destination's one)

In case an I-CSCF is used for hiding, then the I-CSCF must also be dual stack.

2) In case S-CSCF has IPv6 only stack, then it shall:

- ask for an IPv4 address from a NAT-PT developed in the network by using a control protocol. A possible example is to use a small subset of the MEGACO protocol.

- the local name server of the network shall have DNS ALG support

- implement the steps listed above under 1)

- The message shall be routed through a NAT-PT which needs to translate the packet's header.

5 Interworking on SIP user plane

In order for the two endpoints using different version of IP addresses to be able to communicate the S-CSCF has to change the IP address found in the SDP payload of the SIP request and its response.

When an IPv4 host initiates the communication with an IPv6 host, the IPv4 address found in the SDP payload has to be changed to an IPv6 mapped IPv4 address.
When an IPv6 host initiates the communication with an IPv4 host, the IPv6 address found in the SDP payload has to be changed to an IPv4 address which has to be acquired from a device able to provide such an address when requested (NAT-PT). A binding has to be made in NAT-PT in order to enable the communication (NAT functionality).

An example for a control protocol which can be used to ask and provide such addresses between S-CSCF and NAT-PT is MEGACO [RFC3015]. Below an example is shown on how to use MEGACO between S-CSCF and NAT-PT for such a communication:

Step 1: NAT-PT registering for MEGACO control with the CSCF

The NAT-PT shall be able to register with the CSCF for MEGACO-control. This registration is conducted by means of sending a ServiceChange command, and the CSCF may accept the registration attempt with a ServiceChangeAck reply.

- NAT-PT to CSCF:

```
MEGACO/1 [AB.CD.EF::12.34.99]
                          //IPv6 address of NAT-PT
Transaction = 9999 {
    Context = - {
        ServiceChange = ROOT {Services {
            Method=Restart,
            ServiceChangeAddress=55555, Profile=ResNAT/1} } } }
```

- CSCF sends a reply to NAT-PT accepting the registration:

```
MEGACO/1 [AB.CD.EF::12.34.56]:55555
                                    //IPv6 address of CSCF
Reply = 9999 {
   Context = - {ServiceChange = ROOT {
      Services {ServiceChangeAddress=55555, Profile=ResNAT/1} } } }
```

The NAT-PT realizes only ephemeral type of terminations, this also means that the TerminationID and the local transport address in the NAT-PT to be used for the session are allocated by the NAT-PT itself, and returned to the controlling CSCF in the reply message. The CSCF initiates the binding request in NAT-PT by sending an ADD command, and receives a TA from NAT-PT to be used for the session in the reply message.

Step 2: (case when an IPv6 device initiates a call to an IPv4 device) S-CSCF asks for an IPv4 address to replace the address in the SDP payload. It sends a MEGACO ADD command to the NAT-PT

```
MEGACO/1 [AB.CD.EF::12.34.56]:55555
Transaction = 50001 {
   Context = $ {
        Add = $ { Media {
              Stream = 1 {
                 LocalControl {Mode = SendReceive}}},
              Local {
v=0
c=IN IP4 $
m=audio $ RTP/AVP 4
a=ptime:30
              },
              Remote {
v=0
c=IN IP4 media-IP-address of UserA
//The media IP-address and media- port of UserA is received in the SDP part of the INVITE message
m=audio media-port RTP/AVP 4
a=ptime:30 }}}}}}
```

Step 3: NAT-PT answers to S-CSCF:
It also binds the provided IPv4 address with the IPv6 address in the ADD request.

```
MEGACO/1 [AB.CD.EF::12.34.99]:55555
Reply = 50001 {
   Context = 5000 {
        Add = 00001{
           Media {
                Stream = 1 {
                     Local {
v=0
c=IN IP4 111.111.111.1
//CSCF copies this media IP address and port into the SDP part of the INVITE message.
m=audio 1111 RTP/AVP 4 }}}}}}
```

8 Proposal

It is proposed to add the following text to the informational annex of CN3 TS:

3GPP TSG-CN-WG1, Meeting #21
26-30 November 2001,
Cancun, MX

Tdoc N1-011884

For IPv4/IPv6 interworking purposes it is proposed to have the following functionalities and interfaces with protocols in the IMS:

- A NAT-PT device able to translate the IP headers between different IP protocols and able to provide IPv4 addresses from its pool when required
- A control protocol between S-CSCF and NAT-PT for the purpose of communication between the two entities
- Use of MEGACO on the interface between S-CSCF and NAT-PT

The above requirements shall be optional for Rel5 with the purpose of making it mandatory in a later release.

It is proposed to add the following text to the informational annex of 24.229:

For IPv4/IPv6 interworking purposes it is proposed to have the following functionality as part of S-CSCF:

- A new functionality in S-CSCF which enables it to identify whether the endpoints willing to communicate have the same version of the IP protocol. It is assumed that the IMS UE will only have IPv6.

3GPP TSG-CN-WG1, Meeting #21
26-30 November 2001,
Cancun, MX

Tdoc N3-~~011884~~011572

Agenda Item: 8.3

WI / Topic: Interworking

Source: CN3

Title: Interworking between 3GPP UE (IPv6 only) and external SIP device (IPv4 only)'
Effected Specifications / Releases: 24.229, CN3 TSs

Document for: Discussion

Date: 2001-11-20

---

1 Problem statement

In 3GPP Rel5 the terminals shall use IPv6 (exclusively) when communicating with IMS.

As the timeframe for changing/upgrading the current IPv4 devices on the Internet to IPv6 is difficult to foresee, it is assumed that there will be a need for a session between a SIP-client using IPv4 (sitting on the Internet or a corporate network) and a 3G mobile terminal using IPv6, and for such a call to succeed the network needs to provide support for complex translation mechanisms.

The interworking is not limited to simple IP protocol translation (between v4 and v6) since applications like SIP include transport addresses (IP address and port number) in the packet payload to establish new media or data connections.

SIP is a protocol used for the initiation, modification, and termination of sessions. As a core part of its functionality, SIP carries the ports, IP addresses and domain names needed to describe the sessions it controls. There are three issues to be considered when setting up and controlling multimedia sessions with SIP through NAT-like devices:

- conveying the SIP messages themselves through these devices and assure that subsequent requests are correctly routed on the same path as the initial requests were routed.
- conveying the SIP-initiated media session streams through these devices.

2 IPv4/IPv6 translation mechanisms/protocols made available by the IETF community

In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic.

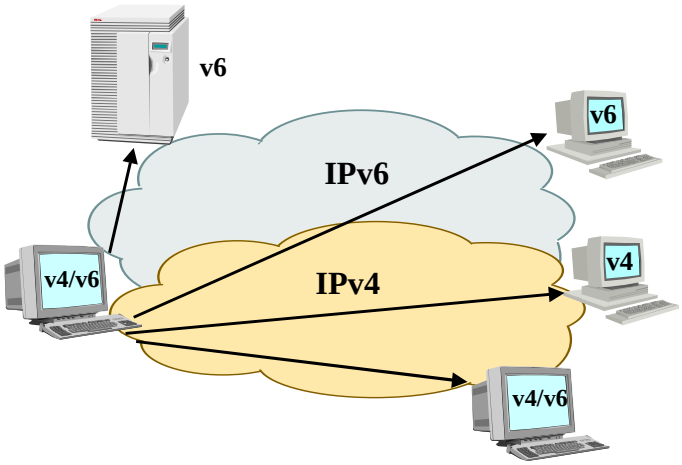
Once the IP addresses of the end points have been determined, appropriate routing mechanisms are necessary to send IP packets back and forth. If both the sender and the recipient have standard IPv6 addresses and direct connections to an IPv6 backbone, routing is

straightforward. If they can reach each other only over an IPv4 network, IPv4 encapsulation is necessary while traversing the IPv4 part of the network. If each end-host supports a different version of IP, then a protocol translator or gateway is needed between them.

IPv6 hosts and routers will need to retain backward compatibility with IPv4 devices for an extended time period (possibly years or even indefinitely) and will probably have the option of retaining their IPv4 addressing. To accomplish these goals, IPv6 transition relies on several special functions that have been built into the IPv6 standards work, including dual-stack hosts and routers; transition mechanisms which temporarily assign an IPv4 address to an IPv6 host; tunnelling IPv6 via IPv4 or convert between IPv6/IPv4 headers.

2.1. Dual stack hosts

Dual stack hosts have both protocol stacks and have an IPv4 address and at least one globally routable IPv6 address.



Once a few nodes have been converted to IPv6, there is the strong possibility that these nodes will require continued interaction with existing IPv4 nodes. This is accomplished with the dual-stack IPv4/IPv6 approach. When running a dual IPv4/IPv6 stack, a host can access both IPv4 and IPv6 resources. Routers running both protocols can forward traffic for both IPv4 and IPv6 end nodes. Dual Stack machines can use totally independent IPv4 and IPv6 addresses, or they can be configured with **an IPv6 address that is IPv4 compatible**.

2.1.1. IPv4 compatible IPv6 addresses

The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that utilize this technique are assigned special IPv6 unicast addresses that carry an IPv4 address in the low-order 32-bits. This type of address is termed as “IPv4 - compatible IPv6 address”:

80 bits	16 bits	32 bits
Network prefix	0000	IPv4 address

A second type of IPv6 address which holds an embedded IPv4 address is also defined. This address is used to represent the addresses of IPv4-only nodes (those nodes, which do not have a dual protocol stack and do not support IPv6) as IPv6 addresses. This type of address is termed as "IPv4 - mapped IPv6 address":

80 bits	16 bits	32 bits
Network prefix	FFFF	IPv4 address

A third type of IPv6 address which holds an embedded IPv4 address is utilized by some transition mechanisms. The “IPv4 - translated” address is used by an IPv6-enabled node when addressing an IPv4 node through an IPv6 - IPv4 protocol translator.

64 bits	16 bits	16 bits	32 bits
Network prefix	FFFF	0000	IPv4 address

2.2. IPv6 over IPv4 tunnelling

In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic. Tunneling provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic.
To be able to carry an IPv6 packet over an IPv4 backbone, an IPv4 header is added to the packet.
The value of the protocol field in the appended IPv4 header will be set to 41, to point that the packet contain an encapsulated packet.

There are two tunneling techniques:
- **automatic**: the encapsulating node determines the endpoint of the tunnel using dynamic routing
- **configured**: the encapsulating node determines the endpoint of the tunnel from an explicit configuration

The underlying mechanism is the same in both tunneling techniques:
- the encapsulating node (tunnel entry point) creates an encapsulating IPv4 header and transmits the encapsulated packet.
- the exit node of the tunnel (the decapsulating node) receives the encapsulated packet, removes the IPv4 header and processes the resulted IPv6 packet

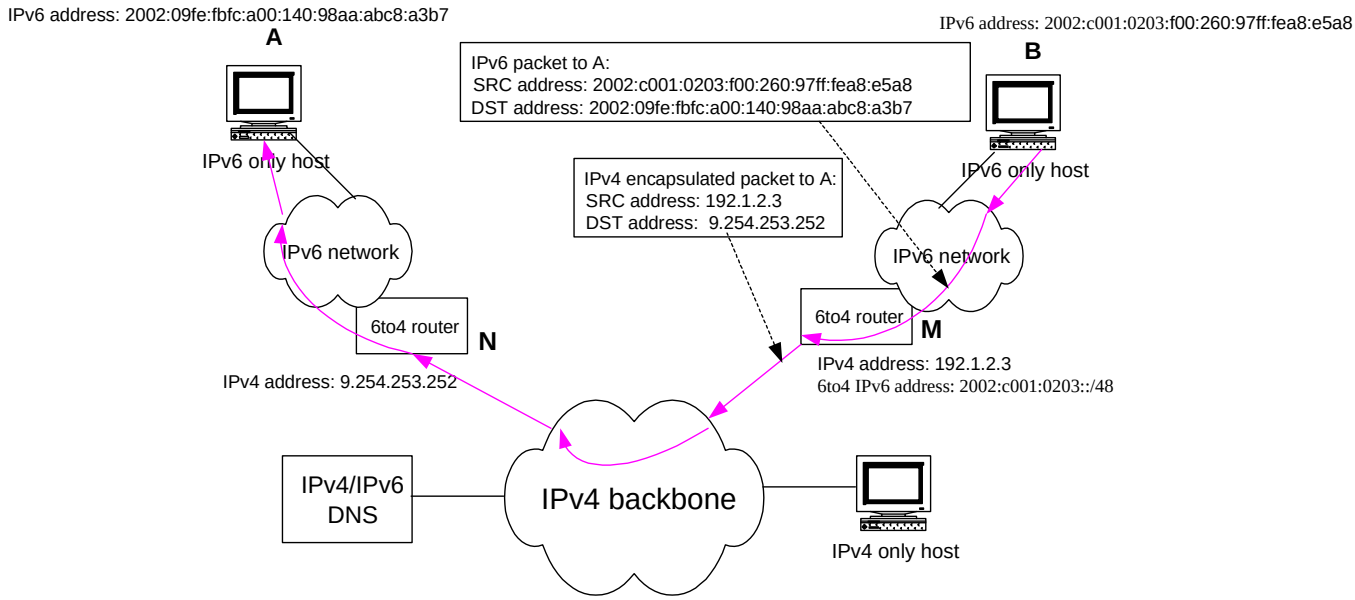
Tunneling techniques are usually classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel.
Tunneling can be done in a variety of ways:
- Host-to-Host: Ipv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves
- Router-to-Host: IPv6/IPv4 routers can tunnel IPv6 packets to their final destination
- Router-to-Router: IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves

- Host-to-Router: IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure

If the tunnel endpoint is the destination itself, the tunnel endpoint can be determined from the destination IPv6 address of the packet - the packet can be encapsulated automatically – this is called **automatic tunneling**

If the tunnel endpoint is an intermediate router which must decapsulate the IPv6 packet and forward to its final destination, the tunnel endpoint must be determined from configuration – this is called **configured tunneling**

2.2.1 Example of automatic encapsulation



In the figure above an IPv6-only node **B** having a 64-bit interface identifier "260:97ff:fea8:e5a8" and a 16-bit site-level aggregator "f00" is connected to the IPv4 Internet via a dual stack 6to4 router **M**.. **M** has a publicly routable IPv4 address ”192.1.2.3" or ”c001:0203" in hexadecimal notation. The 6to4 address of **B** (a valid IPv6 address in fact) is "2002:c001:0203:f00:260:97ff:fea8:e5a8”. Similarly, the IPv6 only node **A** is connected to the IPv4 Internet via the dual stack 6to4 router **N**, which has a publicly routable IPv4 address “9.254.251.252” or “09fe:fbfc”. The 6to4 address of **A** is “2002:09fe:fbfc:a00:140:98aa:abc8:a3b7”.

When a sending host or router (such as **B** or **M**) sees a packet with the destination address of **A**, it first extracts the embedded IPv4 address (in this case ”09fe:fbfc"), and encapsulates the IPv6 packet in an IPv4 packet destined for this embedded address. When the 6to4 router **N** receives this packet, it decapsulates it, and forwards it to **A** using native IPv6 routing within the IPv6 stub network.

This mechanism is an alternative solution for automatic encapsulation. Nodes wishing to communicate using 6to4 addresses must satisfy the following restrictions:

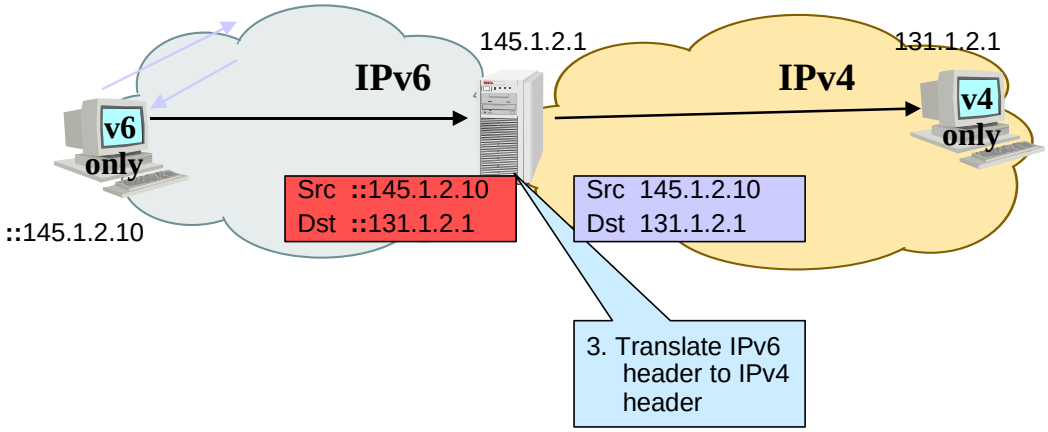
• each 6to4 router must have at least one publicly routable IPv4 address. The so called "6to4" automatic encapsulation mechanism reduces this requirement to just a single publicly routable IPv4 address per site.

each node behind a 6to4 router with the “a.b.c.d” IPv4 address must have an IPv6 address of 2002:ab:cd:SLA:I_faceID, with SLA and I_faceID of the site.

2.3. Protocol Translators

2.3.1. Stateless IP and ICMP translation mechanism

The temporary IPv4 address will be used as an IPv4-translated IPv6 address and the packets will travel through a stateless IP/ICMP translator that will translate the packet headers between IPv4 and IPv6 and translate the addresses in those headers between IPv4 addresses on one side and IPv4-translated IPv6 addresses or IPv4-mapped IPv6 addresses on the other side.
When the IPv4-to-IPv6 translator receives an IPv4 datagram addressed to a destination that lies outside of the attached IPv4 island, it translates the IPv4 header of that packet into an IPv6 header. It then forwards the packet based on the IPv6 destination address. The original IPv4 header on the packet is removed and replaced by an IPv6 header. For ICMP messages all packets need to have the Type value translated and for ICMP error messages the included IP header also needs translation.
When the IPv6-to-IPv4 translator receives an IPv6 datagram addressed to an IPv4-mapped IPv6 address, it translates the IPv6 header of that packet into an IPv4 header. It then forwards the packet based on the IPv4 destination address. The original IPv6 header on the packet is removed and replaced by an IPv4 header. For ICMP messages all packets need to have the Type value translated and for ICMP error messages the included IP header also needs translation.

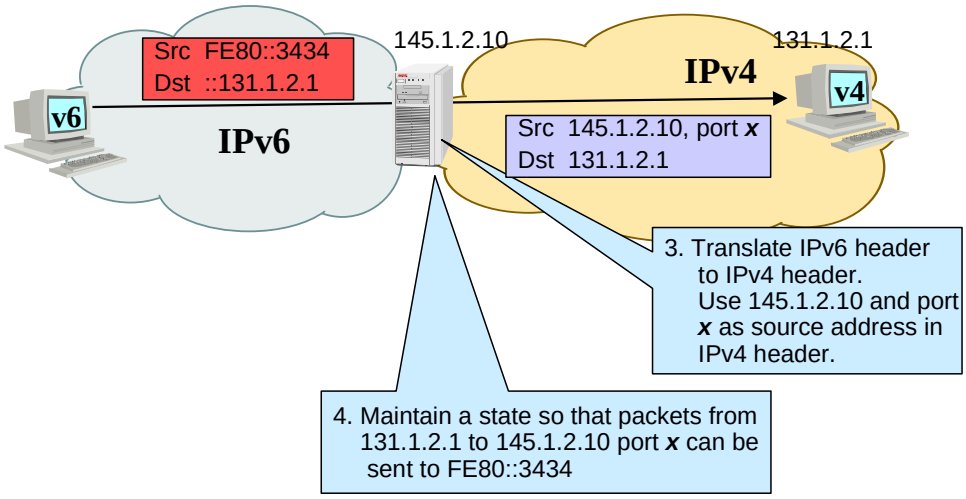


The SIIT specification does not cover how an IPv6 node can acquire a temporary IPv4 address from the pool of IPv4 addresses and how such a temporary address be registered in the DNS.

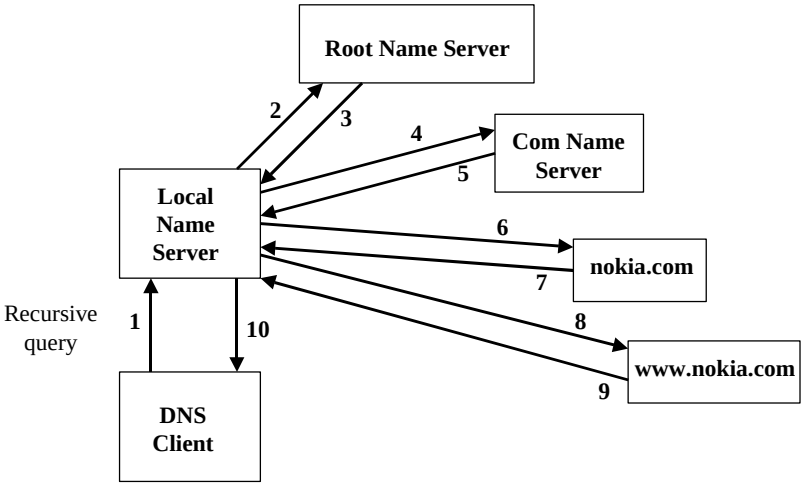
2.3.2. Network Address and Protocol Translator

NAT-PT is an IPv4-to-IPv6 transition mechanism which attempts to provide transparent routing to end-nodes in IPv6 realm trying to communicate with end-nodes in IPv4 realm and vice versa. This is achieved using a combination of Network Address Translation and Protocol Translation. This mechanism does not mandate dual stack in end nodes and does not have any special routing requirement neither requires tunneling support. This mechanism is based on NAT-like address translation and IP header conversion as described in [SIIT].

NAT-PT uses a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries. The IPv4 addresses are assumed to be globally unique. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing for the datagrams traversing between address realms. This requires no changes to end nodes and IP packet routing is completely transparent to end nodes. It does, however, require NAT-PT to track the sessions it supports and mandates that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router.



3 DNS Translation



The figure above shows how a recursive DNS query is made. In case the DNS Client has IPv6 protocol stack only, it will make a DNS query to find out the IP address of www.nokia.com , asking for a AAAA or A6 type record entry. In case the local name server does not receive a valid IPv6 address in response 9 (as www.nokia.com does not have an IPv6 address configured), the local name server will need to make a new DNS query for type A record. Before delivering the IPv4 address to the client, it has to translate it to an IPv6 address (IPv4 mapped IPv6), as the DNS client is IPv6 only. This functionality of the local name server is called DNS ALG (Application Level Gateway).

4 Interworking on SIP control plane

An example of SIP request is shown below:

```
INVITE sip:user2@home1.net
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Record-Route: sip: pcscf1.visited1.net
Route: sip: icscf1@home1.net
Supported: 100rel
From: sip: user1@home1.net
To: sip: user2@home1.net
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Contact: Blaster@home1.net
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
b=AS:64
t=907165275 0
m=video 3400 RTP/AVP 98 99
a=qos:mandatory sendrecv
a=rtpmap:98 H261
a=rtpmap:99:MPV
m=video 3402 RTP/AVP 98 99
a=rtpmap:98 H261
a=rtpmap:99:MPV
a=qos:mandatory sendrecv
m=audio 3456 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
a=qos:mandatory sendrecv
m=audio 3458 RTP/AVP 97 96 0 15
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 G726-32/8000
```

The headers in **bold** are part of the SIP message, the rest is the SDP payload. The headers in **red** are used for routing the SIP requests and their responses. The address found in the Contact: header is used for sending subsequent request to.

Before delivering the message to the recipient, the S-CSCF shall recognize whether the final destination of the message (as far as could be seen from the DNS query – at DNS Zone level) is an IPv6 host or an IPv4 host.

There are two possible cases:

1) S-CSCF is dual stack
2) S-CSCF has IPv6 stack only

1) In case S-CSCF is dual stack, it shall:

- send the message out using the protocol version which corresponds to the one used by the destination (as published at the DNS Zone level) in case it is a one-shot message (no response is coming to it). In all other cases it shall:

- insert its own IP address into headers like Via, Record Route, Path, etc. which are used for routing. The version of IP address shall be the same as the version of IP the first hop outside the domain of the S-CSCF uses.

- in case the Contact: header field contains an IP address of which the protocol version is different than the one of the destination (at DNS Zone level), then change the address to its own address (protocol version to match to the destination's one)

In case an I-CSCF is used for hiding, then the I-CSCF must also be dual stack.

2) In case S-CSCF has IPv6 only stack, then it shall:

- ask for an IPv4 address from a NAT-PT developed in the network by using a control protocol. A possible example is to use a small subset of the MEGACO protocol.

- the local name server of the network shall have DNS ALG support

- implement the steps listed above under 1)

- The message shall be routed through a NAT-PT which needs to translate the packet's header.

5 Interworking on SIP user plane

In order for the two endpoints using different version of IP addresses to be able to communicate the S-CSCF has to change the IP address found in the SDP payload of the SIP request and its response.

When an IPv4 host initiates the communication with an IPv6 host, the IPv4 address found in the SDP payload has to be changed to an IPv6 mapped IPv4 address.
When an IPv6 host initiates the communication with an IPv4 host, the IPv6 address found in the SDP payload has to be changed to an IPv4 address which has to be acquired from a device able to provide such an address when requested (NAT-PT). A binding has to be made in NAT-PT in order to enable the communication (NAT functionality).

An example for a control protocol which can be used to ask and provide such addresses between S-CSCF and NAT-PT is MEGACO [RFC3015]. Below an example is shown on how to use MEGACO between S-CSCF and NAT-PT for such a communication:

Step 1: NAT-PT registering for MEGACO control with the CSCF

The NAT-PT shall be able to register with the CSCF for MEGACO-control. This registration is conducted by means of sending a ServiceChange command, and the CSCF may accept the registration attempt with a ServiceChangeAck reply.

- NAT-PT to CSCF:

```
MEGACO/1 [AB.CD.EF::12.34.99]
                          //IPv6 address of NAT-PT
Transaction = 9999 {
    Context = - {
        ServiceChange = ROOT {Services {
            Method=Restart,
            ServiceChangeAddress=55555, Profile=ResNAT/1} } } }
```

- CSCF sends a reply to NAT-PT accepting the registration:

```
MEGACO/1 [AB.CD.EF::12.34.56]:55555
                                    //IPv6 address of CSCF
Reply = 9999 {
   Context = - {ServiceChange = ROOT {
      Services {ServiceChangeAddress=55555, Profile=ResNAT/1} } } }
```

The NAT-PT realizes only ephemeral type of terminations, this also means that the TerminationID and the local transport address in the NAT-PT to be used for the session are allocated by the NAT-PT itself, and returned to the controlling CSCF in the reply message. The CSCF initiates the binding request in NAT-PT by sending an ADD command, and receives a TA from NAT-PT to be used for the session in the reply message.

Step 2: (case when an IPv6 device initiates a call to an IPv4 device) S-CSCF asks for an IPv4 address to replace the address in the SDP payload. It sends a MEGACO ADD command to the NAT-PT

```
MEGACO/1 [AB.CD.EF::12.34.56]:55555
Transaction = 50001 {
   Context = $ {
        Add = $ { Media {
              Stream = 1 {
                 LocalControl {Mode = SendReceive}}},
              Local {
v=0
c=IN IP4 $
m=audio $ RTP/AVP 4
a=ptime:30
              },
              Remote {
v=0
c=IN IP4 media-IP-address of UserA
//The media IP-address and media- port of UserA is received in the SDP part of the INVITE message
m=audio media-port RTP/AVP 4
a=ptime:30 }}}}}}
```

Step 3: NAT-PT answers to S-CSCF:
It also binds the provided IPv4 address with the IPv6 address in the ADD request.

```
MEGACO/1 [AB.CD.EF::12.34.99]:55555
Reply = 50001 {
   Context = 5000 {
        Add = 00001{
           Media {
                Stream = 1 {
                     Local {
v=0
c=IN IP4 111.111.111.1
//CSCF copies this media IP address and port into the SDP part of the INVITE message.
m=audio 1111 RTP/AVP 4 }}}}}}
```

8 Proposal

It is proposed to add the following text to the informational annex of CN1/CN3 (29.162, 24.229):

3GPP TSG-CN-WG1, Meeting #21
26-30 November 2001,
Cancun, MX

Tdoc N3-~~011884~~011572

For IPv4/IPv6 interworking purposes it is proposed to have the following functionalities and interfaces with protocols in the IMS:

- A NAT-PT device able to translate the IP headers between different IP protocols and able to provide IPv4 addresses from its pool, when required

- A new functionality in IMS for IPv4/IPv6 interworking purposes on SIP control plane
  The allocation of the new functionality to a network element is for further study

- A control protocol between the network element providing the new functionality and NAT-PT for the purpose of communication between the two entities

- Support for DNS ALG in the IMS local name server

- Use of MEGACO on the interface between the new network element providing the new functionality and NAT-PT

It shall be decided whether the above requirements are required for Rel5 or Rel6.