3GPP2 C.S0085-A
Version 1.0
Date: 3 June 2010

VoIP Codecs and Protocols

Revision History

Revision	Description of changes	Date
C.S0085-0 v1.0	Initial publication	18 May 2007
C.S0085-A v1.0	Revision A	3 April 2009
C.S0085-A v1.0	Revision A replacement text	3 June 2010

Note: This specification is a replacement version of C.S0085-A v1.0. This version corrects editorial issues in the foreword, scope, and references sections of the document.

Contents

Foreword

(This foreword is not part of this specification.)

This technical specification recommends codecs as well as protocol configuration for efficient support of VoIP over HRPD. Recommendations are provided for parameter values for transport protocols, RoHC, RLP and RLMAC. Also a pre-configured provisioned session is also defined for use in supporting non-authorized access for VoIP emergency services.

1 Scope

This specification includes recommendations for VoIP codecs as well as protocol configuration to enable efficient support of VoIP over HRPD Rev A and HRPD Rev B. VoIP codecs are chosen from existing 3GPP2 technologies keeping in mind system efficiency as well as quality considerations. Recommendations are provided for transport protocols as well as for 3GPP2-specific system parameter settings for RoHC, RLP and RLMAC.

A pre-configured provisioned session is also defined for use in supporting non-authorized access for VoIP emergency services.

2 References

The following standards are referenced in this text. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based upon this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

Normative References

[1] 3GPP2 C.S0014-B v1.0, "Enhanced Variable Rate Codec, Speech Service Options 3 and 68 for Wideband Spread Spectrum Digital Systems", May 2006.

[2] 3GPP2 C.S0014-A v1.0, "Enhanced Variable Rate Codec, Speech Service Option 3 for Wideband Spread Spectrum Digital Systems", May 2004.

[3] 3GPP2 C.S0014-C v1.0, "Enhanced Variable Rate Codec, Speech Service Options 3, 68 and 70 for Wideband Spread Spectrum Digital Systems", February 2007.

[4] IETF RFC 3095, Borman, et al, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", July 2001.

[5] 3GPP2 C.S0055-A v1.0, "Packet Switched Video Telephony Services (PSVT/MCS)", June 2008.

[6] 3GPP2 C.S0024-A v3.0, "cdma2000 High Rate Packet Data Air Interface Specification", September 2006.

[7] IETF RFC 3264, Rosenberg and Schulzrinne, "An Offer/Answer Model with the Session Description Protocol (SDP)", June 2002.

[8] 3GPP2 X.S0013-004-A v1.0, "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP – Stage 3", November 2005.

[9] Reserved..

[10] 3GPP2 C.S0024-B v2.0, "cdma2000 High Rate Packet Data Air Interface Specification", March 2007

[11] Reserved.

[12] 3GPP2 C.R1001-F "Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards", January 2007.

[13] 3GPP2 C.S0063-A v2.0, "cdma2000 Packet Data Supplemental Services", March 2007.

[14] 3GPP2 X.S0011-D v2.0 "cdma2000 Wireless IP Network Standards: Books 1-6, November 2008.

[15] Reserved.

Informative References

[16] 3GPP2 C.S0076-0 v1.0, “Discontinuous Transmission (DTX) of Speech in cdma2000 Systems”, December 2005

[17] 3GPP2 X.S0049-0 v1.0, “All-IP Network Emergency Call Support”, February 2008

[18] 3GPP2 X.S0060-0 v1.0 “HRPD Support for Emergency Services”, July 2008

3 Definitions, Symbols and Abbreviations

This section contains definitions, symbols and abbreviations that are used throughout the document.

3.1 Symbols and Abbreviations

3GPP2	3rd Generation Partnership Project 2
EMFPA	Enhanced Multi Flow Packet Application
EVRC	Enhanced Variable Rate Codec
EVRC-B	Enhanced Variable Rate Codec-B
EVRC-WB	Enhanced Variable Rate Codec- Wideband
HRPD	High Rate Packet Data
IP	Internet Protocol
IP-ID	Internet Protocol Identifier
MAC	Medium Access Control
QoS	Quality of Service
RFC	Request for Comments
RLMAC	Reverse Link Medium Access Control
RLP	Radio Link Protocol
RoHC	Robust Header Compression
RS-1	Rate Set-1
RTP	Real Time Protocol
SIP	Session Initiation Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol

4 SDP Offer/Answer

The SDP offer typically contains at least one audio media line (m=) offering one or more RTP payload formats. For each media line, the codecs are listed in order of decreasing preference with the most preferred codec listed first.

The SDP answer for each audio media line (m=) typically contains only one codec format, i.e., the first codec format in the offer that can be used by the answering VoIP Terminal for the VoIP session.

The selection of the voice codec and any parameters (for example [9]) associated with the codec used in a VoIP call shall follow [7] for non-IMS call control scenarios and [8] for IMS call control scenarios.

5 Media

5.1 Voice

5.1.1 Narrowband

Narrowband-only VoIP terminals shall support EVRC-B [1] and EVRC [2] codecs. EVRC-B is the default and most preferred voice codec for these VoIP terminals. The audio m-lines of the SDP offer shall contain EVRC-B as one of the offered codecs.

5.1.2 Wideband

Wideband-capable VoIP terminals shall support EVRC-WB [3] in addition to EVRC-B and EVRC codecs. EVRC-WB is the default and most preferred codec for wideband-capable VoIP terminals. The audio m-lines of the SDP offer shall contain EVRC-WB as one of the offered codecs.

5.2 VoIP Transport

5.2.1 RTP Header and Packetization

Maintaining low end-to-end delays is important for VoIP. Thus, a VoIP terminal shall send VoIP frames without any bundling, i.e., each speech frame in a separate RTP packet.

5.2.2 Header Compression

To reduce RTP/UDP/IP overhead, a VoIP terminal shall use Robust Header Compression (RoHC) [4] to compress IP/UDP/RTP headers for VoIP flows. The recommended configuration for RoHC is described below:

The recommended profile to use is the RTP profile.

The recommended mode of operation is the Optimistic 'O' mode (Even this in case, RoHC starts in the Unidirectional 'U' mode, as defined in [4], and then transitions to the 'O' mode).

Timer-based compression is recommended to compress the RTP timestamp.

To ensure robust operation, it is recommended to set the window size (as used in Window-Based LSB encoding) to 6.

To ensure robust operation, it is recommended to set the number of updates sent by the RoHC compressor as per the Optimistic Approach principle to 6.

To ensure that RoHC can tolerate jitter on the air link when doing timer-based compression, it is recommended to set the value of Max_Jitter_CD (Max_Jitter_CD is the upper bound of jitter expected on the communication channel between compressor and decompressor) to 150 msec.

To handle out-of-order packets, it is recommended to set the 'p' value for RTP SN (Sequence Number) to 6. Note that [4] recommends setting this parameter to 1, but it assumes a reordering-free channel. Since reordering is likely to happen over an HRPD channel, it is recommended to set this parameter to a value that is large enough to handle this reordering.

In order to enable timer-based compression, the VoIP Terminal should set the parameter TimerBasedCompressionSupported in the ATSupportedFlowProtocolParameters04 or ATSupportedRouteProtocolParameters04 attribute to 1 when the Flow Protocol or Route Protocol is RoHC. Also, when the Flow Protocol or Route Protocol is RoHC, the parameter TimerBasedCompression in the FlowNNFlowProtocolParametersRev or FlowNNRouteProtocolParametersRev attribute should be set to 1.

To handle the IP-ID (IP Identification) efficiently for IPv4, it is recommended to set the IP-ID to the same value as the RTP SN. This ensures that the IP-ID is completely compressed away by the RoHC compressor.

6 HRPD System Configuration for VoIP Flow

6.1 RLP (Radio Link Protocol) Configuration

The recommended Enhanced Multi-Flow Packet Application [13] RLP configuration for a VoIP flow is as follows (note that not all the RLP parameters are shown here; only those that are critical for efficient support of VoIP are shown):

FlowRRNakEnableFwd: 0x00 (Nak-based retransmission disallowed)

FlowRRNakEnableRev: 0x00 (Nak-based retransmission disallowed)

FlowRRPhysicalLayerNakEnableRev: 0x00 (RLP is to ignore physical layer Reverse Traffic Packets missed indication)

ReservationMMIdleStateFwd: 0x01 (Closes when connection is closed)

ReservationMMIdleStateRev: 0x01 (Closes when connection is closed)

FlowRRSequenceLengthFwd: 0x00 (6-bit sequence number)

FlowRRSequenceLengthRev: 0x00 (6-bit sequence number)

FlowRRFlowProtocolPDUFwd: 0x01 (Packet stream)

FlowRRFlowProtocolPDURev: 0x01 (Packet stream)

FlowRRDataUnitFwd: 0x01 (Segment sequencing)

FlowRRDataUnitRev: 0x01 (Segment sequencing)

FlowRRRouteProtocolPDUFwd: 0x01 (Packet stream)

FlowRRRouteProtocolPDURev: 0x01 (Packet stream)

FlowRROutOfOrderDeliveryToRouteProtocolFwd: 0x01 (Out-of-order delivery allowed)

FlowRRTimersFwd:

AbortTimer: 0x00c8 (200 msec). This assumes that RoHC supports out-of-order delivery.

FlowRRTimersRev:

AbortTimer: 0x00c8 (200 msec). This assumes that RoHC supports out-of-order delivery.

FlowRRTransmitAbortTimerRev: 0x0028 (200 msec).

6.2 RLMAC (Reverse Link Medium Access Control) Configuration

The recommended RLMAC configuration for a VoIP flow is shown below. Note that not all RLMAC parameters are mentioned here; all other RLMAC parameters should be set as per the default values in [6][10]. Also, it is recommended to use direct Rise over Thermal based measurement control on the Reverse Link.

CommonPowerParameters

AllocationStagger: *0000*

TxT2Pmin: *0x1A*

RPCStep: *01*

PowerParameters128

LoLatT2PTransition128: *0x2*

LoLatTerminationTarget128: *0x2*

HiCapT2PTransition128: *0x3*

HiCapTerminationTarget128: *0x3*

T2PLoLatPreTransition128: *0x0D*

T2PLoLatPostTransition128: *0x03*

T2PHiCapPreTransition128: *0x03*

T2PHiCapPostTransition128: *0x03*

PowerParameters256

LoLatT2PTransition256: *0x2*

LoLatTerminationTarget256: *0x2*

HiCapT2PTransition256: *0x3*

HiCapTerminationTarget256: *0x3*

T2PLoLatPreTransition256: *0x1A*

T2PLoLatPostTransition256: *0x0F*

T2PHiCapPreTransition256: *0x0F*

T2PHiCapPostTransition256: *0x0F*

PowerParameters512

LoLatT2PTransition512: *0x2*

LoLatTerminationTarget512: *0x2*

HiCapT2PTransition512: *0x3*

HiCapTerminationTarget512: *0x3*

T2PLoLatPreTransition512: *0x26*

T2PLoLatPostTransition512: *0x1C*

T2PHiCapPreTransition512: *0x1C*

T2PHiCapPostTransition512: *0x1C*

PowerParameters768

LoLatT2PTransition768: *0x2*

LoLatTerminationTarget768: *0x2*

HiCapT2PTransition768: *0x3*

HiCapTerminationTarget768: *0x3*

T2PLoLatPreTransition768: *0x2E*

T2PLoLatPostTransition768: *0x23*

T2PHiCapPreTransition768: *0x23*

T2PHiCapPostTransition768: *0x23*

PowerParameters1024

LoLatT2PTransition1024: *0x2*

LoLatTerminationTarget1024: *0x2*

HiCapT2PTransition1024: *0x3*

HiCapTerminationTarget1024: *0x3*

T2PLoLatPreTransition1024: *0x32*

T2PLoLatPostTransition1024: *0x28*

T2PHiCapPreTransition1024: *0x28*

T2PHiCapPostTransition1024: *0x28*

BucketLevelMaxNN: *0x66*

TransmissionModeNN: *0x01*

BucketFactorNN

NumT2PAxisValues: *0x0*

NumFRABAxisValues: *0x0*

T2PAxis00: *0x00*

FRABAxis0: *0x8*

BucketFactorT2PAxis00FRABAxis0: 0x08

T2PInflowRangeNN (NN > 0)		
T2PInflowmin:	*0x0F*	
T2PInflowmax:	*0x78*	
T2PTransitionFunctionNN (NN > 0)		
NumT2PAxisValues:		*0x2*
NumFRABAxisValues:	*0x0*	
T2PAxis00:		*0x00*
T2PAxis01:		*0x34*
T2PAxis02:		*0x35*
FRABAxis0:	*0x8*	
T2PUpT2PAxis00FRABAxis0:	*0x1C*	
T2PUpT2PAxis01FRABAxis0:	*0x1C*	
T2PUpT2PAxis02FRABAxis0:	*0x88*	
T2PDnT2PAxis00FRABAxis0:	*0xB0*	
T2PDnT2PAxis01FRABAxis0:	*0xB0*	
T2PDnT2PAxis02FRABAxis0:	*0xB0*	

7 HRPD System Configuration for SIP Flow

7.1 RLP (Radio Link Protocol) Configuration

The recommended Enhanced Multi-Flow Packet Application [13] RLP configuration for a SIP flow is as follows (note that not all the RLP parameters are shown here; only those that are critical for efficient support of SIP are shown):

FlowSSNakEnableFwd: 0x01 (Nak-based retransmission enabled)

FlowSSNakEnableRev: 0x01 (Nak-based retransmission enabled)

ReservationMMIdleStateFwd: 0x00 (Reservation does not change states when a connection is closed)

ReservationMMIdleStateRev: 0x00 (Reservation does not change states when a connection is closed)

FlowSSSequenceLengthFwd: 0x02 (22-bit sequence number)

FlowSSSequenceLengthRev: 0x02 (22-bit sequence number)

FlowSSFlowProtocolPDUFwd: 0x01 (Packet stream)

FlowSSFlowProtocolPDURev: 0x01 (Packet stream)

FlowSSDataUnitFwd: 0x00 (Octet sequencing)

FlowSSDataUnitRev: 0x00 (Octet sequencing)

FlowSSRouteProtocolPDUFwd: 0x01 (Packet stream)

FlowSSRouteProtocolPDURev: 0x01 (Packet stream)

FlowSSOutOfOrderDeliveryToRouteProtocolFwd: 0x01 (Out-of-order delivery allowed)

FlowSSTimersFwd:

AbortTimer: 0x01f4 (500 msec).

FlushTimer: 0x0064 (100 msec)

FlowSSTimersRev:

AbortTimer: 0x01f4 (500 msec).

FlushTimer: 0x0064 (100 msec)

FlowSSTransmitAbortTimerRev: 0x00c8 (1000 msec).

7.2 RLMAC (Reverse Link Medium Access Control) Configuration

The recommended RLMAC configuration for a SIP flow is shown below. Note that not all RLMAC parameters are mentioned here; all other RLMAC parameters should be set as per the default values in [6][10].

All the recommended RLMAC parameter values mentioned in Section 6.2 for a VoIP flow also apply to a SIP flow, except for the parameters mentioned below:

T2PTransitionFunctionNN (NN > 0)

T2PUpT2PAxis00FRABAxis0: 0x1B

T2PUpT2PAxis01FRABAxis0: 0x1B

T2PUpT2PAxis02FRABAxis0: 0xB0

8 QoS Configuration/Activation

[5] defines procedures for pre-configuring QoS reservations and Activating QoS at call origination. A VoIP terminal shall follow the QoS procedures defined in [5] to configure and activate QoS for VoIP.

[5] defines procedures for negotiating end-to-end QoS between VoIP terminals. A VoIP terminal should follow the end-to-end QoS negotiation procedures defined in [5].

9 Emergency Services

This section defines how an authorized or a non-authorized access terminal can originate an HRPD Emergency Services VoIP call.

Prior to making an HRPD Emergency Services call at the IMS layer the authorized or non-authorized access terminal first:

Establishes an HRPD session with the access network

Configures air link QoS for the VoIP flow and SIP flow

Configures QoS filters for the VoIP flow and SIP flow with the PDSN

Accesses the HRPD access network to establish air link resources

Activates the QoS for the VoIP flow and SIP flow

Upon finding HRPD service the authorized terminal should establish an HRPD session according to the Default Session Configuration Protocol as defined in [10] and should configure QoS according to Section 8 of this document. Upon making an Emergency Services call the non-authorized terminal may also establish an HRPD session according to the Default Session Configuration Protocol as defined in [10] or may use an alternative approach defined in this document.

Authorized and non-authorized terminals should follow the same steps for accessing the HRPD access network to establish air link resources, configuring QoS filters at the PDSN, and activating access network QoS for the VoIP flow and SIP flow.

9.1 Authorized Terminals

9.1.1 Establishing an HRPD Session with the Access Network

The access terminal and the access network perform session negotiation according to the Default Session Configuration Protocol in [6] or [10]. As a result of the Session Negotiation, the access terminal and the access network should agree to use the following group of application and protocol subtypes in one of the negotiated Personalities:

Enhanced Multi-Flow Packet Application according to [13]

Enhanced Idle State Protocol according to [10]

Enhanced Access Channel MAC Protocol according to [10]

Enhanced Control Channel MAC Protocol according to [6]

Subtype 3 Reverse Traffic Channel MAC Protocol according to [6]

Enhanced Forward Traffic Channel MAC Protocol according to [6]

Subtype 2 Physical Layer Protocol according to [6]

9.1.2 Configuring QoS for VoIP and SIP Flows

The access terminal sends AttributeUpdateRequest messages using the ReservationKKQoSRequest Attribute according to [13], using an appropriate Profile ID as defined in [12] for the VoIP flow and the SIP flow.

The access network creates, configures and activates Link Flows at the access terminal according to [13].

The access network creates, configures, and activates RTCMAC Instances according to [6].

The access network Associates Link Flows in with RTCMAC flows according to [6].

Refer to Section 8 in this document for more information on Configuring QoS at the access network.

9.1.3 Accessing the HRPD Access Network to Establish Air Link Resources

Through the SectorParameters message defined in the Overhead Messages Protocol in [10] the access terminal may find a CDMA channel at the access network that supports Emergency Services. This support is indicated through the AccessHashingChannel mask described in the Overhead Message Protocol in [10].

The access terminal uses the information transmitted in the Access Parameters message to determine if the access network supports the Emergency APersist mechanism as defined in the Enhanced Access Channel MAC Protocol in [10]. The access terminal may use this information to generate and send an Access Capsule accordingly.

The access terminal sends an emergency ConnectionRequest message with Emergency Indicator bit set to 1 as defined in the Enhanced Idle State Protocol according to [10].

9.1.4 Activating QoS for VoIP and SIP Flows

The access terminal sends an emergency ReservationOnRequest message with the Emergency Indication bit set to 1 according to [13].

9.2 Non-Authorized Terminals

9.2.1 Pre-configured HRPD Session

Authorized access terminals should already have an established session and can originate a VoIP call immediately or can negotiate a session and then originate a connection (e.g., just powering up). See previous section.

For non-authorized access terminals a pre-configured provisioned session should be used to support an HRPD Emergency Services VoIP call. The use of a pre-configured provisioned session is desirable as it allows the bypass of session configuration and key generation and allows the access terminal to access the system, for emergency services purposes only, quickly and without the need to pass authentication.

A non-authorized access terminal in this context is not authorized to use Profile IDs 0x0500 or 0x0100. If an access terminal is authorized for other services (e.g., Best Effort), but not for SIP/VoIP as described by this document, the access terminal should purge its existing HRPD Session and use the pre-configured session and PriorSession call flows described in this chapter.

If PriorSessionGAUP is not supported by the access network, then the access terminal may use Generic Configuration Protocol through the ConfigurationRequest message with the PriorSession attribute to instantiate the pre-configured provisioned session. If the access network supports the PriorSessionGAUP the preconfigured provisioned session can be instantiated using the Generic Attribute Update Protocol through the AttributeUpdateRequest message with the PriorSession attribute

9.2.1.1 PriorSessionGAUP Not Supported

Figure 9-1 shows the details on how the pre-configured provisioned session is instantiated when PriorSessionGAUP is not supported by the access network. The access network retrieves the pre-configured provisioned session, through A13 signaling, without performing session configuration exchanges over the air-interface. The visited access network may have an internal SessionStorage entity as an implementation option, in which case there would be no A13 signaling.

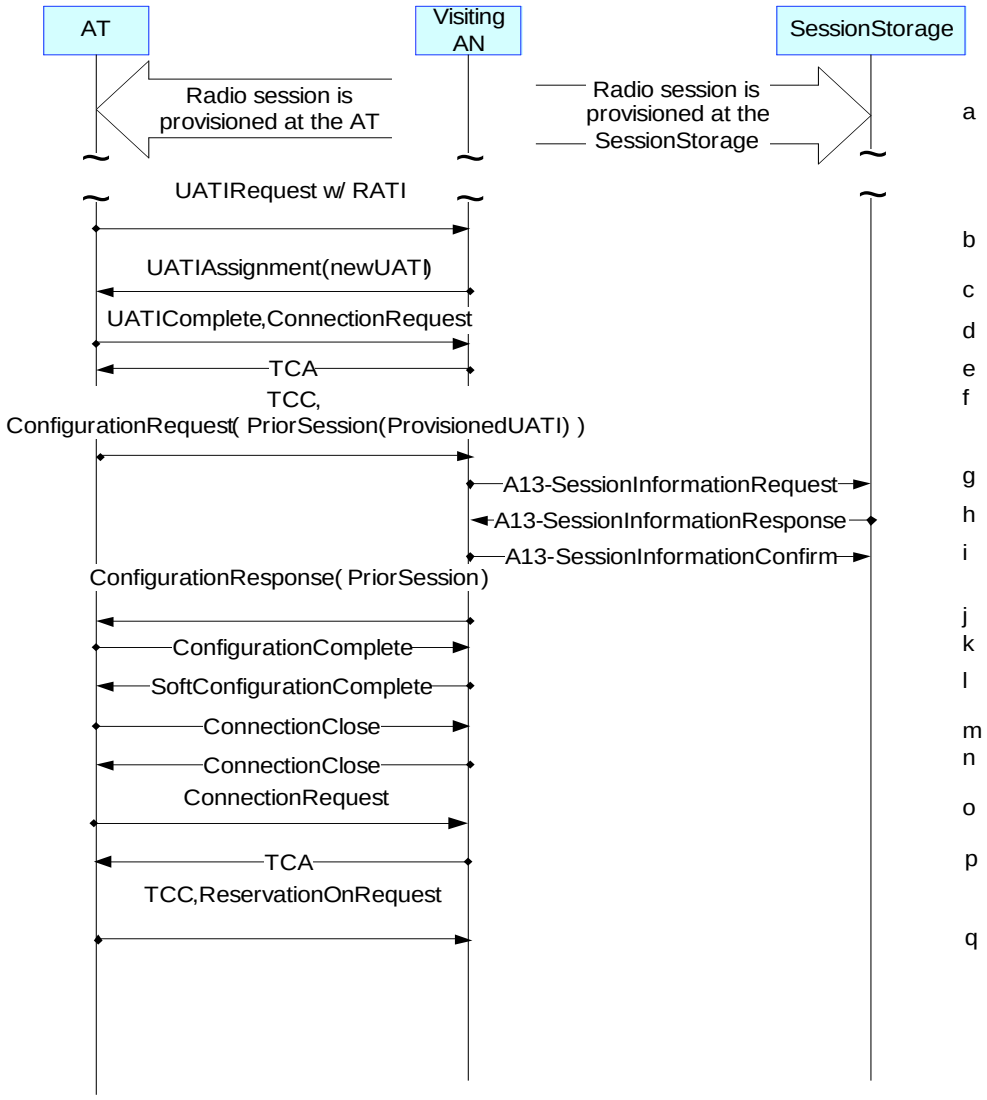

Figure 9-1 PriorSession retrieval when PriorSessionGAUP not supported

a) The pre-configured session is stored on the access terminal and the access network

b) The access terminal requests a new UATI with the UATIRequest message. The Access Channel MAC Header is populated with a RATI.

c) The access network assigns the access terminal a new UATI with the UATIAssignment message

d) The access terminal sends a UATIComplete message, and a ConnectionRequest message.

e) The access network assigns air link resources using the TrafficChannelAssignment message

f) The access terminal completes the assignment of air link resources using the TrafficChannelComplete message, and sends a ConfigurationRequest message with the PriorSession attribute that includes the Pre-provisioned PriorSession information.

g) h) i) The access network retrieves the PriorSession information from the Session Storage entity. If the SessionStorage entity is internal to the access network, then A-13 signaling is not necessary.

j) The access network sends a ConfigurationResponse message to the access terminal indicating that the PriorSession was retrieved.

k) The access terminal sends a ConfigurationComplete message to end the Session Configuration

l) The access network sends a SoftConfigurationComplete message with Continue=0, Commit = 1 and sets the SessionConfigurationToken to indicate the Personality Index the access terminal is to use.

m) n)The access terminal sends a ConnectionClose message and the access network responds with ConnectionClose message

o) The access terminal opens a new Connection

p) The access network assigns air-link resources using the TrafficChannelAssignment message

q) The access terminal completes the assignment of air link resources using the TrafficChannelComplete message and sends the ReservationOnRequest message to turn on the Reservations for the VoIP flow and the SIP flow.

9.2.1.2 PriorSessionGAUP Supported

Figure9-2 shows how the pre-configured provisioned session is instantiated when PriorSessionGAUP is supported by the access network. The access network retrieves the pre-configured provisioned session, through A13 signaling, without performing session configuration exchanges over the air-interface. The visited access network may have an internal SessionStorage entity as an implementation option, in which case there would be no A13 signaling.

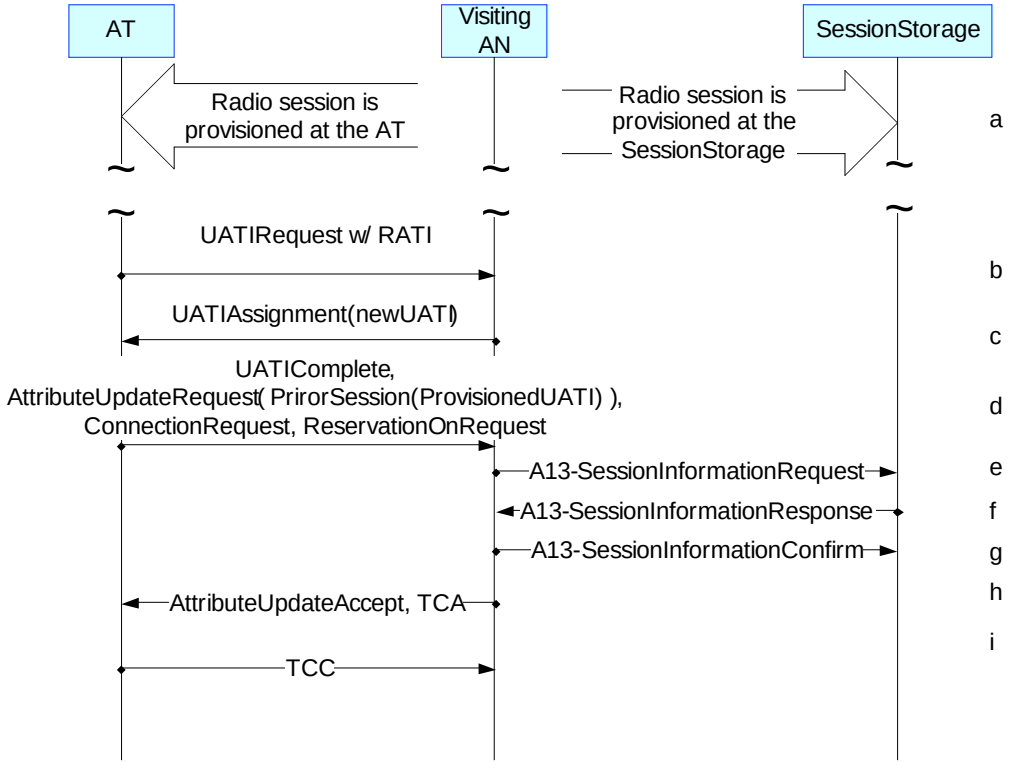

Figure9-2 Prior Session retrieval when PriorSessionGAUP supported

a) The pre-configured session is stored on the access terminal and the access network

b) The access terminal requests a new UATI with the UATIRequest message. The Access Channel MAC Header is populated with a RATI.

c) The access network assigns the access terminal a new UATI with the UATIAssignment message

d) The access terminal sends a UATIComplete message, an AttributeUpdateRequest message for the PriorSession Attribute that includes the pre-provisioned PriorSession information, a ConnectionRequest message and a ReservationOnRequest message to turn on the reservations for the VoIP media and SIP flows.

e) f) g) The access network retrieves the PriorSession information from the Session Storage entity. If the SessionStorage entity is internal to the access network, then A-13 signaling is not necessary.

h) The access network sends the AttributeUpdateAccept message in response to the AttributeUpdateRequest(PriorSession) from the access terminal, and assigns air-link resources to the access terminal using the TrafficChannelAssignment message.

i) The access terminal completes the assignment of air-link resources with the TrafficChannelComplete message.

9.2.2 HRPD Protocol and Application Configuration for Emergency Services VoIP and SIP Flows

The pre-configured provisioned HRPD session defines the non-default HRPD protocol subtypes and application subtypes as defined in [12] to be used for Emergency Services, and the non-default attribute values used within the protocol subtypes and application subtypes. Figure 9-3 depicts the Emergency Services VoIP flow and SIP flow configuration. This configuration depicts the mappings necessary between the Enhanced Multi-Flow Packet Application at the HRPD Application Layer, HRPD Stream Layer, and the HRPD RTCMAC 3 at the MAC Layer to allow for the necessary QoS desired for the Emergency Services VoIP flow and the SIP flow.

The non-authorized access terminal should configure QoS according to Section 9.1.2 of this document, access the HRPD access netwok according to Section 9.1.3 of this document, and activate QoS for the VoIP flow and SIP flow as stated in Section 9.1.4 of this document

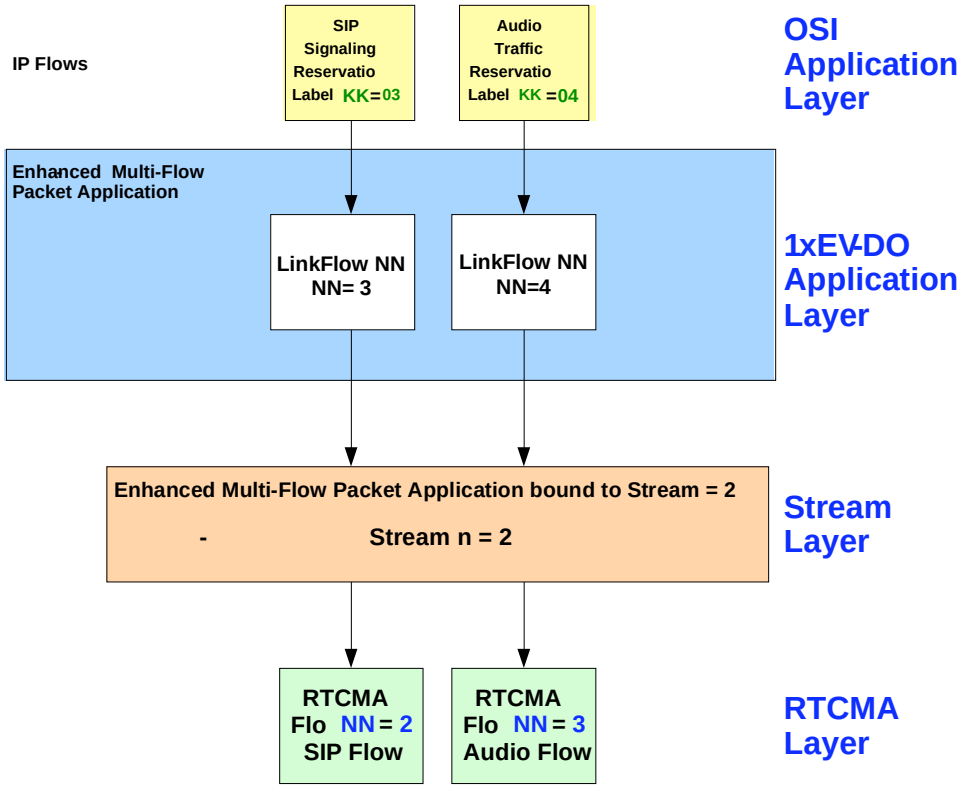

Figure 9-3 Emergency Services VoIP and SIP Flow Protocol and Application Mappings

9.2.2.1 Session Configuration Protocol

This section of the document describes non-default Simple Attribute and Complex Attribute values to be used in the pre-configured session for attributes that are defined in the Session Configuration Protocol. All other Simple and Complex Attributes shall use the default values as per [6][10].

The definition of the HRPD Protocol Subtypes to be used in the pre-configured session for Emergency VoIP Services is defined in the following table. Note that the Enhanced Access Channel MAC and Enhanced Idle State Protocol are as specified in [10]

Table 9-1 Emergency Session Protocol Subtypes

Attribute ID (Protocol Value)	Attribute Value (Sub Protocol Type)	Meaning
0x0000	0x02	Subtype 2 Physical Layer Protocol
0x0002	0x01	Enhanced Access Channel MAC
0x0003	0x01	Enhanced Forward Traffic Channel MAC
0x0004	0x03	Subtype 3 Reverse Traffic Channel MAC
0x000c	0x01	Enhanced Idle State Protocol

The definition of the Attribute Values of the Simple Attributes SessionConfigurationToken and PersonalityCount for the pre-configured session shall be as per the table below.

Table 9-2 SessionConfigurationProtocol Simple Attribute Settings

Attribute ID	Attribute Value	Meaning
0x0100	0xE911	The SessionConfigurationToken shall be set to the value 0xE911[1]
0x0110	0x04	The access terminal supports a PersonalityCount of 4

The definition of the PriorSessionAttribute for the pre-configured session shall be as per the table below. The access network should skip the authentication function of the Security Packet included in the PriorSession attribute. This is PriorSession attribute that will be encapsulated in the AttributeUpdateRequest Message depicted in Figure9-2 if the access network supports PriorSessionGAUP, or in the ConfigurationRequest depicted in Figure 9-1 when the access network does not support PriorSessionGAUP.

Table 9-3 Emergency Session PriorSession Attribute Settings

Field	Length (bits)	Value	Meaning
Length	16		Length of this attribute in octets; excluding the length field
Attribute ID	16	0x0100	PriorSession attribute
ValueID	8	0	Identifier assigned to this complex value
Restore	1	0x1	Request the PriorSession to be restored
Reserved	7	0x0	
UATI	128	0xffffffffffffffff	The provisioned UATI contains all 1's.
SecurityPacketLength	8	Variable	Length of Security Packet Field in octets
SecurityPacket	64	SecurityPacketLengthx8	Created according to section 6.4.6.1.6.1in [10]

9.2.2.2 Stream Protocol

The definition of the Stream Protocol bindings to be used in the pre-configured session for Emergency Services is defined in the following table.

Table 9-4 Emergency VoIP Session Stream Protocol definition

Attribute	Attribute iD	Value	Meaning
Stream0	0x14	0x0000	Default Signaling Application
Stream1	0x15	0xffff	No Application
Stream2	0x16	0x0009	Enhanced Multi-Flow Packet Application bound to Service Network
Stream3	0x17	0xffff	No Application

[1] Note that 4 MSBs represent the personality index, and value 0xE is used to ensure it is outside the typical range of personality index values used.

9.2.2.3 Enhanced Multi-Flow Packet Application

Table 9-5 Emergency VoIP Services ATSupportedFlowProtocol Parameters Definition

Field	Length (bits)	Value	Meaning
Length	8		Length of the packet
AttributeID	0xf004		We are defining support associated with RoHC
ValueID	8	1	Number used to keep track of this record
ProtocolSupported	1	1	RoHC is supported
SupportedProtocolParametersValueLength	8		See 9-6
SupportedProtocolParametersValue			See Table 9-6

9-6 Supported Protocols Parameter Values for ATSupportedFlowProtocolParameters04

Field	Length (bits)	Value	Meaning
MaxSupportedMaxCID	16	0	
LargeCIDSupported	1	0	Large CID is not supported
MaxSupportedMRRU	16	0	No segmentation
TimerBasedCompressionSupported	1	1	Timer based compression is supported
SupportedProfileCount	8	3	There are three profiles supported
SupportedProfile	16	0	Uncompressed
SupportedProfile	16	1	RTP
SupportedProfile	16	2	UDP
Reserved	0-7		Padding as necessary

9.2.3 HRPD system Configuration for SIP Flow

This section of the document defines the non-default attributes to be used in the pre configured HRPD Session for the SIP flow. Non-default attribute values are defined for the Enhanced Multi-Flow Packet Application and the Subtype 3 RTCMAC Protocol.

9.2.3.1 Enhanced Multi-Flow Packet Application

The recommended RLP configuration in EMFPA for an Emergency Services SIP flow is as specified in Section 7.1 with the follow additions. All other RLP parameters shall be set as per the default values in [6].

The EMFPA Simple Attribute values ReservationKKQOSRequestFwd/Rev in the table below defines the ProfileID relationships to the Forward and Reverse ReservationLabels.

Table 9-7 Emergency Services IP Flow to Reservation Label Mappings for SIP Signaling

Attribute Name	Attribute Value	ProfileID	Meaning
ReservationKKQOSRequestFwd KK=3	0x0703	0x0500	ProfileID 1280 for Forward SIP Flow with Reservation Label=3
ReservationKKQOSRequestRev KK=3	0x0803	0x0500	ProfileID 1280 for Reverse SIP Flow with Reservation Label=3

The EMFPA Simple Attribute Values in the table below defines the Forward and Reverse ReservationLabels relationships to the Forward and Reverse Flows created to carry the SIP signaling information.

Table 9-8 Emergency Services Reservation Label to Link Flow Mappings for SIP Signaling

Attribute Name	Attribute Value	Reservation Label	Meaning
FlowNNReservationFwd NN=3	0x0503	0x03	Map SIP Flow Forward Reservation = 3 to Forward Link Flow =3 (SIP Signaling)
FlowNNReservationRev NN=3	0x0603	0x03	Map SIP Flow Reverse Reservation = 3 to Reverse Link Flow=3 (SIP Signaling)

The EMFPA Simple Attribute values in the table below activate the Forward and Reverse Link Flows created to carry the SIP signaling information.

Table 9-9 Emergency Services Link Flow Activation for SIP Signaling

Attribute Name	Attribute Value	Activated	Meaning
FlowNNActivatedFwd nn=3	0xf303	0x01	The Forward Link Flow for the SIP Signaling is Activated
FlowNNActivatedRev nn = 3	0xf203	0x01	The Reverse Link Flow for the SIP Signaling is Activated

9.2.3.2 Subtype 3 RTCMAC Protocol

The recommended RTCMAC Subtype 3 parameters in the RL MAC for an Emergency Services SIP flow is as specified in Section 7.2 with the follow additions. All other RTCMAC Subtype 3 parameters shall be set as per the default values in [6].

The Simple Attribute value defined in the table below defines the associated EMFPA Link Flow instance created to carry SIP signaling information to an RTCMAC instance.

Table 9-10 Emergency Services RTCMAC Flow to EMFPA Link Flow Mapping for SIP Signaling

Attribute Name	Attribute ID	Stream	Substream	Meaning
AssociatedFlowsNN NN=2	0x0102	0x02	0x03	Bind RTCMAC Flow 2 to ReverseLinkFlow 3 running in EMFPA (SIP Signaling)

The Simple Attribute value BucketLevelMaxNN is set to a non-zero number to turn on the instance of Subtype 3 RTCMAC that is created to carry SIP signaling information. This non-zero number activates the RTCMAC flow NN.

Table 9-11 Emergency Services RTCMAC BucketLevelMaxNN Setting for SIP Signaling

Attribute Name	AttributeID	Attribute Value	Meaning
BucketLevelMaxNN NN=2	0xfe02	0x66	Bucket Level Max for RTCMAC Flow 2 (SIP Signaling)

9.2.4 HRPD System Configuration for VoIP Flow

This section of the document defines the non-default attributes to be used in the pre-configured HRPD Session for the VoIP flow. Non-default attribute values are defined for the Enhanced Multi-Flow Packet Application, and the Subtype 3 RTCMAC protocol.

9.2.4.1 Enhanced Multi-Flow Packet Application

The recommendation RLP configuration for an Emergency Services VoIP flow is as specified in Section 6.1 with the follow additions. All other RLP parameters should be set as per the default values in [6].

The EMFPA Simple Attribute values ReservationKKQoSRequestFwd/Rev in the table below defines the ProfileID relationships to the Forward and Reverse ReservationLabels.

Table 9-12 Emergency Services IP Flow to Reservation Label Mappings for VoIP

Attribute Name	Attribute Value	ProfileID	Meaning
ReservationKKQoSRequestFwd KK=4	0x0704	0x0100	ProfileID 256 for Forward VoIP Flow with Reservation Label=4
ReservationKKQoSRequestRev KK=4	0x0804	0x0100	ProfileID 256 for Reverse VoIP Flow with Reservation Label=4

The EMFPA Simple Attribute Values in the table below defines the Forward and Reverse ReservationLabels relationships to the Forward and Reverse Flows created to carry the VoIP information.

Table 9-13 Emergency Services Link Flow to Reservation Label Mapping for VoIP

Attribute Name	Attribute Value	Reservation Label	Meaning
FlowNNReservationFwd NN=4	0x0504	0x04	Map VoIP Flow Forward Reservation = 4 to Forward Link Flow =4 (VoIP)
FlowNNReservationRev NN=4	0x0604	0x04	Map VoIP Flow Reverse Reservation = 4 to Reverse Link Flow=4 (VoIP)

The EMFPA Simple Attribute values in the table below activate the Forward and Reverse Link Flows created to carry the SIP signaling information.

Table 9-14 Emergency Services Link Flow Activation for VoIP

Attribute Name	Attribute Value	Activated	Meaning
FlowNNActivatedFwd NN=4	0xf304	0x01	The Forward Link Flow for VoIP is Activated
FlowNNActivatedRev NN = 4	0xf204	0x01	The Reverse Link Flow for VoIP is Activated

9-15 Flow*NN*FlowProtocolFwd Attribute Settings

Field	Length (bits)	Value	Meaning
Length	8		Length of the packet
AttributeID	0x0b03		Flow*NN*FlowProtocolFwd AttributeID
ValueID	8	1	Number used to keep track of this record
ProtocolSupported	8	0x4	RoHC is supported
ProtocolParametersLength	8		See 9-17
ProtocolParametersValue			See 9-17

9-16 Flow*NN*FlowProtocolRev Attribute Settings

Field	Length (bits)	Value	Meaning
Length	8		Length of the packet
AttributeID	0x0c03		Flow*NN*FlowProtocolRev AttributeID
ValueID	8	1	Number used to keep track of this record
ProtocolSupported	8	0x4	RoHC is used
ProtocolParametersLength	8		See 9-17
ProtocolParametersValue			See 9-17

9-17 ProtocolParameters Record for FlowNNFlowProtocols Attribute

Field	Length (bits)	Value	Meaning
MaxCID	16	0	
LargeCIDs	1	0	
FeedbackForIncluded	1	0	Feedback is for this LinkFlow only
FeedbackFor	5	0	Ommitted since FeedbackFor = 0
MRRU	8	0	No segmentation
ProfileCount	8	3	There are three profiles supported
Profile	16	0	Uncompressed
Profile	16	1	RTP
Profile	16	2	UDP

9.2.4.2 RTCMAC Subtype 3

The recommended RTCMAC Subtype 3 parameters in the RL MAC for an Emergency Services VoIP flow is as specified in Section 6.2 with the follow additions. All other RTCMAC Subtype 3 parameters should be set as per the default values in [6]

The Simple Attribute value defined in the table below defines the associated EMFPA Link Flow instance created to carry VoIP frames to an RTCMAC instance.

Table 9-18 Emergency Services RTCMAC Flow to EMFPA Link Flow Mapping for VoIP

Attribute Name	Attribute ID	Stream	Substream	Meaning
AssociatedFlowsNNNN=3	0x0103	0x02	0x03	Bind RTCMAC Flow 3 to ReverseLinkFlow 4 running in EMFPA

The Simple Attribute value BucketLevelMaxNN is set to a non-zero number to turn on the instance of Subtype 3 RTCMAC that is created to carry VoIP frames. This non-zero number activates the RTCMAC flow NN.

Table 9-19 Emergency Services BucketLevelMaxNN for VoIP

Attribute Name	AttributeID	Attribute Value	Meaning
BucketLevelMaxNNNN=3	0xfe03	0x66	Bucket Level Max for RTCMAC Flow 3 (VoIP)

9.3 PDSN QoS Filter for VoIP and SIP Flows

The access terminal uses RSVP signaling as defined in [14] to install Traffic Flow Templates at the PDSN. Refer to Section 8 in this document for more information on Configuring QoS at the PDSN.