

3GPP2 X.S0011-004-C

Version 2.0

Version Date: July 2005



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

# cdma2000 Wireless IP Network Standard: Quality of Service and Header Reduction

## ***COPYRIGHT NOTICE***

*3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.*

1	<b>Content</b>	
2	<b><u>1 GLOSSARY AND DEFINITIONS.....</u></b>	<b><u>2</u></b>
3	<b><u>2 REFERENCES.....</u></b>	<b><u>3</u></b>
4	<b><u>3 QUALITY OF SERVICE AND MULTIPLE SERVICE INSTANCES .....</u></b>	<b><u>4</u></b>
5	<b>3.1 MULTIPLE SERVICE INSTANCES .....</b>	<b>5</b>
6	3.1.1 MS REQUIREMENTS .....	5
7	3.1.2 PDSN REQUIREMENTS .....	6
8	<b>3.2 FLOW MAPPING AND TREATMENTS .....</b>	<b>7</b>
9	3.2.1 FORWARD TRAFFIC PROCESSING .....	8
10	3.2.2 PROTOCOL OPERATIONS FOR FLOW MAPPING AND TREATMENTS .....	8
11	3.2.3 PACKET FILTER ATTRIBUTES.....	9
12	<b>3.3 SUBSCRIBER QOS PROFILE .....</b>	<b>10</b>
13	3.3.1 ALLOWED DIFFERENTIATED SERVICES MARKING .....	10
14	3.3.2 PDSN-BASED R-P ADMISSION CONTROL .....	11
15	<b><u>4 HEADER REDUCTION FOR VOICE OVER IP SERVICE.....</u></b>	<b><u>12</u></b>
16	<b>4.1 THE LINK-LAYER ASSISTED ROHC PROFILES .....</b>	<b>12</b>
17	<b>4.2 NEGOTIATION OF THE LLA PROFILE.....</b>	<b>12</b>
18	4.2.1 PDSN REQUIREMENTS.....	13
19	4.2.2 MS REQUIREMENTS .....	13
20	<b>4.3 LLA – HEADER COMPRESSION .....</b>	<b>13</b>
21	4.3.1 PROTOCOL STACK .....	13
22	4.3.2 OPERATIONAL OVERVIEW .....	14
23	4.3.3 HRU PARAMETER SETTINGS .....	14
24	4.3.4 PDSN REQUIREMENTS.....	14
25	4.3.5 MS REQUIREMENTS .....	15
26	<b>4.4 LLA – HEADER REMOVAL .....</b>	<b>16</b>
27	4.4.1 PROTOCOL STACK .....	16
28	4.4.2 OPERATIONAL OVERVIEW .....	16
29	4.4.3 HEADER GENERATOR PARAMETER INITIALIZATION .....	17
30	4.4.4 PDSN REQUIREMENTS.....	17
31	4.4.5 MS REQUIREMENTS .....	18
32	<b><u>ANNEX A: HRU PARAMETER SETTINGS FOR LLA HEADER COMPRESSION (NORMATIVE).....</u></b>	<b><u>19</u></b>
33	<b><u>ANNEX B: FLOW MAPPING, TREATMENT AND THE 3GPP2 OBJECT (NORMATIVE).....</u></b>	<b><u>21</u></b>
34	<b><u>B.1 RESV MESSAGE.....</u></b>	<b><u>21</u></b>
35	<b>B.1.1 RESV MESSAGE FORMAT .....</b>	<b>21</b>
36	B.1.1.1 3GPP2_OBJECT .....	22
37	<b><u>B.2 RESVCONF MESSAGE .....</u></b>	<b><u>32</u></b>
38	<b><u>B.3 RESVERR MESSAGE .....</u></b>	<b><u>32</u></b>
39	<b>B.3.1 TFT ERROR (IE TYPE # = 1 AND 3).....</b>	<b>32</b>
40	<b>B.3.2 HEADER REMOVAL ERROR (IE TYPE # = 5).....</b>	<b>33</b>
41	<b>B.3.3 CHANNEL TREATMENT ERROR (IE TYPE # = 7).....</b>	<b>33</b>
42	<b><u>B.4 RELIABLE DELIVERY OF RSVP MESSAGES.....</u></b>	<b><u>34</u></b>
43	<b><u>ANNEX C: EXAMPLE OF VOIP CALL FLOW WITH HEADER REDUCTION TECHNIQUES</u></b>	
44	<b><u>(NORMATIVE) .....</u></b>	<b><u>35</u></b>
45	<b><u>ANNEX D: MAIN SERVICE INSTANCE TIMER (NORMATIVE) .....</u></b>	<b><u>39</u></b>
46		
47		

## 1 **Figures**

2	Figure 1. Graphical Illustration of Multiple Connection Relationships .....	5
3	Figure 2. Protocol stack diagram for Header Compression Operation .....	13
4	Figure 3. Protocol Stack for Header Removal operation .....	16
5		
6	Figure B- 1. 3GPP2_OBJECT .....	22
7	Figure B- 2. IE List .....	22
8	Figure B- 3. IE Type # .....	23
9	Figure B- 4. TFT IPv4 IE Type # = 0 .....	23
10	Figure B- 5. TFT IPv6. IE Type # = 2 .....	23
11	Figure B- 6. Packet filter list for deleting packet filters from existing TFT .....	24
12	Figure B- 7. Packet Filter Layout for TFT create, add, or modify operations.....	25
13	Figure B- 8. Packet Filter Content.....	26
14	Figure B- 9. Packet Filter Treatment (PFT).....	28
15	Figure B- 10. PFT Values.....	28
16	Figure B- 11. PFT Hints .....	28
17	Figure B- 12. Header Removal : IE Type # = 4.....	28
18	Figure B- 13. Header Element List.....	29
19	Figure B- 14. Header Element Types .....	29
20	Figure B- 15. Header Removal Subtype IPv4.....	29
21	Figure B- 16. Header Removal Subtype IPv6.....	29
22	Figure B- 17. Header Removal Subtype IPv6 Extensions .....	30
23	Figure B- 18. Header Removal Subtype UDP .....	30
24	Figure B- 19. Header Removal Subtype RTPv2 .....	30
25	Figure B- 20. Header Removal Subtype GRE .....	30
26	Figure B- 21. Header Removal Subtype Minimal Encapsulation.....	30
27	Figure B- 22. Channel Treatment IE Type # = 6 .....	31
28	Figure B- 23. CT Values.....	31
29	Figure B- 24. CT Hints .....	31
30	Figure B- 25. TFT IPv4 Error: IE Type # = 1 .....	32
31	Figure B- 26. TFT IPv6 Error: IE Type # = 3.....	33
32	Figure B- 27. HR Error: IE Type # = 5.....	33
33	Figure B- 28. Channel Treatment Error: IE Type # = 7 .....	33
34		
35	Figure C- 1. An example of MS originated call flow for VoIP .....	36
36		
37		

1 **Tables**

2 Table A- 1 - Compressor parameter settings..... 19

3 Table A- 2 - List of sizes and attributes of parameter PREFERRED\_PACKET\_SIZES for Data block Types

4 used by Multiplex Sublayer for Multiplex Option 1..... 20

5 Table A- 3 - List of sizes and attributes of parameter PREFERRED\_PACKET\_SIZES for Data block Types

6 used by Multiplex Sublayer for Multiplex Option 2..... 20

7

## 1 **General Description**

2 This Chapter describes Flow Mapping /Treatment mechanisms and protocol used when more than one  
3 service instance is established for the MS. It also describes two optional Header Reduction techniques that  
4 are specific to service instances of SO type 60 and 61, that may be established by the MS for applications  
5 that require a synchronous flow of 20ms frames, such as VoIP application. In this Chapter, a subscriber QoS  
6 profile is defined which consists of:

- 7 • the allowed number of service instances and service options the user is allowed to have,
- 8 • an allowed Diffserv marking per user, used by the PDSN to police and re-mark reverse user IP  
9 traffic, and
- 10 • a Reverse Tunnel marking to provide differential treatment for corporate/home network access  
11 per user.

1

2 **1 Glossary and Definitions**

3 See X.S0011-001-C.

1 **2 References**

2 See X.S0011-001-C.

### 3 Quality of Service and Multiple Service Instances

The cdma2000<sup>®1</sup> service options allow various voice and non-voice services to be defined and specified independently within the confines of the physical layer and the multiplex sub-layer interface [5-9]. The air interface is able to support multiple service instances of the same or different packet data service options. cdma2000 specifications support a maximum of six service instances per MS, each of which may have associated RLP and/or QoS parameter settings. The MS and the RN identify specific service instances with a unique number referred to as the Service Reference ID (SR\_ID). Note that current HRPD specifications [17], [18] do not support auxiliary service instances.

As outlined in [1], the RN transfers data to the PDSN via R-P connections for all service instances to the MS. There shall be one R-P connection for each service instance. The PDSN shall identify a service instance for an MS via an SR\_ID carried in R-P connection signaling. A single R-P session shall be maintained for all the R-P connections associated with an MS. For each R-P session there shall be one main service instance, and optionally one or more auxiliary service instances. A single PPP session shall be associated with the R-P session. There shall be one PPP session between the MS and the PDSN. A given PPP session shall support one or more IP addresses. These IP addresses are not associated with a particular R-P connection.

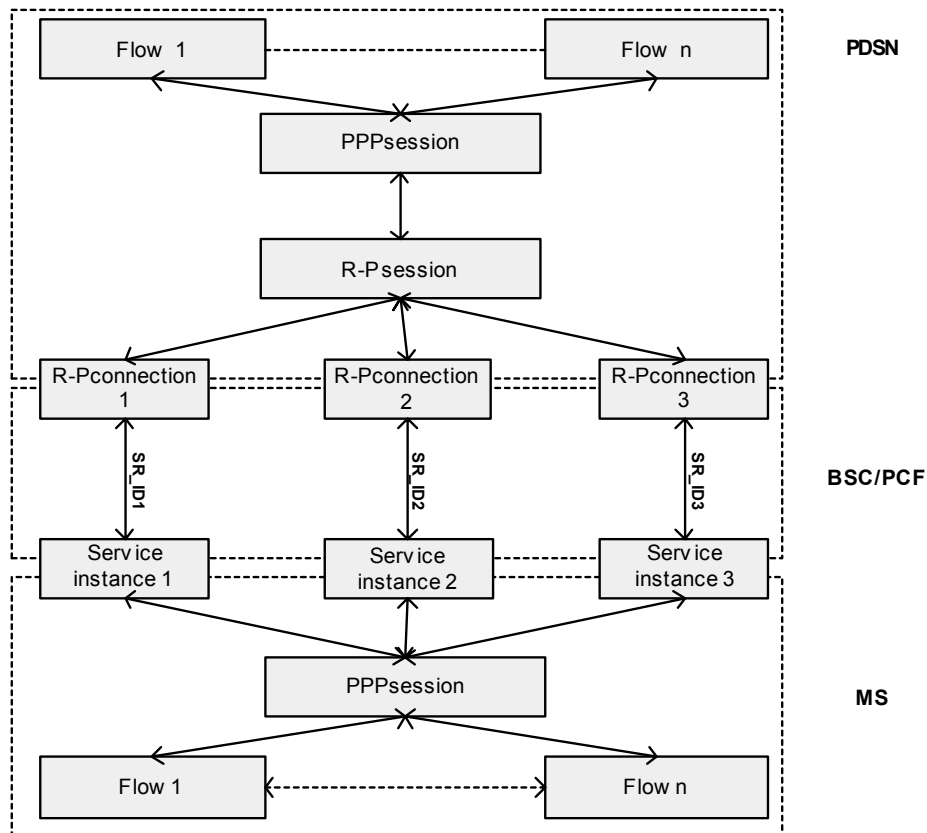
A service instance may carry multiple flows. A flow is a series of packets that share a specific instantiation of IETF protocol layers. For example, an RTP flow may consist of the packets of an RTP/UDP/IP protocol instantiation, all of which share the same source and destination IP addresses and UDP port numbers.

Flows are identified at the PDSN using packet filters. Packet filters are used to map forward traffic to the corresponding service instance.

The following figure is an example graphical illustration for three service instances and shows the relationships between MS IP addresses, PPP session, R-P session, R-P connections, service instances, and SR\_ID.

---

<sup>1</sup> cdma2000<sup>®</sup> is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000<sup>®</sup> is a registered trademark of the Telecommunications Industry Association (TIA USA) in the United States.



1  
2 **Figure 1. Graphical Illustration of Multiple Connection Relationships**

3 The remainder of this section covers the following topics:

- 4
- 5 • Section 3.1: Multiple Service Instances.
  - 6 • Section 3.2: Flow Mapping and Treatments.
  - 7 • Section 3.3: Subscriber QoS Profile.

### 7 **3.1 Multiple Service Instances**

8 The PDSN and the MS may support multiple service instances. The maximum number of Service Instances  
9 that can be supported is limited by the capabilities of the air interface but shall not exceed six [5] – [9]. The  
10 PDSN shall determine the service option type for the service instance from an extension received from the  
11 RN at R-P connection establishment [4], [17].

#### 12 **3.1.1 MS Requirements**

13 When the MS establishes a packet data service, it shall originate a main service instance of SO type 33<sup>2</sup> for  
14 PPP negotiation before originating other auxiliary service instances. The MS shall support a single PPP  
15 session over multiple service instances. The MS shall send PPP control packets only over the main service  
16 instance. The MS shall not send PPP control packets over auxiliary service instances. The MS shall use  
17 octet-oriented HDLC framing per RFC 1662 over octet-oriented service instances such as SO 33. The MS  
18 shall not use octet-oriented HDLC framing over non-octet oriented service instances such as SO 60/61. If the

<sup>2</sup> For HRPD, the RN populates the service option type field with value 59 when establishing the R-P connection with the PDSN for the main service instance.

1 MS uses Mobile IP, the MS shall send Mobile IP agent discovery and registration messages over the main  
2 service instance.

3 If the MS receives the PPP control packets on an auxiliary service instance, the MS shall continue the PPP  
4 negotiation with the PDSN on the main service instance.

5 At dormant handoff of multiple service instances, the MS shall maintain the mapping between service  
6 instance identifier and the main service instance. The MS shall originate the main service instance before  
7 originating other auxiliary service instances.

8 The MS may send Traffic Flow Templates for flow mapping to the PDSN in support of multiple service  
9 instances, and it shall update the TFT when any of the TFT components change (e.g., MS IP address, packet  
10 filter components).

11 At handoff, if PPP renegotiation has occurred, the MS shall re-signal to the PDSN any TFTs associated with  
12 the service instances.

### 13 **3.1.2 PDSN Requirements**

14 The PDSN shall support a single PPP session over multiple R-P connections for the same MS. Each R-P  
15 connection corresponds to a service instance. The PDSN should send PPP control packets only over an R-P  
16 connection corresponding to the main service instance of SO type 33/59. Once the PDSN knows the identity  
17 of the main service instance, it shall only send PPP control packets over that service instance. The PDSN  
18 shall use octet-oriented HDLC framing over R-P connections corresponding to octet oriented service  
19 instances such as SO 33/59. The PDSN shall not use octet-oriented HDLC framing over an R-P connection  
20 corresponding to a non-octet oriented service instances such as SO 60/61. For a Mobile IP MS, the PDSN  
21 shall send Mobile IP discovery and registration messages over an R-P connection corresponding to the main  
22 service instance.

23 If the main service instance is released, the PDSN shall release the R-P connections associated with the  
24 auxiliary service instances. The PDSN shall also clear the packet data session(s) that are associated with  
25 those R-P connections.

#### 26 **3.1.2.1 Initial PPP negotiation**

27 Upon receiving the first R-P connection for an MS, the PDSN shall check the following:

- 28 1. Whether it has any context (PPP and/or Mobile IP context) for the MSID.
- 29 2. Whether it is acting as a Target PDSN for a fast handoff in progress for that MS.

30 If both checks are "negative", the PDSN shall determine if the first established R-P connection is of SO type  
31 33/59 to initiate PPP negotiation with the MS. If the first R-P connection is not of SO type 33/59, the PDSN  
32 shall set the timer Twait\_main<sup>3</sup> to wait for an R-P connection of SO type 33 to carry out PPP negotiation. If  
33 the timer Twait\_main expires and the RN has not established an R-P connection with SO type 33, it shall  
34 release the already setup R-P connections.

35 The PDSN shall store the received CANID from the NVSE field if received in the A11 Registration-  
36 Request and shall associate it with the R-P session for future comparison.

#### 37 **3.1.2.2 PPP renegotiation**

38 Upon receiving an A11-Registration Request with the S bit set to '0' for establishment of an R-P connection of  
39 SO type 33/59 and a PPP session already exists at the PDSN for the MSID, and if the ANID NVSE is  
40 received in the A11 Registration Request, the PDSN shall compare the Previous Access Network Identifier  
41 (PANID) field if non-zero in the ANID NVSE [4] to the stored ANID to determine if PPP shall be renegotiated  
42 with the MS. The PDSN shall renegotiate PPP with the MS if it detects a mismatch between the ANID value  
43 stored at the PDSN and the non-zero PANID value that is received in the A11 Registration-Request.

---

<sup>3</sup> Twait\_main is described in Annex D.

- 1 The PDSN may use the MEI to renegotiate PPP with the MS if the PANID field is zero or the ANID NVSE is  
2 not contained in the A11 Registration Request.
- 3 The PDSN shall make its PPP renegotiation determination based on the first A11 Registration-Request of SO  
4 type 33/59 it receives from the RN.
- 5 If the PDSN determines that PPP shall be renegotiated at handoff, it shall check the SR\_ID and the SO type  
6 received in the first A11 Registration-Request. If the SR\_ID/SO type does not correspond to the previous  
7 main service instance, the PDSN shall send its LCP Configure-Request to the MS over the R-P connection if  
8 it is of SO type 33/59. If the PDSN receives PPP negotiation messages from the MS over a different R-P  
9 connection of SO type 33 established after the negotiation started, it shall continue PPP negotiation over that  
10 R-P connection.
- 11 The PDSN shall not release the R-P connection that it selected to send LCP-Configure Request. The PDSN  
12 shall thenceforth treat that R-P connection as an auxiliary service instance.
- 13 If the first R-P connection is not of SO type 33/59, and the PDSN determines that PPP shall be renegotiated,  
14 the PDSN shall set the timer Twait\_main<sup>4</sup> to wait for an R-P connection of SO type 33 to carry out PPP  
15 negotiation. If the timer Twait\_main expires and the RN has not established an R-P connection with SO type  
16 33, it shall release the already setup R-P connections.
- 17 If a previous PPP session is maintained at the PDSN, but PPP renegotiation has been performed with the  
18 MS, the PDSN shall clear all service instance context information associated with the A10 connections from  
19 the previous PPP session, which include TFT, Header Generator parameters, and IP header compressor  
20 context.

### 21 **3.2 Flow Mapping and Treatments**

- 22 The MS may open one or more auxiliary service instances, to carry application traffic that is not suitable for  
23 the main service instance (a service instance corresponds to an R-P connection and is also referred to as  
24 "channel" in the Flow Mapping and Treatment procedures). For example, the MS may have a main service  
25 instance for TCP/IP and an auxiliary service instance to carry an RTP video stream. To make effective use of  
26 this service instance or R-P connection also referred to as channel in the Flow Mapping and Treatment  
27 procedures, the PDSN may be informed which packets should be sent on it. Annex B describes the protocol  
28 used for this purpose. This section provides an overview of the protocol. Annex B specifies the detailed  
29 description of the protocol.
- 30 The MS shall use a Resv message to signal to the PDSN one or more Traffic Flow Template Information  
31 Elements (TFT IE) over the main service instance. The TFTs are used to map forward traffic to the main or  
32 the auxiliary service instances and to indicate if a specific flow treatment (e.g., Header Compression  
33 technique) should be applied for the matching forward packet. An MS may be assigned multiple IP addresses  
34 through a combination of Simple IP and Mobile IP services. There is one TFT for each MS IP address and  
35 service instance pair.
- 36 Each TFT IE contains one or more packet filters that are matched against incoming forward traffic at the  
37 PDSN. The packet filters identify a flow and contain components such as destination IP address, destination  
38 port number, Protocol Type or Traffic Class (IPv6)/Type of service (TOS in IPv4) used to identify different  
39 forward direction packet flows in the PDSN.
- 40 For each packet filter, the TFT IE shall include an evaluation precedence value and may include a flow  
41 treatment for packets matching the filter. The precedence value may be used by the PDSN as an aid for  
42 packet filter matching. If the PDSN receives a TFT that contains a packet filter evaluation precedence (other  
43 than 255) equal to any other currently active packet filter for that MS IP address (for any SR\_ID) it shall  
44 respond with a ResvErr message and shall include the TFT Error code 5 (Evaluation Precedence  
45 Contention).

---

<sup>4</sup> Twait\_main is described in Annex D

1 If available, a flow treatment indicates to the PDSN which compression technique to apply for a flow that  
2 matches the associated packet filter.

3 The Resv message may include a Channel Treatment Information Element (CT IE) that indicates to the  
4 PDSN which compression techniques to apply on a main or an auxiliary service instance. The CT IE is  
5 applied for all the flows that are mapped on that service instance unless overridden by a specific per-flow  
6 treatment.

7 The PDSN shall not tear down the A10 connection because it does not receive the associated packet filters  
8 from the MS. This allows the MS to set up auxiliary service instance to be used only in the reverse direction.

### 9 **3.2.1 Forward Traffic Processing**

10 When a packet arrives at the PDSN from the external IP network, the destination IP address is checked to  
11 determine which set of TFTs should be consulted. Then, each service instance's associated TFT is checked  
12 for a match against any of the packet filters contained in the TFT. If a match is found, the packet is sent down  
13 that service instance with the flow treatment specified for that packet filter. If no flow treatment is specified for  
14 that matching packet filter, the channel treatment is applied to the packet, if provided by the MS; otherwise,  
15 the default treatment should be applied. Determining the default treatment is implementation specific and is  
16 based on the compression capabilities negotiated during PPP establishment such as IPCP.

17 If an incoming forward packet does not match any packet filter within the corresponding TFT(s), the packet  
18 shall be sent over the main service instance.

### 19 **3.2.2 Protocol Operations for Flow Mapping and Treatments**

20 The MS shall define TFTs in such a way that downlink packets are routed to a service instance that matches  
21 the characteristics of the receiving application. The MS shall transmit the TFT IE to the PDSN using a Resv  
22 message based on the RSVP protocol [RFC2205]. Note that some protocol exceptions apply as described in  
23 this specification. The destination IP address of the Resv message shall be set by the MS to the IP address of  
24 the PDSN, i.e., the IP address received during IPCP negotiation or FA CoA address, and not the IP address  
25 of the correspondent node.

26 For flow mapping and treatment purposes, each Resv message shall contain a RESV\_CONFIRM object and  
27 may contain one or more TFT IE and/or one or more CT IE coded in one 3GPP2 OBJECT. The 3GPP2  
28 OBJECT shall have Class Number = 231, Class Name = 3GPP2\_OBJECT and Class Type or C-Type = 1.

29 A Resv message with a TFT IE is a request to insert, modify, or delete one or more packet filters from the  
30 TFT and may include a request for a specific flow treatment for each packet filter. The PDSN processes the  
31 request and if the IE is successfully processed, the PDSN shall return a ResvConf message containing the  
32 MS IP address. If the PDSN fails to process the IE, the PDSN shall return a ResvErr message to indicate  
33 failure in processing the request.

34 Upon receipt of a TFT from the MS for which the corresponding service instance is not established at the  
35 PDSN, the PDSN shall reject the TFT with a failure code indicating Channel Not Available, unless the 'P'  
36 (Persistency) bit is set in the request and allowed by the Subscriber QoS profile and the local policy.

37 If the 'P' bit is set, and if the user is not authorized for persistent TFTs in accordance with the Subscriber QoS  
38 profile and local policy, the PDSN shall reject the TFT with a failure code indicating Persistency Not Allowed.

39 If 'P' bit is set, and if the user is authorized through the user profile and the local policy allows for persistent  
40 TFTs but the user has already used up the maximum allowed number of persistent TFTs as per the user's  
41 profile, the PDSN shall reject the TFT with a failure code indicating Persistency Limit Reached. Otherwise, the  
42 PDSN shall process the TFT and return a ResvConf message to the MS, in which case the PDSN shall retain  
43 TFTs that have the 'P' bit set even when the corresponding service instance is disconnected.

44 If the user is authorized for a number of persistent TFTs, the PDSN shall also allow the same number of  
45 persistent Header compression contexts and Header Removal Initialization Parameter IEs.

46 If the PDSN receives any packet that matches persistent TFT and there is no associated A10 connection  
47 established, the PDSN shall discard the packet.

### 1 3.2.3 Packet Filter Attributes

2 Each packet filter has a unique identifier within a given TFT. A packet filter consists of an evaluation  
3 precedence index and a list of packet filter content sub-options. The packet filter contents sub-option gives a  
4 list of values to be matched against particular header fields.

5 Two packet filter sub-option PF types are defined in this specification. PF Type 0 applies to the outer IP  
6 header of the packet that the PDSN is transmitting to the MS. PF Type 0 may also include transport header  
7 fields if no encapsulation is in use. PF Type 1, if included, applies to the encapsulated transport layer header  
8 of the forward direction traffic. Note that the transport layer header shall appear within one or more layers of  
9 encapsulated IP headers if PF Type 1 is used.

10 The PDSN shall match through all encapsulation headers mapping PF Type 1 in the forward direction traffic.

11 The PDSN shall use the transport layer header (e.g., port numbers, SPI) from PF Type 1 and ignore any  
12 transport layer information if received in PF Type 0.

13 The Protocol Identifier/Next Header if included in PF Type 0 shall be matched with the outer IP header. The  
14 protocol ID / Next Header if included in PF Type 1 shall be matched against the IP header immediately  
15 preceding the transport layer header.

16 Following the packet filter contents sub-options is an optional flow treatment sub-option, which specifies  
17 whether techniques such as Header Compression should be applied to matching packets.

18 PF Type 0 may include one or more of the following components specified below:

- 19 • IPv4 Source Address with Subnet Mask.
- 20 • IPv6 Source Address<sup>5</sup> with Prefix Length.
- 21 • IPv4 Destination Address.
- 22 • IPv6 Destination Address with Prefix Length.
- 23 • Protocol Type (IPv4) / Next Header (IPv6).
- 24 • Destination Port Range.
- 25 • Source Port Range.
- 26 • Single Destination Port.
- 27 • Single Source Port.
- 28 • IPsec Security Parameter Index (SPI).
- 29 • Type of Service (TOS) (IPv4) / Traffic Class (IPv6) with Type of Service/Traffic Class Mask.
- 30 • Flow Label (IPv6).

31 PF Type 1 may include:

- 32 • Protocol Identifier (IPv4) / Next Header (IPv6).
- 33 • Destination Port Range.
- 34 • Source Port Range.
- 35 • Single Destination Port.

---

<sup>5</sup> Source addresses of forward direction packet flows belong to correspondent nodes and are sometimes subject to change due to e.g., renumbering [RFC 2461] or privacy [RFC 3041]. The MS should not include a source address packet filter component unless it is reasonably sure that the IP address of the correspondent node will not change for the life of the application flow or is willing to update the TFT when such a change takes place.

- 1           • Single Source Port.
  - 2           • IPsec Security Parameter Index (SPI).
- 3 Some of the listed components may coexist in a packet filter while others mutually exclude each other. The  
4 following rules shall be observed when adding packet filter components to a packet filter contents sub-option:
- 5           • If the IPsec SPI or port related components are included in PF Type 0, the MS shall not include  
6 PF Type 1.
  - 7           • If the IPsec SPI component is given, no port-related components shall be specified. Similarly, If  
8 port related components are specified, no IPsec SPI shall be specified.
  - 9           • Some components are specific to IPv6, while others are specific to IPv4. Components for IPv4  
10 and IPv6 shall not be mixed within the same packet filter sub-option; for example, the IPv4/IPv6  
11 address components shall not appear mixed in the same packet filter component, and the IPv6  
12 Flow Label shall not be used with IPv4 source/destination addresses. For a packet header to  
13 match an IPv4-specific component, the header shall be IPV4, and similarly only an IPV6 header  
14 may match an IPv6-specific component. The IP version of the packet filter contents shall match  
15 the TFT Type (TFT IPv4 or TFT IPv6). Note, however, that an encapsulated packet may have a  
16 version different from its outer header.
- 17 See Annex B for the complete specification of the flow mapping protocol.

### 18 3.3 Subscriber QoS Profile

19 When the MS establishes Mobile IP and Simple IP service, the PDSN shall perform authentication and  
20 authorization of the MS with the HAAA server. When the MS is authenticated, the HAAA may return  
21 Subscriber QoS Profile information via the VAAA to the PDSN in the authentication and authorization  
22 response. The Subscriber QoS Profile consists of the following 3GPP2 RADIUS attributes (see X.S0011-005-  
23 C):

- 24           • The Allowed Differentiated Services Markings.
- 25           • The Service Option Profile.
- 26           • The Allowed Persistent TFTs.

27 The attributes are specified in X.S0011-005-C. The PDSN shall use the Subscriber QoS Profile as part of the  
28 authorization for service instances. The PDSN shall store this information for subsequent use. In the event of  
29 multiple NAIs per MS, the PDSN may receive a Subscriber QoS Profile for each NAI. The PDSN shall store  
30 and handle multiple Subscriber QoS Profiles per MS.

31 When the MS establishes Simple IP service, the carrier may permit no PPP session authentication<sup>6</sup> as  
32 specified in X.S0011-002-C, in which case the PDSN shall apply the default QoS settings, as provisioned by  
33 the Access Provider Network. The default QoS settings give default values for all attributes of the subscriber  
34 QoS profile and shall be used for the no PPP session authentication case and whenever the subscriber QoS  
35 profile is not included in the RADIUS Access-Accept message. The default QoS setting shall not allow setup  
36 of auxiliary service instances.

#### 37 3.3.1 Allowed Differentiated Services Marking

38 In accordance with differentiated services standards [RFC2474], the MS may mark packets (i.e., in the  
39 reverse direction). The PDSN, however, may limit the differentiated services markings that the MS applies to  
40 packets based on the User Profile received from the Home RADIUS server or based on its local policy. The  
41 PDSN may provide a fixed marking for Mobile IP based reverse tunneled traffic based on the User Profile  
42 received from the Home RADIUS server or based on its local policy.

---

<sup>6</sup> This is the case in which the MS is permitted to negotiate Simple IP without CHAP or PAP.

1 The Differentiated Services Code Points (DSCPs) supported in this specification shall be based on the  
2 following RFCs:

- 3 • Class selectors: [RFC 2474] defines these as code points, whose lower three bits (3, 4, 5) are all  
4 zero. Therefore, there are eight such classes.
- 5 • Default Forwarding (often called Best Effort) is a class selector with class equal to 0.
- 6 • Assured Forwarding (AF) classes: see [RFC 2597].
- 7 • Expedited Forwarding (EF) Classes: see [RFC 2598].

8 When the MS marks IP packets with DSCPs, the PDSN shall ensure that only allowed DSCPs are used as  
9 authorized by the HAAA in the users Subscriber QoS Profile. If the HAAA does not include the Subscriber  
10 QoS Profile of the user in the RADIUS Access-Accept message, the PDSN shall offer default QoS settings to  
11 the user's packets as provisioned by the service provider.

12 The Allowed Differentiated Services Marking attribute indicates the type of marking the user may apply to a  
13 packet. The PDSN may re-mark the packet according to local policy if the type of marking is not authorized by  
14 the user's Allowed Differentiated Services Marking attribute. The attribute contains three bits, the 'A', 'E', and  
15 'O' bits. When the 'A' bit is set, the user may mark packets with any AF class. When the 'E' bit is set, the user  
16 may mark packets with EF class. When the 'O' bit is set, the user may mark packets with experimental/local  
17 use classes. The Max Class Selector field specifies the maximum class selector for which a user may mark a  
18 packet. When all three bits are clear, and when the Max Class Selector is zero, the user may only send  
19 packets marked best effort.

20 When reverse direction traffic arrives at the PDSN, the PDSN shall match the source address of such packets  
21 to a source address that is associated with an authenticated NAI. The PDSN shall apply to the packet the  
22 default QoS settings and the subscriber QoS profile if available.

### 23 **3.3.1.1 Differentiated Services and Tunnels**

24 The Allowed Differentiated Services Marking attribute contains a reverse tunnel marking ('RT Marking', see  
25 RADIUS VSAs in X.S0011-005-C), which is the marking level the PDSN shall apply to reverse tunneled  
26 packets when those packets are not marked [RFC 2983]. If the packets received from the MS are marked,  
27 and traffic is to be reverse tunneled to the HA, the PDSN shall copy the (possibly re-marked) inner packet  
28 marking to the outer header of reverse Mobile IP tunnels.

29 For forward traffic to the MS, the HA should set the differentiated services field of the HA-FA tunnel to the  
30 differentiated services class of each received packet bound to the MS.

### 31 **3.3.2 PDSN-Based R-P Admission Control**

32 The PDSN shall reject a new R-P connection request from the RN if:

- 33 • the number of connections requested by the user exceeds limits set by the Service Option Profile  
34 attribute; or,
- 35 • the service option is not on the list of allowed service options for the user; or
- 36 • the PDSN lacks available R-P connection resources; or

37 In the event there are multiple Subscriber QoS Profiles due to multiple NAIs per MS, the PDSN should have  
38 the capability to combine the QoS parameters into a single Subscriber QoS Profile in accordance with the  
39 local policy except for the allowed Differentiated service marking. The default local policy for combining the  
40 subscriber QoS profiles is as follows:

- 41 • The total set of all allowed service options,
- 42 • The maximum of the maximum number of service instances.

## 4 Header Reduction for Voice over IP service

Two service options (60 and 61) have been defined [16] to allow for the efficient transport of Voice-over-IP (VoIP) without the overhead that would be present from PPP and RLP framing on ordinary packet data services. Each of the service options is optional at the PDSN and at the MS. In addition, the PDSN shall only allow establishment of the service option if it is allowed in the Service Option Profile (see section 3.3.2).

Service Option 61 supports Link-Layer Assisted (LLA) Robust Header Compression [RFC 3242, RFC 3408] which uses the physical channel timing along with re-synchronization procedures to replace the normal ROHC header most of the time. This allows IP/UDP/RTP-encapsulated voice to be sent with very close to zero or zero overhead. Service Option 60 supports Header Removal, which does not attempt to send any header information over the air in the forward direction. Header Removal uses the physical channel timing to regenerate IP/UDP/RTP header information in the PDSN and is appropriate when the MS voice application does not use IP/UDP/RTP header information. Sections 4.1, 4.2, and 4.3 discuss Header Compression with LLA ROHC, and Section 4.4 discusses Header Removal.

The MS may maintain the over the air service instance identifier when the LLAROHC or Header Removal service instance is disconnected. The MS shall use the maintained over the air service instance identifier whenever it attempts to re-connect the LLAROHC or Header Removal service instance. The MS is not required to send the TFT to the PDSN if the MS re-connects the same LLAROHC or Header Removal service instance and the 'P' bit was set in the corresponding TFT, which was acknowledged by the reception of ResvConf message from the PDSN.

### 4.1 The Link-Layer Assisted ROHC profiles

RObust Header Compression (ROHC) [RFC3095] is an extensible framework for which profiles for compression of different protocols may be defined. For VoIP, the application data is transported end-to-end within an IP/UDP/RTP stream. Header Compression of IP/UDP/RTP is defined by the ROHC RTP profile (profile 0x0001), which is one of the profiles defined in RFC 3095. Note that the ROHC RTP profile supports different header compression modes: the Uni-directional mode (U-mode), the bi-directional Optimistic mode (O-mode) and the Reliable mode (R-mode). A Link-Layer Assisted ROHC profile (LLA) is an extension to the ROHC RTP profile that provides increased compression efficiency by using functionality of an assisting layer (cdma2000 link). There are two ROHC LLA profiles. Profile 0x0005 defined in RFC 3242 supports 0-byte operation for U/O-mode. Profile 0x0105 defined in RFC 3408 (incorporates by reference all functionality of RFC 3242) supports 0-byte operation for all modes (U/O/R).

Additional control logic is required at the PDSN to adapt the LLA profiles to the cdma2000 link layer. The capabilities required by the cdma2000 link to support the LLA profiles are described in [16]. The combination of one of the LLA profiles and the additional control logic is referred to as Header Reduction Upper (HRU) application. The HRU inter-works with a control logic at the BSC via an interface described in [16] over an auxiliary R-P connection. The control logic at the BSC is referred to as Header Reduction Lower (HRL) and is described in [16]. The HRU thus harmonizes the LLA compressor with the interface to the HRL to ensure their compatibility and proper operation.

Sections 4.2 and 4.3 of this specification are based on RFC3242, RFC3408 and RFC 3241 and describe the control logic of the HRU required for negotiation of the LLA profile, parameter settings as well as control of the interface towards the HRL.

### 4.2 Negotiation of the LLA profile

ROHC compression is negotiated during IPCP using the ROHC IP-Compression-Protocol Configuration option defined in RFC 3241. In particular for SO 61, note that profile negotiation always results in only one of the LLA profile numbers (either 0x0005 or 0x0105) being present within the final set of negotiated ROHC profiles, as a consequence of the negotiation mechanism provided by ROHC-over-PPP [RFC3241].

### 1 4.2.1 PDSN requirements

2 If the PDSN supports compression/decompression of LLA ROHC packets, it shall include the LLA ROHC  
 3 profile number in the ROHC IP-Compression-Protocol Configuration option during its IPCP negotiation with  
 4 the MS as per RFC 3241. The PDSN shall include at least the ROHC LLA profile number 0x0005, and may  
 5 additionally include profile number 0x0105, in the set of supported ROHC profiles.

### 6 4.2.2 MS requirements

7 If the MS supports compression/decompression of LLA ROHC packets, the MS shall include the LLA ROHC  
 8 profile number in the ROHC IP-Compression-Protocol Configuration option during its IPCP negotiation with  
 9 the PDSN as per RFC3241.

10 The MS shall include at least the ROHC LLA profile number 0x0005, and may additionally include profile  
 11 number 0x0105, in the set of supported ROHC profiles.

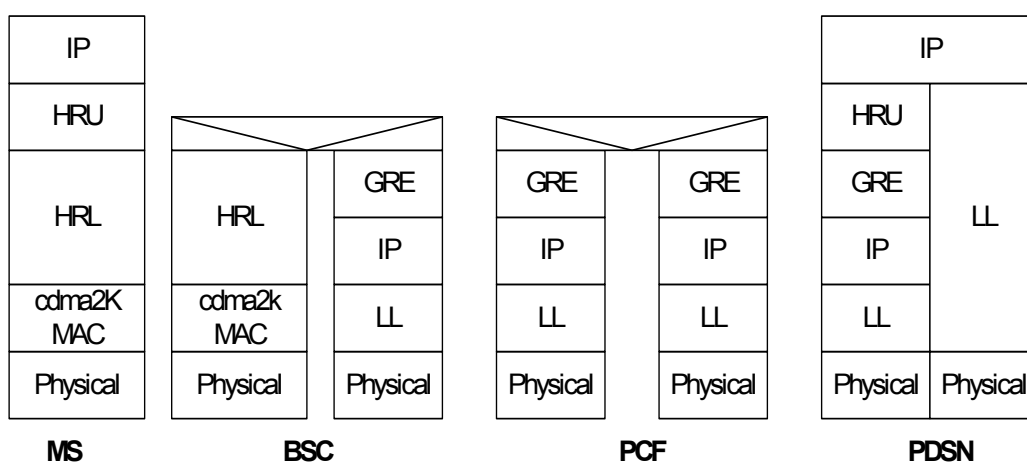
## 12 4.3 LLA – Header Compression

13 Link-Layer Assisted Header Compression in cdma2000 systems is applicable for end-to-end IP/UDP/RTP  
 14 flows, in particular VoIP flows with cdma2000 vocoders used as IP applications in the MS. It transparently  
 15 compresses and decompresses the IP/UDP/RTP headers in both the forward and the reverse direction  
 16 between the MS and the PDSN. When the MS wants to use LLA Header Compression, it shall request an  
 17 auxiliary Voice over IP service instance of service option type 61. Using the main service instance, it shall  
 18 also signal the packet filter associated with that service instance using the messages defined in Annex B if the  
 19 MS wants the PDSN to match the forward direction traffic over the A10 connection that corresponds to the  
 20 service instance of SO 61.

21 The operation of the MS and PDSN with LLA Header Compression is described below. In this section, a  
 22 packet with a 0-byte header (e.g., RTP payload only) is referred to as a No Header Packet (NHP) being of  
 23 type NHP, otherwise the packet is of type RHP.

### 24 4.3.1 Protocol stack

25 Figure 2 shows the protocol stack diagram when operating using Header Compression.  
 26



27

28

**Figure 2. Protocol stack diagram for Header Compression Operation**

29 Note that in both the MS and network the link layer assisting functions are divided into an HRU part and an  
 30 HRL part. On the network side, a GRE tunnel corresponding to the service instance connection separates the

1 HRU and HRL. On the MS side, these are connected by an internal interface. In either case, the primitives  
2 defined by SO 61 are used for communication between the HRU and HRL.

### 3 **4.3.2 Operational overview**

4 Header Compression operation is conceptually divided into two phases: the context initialization and the  
5 normal operation. During context initialization, the LLA compressor outputs IR packets (see RFC 3095,  
6 section 5.3 for details on context initialization operation). Under normal operation, the LLA compressor  
7 outputs packets without <sup>7</sup>any compressed headers most of the time, and packets with a small compressed  
8 header otherwise.

9 The HRU sends context updating information in-band over SO 61. This includes context initialization packets  
10 and packets with small compressed headers. More information can be found in section 2.1 of [16].

11 Below we describe the parameter settings and other procedures that shall be followed by the MS and PDSN  
12 for successful LLA-ROHC operation.

### 13 **4.3.3 HRU parameter settings**

14 Section 5 of RFC3242 provides guidelines for implementation of the LLA profile. In particular, parameters  
15 useful to LLA implementations are suggested. The parameter values required by this specification for the LLA  
16 compressor to be properly supported by the cdma2000 link are specified in Annex A.

### 17 **4.3.4 PDSN requirements**

#### 18 **4.3.4.1 Interface to HRL, transmitting side**

19 The HRU supports the interface logic defined in [16]. To enforce the Optimistic Approach Agreement (OAA)  
20 defined in RFC3242, the HRU shall set the OAA\_VALUE to '011' over the SO 61 interface.

21 In addition, the HRU shall inspect the first 2 octets of every NHP to be sent over SO 61. If the first two octets  
22 are identical to the leading sequence<sup>8</sup> used for packet type identification (see Annex A, ALWAYS-PAD), the  
23 HRU shall set the NA (NHP Allowed) flag to '0'. This prevents an RTP payload to be sent over the air with a 0-  
24 byte header to collide with the leading sequence and be falsely interpreted as a packet with a compressed  
25 header.

26 If the Data Block Type is Rate 1/8, the HRU shall inspect the first octet of the NHP. If this octet matches the  
27 pattern '11111011'<sup>9</sup>, the HRU shall set the NA (NHP Allowed) flag to '0'.

28 When profile 0x0105 is used for SO 61 and the LLA compressor is operating in the bi-directional Reliable  
29 compression mode (R-mode), if the HRU receives an HR-Update Indication from the HRL, the HRU should  
30 indicate the presence of the HR-Update indication and forward the RTP\_SN\_BREAK value carried in the PDU  
31 to the LLA compressor. This supports the Update\_Request interface defined in RFC 3408. The HRU shall  
32 also obtain the latest SN\_ACKed value from the compressor and shall transmit it to the HRL in the  
33 RTP\_SN\_ACKED field of every HR-Data\_Request.

#### 34 **4.3.4.2 Interface to HRL, receiving side**

35 When the HRU receives PDUs from SO61, the HRU shall provide one indication of packet loss to the  
36 decompressor<sup>10</sup> for each 20ms gap in the PDU field SYSTEM\_TIME, i.e. when the value of the

---

<sup>7</sup> Packets for which the IP/UDP/RTP header was compressed down to a size of zero octet.

<sup>8</sup> The leading sequence consists of two consecutive ROHC padding octets. The ROHC padding octet (11100000) is defined in RFC 3095, section 5.2.

<sup>9</sup> This is the Context Check Packet defined in RFC 3242. The two ROHC padding octets leading sequence is not required when sending CCP in a rate 1/8 frame.

<sup>10</sup> Indication of packet loss is defined in RFC 3242.

- 1 SYSTEM\_TIME field in the PDU does not indicate a continuous sequential increment of 20ms with respect to  
2 value of the SYSTEM\_TIME field received in the previous PDU.
- 3 If the DATABLOCK attribute [16] is not present (as inferred from the length of the PDU), the HRU shall  
4 provide an indication of packet loss to the decompressor<sup>10</sup>; the HRU shall then discard the PDU without  
5 additional processing.
- 6 If the Data Block Type is Rate 1/8, the HRU shall inspect the first octet of the received packet. If the octet  
7 matches the pattern '11111011'<sup>9</sup>, the HRU shall indicate the presence of a compressed header. Otherwise,  
8 the HRU shall indicate the presence of a packet of type NHP to the decompressor.
- 9 If the Data Block Type is rate other than Rate 1/8, then in addition to the interface logic defined in [16], the  
10 HRU shall inspect the first two octets of each packet received from the HRL to determine its type. If the first  
11 two octets match the leading sequence<sup>8</sup>, then the HRU shall indicate the presence of a compressed header to  
12 the decompressor.
- 13 For every packet with a compressed header, the HRU shall inspect the packet type field, which is the first  
14 octet following any ROHC padding octets in the packet. If this field matches the pattern '11111011', the HRU  
15 shall provide an indication of packet loss to the decompressor.
- 16 The following logic shall be used at the receiving side prior to forwarding the received packets to the LLA  
17 decompressor. This logic is based on the identified packet type and makes use of the values of the  
18 compressor parameter PREFERRED\_PACKET\_SIZES [RFC3242] as specified in Annex A:
- 19 • If the size of the received packet matches one of the sizes<sup>11</sup> for which RESTRICTED\_TYPE is  
20 NHP\_ONLY, then:
    - 21 ➤ if the packet is of type RHP, the last octet is padding that was used to handle the non-  
22 octet aligned format of the physical frame used during transmission over SO 61 (see also  
23 [16]). The HRU shall then remove the last octet and the HRU shall forward the packet  
24 along with its type to the LLA decompressor;
    - 25 ➤ otherwise, the HRU shall forward the packet along with its type to the LLA decompressor  
26 without additional processing.
  - 27 • Otherwise, the size of the received packet will match one of the sizes<sup>12</sup> for which  
28 RESTRICTED\_TYPE is NO\_RESTRICTION, and the HRU shall forward the packet along with its  
29 type to the LLA decompressor without additional processing.

30 Note that a packet of an RHP\_ONLY size should never be received by the HRU from the HRL, because these  
31 sizes are not available from the multiplex sublayer at the HRL. Instead, the HRU will receive the RHP padded  
32 by one octet in a packet of an NHP\_ONLY size, which will be handled by the first rule. Receipt of an RHP in a  
33 packet of an NHP\_ONLY size is legal because the restrictions set forth in Section 5.1.1 of RFC3242 only  
34 prohibit transmission, not reception, of such a packet.

### 35 4.3.5 MS requirements

#### 36 4.3.5.1 Interface to HRL, transmitting side

37 Same as 4.3.4.1.

#### 38 4.3.5.2 Interface to HRL, receiving side

39 Same as 4.3.4.2.

---

<sup>11</sup> E.g., Octet-aligned value sizes (22) for Multiplex Option 1, and (3, 7, 16, 34) for Multiplex Option 2.

<sup>12</sup> E.g., Octet-Aligned value sizes (2, 5, 10) for Multiplex Option 1.

## 1 4.4 LLA – Header Removal

2 Header Removal in cdma2000 systems is applicable when the application interfaces directly with the  
3 multiplex sub-layer/HRL, in particular VoIP flows with cdma2000 vocoders directly connected to the HRL in  
4 the MS.

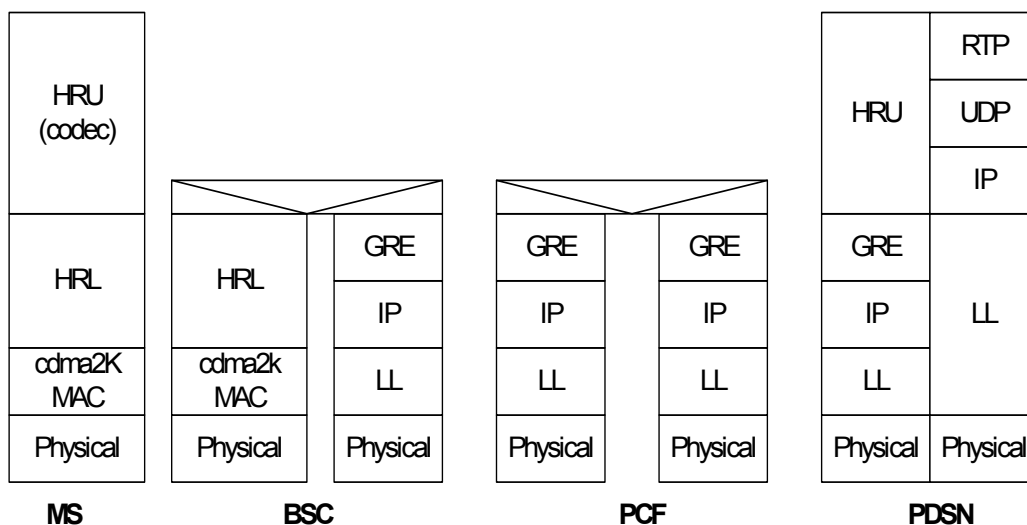
5 When the MS wants to use Header Removal, it requests an auxiliary Voice over IP service instance of service  
6 option type 60. Note that the MS need not negotiate any form of IP Header Compression during IPCP to  
7 make use of Header Removal.

8 In Header Removal operation, the (possibly encapsulated) IP/UDP/RTP flow is terminated at the PDSN for  
9 forward direction traffic. This means that IP/UDP/RTP headers are removed and that only the RTP payloads  
10 are sent over the air to the MS. For reverse direction traffic, the PDSN generates the (possibly encapsulated)  
11 IP/UDP/RTP header and forwards the packet to its destination.

12 Note that the use of Header Removal for one VoIP application in the MS does not preclude the use of other  
13 header reduction schemes for other applications.

### 14 4.4.1 Protocol stack

15 Figure 3 shows the protocol stack diagram when operating using Header Removal.



16

17

**Figure 3. Protocol Stack for Header Removal operation**

18 Note that in both the MS and the network the Header Removal process is divided into an HRU part, which is  
19 co-located with the application, and an HRL part, which is co-located with the cdma2000 MAC layer. In the  
20 MS, the HRL and the HRU (codec) are connected by an internal interface. On the network side, a GRE tunnel  
21 corresponding to the service instance connection separates the HRU and HRL. In either case, the primitives  
22 defined by SO 60 are used for communication between the HRU and HRL, including sending/receiving  
23 application data.

### 24 4.4.2 Operational overview

25 Header Removal is conceptually divided in two phases: the Header Generator parameter initialization<sup>13</sup> in the  
26 reverse direction and the normal operation.

<sup>13</sup> There is no context initialization in the forward direction

### 1 **4.4.3 Header Generator Parameter Initialization**

2 If the PDSN supports Header Removal, it uses the service option number (SO 60) received at A10 connection  
3 establishment, to determine that Header Removal treatment shall be applied for the service instance. Header  
4 Removal treatment indicates to the PDSN that the Header Generator (HG) parameter initialization, parameter  
5 update and any compression/decompression operations for the forward direction are not supported by the MS  
6 for the requested service option. The HG parameter initialization is only required at the HRU in the PDSN.

7 The HRU context is initialized locally at the PDSN using static parameters received from the MS in a Resv  
8 message over the main service instance. See section 4.4.5 for MS's procedures. The dynamic parameters  
9 necessary for the Header Generator are set locally at the PDSN.

#### 10 **4.4.3.1 Normal operation**

11 For normal operation in the reverse direction, the MS outputs application payload frames over the SO 60  
12 service instance. The packets are received by the HRU in the PDSN, which effectively acts as the  
13 IP/UDP/RTP originating point by adding a header to each received application payload frame. In the forward  
14 direction, the HRU in the PDSN removes the headers and uses the interface to the HRL as specified in [16] to  
15 forward 20ms application payload frames to the MS. The MS forwards the received application payload  
16 frames directly to the HRU (codec).

### 17 **4.4.4 PDSN requirements**

#### 18 **4.4.4.1 Interface to HRL, transmitting side**

19 The sending HRU in the PDSN fulfills the interface with the HRL as defined in [16] for Header Removal. The  
20 HRU in the PDSN shall not perform the HG parameter initialization in the forward direction. The PDSN shall  
21 remove the IP/UDP/RTP headers at the HRU in the forward direction.

22 Along with each application payload frame, the PDSN shall supply a sequence number to the HRL that  
23 increments by one for each 20ms increment of the RTP Timestamp field that was removed from the frame.

#### 24 **4.4.4.2 Interface to HRL, receiving side**

25 The receiving HRU in the PDSN fulfills the interface with the HRL as defined in [16] for Header Removal.

26 The PDSN shall use the service option number (SO 60) to determine that parameters necessary for the  
27 Header Generator shall be initialized using the static parameters received from the MS.

28 Upon receiving the Resv message containing the HRIP IE, the PDSN shall validate the received fields and  
29 send a ResvConf if the HG parameter initialization was successful.

30 The PDSN shall use the static parameters included in the HRIP IE to initialize the static HG parameters. See  
31 Annex B for the complete definition of the HRIP IE.

32 The PDSN shall also populate internally the other required IP/UDP/RTP header fields, which are dynamic in  
33 nature, including RTP TS and RTP SN. How the PDSN populates the rest of the fields is an implementation  
34 issue. Subsequent RTP timestamps and sequence numbers are derived during normal operation based on  
35 the functionality of SO 60.

36 The PDSN shall increment the RTP Sequence Number by one for each generated packet, and shall set the  
37 RTP TS according to the System Time received with each application payload frame. The RTP Timestamp  
38 shall be expressed in units of codec input samples; the number of samples per 20ms frame is given in the  
39 TS\_STRIDE parameter of the RTPv2 Header Removal Subtype (see Annex B).

40 If the PDSN fails in processing the HRIP IE, it shall send a ResvErr with the appropriate error code. See  
41 section 3.2.2 for more details of processing of the Resv message. If the PDSN fails in processing some of the  
42 fields from the HRIP IE, and recovery attempts were unsuccessful, it shall send a ResvErr (see Annex B for  
43 details of the messages and object layout). If the PDSN receives application payload frames from the MS  
44 over SO 60 prior to successful completion of the HG parameter initialization phase, the frames shall be  
45 discarded.

#### 1 **4.4.5 MS requirements**

2 If the MS supports Header Removal, it shall use SO 60 when requesting establishment of an auxiliary Header  
3 Removal service instance to carry only application payload frames.

4 The MS shall populate the Header Removal Initialization Parameters Information Element (HRIP IE) within  
5 the 3GPP2 object in the Resv message with static header elements; for example, if the MS is using SIP for  
6 VoIP call control, it can use some of the SDP information [RFC2327] received during VoIP session  
7 establishment procedures. At a minimum, the following static header information shall be present in the HRIP  
8 IE:

- 9       • IPv4 or IPv6 Header Removal Subtype.
- 10       • UDP Header Removal Subtype.
- 11       • RTPv2 Header Removal Subtype.

12 Other static fields and/or encapsulation headers should also be provided.

13 The MS should wait for ResvConf before sending the application payload frames to the PDSN. If a ResvErr  
14 message is received, the MS should use its internal policy to determine if the VoIP session should be closed  
15 or send a new Resv message to the PDSN.

16 The MS shall send application payload frames from the HRU (codec) to the multiplex sub-layer. The MS shall  
17 forward the received application payload frames to the HRU (codec).

## 1 **Annex A: HRU parameter settings for LLA Header Compression**

### 2 **(normative)**

3 This section defines compressor parameter settings required by this specification for the LLA compressor to  
 4 be properly supported by the cdma2000 link. The parameters<sup>14</sup> shown in Table A- 1 shall be used as  
 5 described in section 5 of RFC3242:

Parameter name	Value type	Value	Description
ALWAYS_PAD	boolean	Shall be set to 'True'	The HRU uses the ROHC padding <sup>15</sup> (section 5 of RFC3242) to provide type identification for packets with compressed headers. The HRU shall ensure that a minimum of two padding octets is used as a leading sequence for such packets.
PREFERRED_PACKET_SIZES (list of):  SIZE:  RESTRICTED_TYPE:	Integer	Number of octets  [NHP_ONLY, RHP_ONLY, NO_RESTRICTION]	This parameter shall be set to octet-aligned values corresponding to the Data block Types of Multiplex Option 1 and Multiplex Option 2 as supported by SO 61. This parameter is required for handling non-octet aligned format of the Data blocks. Table A- 2and Table A- 3 specifies the required values for this parameter.

6 **Table A- 1 - Compressor parameter settings**

7

<sup>14</sup> The setting of other parameters suggested in RFC3242 is left to implementation

<sup>15</sup> Note that the Context Check Packet sent by the HRL is not a packet with a compressed header and is not required to be padded for rate 1/8.

1

Data block Type	Bits per Data block	Associated octet-aligned values - SIZE	RESTRICTED_TYPE
Rate 1	171 bits	22 octets (176 bits)	NHP_ONLY
		21 octets (168 bits)	RHP_ONLY
Rate 1/2	80 bits	10 octets (80 bits)	NO_RESTRICTION
Rate 1/4	40 bits	5 octets (40 bits)	NO_RESTRICTION
Rate 1/8	16 bits	2 octets (16 bits)	NO_RESTRICTION

2

**Table A- 2 - List of sizes and attributes of parameter PREFERRED\_PACKET\_SIZES for Data block Types used by Multiplex Sublayer for Multiplex Option 1**

3

Data block Type	Bits per Data block	Associated octet-aligned values - SIZE	RESTRICTED_TYPE
Rate 1	266 bits	34 octets (272 bits)	NHP_ONLY
		33 octets (264 bits)	RHP_ONLY
Rate 1/2	124 bits	16 octets (128 bits)	NHP_ONLY
		15 octets (120 bits)	RHP_ONLY
Rate 1/4	54 bits	7 octets (56 bits)	NHP_ONLY
		6 octets (48 bits)	RHP_ONLY
Rate 1/8	20 bits	3 octets (24 bits)	NHP_ONLY
		2 octets (16 bits)	RHP_ONLY

4

**Table A- 3 - List of sizes and attributes of parameter PREFERRED\_PACKET\_SIZES for Data block Types used by Multiplex Sublayer for Multiplex Option 2**

5

## 1 **Annex B: Flow Mapping, Treatment and the 3GPP2\_OBJECT (normative)**

2 The RSVP protocol [RFC 2205] provides a mechanism that can be used to signal generic QoS parameters at  
 3 the IP layer between network entities. This mechanism is largely independent of the underlying layer 2  
 4 technologies. This 3GPP2 application of flow mapping, treatment protocol is based on RSVP [RFC 2205] with  
 5 any extensions and limitations as described in this specification. The protocol is not intended to address  
 6 generic network level QoS requirements; instead, it uses RSVP based messages only to support Flow  
 7 Mapping, Header Removal, and Flow/Channel Treatment capabilities defined within a 3GPP2\_OBJECT. This  
 8 Annex describes the details of the 3GPP2\_OBJECT. The following RSVP messages [RFC 2205] shall be used  
 9 between the MS and the PDSN to support flow mapping and treatment:

- 10 • Resv message
- 11 • ResvConf message
- 12 • ResvErr message.

13 RSVP operation is restricted to the Access Network, i.e., the RSVP Resv messages are sent only from the  
 14 MS to the PDSN. The destination address of the RSVP Resv signaling messages sent from the MS is the  
 15 address of the PDSN received during the IPCP negotiation phase. This specification doesn't require the MS  
 16 to send or receive the path message for Flow mapping and treatment purposes. The MS shall be able to send  
 17 Resv messages without receiving a corresponding Path message.

18 The PDSN shall respond to the Resv message back to the MS with either a ResvConf message or a ResvErr  
 19 message to indicate whether the PDSN could act upon the object successfully. The MS may send the Resv  
 20 message a configurable number of times until a confirmation is received, or until expiry of the configurable  
 21 timer.

22 All the RSVP messages used in this specification are sent over UDP with the Protocol ID of 17 with registered  
 23 port number of 3455. All the messages (i.e., Resv, ResvErr, ResvConf) shall be sent using the destination  
 24 port of 3455 by both the PDSN and the MS. All the source port numbers may be set to any value.

### 25 **B.1 Resv Message**

#### 26 ***B.1.1 Resv Message Format***

27 All objects in the Resv message are defined to be consistent with RFC 2205.

28 The STYLE object shall occur at the end of the message. The objects shall follow the procedures specified in  
 29 RFC 2205. There are no other requirements on transmission order, although the above order is  
 30 recommended. In the usage of RSVP in this specification the order of appearance of the 3GPP2\_OBJECT  
 31 shall follow the RESV\_CONFIRM object. The Resv message format used in this specification is as follows:

```
32 <Resv Message> ::= <Common Header>
33     <SESSION> <TIME_VALUE>
34     [ <RESV_CONFIRM> ] <3GPP2_OBJECT>
35     <STYLE>
```

36 **Common Header**: mandatory, see section 3.1 of RFC 2205.

37 **SESSION**: mandatory object, see Annex A of RFC 2205. Destination IP address shall be the PDSN  
 38 IP Address, Protocol ID of 17 and DstPort of 3455. The flags field shall be zero.

39 **TIME VALUES**: mandatory object, see Annex A of RFC 2205.

40 **RESV\_CONFIRM**: optional object that shall be used by the MS in this specification. It carries the IP  
 41 address of the MS that requested the confirmation.

42 **3GPP2\_OBJECT**: see B.1.1.1.



TFTIPv6 Error	3
Header Removal	4
Header Removal Error	5
Channel Treatment	6
Channel Treatment Error	7

**Figure B- 3. IE Type #**

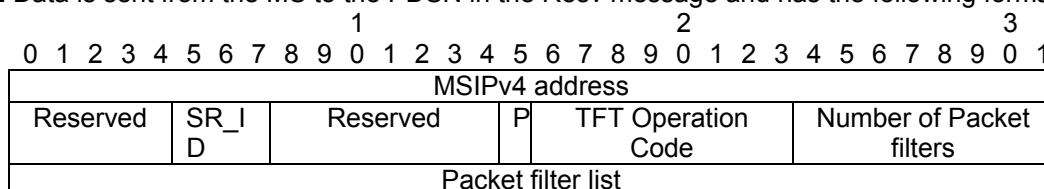
**IE Data:**

This field is specified in section B.1.1.1.1 to section B.1.1.1.3.

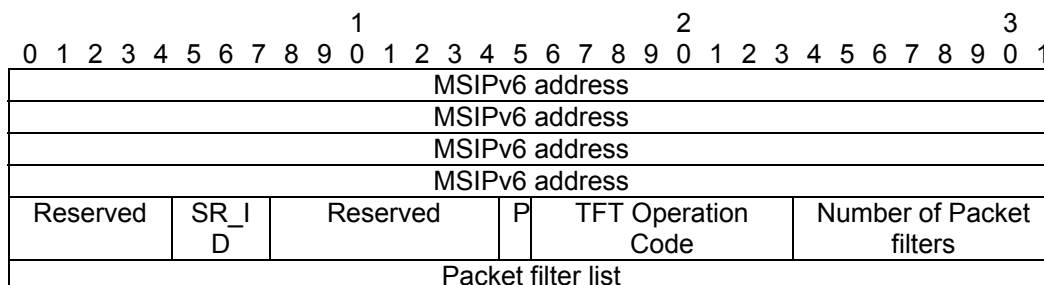
**B.1.1.1.1 Traffic Flow Template (TFT, IE Type # 0 and 2)**

The MS shall include the TFT when flow mapping of downlink traffic over multiple service instances is required in the PDSN. The MS may define a TFT for each MS IP address and per service instance. This is because an MS may have more than one IP address over a single PPP session.

The IE Data is sent from the MS to the PDSN in the Resv message and has the following format:



**Figure B- 4. TFT IPv4 IE Type # = 0**



**Figure B- 5. TFT IPv6. IE Type # = 2**

The TFT for each is coded with the following fields:

**MS IP address:**

The MS IP address is used to identify the TFT. For IE Type # = 0, the MS IP address applies to IPv4, and for IE Type # = 2, the MS IP address applies to IPv6.

**SR\_ID:**

Contains the identifier for the service instance on which the TFT applies.

**Reserved:**

This field shall be filled with all 0.

**P:**

The P (Persistency) bit is set to '1' to indicate a request from the MS to keep the TFT even if the service instance is not established or disconnected at the PDSN. Otherwise, it shall be set to '0'.

## 1 TFT operation code:

2 TFT operation code indicates an operation to be performed by the PDSN. Operation codes 0-7 are  
3 defined below and other values are reserved for future use.

4	0 0 0	Spare
5	0 0 1	Create new TFT
6	0 1 0	Delete existing TFT
7	0 1 1	Add packet filters to existing TFT
8	1 0 0	Replace packet filters in existing TFT
9	1 0 1	Delete packet filters from existing TFT
10	1 1 0	Reserved
11	1 1 1	Reserved

## 12 Number of packet filters:

13 The number of packet filters contains the binary coding for the number of packet filters in the packet  
14 filter list. For the "delete existing TFT" operation, the number of packet filters shall be coded as 0. For  
15 all other operations, the number of packet filters shall be greater than 0 and less than or equal to 15.

## 16 Packet filter list:

17 The packet filter list contains a variable number of packet filters. For the "delete existing TFT"  
18 operation, the packet filter list shall be empty.

19 For operations other than the "delete packet filters from existing TFT" operation, the packet filter list  
20 shall contain a variable number of packet filter identifiers as given in the number of packet filters field.  
21 When the code in the TFT data indicates delete packet filters (code=101), the packet filter  
22 precedence, length, and contents are not included, only the packet filters Identifiers are included.  
23 Figure B- 6 shows the packet filter list.

0	1	2	3	4	5	6	7
MSB							
Reserved				Packet filter identifier 1			
Reserved				Packet filter identifier 2			
...							
Reserved				Packet filter identifier N			

24 **Figure B- 6. Packet filter list for deleting packet filters from existing TFT**

## 25 Reserved:

26 This field shall be filled with all 0.

27 For the "create new TFT", "add packet filters to existing TFT", and "replace packet filters in existing TFT"  
28 operations, the packet filter list shall contain a variable number of packet filters. This number shall be derived  
29 from the coding of the number of packet filters field. Figure B- 7 shows the packet filter list for this case.

0	1	2	3	4	5	6	7
MSB							
Reserved				Packet filter identifier 1			
Packet filter evaluation precedence 1							
Packet filter length							
Packet filter length							
Packet filter contents 1							
...							
Packet filter treatment 1							
...							
Reserved				Packet filter identifier 2			
Packet filter evaluation precedence 2							
Packet filter length 2							
Packet filter length 2							

Packet filter contents 2
...
Packet filter treatment 2
...
...
Reserved
Packet filter identifier N
Packet filter evaluation precedence N
Packet filter length N
Packet filter length N
Packet filter contents N
...
Packet filter treatment N
...

**Figure B- 7. Packet Filter Layout for TFT create, add, or modify operations**

Each packet filter is of variable length and consists of following fields:

- A packet filter identifier (4 bitd);
- A packet filter evaluation precedence (1 octet);
- The length of the packet filter (2 octet);
- The packet filter contents sub-options (variable number of octets);
- An optional flow treatment sub-option (variable number octets).

**Packet filter identifier (PFid) (4 bits):**

The packet filter identifier field is used to identify each packet filter in a TFT. The maximum number of packet filters in a TFT is 15. The packet filter identifier occupies the least significant 4 bits.

**Packet filter evaluation precedence (1 octet):**

The packet filter evaluation precedence field is used to specify the precedence for the packet filter among all packet filters in all TFTs associated with the MS IP address. The evaluation precedence index is in the range of 0-255. The higher the value of the packet filter evaluation precedence field, the lower the precedence of that packet filter. The first bit in transmission order is the most significant bit. If a given packet matches more than one of the currently active packet filters, the SR\_ID and flow treatment for the packet should be taken from the packet filter of highest precedence. A given precedence level may be used only once per MS IP address, except 255 which is used as an indication of no precedence.

**Packet filter length (2 octets):**

The length of the packet filter length field contains the binary coded representation of the length of the packet filter including the packet filter content sub-option and packet flow treatment sub-option if included. The length is coded as two octets. The first bit in transmission order is the most significant bit.

**Packet filter content (variable octets):**

The packet filter content is coded in a TLV format and may be included in the packet filter. The PF Type 0 indicates components of the outer or first IP header. PF Type 0 may also include transport header fields if no encapsulation is in use. PF Type 1 indicates packet filter content of the transport layer (e.g., UDP or TCP port number, SPI, etc.).

Each Packet filter content is structured as a sequence of header components. A header component is a component type identifier, which indicates what IP header field is to be matched, followed by a value to be matched against. Components type identifier within a packet filter may appear in any

1 order but a given component type identifier shall not appear more than once inside the same packet  
2 filter content.

3 The packet filter content contains a type, length and value. The packet filter type is one octet. The  
4 length is one octet and indicates the length of the packet filter component type identifiers and the  
5 associated fixed size packet filter component values. The value is a variable size list of packet filter  
6 components. Each component is associated with a packet filter component identifier. The format of a  
7 packet filter contents is as follows:

0	1	2	3	4	5	6	7	
MSB								
PF Type (0-1)								1 octet
Length								1 octet
Packet filter component type identifier								1 octet
Packet filter component								variable
...								
Packet filter component type identifier								1 octet
Packet filter component								variable
...								

8 **Figure B- 8. Packet Filter Content**

9 **PF Type:**

10 The Packet Filter Type value ranges from 0 to 1. PF Type 0 applies to the outer IP header of the  
11 packet that the PDSN is transmitting to the MS. PF Type 0 may also include transport header fields if  
12 no encapsulation is in use. PF Type 1, if included, applies to the encapsulated transport layer header  
13 (e.g., port numbers, SPI, etc.) of the forward direction traffic.

14 **Length:**

15 The length is one octet and indicates the length of the packet filter associated to the PF Type. Its  
16 value includes the length of the PF Type field, the length field and the packet filter components fields.

17 **Packet filter component identifier (1 octet):**

Bits		
0 1 2 3 4 5 6 7		
0 0 0 1 0 0 0 0	(16)	IPv4 Source Address <sup>16</sup>
0 0 1 0 0 0 0 0	(32)	IPv6 Source Address
0 0 0 1 0 0 0 1	(17)	IPv4 Destination Address
0 0 1 0 0 0 0 1	(33)	IPv6 Destination Address / Prefix Length
0 0 1 1 0 0 0 0	(48)	Protocol /Next header
0 1 0 0 0 0 0 0	(64)	Single Destination Port
0 1 0 0 0 0 0 1	(65)	Destination Port range
0 1 0 1 0 0 0 0	(80)	Single Source Port
0 1 0 1 0 0 0 1	(81)	Source Port range
0 1 1 0 0 0 0 0	(96)	Security Parameter Index
0 1 1 1 0 0 0 0	(112)	Type of Service/Traffic Class
1 0 0 0 0 0 0 0	(128)	Flow label

32 All other values are reserved.

33 **Packet filter component (variable octets):**

34 In each packet filter content, there shall not be more than one occurrence of each packet filter  
35 component. Among the "IPv4 Source Address" and "IPv6 Source Address " packet filter components,  
36 only one shall be present in one packet filter. Among the "single destination port" and "destination

<sup>16</sup> For SIP based signaling, IPv4/IPv6 Destination Address and Destination Port correspond to those used in SDP negotiation.

1 port range" packet filter components, only one shall be present in one packet filter. Among the "single  
2 source port" and "source port range" packet filter components, only one shall be present in one  
3 packet filter.

4 The IPv4 Source Address shall be transmitted first, if it is included in the packet filter content. It  
5 consists of an IPv4 Source Address and a Subnet Mask. The IPv4 Source Address and Subnet Mask  
6 are matched against the IPv4 Source Address in the outer IPv4 header of the forward direction  
7 packet.

8 The IPv6 Source Address<sup>17</sup>, packet filter component value field shall be encoded as a sequence of a  
9 sixteen octet IPv6 Source Address field and a one octet Prefix Length field. The IPv6 Source Address  
10 field shall be transmitted first, if it is included in the packet filter content. The address up to the Prefix  
11 Length is matched against the IPv6 Source Address in the outer IPv6 header of the forward direction  
12 packet.

13 The IPv4 Destination Address packet filter component shall be encoded as a sequence of a four  
14 octets IPv4 Destination Address field. An address mask is not included with this element. The  
15 address is matched against the destination address in the outer IPv4 header of the forward direction  
16 packet.

17 The IPv6 Destination Address packet filter component shall be encoded as a sequence of a sixteen-  
18 octet IPv6 address field. The prefix length is included with this element. The address shall be  
19 matched against the destination address in the outer IPv6 of the forward direction packet.

20 The Protocol /Next Header packet filter component shall be encoded as one octet that specifies the  
21 Protocol field of the IPv4 header or IPv6 Next Header. The value range is from 0 to 255.

22 The Single Destination Port and Single Source Port packet filter component value field shall be  
23 encoded as two octets that specify a port number. Port numbers range between 0 and 65535.

24 The Destination Port range and Source Port range packet filter component value field shall be  
25 encoded as a sequence of two octets for the lower limit of the range and two octets for the higher limit  
26 of the range. The lower limit field of the port range shall be transmitted first. Port numbers range  
27 between 0 and 65535.

28 The Security Parameter Index packet filter component field shall be encoded as four octets that  
29 specify the IPsec SPI.

30 The Type of Service (IPv4)/Traffic Class (IPv6) packet filter component shall be encoded as a  
31 sequence of a one octet Type of Service/Traffic Class field and a one octet Type of Service/Traffic  
32 Class mask field. The Type of Service /Traffic Class mask determines which bits of the Type of  
33 Service or Traffic Class octet the PDSN will use to match against the actual value of the  
34 corresponding field in the IP packets. The mask contains ones in the bit positions to be used in the  
35 matching operation.

36 The Flow label packet filter component shall be encoded as three octets that specify the IPv6 flow  
37 label. The bits 0 through 3 of the first octet shall be used for padding whereas the remaining 20 bits  
38 shall contain the IPv6 flow label as per RFC 2460.

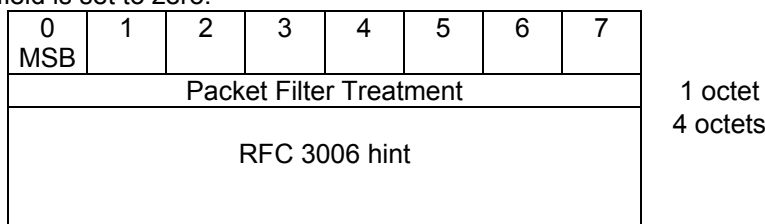
### 39 **Packet Filter (flow) Treatment:**

40 The packet flow treatment specification is optionally provided as a way for MSs to specify per-flow treatments.  
41 If any octets remain after parsing the packet filter contents, they are interpreted as a packet filter treatment.

---

<sup>17</sup> Source addresses of forward direction packet flows belong to correspondent nodes and are sometimes subject to change due to e.g., renumbering [RFC 2461] or privacy [RFC 3041]. The MS should not include a source address packet filter component unless it is reasonably sure that the IP address of the correspondent node will not change for the life of the application flow or is willing to update the TFT when such a change takes place.

1 The first octet indicates the packet filter treatment (PFT) type, and 4 octets indicate flow treatment  
 2 specification. Only the treatments given in the packet filter hints table make use of the hints field; for other  
 3 treatments the hints field is set to zero.



4 **Figure B- 9. Packet Filter Treatment (PFT)**

Treatment	PFT
Header Compression	0
Reserved	1-255

6 **Figure B- 10. PFT Values**

7 RFC 3006 hints are four octets and the following are applicable herein:

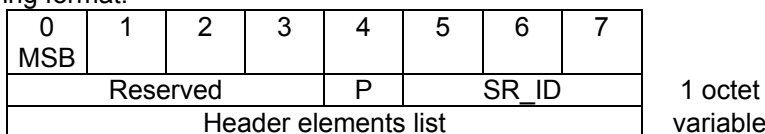
Type	Value
IP/TCP data that may be compressed according to [RFC 1144]	0x002d0000
IP data that may be compressed according to [RFC 2507]	0x00610000
ROHC uncompressed profile [RFC3095]	0x00030000
ROHC RTP profile [RFC3095]	0x00030001
ROHC UDP profile [RFC3095]	0x00030002
ROHC ESP profile [RFC3095]	0x00030003
ROHC LLA profile [RFC3242]	0x00030005
ROHC LLA profile [RFC3408] (extension for R-Mode)	0x00030105
ECRTP [RFC 3545]	0x00610200

8 **Figure B- 11. PFT Hints**

9 Note that no specific treatment or hint is needed for Header Removal or ROHC LLA compression operation,  
 10 because the PDSN can infer the use of LLA Header Removal or LLA Header Compression from the service  
 11 option number (e.g., SO 60 or SO 61) of the service instance (given by the SR\_ID in the TFT IE header) onto  
 12 which the flow is being mapped.

#### 13 B.1.1.1.2 Header Removal Initialization Parameters (IE Type # = 4)

14 This IE is included when header initialization is required for the purpose of Header Removal operation. The  
 15 field is sent from the MS to the PDSN in the Resv message. The field includes static header information and  
 16 is coded in the following format.



17 **Figure B- 12. Header Removal : IE Type # = 4**

18 **Reserved:**

1 This field shall be filled with all 0.

2 **P:**

3 The P (Persistency) bit is set to '1' to indicate a request from the MS to keep the Header Removal  
4 Initialization Parameters even if the service instance is not established or disconnected at the PDSN.  
5 Otherwise, it shall be set to '0'.

6 The following figure shows the detail of each element of the header element list in the previous figure:

0	1	2	3	4	5	6	7	
MSB								
Header Type								1 octet
Length								1 octet
Header Contents								variable

7 **Figure B- 13. Header Element List**

8 Each header element is coded per Figure B- 14:

IPv4	1
IPv6	2
IPv6 extension header	3
UDP	4
RTPv2	5
GRE	7
Minimal Encapsulation Header	8

9 **Figure B- 14. Header Element Types**

10 **Subtype value: IPv4**

0	1	2	3	4	5	6	7	
MSB								
Protocol								1 octet
Source address								4 octets
Destination address								4 octets
Type of service								1 octet
Time to Live								1 octet

11 **Figure B- 15. Header Removal Subtype IPv4**

12 **Subtype value: IPv6**

0	1	2	3	4	5	6	7	
MSB								
0	0	0	0	Flow label (msb)				1 octet
Flow label (lsb)								2 octets
Next header								1 octet
Source address								16 octets
Destination address								16 octets
Traffic class								1 octet
Hop limit								1 octet

13 **Figure B- 16. Header Removal Subtype IPv6**

14 **Subtype value: IPv6 extension header**

0	1	2	3	4	5	6	7	
MSB								
Next header								1 octet

Header extension length	1 octet
Extension payload data	variable

1 **Figure B- 17. Header Removal Subtype IPv6 Extensions**

2 This extension header is suitable for carrying Routing Headers, Hop-by-Hop Options, or Destination Options.

3 **Subtype value: UDP**

0	1	2	3	4	5	6	7
MSB							
Source port				2 octets			
Destination port				2 octets			

4 **Figure B- 18. Header Removal Subtype UDP**

5 **Subtype value: RTPv2**

0	1	2	3	4	5	6	7
MSB							
SSRC				4 octets			
Rese	PT			1 octet			
rved							
TS_STRIDE				2 octets			

6 **Figure B- 19. Header Removal Subtype RTPv2**

7 **Reserved:**

8 This field shall be set to 0.

9 **Subtype value: GRE**

0	1	2	3	4	5	6	7
MSB							
C	rsvd	K	S	Reserved			
Protocol type				1 octet			
Key field				4 octets			

10 **Figure B- 20. Header Removal Subtype GRE**

11 **Reserved:**

12 This field shall be set to 0.

13 **Subtype value: Minimal encapsulation**

0	1	2	3	4	5	6	7
MSB							
Protocol type				1 octet			
S	Reserved			1 octet			
Original destination address				4 octets			
Original Source Address (if S=1)				4 octets			

14 **Figure B- 21. Header Removal Subtype Minimal Encapsulation**

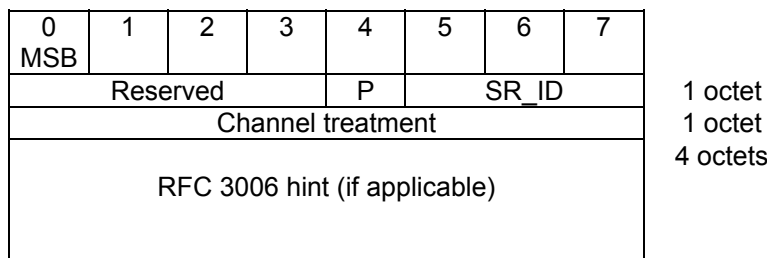
15 **Reserved:**

16 This field shall be filled with all 0.

17 **B.1.1.1.3 Channel Treatment (IE Type # = 6)**

18 This IE is included when channel treatment is required. The field is sent from the MS to the PDSN in a Resv message. The field includes channel treatment information and is coded in the following format.

1



2

**Figure B- 22. Channel Treatment IE Type # = 6****Reserved:**

4 This field shall be filled with all 0.

**P:**

6 The P (Persistency) bit is set to '1' to indicate a request from the MS to keep the Header  
7 Compression context even if the service instance is not established at the PDSN. Otherwise, it shall  
8 be set to '0'.

**Channel Treatment:**

10 The channel treatment specification is provided as a way for MSs to specify per-channel default  
11 treatments. First octet indicates channel treatment (CT) type, and 4 octets indicate channel treatment  
12 specification, which is applicable for CT values 0-4.

Treatment	CT
Header Compression	0
Reserved	1-255

13

**Figure B- 23. CT Values**

14 RFC 3006 hints are four octets and the following are applicable herein. Only the treatments given in  
15 the channel treatment hints table make use of the hints field; for other treatments the hints field is set  
16 to zero.

Type	Value
IP/TCP data that may be compressed according to [RFC 1144]	0x002d0000
IP data that may be compressed according to [RFC 2507]	0x00610000
ROHC uncompressed profile [RFC3095]	0x00030000
ROHC RTP profile [RFC3095]	0x00030001
ROHC UDP profile [RFC3095]	0x00030002
ROHC ESP profile [RFC3095]	0x00030003
ROHC LLA profile [RFC3242]	0x00030005
ROHC LLA profile R-Mode [RFC3408] (extension for R-Mode)	0x00030105
ECRTP [RFC 3545]	0x00610200

17

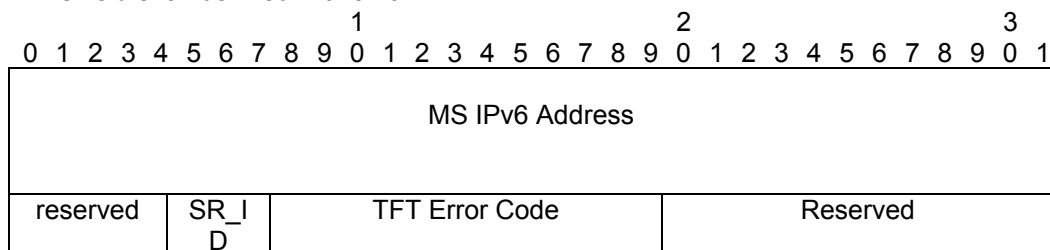
**Figure B- 24. CT Hints**

18 Note that no specific treatment or hint is needed for Header Removal or ROHC LLA compression operation,  
19 because the PDSN can infer the use of Header Removal or LLA compression from the service option number  
20 (e.g., SO 60 or SO 61) of the service instance given by the SR\_ID in the Channel Treatment IE header.



1 **Reserved:**

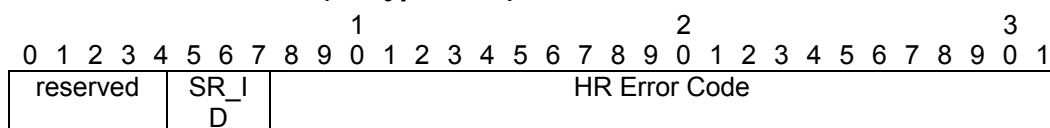
2 This field shall be filled with all 0.

3 **Figure B- 26. TFT IPv6 Error: IE Type # = 3**4 **Reserved:**

5 This field shall be filled with all 0.

6 **TFT error code:**

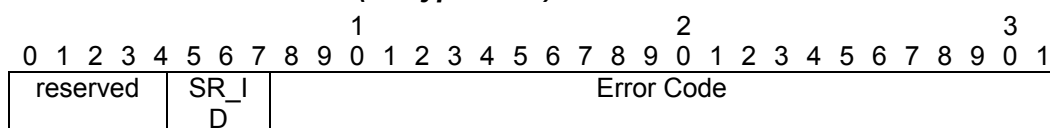
7	TFT error codes indicate that the TFT operation requested by the MS was unsuccessful.	
8	00000000	Reserved
9	00000001	Packet filter add failure
10	00000010	Packet filter unavailable
11	00000011	Unsuccessful TFT processing
12	00000100	Channel not available
13	00000101	Evaluation precedence contention
14	00000110	Treatment not supported
15	00000111	Packet filter replace failure
16	00001000	Persistency Limit Reached
17	00001001	Persistency Not Allowed

18 **B.3.2 Header Removal Error (IE Type # = 5)**19 **Figure B- 27. HR Error: IE Type # = 5**20 **Reserved:**

21 This field shall be filled with all 0.

22 **HR Error Code:**

23	00000000	Reserved
24	00000001	Invalid header parameter
25	00000100	Channel not available
26	00000111	Persistency Limit Reached
27	00001000	Persistency Not Allowed

28 **B.3.3 Channel Treatment Error (IE Type # = 7)**29 **Figure B- 28. Channel Treatment Error: IE Type # = 7**30 **Reserved:**

1 This field shall be filled with all 0.

2 **Treatment Error Code:**

3	00000000	Reserved
4	00000001	Invalid Treatment
5	00000010	Treatment not supported
6	00000100	Channel not available
7	00000110	Treatment not supported
8	00000111	Persistency Limit Reached or
9	00001000	Persistency Not Allowed

10 **B.4 Reliable Delivery of RSVP Messages**

11 The MS shall include the RESV\_CONFIRM object in the Resv message and send it to the PDSN. The MS  
12 may send the Resv message a configurable number of times until a confirmation is received.

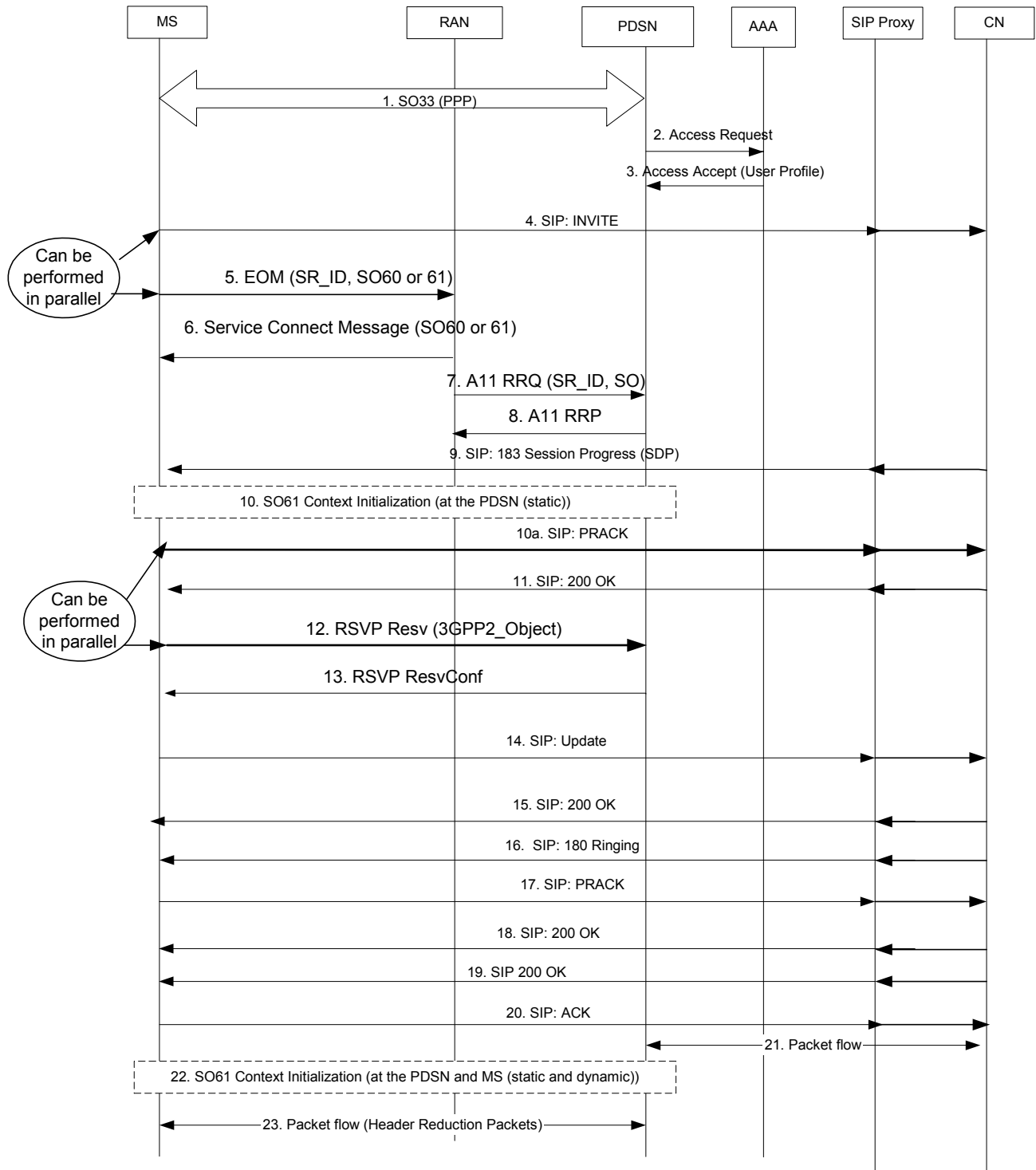
## 1 **Annex C: Example of VoIP call flow with Header Reduction techniques** 2 **(normative)**

### 3 **Introduction:**

4 This Annex includes an informative VoIP setup call flow over the main service instance and shows the flow of  
5 SIP signaling, setup of an auxiliary service instance of SO type 60 or 61, signaling for TFT, Header Removal  
6 parameter initialization (for Header Removal, SO 60) over the main service instance and in-band context  
7 initialization (for LLA ROHC over SO 61) and bearer path establishment. The order in which some of the  
8 steps are performed is shown as an example only and is not part of this specification. Some steps in the  
9 figure can also be performed in parallel.

### 10 **Call Flow:**

11 Figure C- 1 shows an example of an MS originated call flow for VoIP.



1  
2  
3  
4  
5  
6  
7

**Figure C- 1. An example of MS originated call flow for VoIP**

1. The MS establishes the SO33 (main service instances) with RLP retransmissions enabled. The MS establishes a PPP session with the PDSN. The MS indicates its Header Compression capabilities (e.g., ROHC, LLAROH, VJHC) to the PDSN. The main service instance provides a communication channel for the MS to send and receive control messages and user data.

- 1 2. The PDSN sends a RADIUS Access-Request message to the RADIUS server containing the MS's
- 2 Network Access Identifier (NAI) and credential. The credential is an authenticator computed by the MS in
- 3 response to CHAP (if Simple IP is used) or FA Challenge (if Mobile IP is used).
- 4 3. If the MS is authenticated successfully, the RADIUS server sends a RADIUS Access-Accept message
- 5 containing the user subscription profile.
- 6 The steps 4 and 5 described as follows can be performed in parallel.
- 7 4. The MS sends a SIP Invite to the correspondent Node (CN).
- 8 5. The MS sends EOM with SO set to 60 or 61 to establish the auxiliary service instance. If the MS cannot
- 9 determine which codec to use it may send an EOM for SO 60 or SO 61 after codec negotiation is
- 10 performed at step 9.
- 11 6. The RAN sends a Service Connect Message to connect the service.
- 12 7. The RAN sets up A8 and A10 connection. The figure only shows the A10 connection setup via A11 RRQ
- 13 Message sent from the RAN to the PDSN.
- 14 8. The PDSN sends an A11 RRP to the RAN.
- 15 9. In response to step 4, the CN sends a SIP 183 Session Progress including SDP.
- 16 The steps 10 and 12 described as follows can be performed in parallel.
- 17 10. If the MS has established SO 61, it may start context initialization operation of the decompressor at the
- 18 PDSN to initialize the static context (IR packet with zero payload), in band over SO 61. The MS responds
- 19 with a SIP PRACK to the CN.
- 20 a. The MS responds with SIP PRACK to the CN.
- 21 11. The CN responds with a SIP 200OK.
- 22 12. Triggered by the step 9 (SIP: 183 Session Progress), the MS sends an RSVP Resv Message including
- 23 the 3GPP2\_OBJECT: TFT IE, and Header Removal Initialization Parameters (if Header Removal is
- 24 used). If the MS negotiates SDP in the step 10, this step may be triggered by the step 11.
- 25 13. The PDSN sends an RSVP ResvConf message to the MS.
- 26 14. After bearer path and flow mapping are successfully established, the MS sends a SIP Update message to
- 27 the CN.
- 28 15. The CN sends 200OK to the MS.
- 29 16. The CN sends SIP 180 ringing to the MS after the CN starts to ring.
- 30 17. The MS sends SIP PRACK for acknowledgement.
- 31 18. The CN responds with SIP 200OK to the MS.
- 32 19. The CN user picks up the call and the CN sends SIP 200OK to the MS.
- 33 20. The MS sends an SIP ACK to the CN.
- 34 21. Packet Data (VoIP) flows.
- 35 22. For SO 61, the PDSN performs in-band over SO 61 service instance the static and dynamic context
- 36 initialization of the decompressor at the MS based on the first IP/UDP/RTP header packet(s) it receives
- 37 from the CN. For completion of the PDSN decompressor context initialization, the MS initializes the
- 38 dynamic context at the PDSN over SO 61 service instance during the first IP/UDP/RTP packet(s) it sends
- 39 to the CN.
- 40 23. The PDSN and the MS are sending Header Reduction packets.

41 **Notes:**

- 1 1. SIP signaling is used as an example for this call flow. If SIP signaling is not used for call control,  
2 the MS can perform step 5 or step 12 once the main service instance is established and the MS  
3 knows the session related characteristics.
- 4 2. Based on step 3 (user profile) and its capability, the PDSN determines whether to accept step 7  
5 (bearer path setup).
- 6 3. In case that the PDSN receives RSVP Resv containing the TFT IE, the HRPI IE or the CT IE and  
7 the A10 connection hasn't been established yet, the PDSN determines based on the presence of  
8 the persistency bit and the user profile if it accepts the request. If the PDSN determines that the  
9 request shall be rejected, it shall return ResvErr to the MS to indicate that the channel is not  
10 available or persistency not allowed or persistency limit reached. Else it sends a ResvConf  
11 message. If the MS receives ResvErr with error code of channel not available, the MS may  
12 retransmit the Resv message a configurable number of times until a ResvConf message is  
13 received, or until expiry of the configurable timer. If flow mapping has failed, the MS shall tear  
14 down the over the air service connection, which will trigger the A8 and 10 connections released.
- 15 4. The PDSN should not tear down the A10 connection even it does not receive Resv for packet  
16 filter. This allows the MS to set up auxiliary service instance only used for reverse link.

**1 Annex D: Main Service Instance Timer (normative)**

Timer	Description	Default
Twait_main	This timer is used when an R-P connection request for a new MS is received at the PDSN and the request does not correspond to an SO type of 33/59. This timer is provisioned at the PDSN to wait for an R-P connection of SO type 33/59 to initiate PPP negotiation with the MS.	2s

2

3