Attachment 4-2-9

WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

Robust Header Compression (RoHC) Support

WMF-T33-108-R015v01

WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

Robust Header Compression (RoHC) Support

WMF-T33-108-R015v01

WiMAX Forum® Approved

(2009-11-21)

WiMAX Forum Proprietary

Table of Contents

Table of Figures

Revision History

Date	Revision	Editor Note
November 6, 2009	V01	Initial version of Release 1.5.

1. Introduction and Scope

This document describes system architecture and clarifies signaling procedures for ROHC, and data handling mechanism between ROHC entity peers in WiMAX Network

1.1 Scope

This document describes the architecture and procedure regarding ROHC function of WiMAX network which is located in the ASN-GW. This specification builds the WiMAX ROHC architecture on top of the generic ROHC framework and ROHC profile definitions in [RFC 3095].

The ROHC feature is optional for ASN-GW and the MS. ROHC function in the MS and the ASN-GW SHALL be compliant to the ROHC framework described in [RFC3095], [RFC3759], [RFC4815] and [RFC4995].

Uncompressed profile in [RFC3095] is mandatory for both ASN-GW and the MS. All other ROHC profiles described in [RFC3095], [RFC3242], [RFC3843] and [RFC4996] are optional and open to negotiation.

2. Definitions

ROHC Function: A functional entity including a ROHC compressor and De-compressor functions defined in [RFC3095].

ROHC SF: An 802.16 Service Flow which is mapped to a ROHC channel carrying ROHC packets.

ROHC Channel: A logical unidirectional point to point channel carrying ROHC packets from a compressor to a de-compressor. See Section 2 of [RFC3759]

ROHC Compressor: Functional entity which inspects and compresses IP headers to ROHC packet header with ROHC header context. See the definition of ROHC compressor instance in Section 2 of [RFC3759]

ROHC De-compressor: Functional entity which maintains header contexts and reconstructs original headers from compressed headers. See the definition of ROHC decompressor instance in Section 2 of [RFC3759]

Per-Channel Negotiation: During ROHC SF creation or modification, procedure to negotiate Per-Channel Parameters between ROHC Compressor and ROHC De-compressor.

Per-Channel Parameters: A set of parameters MAX_CID, LARGE_CIDs, PROFILES, FEEDBACK_FOR, MRRU that form part of the established channel state and the per-context state of a ROHC Channel.

3. References

[IEEE802.16Rev2] IEEE 802.16Rev2/D6 July 2008, Draft Standard for Local and metropolitan area networks, Part16: Air Interface for Broadband Wireless Access Systems, Draft 6, July 2008

[NWG-PCC] WiMAX Forum T33-109-R015v01, "Architecture, detailed Protocols and Procedures, Policy and Charging Control", Release 1.5.

[NWGSTG3] WiMAX Forum, T33-001-R015v01, “Detailed Protocols and Procedures, Base Specification", Release 1.5

[RFC3095] Bormann, C., et al, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001

[RFC3242] L. Jonsson and G. Pelletier, "A Link-Layer Assisted ROHC Profile for IP/UDP/RTP", RFC 3242, April 2002.

[RFC3759] “RObust Header Compression (ROHC): Terminology and Channel Mapping Examples”, L-E. Jonsson, April 2004

[RFC3843] L-E. Jonsson and G. Pelletier, "RObust Header Compression (ROHC): A Compression Profile for IP", RFC 3843, June 2004.

[RFC4815] L-E. Jonsson, K. Sandlund, G. Pelletier, P. Kremer, “RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095”, RFC4815, February 2007

[RFC4995] L-E. Jonsson, G. Pelletier, K. Sandlund, "The RObust Header Compression (ROHC) Framework", RFC 4995, July 2007.

[RFC4996] G. Pelletier, L. Jonsson, K. Sandlund and M. West, "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)", RFC 4996, July 2007.

4. Network Architecture and Functional Decomposition

This section describes the detailed architecture and procedures using ROHC functional entities.

4.1 Network Architecture for ROHC

The following figure describes network architecture for supporting ROHC. ROHC Function is located in MS and ASN-GW.

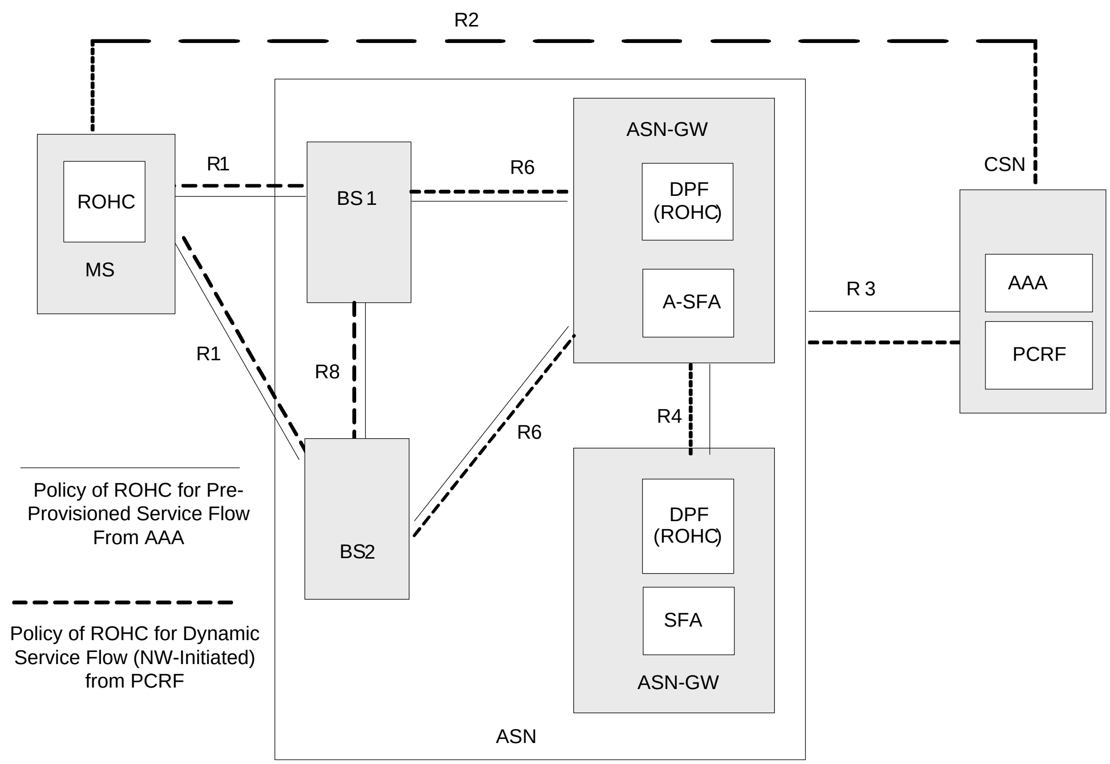

Figure 4-1 ROHC in MS and ASN-GW

In the Network, ROHC function is collocated with Anchor Data Path Function to perform header compression and decompression. In order to manage ROHC SFs, the existing SFA functions are used for assigning and managing dynamic ROHC SF. The policy which indicates if ROHC is enabled for a SF is used is downloaded from AAA or PCRF. In other words, AAA delivers the subscriber profile including the ROHC policy to ASN-GW during an authentication procedure for the Pre-provisioned service flow, and PCRF delivers the subscriber profile including ROHC policy and charging rules to ASN-GW for the dynamic service flow management. Based on these policies and resource availability, ASN-GW decides to enable ROHC for a given Service Flow. In other words, AAA delivers the subscriber profile including the ROHC policy to ASN-GW during an authentication procedure for the Pre-provisioned service flow, and PCRF delivers the subscriber profile including ROHC policy to ASN-GW for the dynamic service flow.

4.2 Functional Entities Description

1) ASN-GW

- SFA
  - Receives ROHC policy from the HAAA, if ROHC is to be enabled for this Service Flow. The ASN may locally configure the ROHC Policy. The local policy shall supercede the global policy.
  - Generates and distributes the classification rule for ROHC.
  - Exchanges ROHC related information of service flow with MS through the SFM of BS.
  - If MS accepts the service flow containing ROHC classification, SFA triggers ROHC Per-Channel Negotiation after the procedure of the service flow negotiation.
  - In the case for the deletion of Service Flow with ROHC, the SFA should notify the Anchor ASN.
- ROHC Function in ASN-GW
  - Initiates Per-Channel Negotiation with the ROHC in MS.
  - Per-Channel Negotiation: ROHC Compressor and ROHC De-compressor negotiate Per-Channel Parameters. Since ROHC Channel is one-to-one mapped to a service flow, the Per-Channel Parameters are negotiated by using DSA-REQ/DSA-RSP (DSC-REQ/DSC-RSP).
  - ROHC Compressor: inspects and compresses IP headers to ROHC packet header by maintaining ROHC header context.
  - ROHC De-compressor: maintains header contexts and reconstruct original headers from compressed headers.
- DPF
  - Performs classification for the DL packet.
  - Determines if Service Flow for DL packet is ROHC enabled.
  - If DL packet belongs to a ROHC enabled Service Flow, forwards the DL packet to the ROHC Compressor.
  - Performs ROHC Compressor processing of DL packet.
  - Performs encapsulation of R6 Data Path ID and transmits to the BS.
  - Receives UL packet from BS, and if UL packets belong to a ROHC Channel, forwards the UL packet to the ROHC De-compressor.

2) BS

- BS should maintain the relationship between R6 Data Path ID and 802.16e CID.
- BS should process the DL packet by replacing R6 Data Path ID with 802.16e CID and process UL packet by replacing 802.16e CID with R6 Data Path ID.
- Notifies MS and ASN-GW of ROHC Per-Channel Parameters during Per-Channel Negotiation.

3) AAA

- AAA maintains subscriber profile including ROHC policy.
- AAA delivers the subscriber profile including ROHC policy to ASN-GW during an authentication procedure.

4) PCRF

- PCRF delivers subscriber policies and charging rules for different service classes; for conversational class, based on the ASN capabilities, ROHC may be enabled.

5) MS

- Support ROHC feature negotiation during initial network entry with the network.
- When a DSA message contains the ROHC Parameter, MS which supports ROHC should allocate an instance of the ROHC function (Compressor/De-compressor) within its CS layer. If DL packets belong to a ROHC Channel, then forwards the DL packet to the ROHC De-compressor.
- For UL traffic, performs classification to identify whether the packet requires ROHC compression or not.
- Performs ROHC compression if the UL packet belongs to a ROHC Channel.
- Maps the ROHC Channel to an appropriate 802.16e CID and transmit to BS.

5. Data Plane

5.1 Relationship among SFID, Connection ID, ROHC Context ID

The Figure 5-1 depicts the relationship among SFID, 802.16e CID and ROHC context ID.

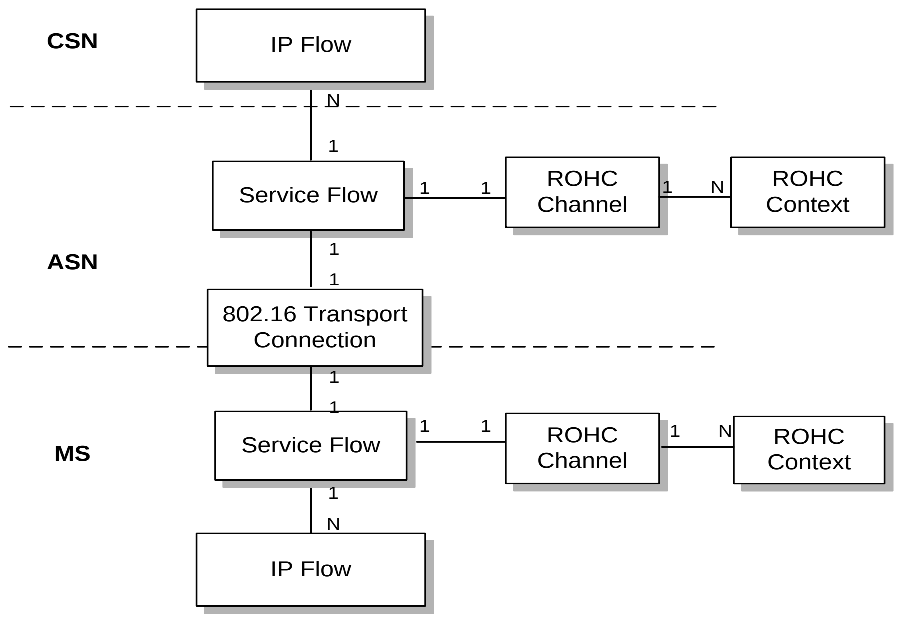

Figure 5-1 ROHC service bearer examples

A service flow is one-to-one mapped to a ROHC Channel and a ROHC Channel can have multiple ROHC Contexts.

Note that the Figure 5-1 is informative.

Mapping relationship between IP-Flow and Service Flow is described in the air interface specification [IEEE802.16Rev2].

Mapping relationship between ROHC Channel and ROHC Context is described in [RFC3095].

5.2 Data Plane Operation

The subsection explains the ROHC Data Plane Operation in ASN-GW and MS.

5.2.1 Data Plane Operation in ASN-GW

Figure 5-2 describes the functional entities and their interaction to explain ROHC operation in ASN-GW. The figure shows the functional entities such as Classifier, ROHC Function including a ROHC Compressor and a ROHC Decompressor, a Data Path Encapsulation/ Data Path Decapsulation function.

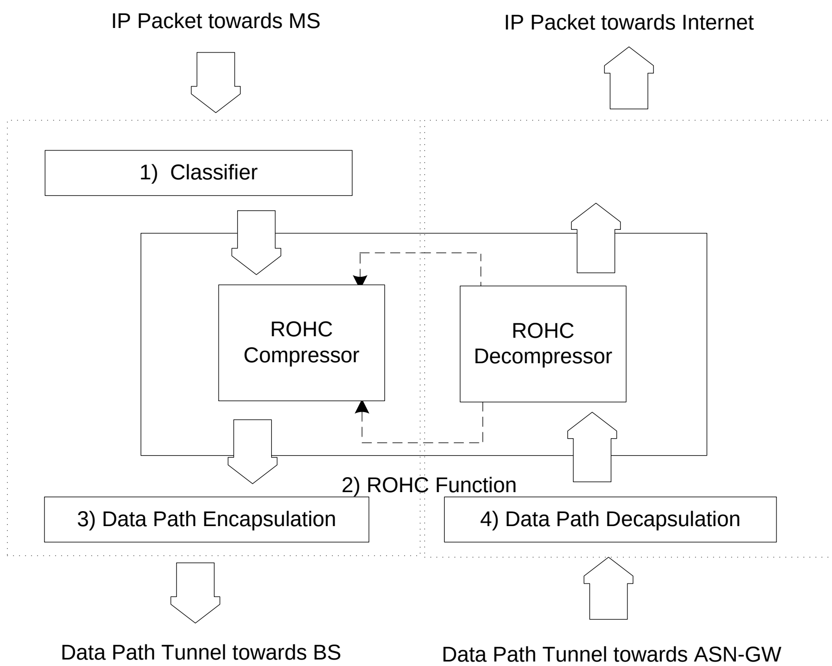

Figure 5-2 Data Plane in ASN-GW

The following functional entities are described only for explanation of ROHC behavior. Since all of the following functions are collocated together with the Anchor Data Path Function, the interactions between them are not in the scope of this specification.

1) Classifier

   In order to classify the IP packet into a proper service flow for the downlink traffic towards to a MS, the Classifier performs classification function. When IP flows which are assigned to the downlink ROHC SF are coming to Classifier, it forwards the packet to the instance of ROHC Function which is assigned to the service flow.

2) ROHC Function

   An instance of ROHC Function is composed of one ROHC Compressor and one ROHC Decompressor. It is assumed that one uplink and one downlink ROHC SFs composes a bi-directional ROHC Channel as described in Section 6.2 of [RFC3759].

3) Data Path Encapsulation

After performing ROHC compression for the incoming IP packet, Data Path Encapsulation function tags the outer IP and GRE header for the compressed packet or the feedback packet for the reverse direction in order to deliver the packet towards BS. The destination address field of outer IP header and the key field of GRE header are set through the mapping information associated with the service flow and mobile stations identifier (MSID).

4) Data Path Decapsulation

When a packet is received at the Data Path tunnel endpoint in the ASN-GW Data Path Decapsulation function performs the decapsulation of the incoming packet and forwards it to the upper layer. In case of ROHC SF, it forwards it to ROHC Decompressor. The Data Path Decapsulation function finds out the proper service flow from the information available in the key field of the GRE header.

For the following operation scenarios, it is assumed that one uplink and/or one downlink ROHC SF have been established successfully.

1) ROHC compression for the downlink IP packet

An Anchor data path function receives a data packet from CSN and Classifier classifies the IP flow with a packet classification rule. The classification rule determines whether ROHC header compression shall be performed. If the 5-tuple of the incoming packet is belonging to the ROHC SF, Classifier forwards the packet to the ROHC Compressor. ROHC Compressor performs the header compression as described in [RFC3095]. The ROHC peers in the ASN-GW and in the MS SHALL support uncompressed profile as the default profile. If an incoming packet does not belong to the negotiated and established profiles by both ROHC peers, then the packet shall not be discarded, but shall be processed as an uncompressed profile packet. The CS PDU which is composed of the compressed ROHC Header and the IP payload is encapsulated by per-SF Data Path tunnel, i.e. GRE tunnel and is sent towards BS through Data Path tunnel. Then, BS sends the compressed packet to MS through the associated air link connection.

2) ROHC decompression for the uplink IP packet

The Anchor Data Path function received the ROHC compressed packet through the data path tunnel from the BS. The proper ROHC Decompressor which belongs to the ROHC SF is identified by Data Path ID, i.e. GRE key. After the decapsulation of the outer IP header and GRE header, the CS PDU which consists of ROHC Header and IP Payload is decompressed by the ROHC Decompressor. The decompressed IP packet is sent to the CSN.

3) Sending downlink feedback packets for the uplink ROHC Channel.

If the ROHC Decompressor in the Anchor DPF needs to send a feedback packet to the MS for the uplink ROHC SF, it uses the downlink ROHC SF. This Piggybacked/Interspersed ROHC Feedback is sent to the downlink ROHC SF towards BS.

4) Receiving uplink feedback packets for the downlink ROHC Channel

If the ROHC Decompressor receives the Piggybacked/Interspersed ROHC Feedback through the uplink ROHC SF, it passes it to the ROHC Compressor within the ROHC Function itself.

5.2.2 Data Plane Operation in MS

Figure 5-3 describes the functional entities and their interaction to explain ROHC operation in MS. The figure shows the functional entities such as Classifier, ROHC Function including a ROHC Compressor and a ROHC Decompressor.

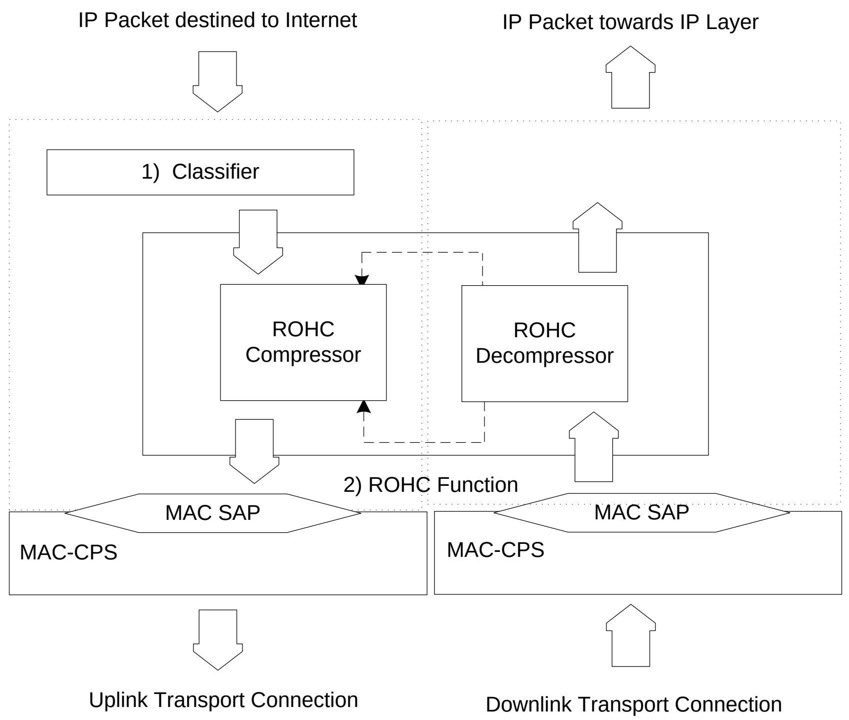

Figure 5-3 Data Plane in MS

The following functional entities are described only for explanation of ROHC behavior. Since all of the following functions are collocated together within the MS, the interactions between them are not in the scope of this specification.

1) Classifier

In order to classify the IP packet into a proper service flow for the uplink traffic towards the Internet,, the Classifier performs classification function. When IP flows which are assigned to the uplink ROHC SF are coming to Classifier, it forwards the packet to the instance of ROHC Function which is assigned to the service flow.

2) ROHC Function

An instance of ROHC Function composes of one ROHC Compressor and/or one ROHC Decompressor. It is assumed that one uplink and one downlink ROHC SFs consists of a bi-directional ROHC Channel as described in Section 6.2 of [RFC3759].

For the following operation scenarios, it is assumed that one uplink and/or one downlink ROHC SF have been established successfully.

1) ROHC compression for the uplink IP packet

The classification rule determines whether ROHC header compression shall be performed. If the 5-tuple of the incoming packet is belonging to the ROHC SF, the Classifier forwards the packet to the ROHC Compressor. ROHC Compressor performs the header compression as described in RFC3095. Both ROHC peers, MS and ASN-GW SHALL support uncompressed profile as the default profile. If an incoming packet does not belong to the negotiated and established profiles by both ROHC peers, then the packet shall not be discarded, but shall be processed as an uncompressed profile packet. The CS PDU which is composed of the compressed ROHC Header and the IP payload is passed over to the MAC layer.

2) ROHC decompression for the downlink IP packet

3) The peer shall identify the corresponding ROHC Decompressor associated with the ROHC SF by the transport CID assignment, through the MAC-SAP. The CS PDU from the MAC-SAP, which consists of ROHC Header and IP Payload, is decompressed by the ROHC Decompressor. The decompressed IP packet is sent to the IP layer. Sending uplink feedback packets for the downlink ROHC channel.

If the ROHC Decompressor in the MS needs to send a feedback packet to the ROHC peer for the downlink ROHC Channel, it uses the uplink ROHC SF. This Piggybacked/Interspersed ROHC Feedback is sent to the uplink ROHC SF towards the BS.

4) Receiving downlink feedback packets for the uplink ROHC channel

If the ROHC Decompressor receives the Piggybacked/Interspersed ROHC Feedback through the downlink ROHC SF, it passes it to the ROHC Compressor within the same ROHC Function.

6. Control Plane Protocols and Procedures

This section describes the detailed message flows and procedures to establish a ROHC SF.

The procedures for creation, modification and deletion of a ROHC SF are the same as those of other service flows such as Initial Service Flow, Pre-provisioned Service Flow or Dynamic Service Flow. When required, a set of IP packet classification rules SHALL be transferred between two ROHC peers to identify the IP Flows which are belonging to ROHC SF. When creating a ROHC SF, the ROHC Per-Channel Parameters SHALL be negotiated between the ROHC peers, MS and ASN-GW.

6.1 ROHC Feature Negotiation Procedure

MS and ASN GW SHALL negotiate the support for ROHC. As shown in the Figure 4-1Figure 6-1, this is done by using REG REQ / RSP (as in section 11.7.7.1 of [IEEE802.16Rev2]) message between MS and BS. These messages are extended over R6 (BS to ASN GW) by using MS Attachment Req / Rsp messages to set up the ROHC function for SF in the ASN-GW. Note: [NWGSTG3] provides the definitions for MS Attachment Req / Rsp messages and timers T5 and T6.

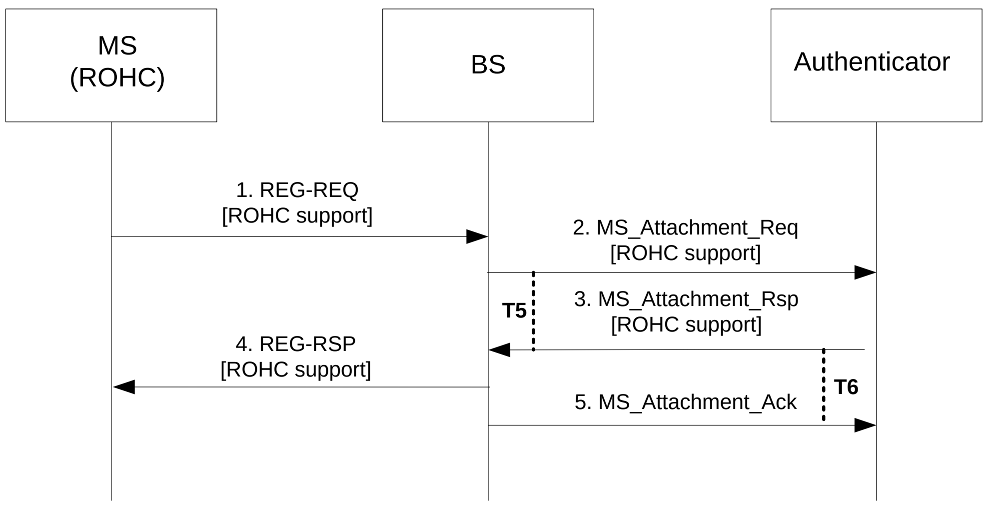

Figure 6-1 ROHC Feature Negotiation Procedure

STEP 1

MS includes the ROHC support TLV [IEEE802.16Rev2] within the REG-REQ message with value set to 0x01 to indicate its support of ROHC feature, and sends the REG-REQ message to the BS.

STEP 2

BS sends *MS_Attachment_Req* message to the Authenticator that includes ROHC support TLV within the REG Context of the MS Info parent TLV, in which the value is set in accordance with the information received from the MS in step 1. Absence of ROHC support TLV from REG-REQ means the MS does not hold any ROHC functionality, in which case the BS abstains from including the ROHC Support in the *MS_Attachment_Req*.

Upon sending the MS_Attachment_Req message, the BS starts the timer T5.

STEP 3

Upon receiving *MS_Attachment_Req* message, the Authenticator discovers the ROHC capability of the MS by looking at the ROHC support TLV contained in the REG Context TLV of the request message, and appropriately stores that information. To indicate both MS and the network's support for ROHC, the Authenticator sets the ROHC support TLV value to 0x01 in the *MS_Attachment_Rsp* message and responds to the BS.

Upon sending the MS_Attachment_Rsp message, the Authenticator starts the timer T6.

STEP 4

If ROHC support TLV was included in the *MS_Attachment_Req*, the BS shall wait to obtain *MS_Attachment_Rsp* before sending the REG-RSP to the MS. Based on the response received from the Authenticator, BS shall set the value of ROHC support TLV in the REG-RSP message.

The BS sends REG-RSP message to MS as specified in IEEE 802.16[IEEE802.16Rev2] formatting the appropriate parameters (from BS policy and/or Authenticator response).

If ROHC support TLV was not included in the *MS_Attachment_Req*, depending on the implementation decision the BS may send the REG-RSP before or after performing the *MS_Attachment_Req* and *MS_Attachment_Rsp* exchange with the Authenticator,In case the MS does not receive REG-RSP, it will retransmit REG-REQ.

STEP 5

The BS sends *MS_Attachment_Ack* message to the Authenticator in the ASN/ASN-GW indicating that *MS_Attachment_Rsp* message from the Authenticator has been received and REG-RSP message has been sent to MS. This message serves as a trigger to the Authenticator to instigate the process of pre-provisioned service flow establishment.

6.1.1 ROHC Feature Negotiation between ASN and CSN

During the access authentication, ASN informs its ROHC capability to AAA server by WiMAX capability TLV (ROHC Support).

If the AAA server receives the ROHC Support Indication (in the WiMAX capability TLV) from ASN, the AAA server shall set the ROHC indication (in WiMAX capability TLV) in the Access-Accept message, based on the operator policies, and send it to the ASN after successful access authentication.

If the AAA server receives the ROHC Support Indication (in the WiMAX capability TLV) from ASN, the AAA server may decide and provide the ROHC indication in the transmission policy TLV to trigger ROHC service flow creation by the ASN GW if ROHC is needed.

6.2 ROHC Service Flow Creation

ROHC Per-Channel Negotiation and ROHC SF creation SHALL take place only if ROHC feature negotiation procedure (described in Section 6.1) was completed successfully. If the ROHC feature negotiation was not successful, then the peers SHALL NOT include *ROHC Parameter TLV* in the DSA/DSC-REQ and DSA/DSC-RSP messages.

Since ROHC Compressor and Decompressor need to negotiate their capabilities, ROHC Per-Channel Parameters SHALL be negotiated between two ROHC peers i.e. MS and ASN-GW. The Per-Channel Parameters are described in the section 5.1.1 of RFC3095 [RFC3095]. When the ROHC SF is established, MAX_CID, LARGE_CIDs, PROFILES, FEEDBACK_FOR SHALL be negotiated between two ROHC peers during SF creation procedure. The type of FEEDBACK_FOR SHALL be the same as that of SFID since a ROHC Channel has a one-to-one relationship with SF. If MRRU is not negotiated, both ROHC peers assume no segment headers are allowed on the ROHC Channel.

The ROHC negotiation procedure is implemented by DSA-REQ/RSP messages or DSC-REQ/RSP messages on the radio interface, R1 according [IEEE802.16Rev2]. The Path_Reg_Req and Path_Reg_Rsp are the respective, corresponding messages for negotiation on the R6/R4 interface. The DSA/DSC_REQ and the R6/R4 Path_Reg_Req messages carry the *ROHC Parameter TLV*. The ROHC parameters will not be included in the DSA/DSC-RSP and R6/R4 *Path_Reg_Rsp* messages, unless the MS rejects ROHC per-channel parameters proposed by the network and uses the DSA/DSC-RSP to indicate its restrictions as described in Section 6.2.1.2. The absence of ROHC Parameter TLV in DSA/DSC-RSP indicates the peer is unwilling to enable ROHC with the offered ROHC Parameter set. The inclusion of an empty ROHC Parameter TLV in a DSA/DSC-RSP with a reject code indicates the peer is unwilling to enable ROHC support on the SF. Additionally, in order to enable ROHC for a specific service flow, the Bit #7 in the Request/Transmission Policy TLV SHALL be set to 0.

ROHC Per-Channel Parameters are exchanged between MS and ASN-GW, the two ROHC peers. The unidirectional ROHC mode is established if no feedback channel identifier is specified (FEEDBACK_FOR field in ROHC Parameter TLV set to 0).

However, more reliable mechanism for ROHC payload delivery SHOULD be a default mode of operation:

• The Piggybacked/Interspersed mode requires one UL and one DL SF for bi-directional IP session. In this case ROHC peers negotiate on the use of the feedback reporting with Piggybacked/Interspersed method by setting the corresponding identifiers in the FEEDBACK_FOR parameter field. The channel for DL ROHC payload packets shall also carry Feedback for UL channel that is identified by 802.16 CID (on R1) and GRE key (on R6). Analogously, the channel for ROHC UL payload shall transport feedback for DL ROHC packets. The Piggybacked/Interspersed ROHC Feedback Mode described in Section 6.2 of [RFC3759] SHALL be supported.

· Another way of creating bidirectional ROHC channel is to create two dedicated feedback channels for both directions. Namely, one uplink ROHC SF has its own downlink ROHC feedback channel and one downlink ROHC SF has its own uplink ROHC feedback channel, which in total requires 4 service flows. The service flows for the dedicated ROHC channels only carry the ROHC feedback packets from one peer to the other peer. The Dual-Channel dedicated ROHC Feedback Mode described in the section 6.3 of RFC3759 MAY be supported.

6.2.1 Network Initiated ROHC Service Flow Creation

ROHC SF creation procedure can take place in two different ways:

1. As part of the Pre-provisioned SF establishment
2. In a dynamic manner triggered by the PCRF

For pre-provisioned service flow the AAA policy provides recommendation to the ASN-GW for ROHC service initiation. Specific AAA information tag in the Request/Transmission Policy TLV indicates whether the service flow should be ROHC enabled or not. In case of dynamic service flow establishment, PCEF derives the ROHC policy from the QoS profile provided by the PCRF. The PCRF then triggers Anchor SFA to initiate the ROHC negotiation. The choice between the two different methods is based on the SF policy operating the ASN GW.

For enabling ROHC in the bidirectional mode with feedback, the ASN-GW (Anchor SFA) SHALL simultaneously allocate and deliver the SFID for DL and UL to achieve the correct pairing of the ROHC payload channels which serve as corresponding feedback channels for each other. The R6 control message initiated by the network (SFA) and corresponding DSA-REQ message for creating the DL ROHC service flow SHALL include the SF ID of the UL ROHC SF within the FEEDBACK_FOR parameter, to indicate that the DL ROHC Channel carries the feedback for the UL ROHC Channel.

In the event that ROHC is not supported by MS, the MS SHALL respond by setting Confirmation Code = 1 (reject-other) in DSA-RSP. In order to signal the ASN-GW that MS does not support ROHC, the BS SHALL send the R6 *Path_Reg_Rsp* with the corresponding Failure Indication TLV (code 0x34 = Failure by rejection of MS) and will also include an empty ROHC Parameter TLV in the message. In this case, depending on the subscriber profile and network policy, the SFA SHALL abort the ROHC SF activation and MAY attempt to activate the service without ROHC.

Figure 6-2 presents a functional description of the ROHC SF creation procedure.

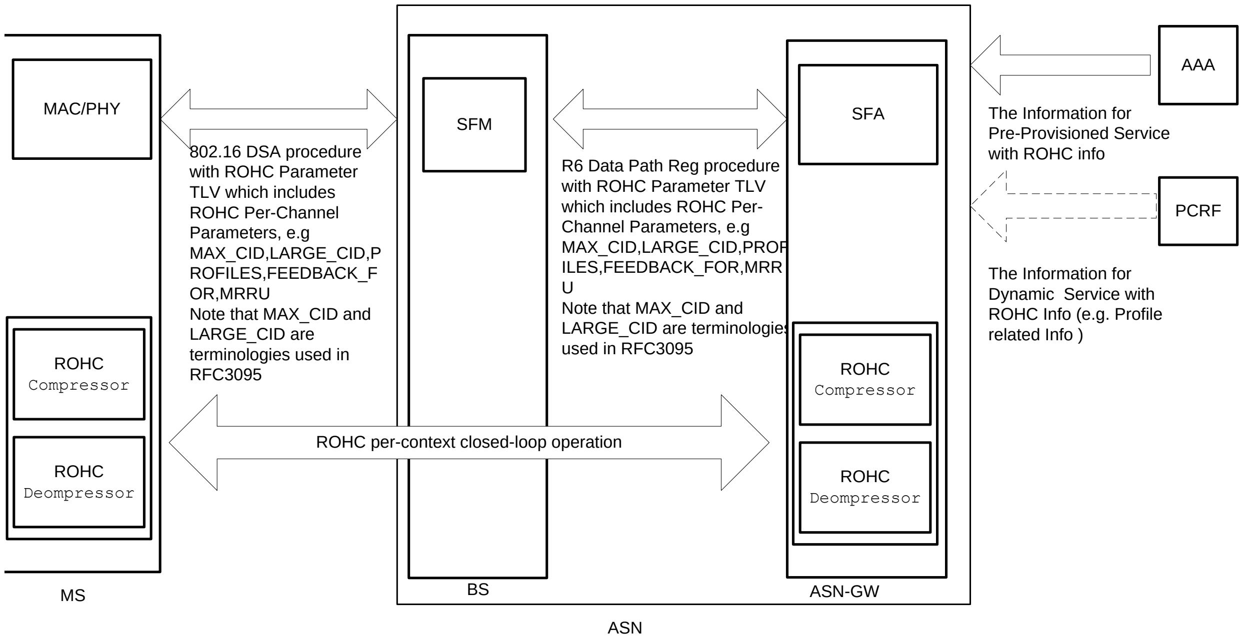

Figure 6-2 The functional diagram of ROHC SF creation

Note that if RoHC is established dynamically (later), A-SFA and SFA may not be the same.

Similar to the normal Service Flow deletion scenarios, RoHC enabled service flows also needs to be deleted upon network exit by the MS, either initiated by the MS or initiated by the network.

6.2.1.1 Successful ROHC Service Flow Creation

Figure 6-3 is a ROHC SF creation procedure.

In Piggybacked/Interspersed mode of ROHC, the SFA iterates two rounds of the following procedure. The first round of the ROHC SF creation procedure is performed and followed by the second round of the ROHC SF creation procedure of the opposite direction.

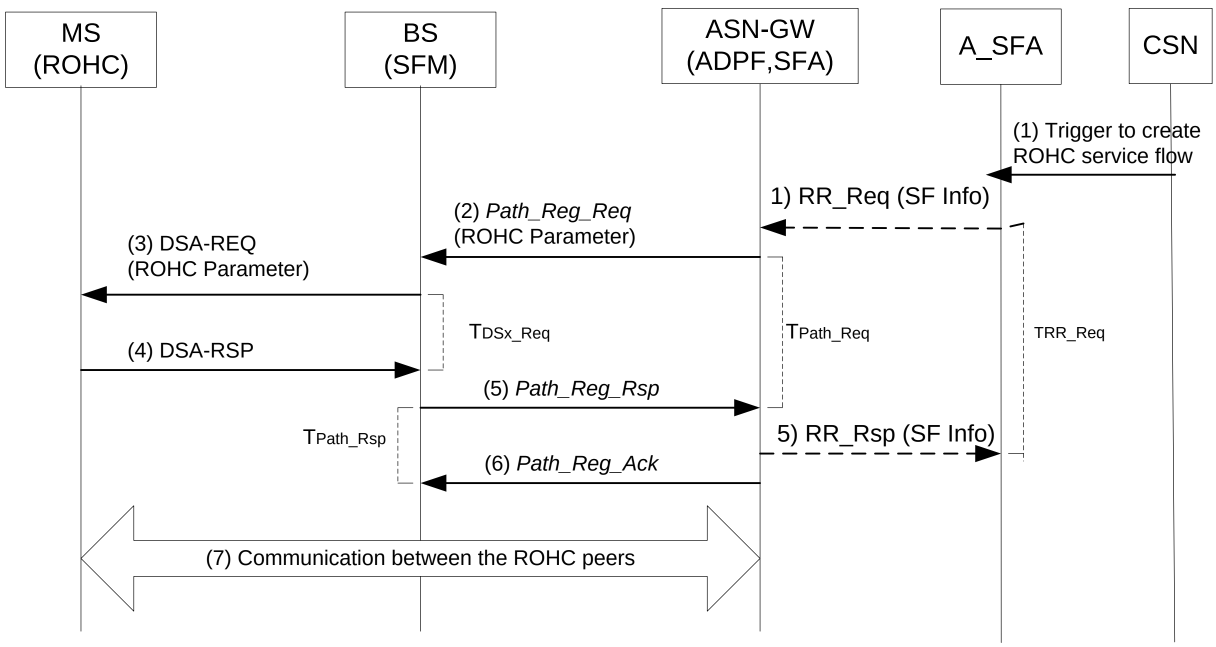

Figure 6-3 ROHC Service Flow creation

STEP 1

CSN triggers the A_SFA to create the ROHC SF And when A_SFA ADPF are not co-located, the A_SFA triggers the serving SFA.

The creation of pre-provisioned ROHC SF is triggered by the AAA. The Transmission Policy TLV carried by Access-Accept message during the access authentication procedure indicates whether ROHC service should be enabled for the given SF.

The creation of dynamic ROHC SF is recommended by PDF/PCRF.

STEP 2

If the ASN-GW decided to activate ROHC service based on AAA recommendation or locally configured policy, the SFA sends the *Path_Reg_Req* message including the ROHC Parameter TLV to the SFM. In Piggybacked/Interspersed mode, the SFA simultaneously allocates one DL SFID and one UL SFID and associates the two service flows for feedback channel. When sending the *Path_Reg_Req,* the SFA include the FEEDBACK_FOR with value set to the SFID of the opposite direction.

STEP 3

The SFM verifies whether there are sufficient radio resources and it decides (based on the QoS-Info parameters and the available resources) whether the request can be accepted. In case of acceptance, a DSA-REQ message is sent to the MS and SHALL include ROHC Parameter TLV.

STEP 4

MS sends a DSA-RSP message to SFM after checking its ROHC capability and supported profiles. If the MS supports the Per-Channel Parameters which the network provided in the ROHC Parameter TLV and the MS accepts other parameters carried in DSA-REQ associated with the service flow, the MS sends DSA-RSP accepting the SF creation.

STEP 5

The SFM sends *Path_Reg_Rsp* messages to the SFA and the SFA sends *RR_Rsp* message to the A_SFA confirming the reservations. In the case that reduced resources was granted by the SFM, the QoS parameter set of the granted resources SHALL be returned by the SFM and the serving SFA in the response back to the Anchor SFA.

STEP 6

The SFA sends *Path_Reg_Ack* messages to the SFM.

In the Piggybacked/Interspersed mode of ROHC, the following procedure SHALL be performed after the step 6.

The second round of the ROHC SF creation procedure (i.e. step 2 through step 6) is performed one more time. During the second round of the procedure, the MS receives the DSA-REQ including FEEDBACK_FOR value set to the SFID of the opposite direction which is allocated from the previous procedure. The MS checks if the value of SFID of FEEDBACK_FOR TLV matches the value of the SFID previously allocated, and also checks if the SFID being created matches the SFID of FEEDBACK_FOR TLV of the previous procedure.

If the both values match each others, the MS associate the first round ROHC SF with the second round ROHC SF, and the Piggybacked/Interspersed mode of ROHC Channel and feedback channels are established.

STEP 7

After establishing ROHC SF between the MS and ASN-GW, ROHC communication between two ROHC peers is performed over R1 connection and the R6 Data Path.

6.2.1.2 Failure of ROHC Service Flow Creation

In case the ROHC feature negotiation completed successfully, the ROHC SF creation can still fail due to mismatch of Per-Channel Parameters negotiated between the two ROHC entities (inability of the ROHC Decompressor side to support specific parameters specified by the ROHC Compressor). Failure could occur in the following cases:

- MS supporting ROHC Function is not capable of accepting one or more ROHC Per-Channel Parameters that were proposed by the network for the UL/DL ROHC SF creation. The conflicting Per-Channel Parameters may include one or more incompatible ROHC profile or an unacceptable Maximum Reconstructed Reception Unit size (MRRU) value if ROHC segmentation is allowed.
- In this case the MS may try to adjust ROHC Per-Channel Parameters as suited by renegotiating those values through the responding DSA/DSC-RSP message. In case of failed ROHC negotiation, the MS SHALL always respond with DSA/DSC-RSP message with Confirmation Code TLV set to value reject-other (i.e., Confirmation Code = 1). When MS explicitly rejects ROHC SF setup it SHOULD additionally include an empty ROHC Parameter TLV. The BS SHALL relay the empty ROHC Parameter TLV over the R6 including the corresponding Failure Indication code (0x34), signaling to ASN-GW that MS intentionally rejected ROHC SF setup. In case MS attempts to renegotiate parameter values other than proposed in DSA-REQ messages it SHALL also include *ROHC Parameter T*LV containing new proposed values for per-Channel Parameters in the corresponding DSA-RSP message. There are three possible outcomes of the failed initial ROHC SF creation procedure:

1. In the event that ROHC is not supported by MS, the SFA MAY abort the service flow activation and attempt to activate the same service flow without ROHC.

2. If MS attempted to renegotiate ROHC Per-Channel Parameters by including the ROHC Parameter TLV, the network MAY accept modifications of the specific ROHC parameters proposed by the MS. In this case, network MAY initiate another attempt to setup the ROHC-compressed SF by repeating the DSA-REQ/RSP procedure for ROHC SF creation with a new set of parameters.

3. In case the MS did include the ROHC Parameter TLV, but the network-side ROHC entities in ASN-GW cannot fulfill request for ROHC SF creation (unacceptable Per-Channel Parameters, lack of resources or other reasons) then the Anchor SFA SHALL withdraw from setting up of the ROHC compression for that service flow. In order to provide service for the MS the network SHOULD instead proceed as described in Section 4.6.4.4.1 of [NWGSTG3], by setting up a regular service flow without the ROHC compression. Alternatively, the network MAY decide to abstain from any further attempt of the SF creation.

The Figure 6-4 illustrates a failure scenario for the ROHC SF creation attempt followed by renegotiation of ROHC Per-Channel Parameters.

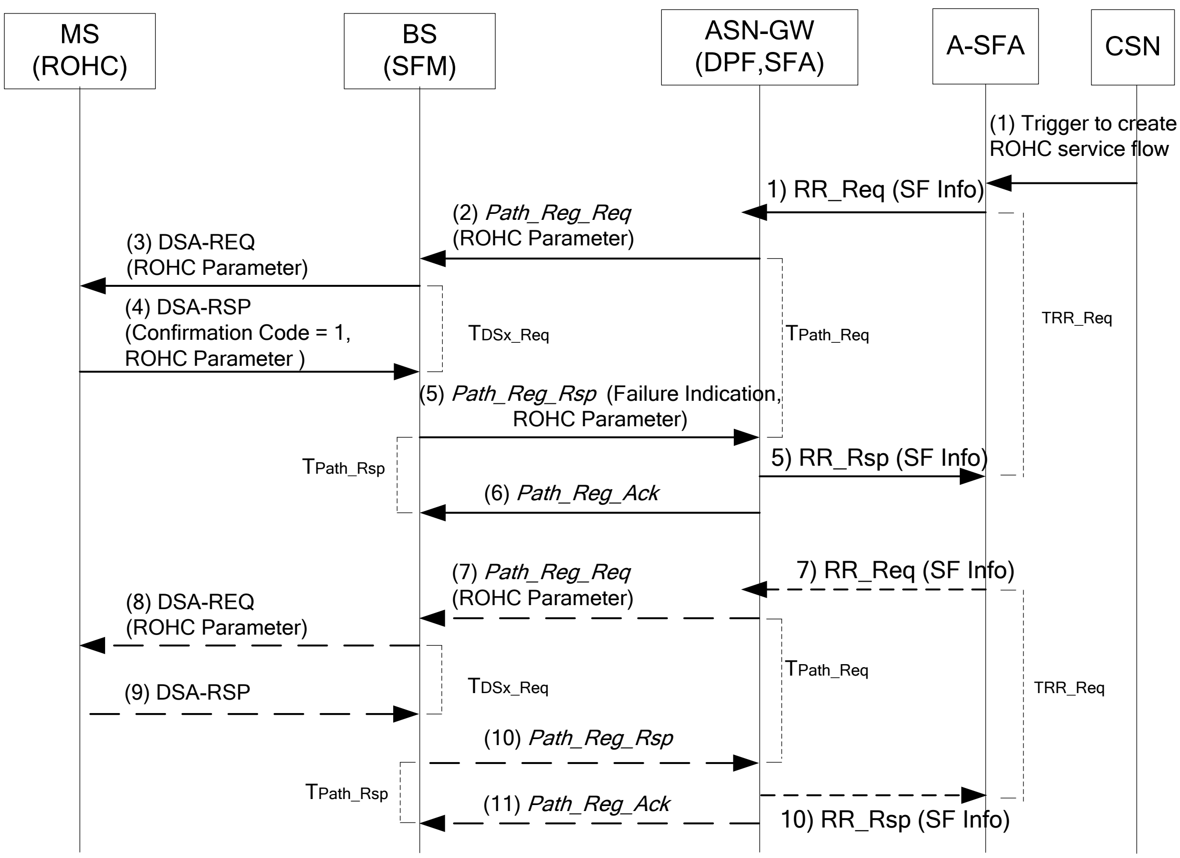

Figure 6-4 Failure of the ROHC SF creation followed by parameter renegotiation

STEP 1 - 3

The steps 1, 2 and 3 are correspondent to the steps 1, 2 and 3 of the ROHC SF creation procedure described in the previous section.

STEP 4

If MS cannot accept ROHC profile or Per-Channel Parameters it previously obtained, it responds with DSA-RSP message that includes Confirmation Code set to value 1, and that MAY include ROHC Parameter TLV with new ROHC configuration parameters proposed by the MS.

STEP 5

The ROHC parameters proposed by the MS are transferred to the SFA and the corresponding ROHC Function in the ASN-GW in the *Path_Reg_Rsp*. The SFA sends *RR_Rsp* message to the A_SFA confirming the reservations. The responding R4/R6 messages SHALL include Failure Indication TLV *(error code set to value 0x34 = Failure by rejection of MS)*, and SHALL include ROHC Parameter TLV if the MS included ROHC Parameter TLV within the DSA-RSP in STEP 4.

STEP 6

The SFA sends *Path_Reg_Ack* messages to the SFM. The initial ROHC SF creation attempt is now terminated.

The SFA may evaluate the ROHC configuration parameters, if such were proposed by the MS (in step 4), in order to determine whether it is possible to achieve a different ROHC per-channel configuration for the given SF. At this point the SFA MAY accept ROHC Per-Channel Parameter values proposed by the MS. If the SFA has accepted them, the SFA SHALL reinitiate ROHC SF creation procedure with those new Per-Channel Parameters.

If the MS rejected the SF creation and did not propose alternative ROHC Per-channel configuration, or the SFA and ROHC entity in the ASN-GW cannot provide a compatible ROHC configuration based on the parameters proposed by the MS, then the procedure MAY continue by setting up a new SF without ROHC depending on network policy.

STEP 7 - 11

The A_SFA and SFA initiate ROHC SF creation as described in steps 2 through 6 of Section 6.2.1.1. The ROHC Parameter TLV included in the corresponding R4/R6 and R1 messages SHOULD include a different set of ROHC per-channel parameters values as discussed in the preceding STEP 6.

6.2.2 Network Initiated ROHC SF Deletion

In case of pre-provisioned SF, ROHC SF deletion is done similar to any other SF deletion specified in [NWGSTG3].

In case of PCC initiated SF, ROHC SF deletion is done similar to any other SF deletion specified in [NWG-PCC].

6.3 ROHC Context in Idle Mode

When the MS is going into the idle mode state by performing Idle Mode Entry procedure, the negotiated ROHC Per-Channel Parameters SHALL be stored in the Anchor DPF.

The internal states and dynamically established contexts such as ROHC Context ID for ROHC instances for the given MS SHALL be reset when the MS enters idle mode by performing Idle Mode Entry procedure.

6.4 Relocation Impact on ROHC

6.4.1 Handover without ROHC Entity Relocation

Handovers that do not include Anchor-DPF relocation do not involve relocation of ROHC functional entity in the ASN. Hence, there are no requirements for MS and ASN functional entities additional to those imposed by [NWGSTG3] due to ASN Anchored mobility with ROHC support.

6.4.2 The Success Case of Handover with ROHC Entity Relocation

Relocation of Anchor DPF involves relocation of ROHC functional entity as they are collocated with each other. ROHC capability, parameters and elements of context information have to be transferred from the old Anchor DPF to the new Anchor DPF when the relocation occurs. Impact on ROHC relocation for both PMIP4 and CMIP4 scenarios are addressed in the subsequent sections.

6.4.2.1 PMIP4 Scenario

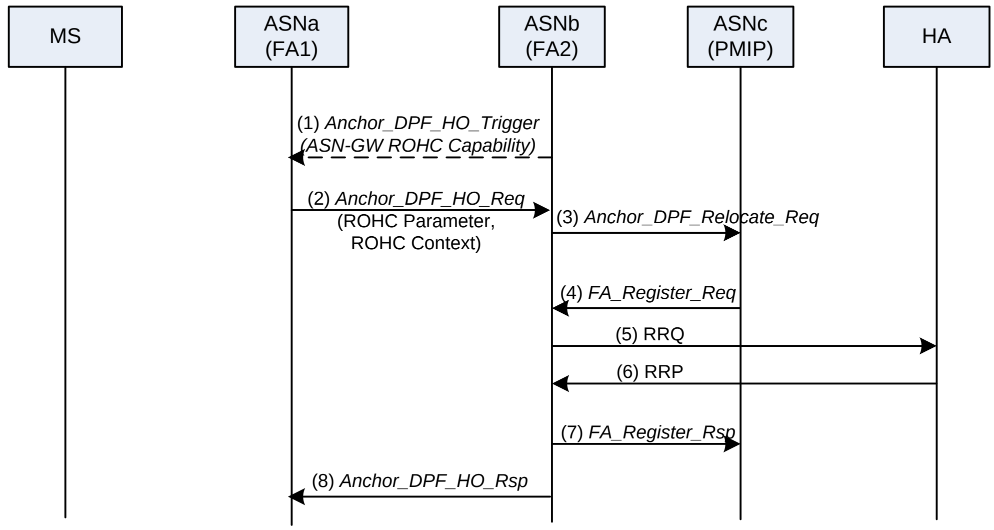

Figure 6-5 ROHC Relocation (PMIPv4)

STEP 1

The new FA (FA2) triggers the R3 relocation by sending Anchor DPF HO trigger message to the old FA (FA1). Since ROHC entity should be collocated with FA/Anchor DPF, ROHC entity is relocated with FA/Anchor DPF. The ROHC Capability of the ASNb/FA2 is contained in the *Anchor_DPF_HO_Trigger* message to indicate ROHC support at the target ASN-GW. This step is optional.

STEP 2

The old ASNa (FA1) sends the Anchor_DPF_HO_Req which contains ROHC Per-Channel Parameters of every service flow.

FA2 triggers PMIP client to construct MIP-RRQ.

STEP 3

PMIP client sends constructed MIP-RRQ and security information to FA2.

STEP 4

FA2 sends MIP-RRQ to HA.

STEP 5

HA responds with MIP-RRP to FA2.

STEP 6

FA2 sends FA register response to PMIP client.

STEP 7

FA2 sends Anchor_DPF_HO_Rsp to FA1 to confirm that R3 relocation has been completed. After the relocation the ROHC service flows retain the exact ROHC Per-Channel configuration allowing identical processing of ROHC payload at the new ASN. ROHC context SHALL be re-established if it was not transferred from the old anchor ASN.

If new anchor ASNb detects that it can not provide the same ROHC capability as the previous anchor, it SHALL initiate R6 Path-Release procedure defined in [NWGSTG3] 802.16 DSD procedure for deletion of SFs with ROHC. The new anchor ASNb then self initiates ROHC SF creation procedure as defined in section 6.2.1.

6.4.2.2 CMIP4 scenario

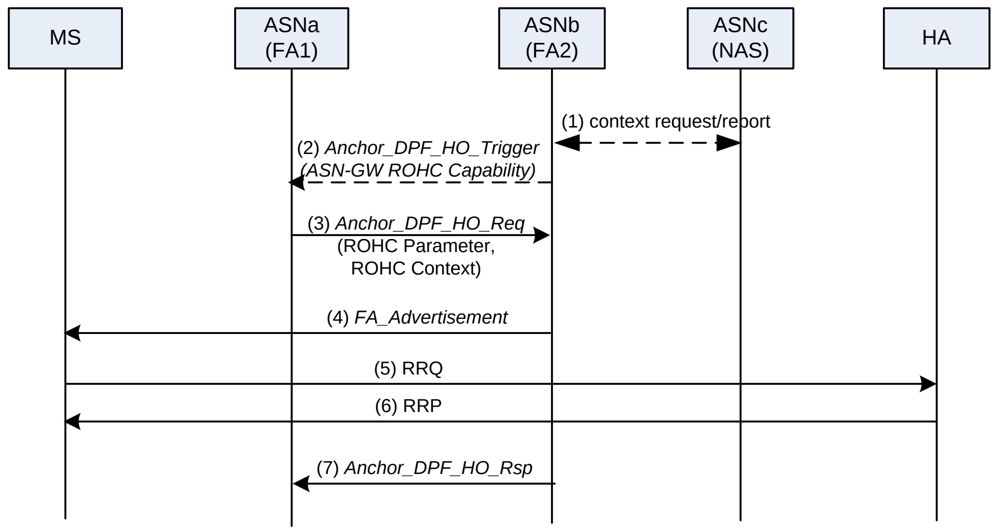

Figure 6-6 ROHC Relocation (CMIPv4)

STEP 1

ASNb sends a *Context_Req* message to the Authenticator in ASNc for obtaining MIP keys. The Authenticator sends *Context_Rpt* that contains the FA-HA and MN-FA MIP keys if these key are used.

STEP 2

The new FA (FA2) triggers the R3 relocation by sending *Anchor_DPF_HO_Trigger* message (Pull Mode) to the old FA (FA1). Since ROHC entity should be collocated with FA/Anchor DPF, the ROHC entity is relocated with FA/Anchor DPF. The ROHC Capability of the ASNb/FA2 is contained in the Anchor DPF HO trigger message. This step is optional for the PULL mode.

STEP 3

The old FA (FA1) either PUSH or responses with *Anchor_DPF_HO_Request* message, which contains the ROHC parameters for each service flow (applied for ROHC Channels before R3 relocation) and optionally the ROHC contexts.

STEP 4

The new FA in ASNb sends Agent Advertisement to the MS.

STEP 5 - 6

The MS responds with RRQ. ASNb relays RRQ to HA after validating MN-FA authentication extension (if required) and appending FA-HA authentication extension. HA responds with RRP. ASNb relays the RRP to MS. At this point, ASNb/FA gets registered with HA.

STEP 7

The target ASNb also replies to the source ASNa with an *Anchor_DPF_HO_Rsp* message indicating a successful FA relocation. If the Target ASNb does not accept FA relocation it responds with an *Anchor_DPF_HO_Rsp* message with *Accept/Reject Indicator* indicating Reject as specified in Section 4.8.3.3.7.1 of [NWGSTG3].

Service flows with ROHC parameters unchanged after R3 relocation can resume ROHC SF processing with the previous ROHC parameters. ROHC context can be reused or re-established all over between the ROHC peers.

If new anchor ASNb detects that it can not provide the same ROHC capability as the previous anchor, it SHALL initiate R6 Path-Release procedure defined in [NWGSTG3] 802.16 DSD procedure for deletion of SFs with ROHC. The new anchor ASNb then self initiates ROHC service flow creation procedure as defined in Section 6.2.1of [NWGSTG3].

[Editor's Note: If any external ROHC specification or RFC allows falling back to the uncompressed mode in the case of profile incompatibilities between compressor and decompressor, such approach is applicable in the R3 relocation scenario as the alternative to SF deletion and recreation].

6.4.3 The Handling of Handover Failure with ROHC Entity Relocation

6.4.3.1 ROHC Relocation from ASN Supporting ROHC to ASN not Supporting ROHC

[This scenario is for both PMIPv4 and CMIPv4]

Figure 6-7 is the scenario of checking ASN-GW ROHC capability before ROHC relocation where target ASN-GW detects that it can not provide the same capability of ROHC and then rejects Anchor_DPF_HO_Trigger, thus keeps maintaining the function of Anchor DPF for MS.

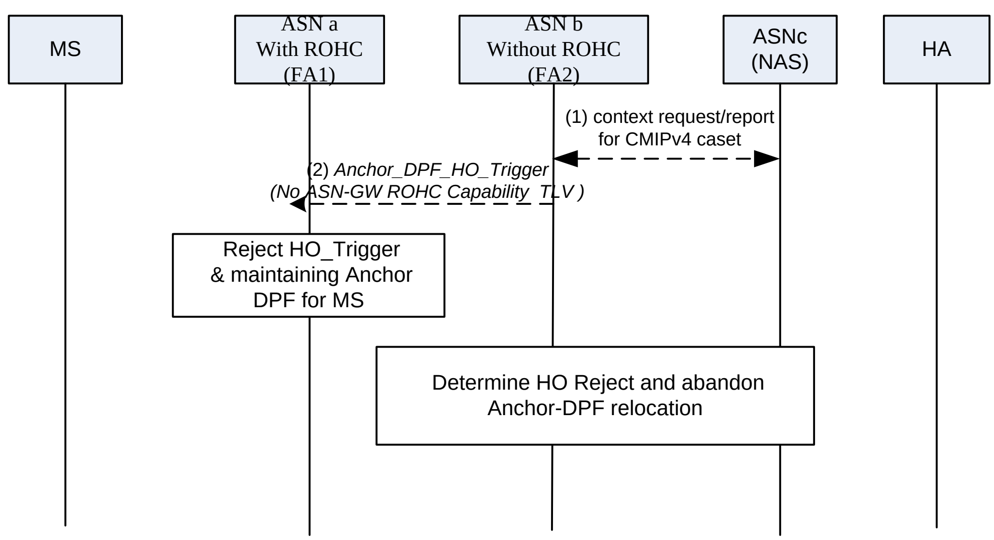

Figure 6-7 ROHC Relocation (Failure)

STEP 1

The step 1 is the same as that of CMIPv4 scenario in Section 6.4.2.2 CMIPv4 scenario. This step is optional

[Editor's Note: It is only optional procedure for CMIPv4]

STEP 2

The target ASN b (FA2) triggers the R3 relocation by sending Anchor DPF HO trigger message with ASN-GW ROHC Capability TLV to the anchor ASN a (FA1).

The Behavior of ASNa:

The anchor ASN a (FA1) receives the Anchor DPF HO trigger message with ASN-GW ROHC Capability TLV and then determine whether it accepts Anchor DPF HO or not. ASNa rejects Anchor DPF HO in following cases.

The Behavior of ASNb:

The target ASN b (FA2) detects the rejection of Anchor DPF HO and then abandons it.

6.5 ROHC Accounting

6.5.1 Accounting Requirements

The accounting procedure for ROHC SF shall support the normal accounting procedure for all service flows. Accounting may also be supported on ROHC SF, after the header compression stage.

ASN and AAA negotiate the supported accounting mode. During the initial network entry, the ASN downloads the accounting policy from the AAA server. The accounting client in the A-DPF will generate for the ROHC service flows UDRs in a single accounting mode at a time, either normal uncompressed accounting (as specified in [NWGSTG3]) or ROHC accounting after the compression.

6.5.2 Accounting Procedure for ROHC Service Flow

Figure 6-8 shows the ROHC SF accounting procedure.

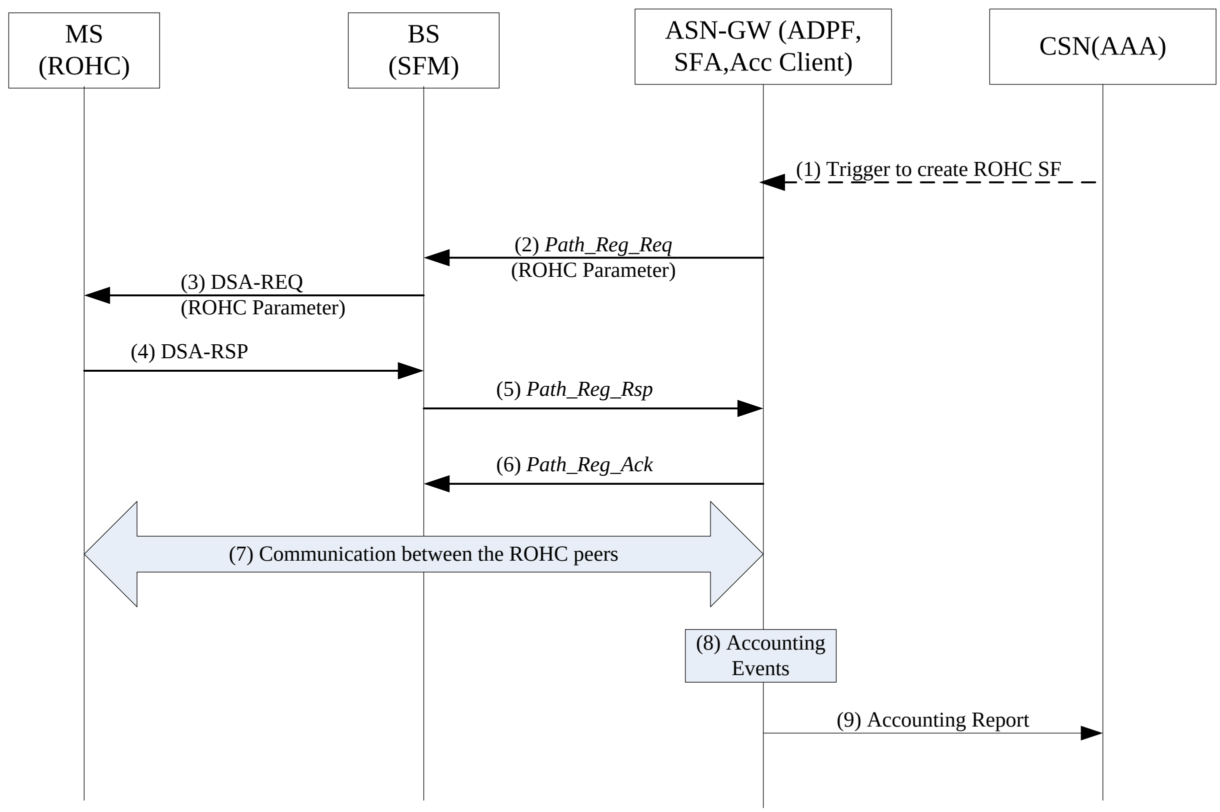

Figure 6-8 The accounting Procedure for ROHC SF

STEP 1 – STEP 7

The same as Figure 6-2 in Section 6.2.1.1.

STEP 8

The Accounting Agent collects accounting data for the ROHC SF and reports to the Accounting Client based on accounting events specified in [NWGSTG3].

STEP 9

The Accounting Client generates UDR based on the received accounting information from Accounting Agent and reports the UDR to the AAA Server.

6.6 ROHC Termination

In case of either ISF or PPSF with ROHC, the network exit procedure results in termination of the ROHC Functions in both MS and ASN-GW.

In case of Dynamic Service Flow with ROHC, Dynamic Service Flow Deletion Procedure triggered from PCRF terminates ROHC Functions in both MS and ASN-GW.

7. Message and Parameter Definitions

7.1 Constants and Counters

No new constants and counters are identified to support ROHC operation.

7.2 Message Definition

Table 7-1 Anchor DPF HO Trigger Message

IE	Reference	M/O	Notes
ASN-GW ROHC Capability	7.3.2.7	O	Shall be included when ROHC is supported at the target ASN.

Table 7-2 Anchor DPF HO_Req Message

IE	Reference	M/O	Notes
ROHC Parameter	7.3.2.1	O	Shall be included when ROHC is applied to the service flows at the Anchor ASN.

7.3 TLV Definitions and TLV Encoding

This TLV Definition and TLV Encoding is used for R6 and R4 to support ROHC operation.

7.3.1 TLV Format

The TLV Format is defined in Section 5.3.1 of [NWGSTG3].

7.3.2 TLV Encoding

This section defines new TLVs required for support of ROHC in Release R1.5. These extend the TLVs of Section 5.3.2 of [NWGSTG3]. The TLV definitions follow the definitions of the corresponding radio interface TLVs.

The TLV with Type 155 replaces the already existing one in the current [NWGSTG] Section 5.3.2.155 which has been reserved for Release R1.5. The other TLVs are new, and suitable new TLV Types will need to be assigned.

7.3.2.1 ROHC Parameter

This TLV replaces TLV 155 of Section 5.3.2.155 of [NWGSTG3].

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	155
Length in octets	Variable
Value	Compound TLV

Description	Includes the Per-Channel Parameters according Section 5.1.1 of [RFC3095] for a single ROHC SF.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	ROHC_MAX_CID	M
	ROHC_LARGE_CIDS	M
	ROHC_PROFILES	M
	ROHC_FEEDBACK_FOR	O
	ROHC_MRRU	O
Parent TLV	SF Info	

7.3.2.2 ROHC_MAX_CID

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	418
Length in octets	2
Value	Nonnegative integer in the most-significant-first order
Description	Highest context ID number to be used by the ROHC Compressor on this ROHC Channel, i.e. on this SF. See Section 5.1.1 of [RFC3095]
Parent TLV	ROHC Parameter

7.3.2.3 ROHC_LARGE_CID

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	419
Length in octets	1
Value	0x00 - False (Use of small Context ID range) 0x01 - True (Use of large Context ID range) All other values are RESERVED.
Description	Boolean; if false, the short CID representation (0 bytes or 1 prefix byte, covering CID 0 to 15) is used; if true, the embedded CID representation (1 or 2 embedded CID bytes covering CID 0 to 16383) is used. See Section 5.1.1 of [RFC3095].
Parent TLV	ROHC Parameter

7.3.2.4 ROHC_PROFILES

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	420
Length in octets	2n (Variable)
Value	A sequence of nonnegative integers (in the most-significant-first order)

Description	Each integer of the set is 2-bytes in length indicating an identifier of the ROHC profile supported by the ROHC Decompressor. The profile value maps directly to a non-reserved ROHC profile identifier defined in IANA registry ("RObust Header Compression (ROHC) Profile Identifiers", http://www.iana.org/assignments/rohc-pro-ids) The following profiles shall be mandatory: 0x0000 - ROHC uncompressed
Parent TLV	ROHC Parameter

7.3.2.5 ROHC_FEEDBACK_FOR

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	421
Length in octets	4
Value	0x00000000 – No associated ROHC feedback Otherwise – SFID of the associated ROHC Channel
Description	Optional reference to a ROHC SF (ROHC Channel) in the opposite direction. If provided, this parameter indicates the ROHC Channel to which any feedback sent on this SF refers to. See [RFC3095].
Parent TLV	ROHC Parameter

7.3.2.6 ROHC_MRRU

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	422
Length in octets	2
Value	0x0000 – No segmentation Otherwise – MRRU size
Description	Maximum reconstructed reception unit. This is the size of the largest reconstructed unit in octets that the ROHC Decompressor is expected to reassemble from segments. See Sections 5.1.1 and 5.2.5 of [RFC3095]. Note that this size includes the CRC. If MRRU is negotiated to be 0, or if the MRRU TLV is not included then segmented headers are not allowed on the channel.
Parent TLV	ROHC Parameter

7.3.2.7 ASN-GW ROHC Capability

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	423
Length in octets	1
Value	0x00 = ROHC is not supported 0x01 = ROHC is supported

Description	When this TLV is included in Anchor DPF HO Trigger message, it is used for indicating the ROHC capability of the target ASN for the purpose of completing the R3 relocation with ROHC.
Parent TLV	MS Info

7.3.2.8 ROHC Support

This TLV SHALL NOT be included for any WiMAX Release prior to R1.5.

Type	424
Length in octets	1
Value	0x00 = ROHC is not supported 0x01 = ROHC is supported
Description	This TLV is used during the registration procedure to indicate if the ROHC compression is supported by the MS, or from the network side. The definition correlates to the R1 ROHC support TLV definition given in [IEEE802.16Rev2].
Parent TLV	REG Context

7.3.2.9 Request/Transmission Policy

This TLV replaces TLV 150 of Section 5.2.3.150 of [NWGSTG3].

[Editor Note: please modify the following table of Section 5.2.3.150 of [NWGSTG3]]

Type	150
Length in octets	4
Value	32-bit bitmask. • Bit #0 = Service flow SHALL not use broadcast bandwidth request opportunities. (Uplink only) • Bit #1 = Reserved. • Bit #2 = Service flow SHALL not piggyback requests with data. (Uplink only) • Bit #3 = Service flow SHALL not fragment data. • Bit #4 = Service flow SHALL not suppress payload headers (CS parameter). [Note that the following description is an excerption from IEEE802.16Rev2.] If bit #4 is set to'0' and both the SS and the BS support PHS (according to section 11.7.7.3 of IEEE std 802.16), each SDU for this service flow shall be prefixed by a PHSI field, which may be set to 0 (see section 5.2). If bit #4 is set to '1', none of the SDUs for this service flow will have a PHSI field. • Bit #5 = Service flow SHALL not pack multiple SDUs (or fragments) into single MAC PDUs. • Bit #6 = Service flow SHALL not include CRC in the MAC PDU. • Bit #7 = The service flow shall not compress payload headers using ROHC. [Note that the following description is an excerption from IEEE802.16Rev2]. If bit #7 is set to'0' and both the SS and the BS support ROHC (according to section 11.7.7.4 of IEEE std 802.16), each SDU for this service flow shall be compressed using ROHC. If bit 7 is set to '1', none of the SDUs shall be compressed. All other bit positions are reserved.
Description	The value of this parameter provides the capability to specify certain attributes for the associated service flow. These attributes include options for PDU formation, and for uplink service flows, restrictions on the types of bandwidth request options that may be used. An attribute is enabled by setting the corresponding bit position to 1. The bit#7 is reserved prior to NWG release 1.5
Parent TLV	QoS Parameters

7.4 RADIUS Message and Attributes

7.4.1 RADIUS Messages

No new messages are identified to support ROHC operation.

7.4.2 WIMAX RADIUS VSAs Definitions

[Editor Note: Please replace the following description for the table Transmission Policy TLV on the top of the section 5.4.2.29]

TLV ID	17 for Transmission Policy
Description	The parameter indicates the transmission policy of a service flow.
Length	2+1
Value	Octet enumeration with the following values defined: Bit #0 – Service flow shall not use broadcast bandwidth request opportunities. (Uplink only) Bit #1 –Service flow shall not use multicast bandwidth request opportunities. (Uplink only). Bit #2 – The service flow shall not piggyback requests with data. (Uplink only) Bit #3 – The service flow shall not fragment data. Bit #4 – The service flow shall not suppress payload headers (CS parameter). Bit #5 – The service flow shall not pack multiple SDUs (or fragments) into single MAC PDUs. Bit #6 – The service flow shall not include CRC in the MAC PDU. Bit #7 – The service flow shall not compress payload headers using ROHC.

Note: The bit#7 is reserved prior to NWG release 1.5

7.4.3 WIMAX Capability

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    Vendor-Id (cont)           | WiMAX TYPE    |    Length     |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  Continuation |            TLVs
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	1 for WiMAX Capability Attribute
Description	In an Access-Request the attribute identifies the WiMAX Capabilities supported by the ASN or the HA. In an Access-Accept, identifies the options selected by the RADIUS server.
Length	6 + 3 + TLVs
Continuation	C-bit = 0
Value	One or more of the following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	WiMAX Release	6	1	0	0	0
2	Accounting Capabilities	3	1	1	0	0
3	Hotlining Capabilities	3	0-1[a]	0	0	0
4	Idle Mode Notification Capabilities	3	0-1[b]	0-1[c]	0	0
5	ROHC Support	3	0-1[d]	0-1[e]	0	0

Notes:

[a] The absence of this sub-TLV in an Access-Request (AR) means that the NAS or HA does not support hotlining.

[b] The absence of this sub-TLV in an Access-Request (AR) means that the NAS does not support Idle Mode Notification. This sub-TLV SHALL NOT appear in Access-Request originating from an HA. The HAAA SHALL silently ignore this sub-TLV in messages originating from an HA.

[c] The absence of this sub-TLV in an Access-Accept (AA) message means that the HAAA does not require Idle Mode Notification. The HAAA SHALL NOT send this sub-TLV to a HA. An HA SHALL silently ignore this sub-TLV.

[d] The absence of this sub-TLV in an Access-Request (AR) means that the ASN does not support ROHC.

[e] The absence of this sub-TLV in an Access-Accept (AA) message means that the HAAA does not require ROHC. The HAAA SHALL NOT send this sub-TLV to a HA. An HA SHALL silently ignore this sub-TLV.

7.5 DIAMETER Message and Attributes

[Editor Note: Please replace the following description for the table Transmission Policy TLV on the top of Section 5.4.2.29 in [NWGSTG3]]

TLV ID	17 for Transmission Policy
Description	The parameter indicates the transmission policy of a service flow.
Length	2+1
Value	Octet enumeration with the following values defined: Bit #0 – Service flow shall not use broadcast bandwidth request opportunities. (Uplink only) Bit #1 –Service flow shall not use multicast bandwidth request opportunities. (Uplink only). Bit #2 – The service flow shall not piggyback requests with data. (Uplink only) Bit #3 – The service flow shall not fragment data. Bit #4 – The service flow shall not suppress payload headers (CS parameter). Bit #5 – The service flow shall not pack multiple SDUs (or fragments) into single MAC PDUs. Bit #6 – The service flow shall not include CRC in the MAC PDU. Bit #7 – The service flow shall not compress payload headers using ROHC.

Note: The bit#7 is reserved prior to NWG release 1.5

7.6 R3-PCC Message and Attributes

No new R3-PCC attributes are required when performing a PDF/PCRF-initiated ROHC SF creation.

However, if PCC system is used, the A-PCEF can decide to create the ROHC-SF by looking at the QCI value as a hint for indicating ROHC SF.