



WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures
Network Architecture Femtocell Core Specification

WMF-T33-118-R016v02

WMF Approved
(2011-11-14)

WiMAX Forum Proprietary

Copyright © 2011 WiMAX Forum. All Rights Reserved.

1 Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability

2
3 Copyright 2011 WiMAX Forum. All rights reserved.

4
5 The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for
6 download from the WiMAX Forum and may be duplicated for internal use by the WiMAX Forum members, provided that all
7 copies contain all proprietary notices and disclaimers included herein. Except for the foregoing, this document may not be
8 duplicated, in whole or in part, or distributed without the express written authorization of the WiMAX Forum.

9
10 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance
11 of the following terms and conditions:

12
13 **THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST**
14 **EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND**
15 **STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE,**
16 **NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX**
17 **FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND**
18 **DISCLAIMS ANY WARRANTIES TO THE CONTRARY.**

19
20 Any products or services provided using technology described in or implemented in connection with this document may be
21 subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely
22 responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all
23 required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable
24 jurisdiction.

25
26 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**
27 **APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY**
28 **OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.**

29
30 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**
31 **SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY**
32 **CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.**

33
34 The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any
35 technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any
36 technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual
37 property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology,
38 standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies,
39 technologies, standards, and specifications, including through the payment of any required license fees.

40
41 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH**
42 **RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED**
43 **INTO THIS DOCUMENT.**

44
45 **IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD**
46 **PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING,**
47 **WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL**
48 **PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY**
49 **USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS**
50 **MEMBERS RELATING TO THE USE OF THIS DOCUMENT.**

51
52 The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is
53 solely responsible for determining whether this document has been superseded by a later version or a different document.

54
55 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum
56 Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks
57 of the WiMAX Forum. All other trademarks are the property of their respective owners. Wi-Fi® is a registered
58 trademark of the Wi-Fi Alliance.

1	Table of Contents	
2	1. INTRODUCTION AND SCOPE.....	9
3	1.1 Document Scope.....	9
4	2. DEFINITIONS AND CONVENTIONS.....	10
5	2.1 Definitions.....	10
6	2.1.1 <i>Broadband Connection</i>	10
7	2.1.2 <i>WiMAX® Femto Access Point</i>	10
8	2.1.3 <i>Exclusion Zone</i>	10
9	2.1.4 <i>WiMAX® Femtocell</i>	10
10	2.1.5 <i>WiMAX® Macro-network</i>	10
11	2.1.6 <i>Closed Subscriber Group (CSG)</i>	10
12	2.1.7 <i>Non-CSG Authorized User</i>	10
13	2.1.8 <i>FemtoCell Subscriber</i>	11
14	2.1.9 <i>Self-Organizing Networks</i>	11
15	2.1.10 <i>CSG white list</i>	11
16	2.1.11 <i>Femto Gateway</i>	11
17	2.1.12 <i>Security Gateway</i>	11
18	2.2 Conventions.....	11
19	3. REFERENCES.....	12
20	4. NETWORK REFERENCE MODEL.....	13
21	4.1 Overview.....	13
22	4.2 Reference Model.....	14
23	4.2.1 <i>WiMAX® Femto Access Points (WFAP)</i>	14
24	4.2.2 <i>Femto Gateway (Fe-GW)</i>	14
25	4.2.3 <i>Security Gateway (Se-GW)</i>	15
26	4.2.4 <i>SON</i>	15
27	4.2.5 <i>WFAP Management System</i>	15
28	4.2.6 <i>Bootstrap server</i>	15
29	4.2.7 <i>Femto-AAA server</i>	15
30	4.3 Reference Points.....	15
31	4.3.1 <i>Reference Point R1</i>	15
32	4.3.2 <i>Reference Point R3</i>	15
33	4.3.3 <i>Reference Point R4</i>	16
34	4.3.4 <i>Reference Point R6-F</i>	16
35	4.3.4.1 <i>R6-F control plane</i>	16
36	4.3.4.2 <i>R6-F bearer plane</i>	16
37	4.3.5 <i>Reference Point R3-F</i>	16
38	4.3.6 <i>Reference Point Rb</i>	16
39	5. CONTROL PLANE PROTOCOLS AND PROCEDURES.....	17
40	5.1 WFAP Initialization and authentication.....	17
41	5.1.1 <i>WFAP Initialization</i>	17
42	5.1.2 <i>Discovery of Bootstrap Server by WFAP using DHCP</i>	19
43	5.1.3 <i>WFAP Bootstrapping over Rb</i>	20
44	5.1.3.1 <i>Femto-WIB Protocol Requirements</i>	20
45	5.1.3.2 <i>Bootstrap message encoding</i>	21
46	5.1.4 <i>WFAP-Se-GW Authentication and IPsec Tunnel Management</i>	22
47	5.1.4.1 <i>Authentication and Tunnel Setup</i>	22
48	5.1.4.1.1 <i>WFAP R6 Identifier</i>	22

Femto-Core

1	5.1.4.1.2	WFAP Requirements	22
2	5.1.4.1.3	Se-GW Requirements	23
3	5.1.4.1.4	Femtocell GW Requirements	23
4	5.1.4.1.5	Femto-AAA Server Requirements	24
5	5.1.4.1.6	Call Flow	24
6	5.1.4.2	Tunnel Tear Down	26
7	5.1.4.2.1	WFAP Requirements	26
8	5.1.4.2.2	Se-GW Requirements	26
9	5.1.4.2.3	Femto-AAA Requirements	26
10	5.1.5	WFAP Location authorization	27
11	5.1.6	WFAP Registration to Fe-GW	27
12	5.2	WFAP Network Exit	28
13	5.2.1	WFAP triggered WFAP network exit	28
14	5.2.2	Network triggered WFAP exit (Graceful)	29
15	5.2.3	Fe-GW triggered WFAP Network Exit (Ungraceful)	30
16	5.2.4	WFAP De-registration with Fe-GW	31
17	5.2.4.1	WFAP initiated De-registration	31
18	5.3	CSG White-list on the MS	33
19	5.4	MS Network entry and exit	33
20	5.4.1	MS Network entry into CSG WFAP	33
21	5.4.1.1	MS Network entry into CSG-Closed WFAP	33
22	5.4.1.2	MS Network entry into CSG-Open WFAP	34
23	5.4.1.3	MS Network entry for Emergency access	34
24	5.4.2	MS Network exit	35
25	5.5	Mobility Management	35
26	5.5.1	WFAP to Macro-BS mobility	35
27	5.5.2	Macro-BS to WFAP mobility	35
28	5.5.3	WFAP to WFAP mobility	35
29	5.6	Idle-Mode and Paging	36
30	5.6.1	Location Update at WFAP	36
31	5.6.1.1	Secure Location Update Failure	36
32	5.6.2	Paging	36
33	5.6.3	Idle-mode Exit in WFAP	36
34	5.6.4	Idle-mode Entry in WFAP	36
35	5.7	QoS Control	36
36	5.8	Radio Resource Management	37
37	5.9	Accounting	37
38	5.9.1	Accounting of the MS session	37
39	5.9.2	Accounting of the WFAP session	37
40	5.10	WFAP backhaul fault detection and mitigation	37
41	6.	MESSAGE AND PARAMETER DEFINITIONS	38
42	6.1	Constants and Counters	38
43	6.2	Message Definitions	38
44	6.3	AAA Exchanges between Se-GW, Femtocell GW and Femtocell AAA Server	38
45	6.3.1	RADIUS exchanges between Se-GW, Femtocell GW and Femtocell AAA Server	39
46	6.3.2	Diameter exchanges between Se-GW, Femtocell GW and Femtocell AAA Server	43
47	6.3.2.1	WiMAX® Femtocell Authentication-Authorization Request/Answer (WFAAR/A) command	44
48	6.3.2.2	WiMAX® Femtocell Re-Auth-Request/Re-Auth-Answer command	45
49	6.3.2.3	WiMAX® Femtocell Abort Session Request/ Answer command	47
50	6.3.2.4	WiMAX® Femtocell Session Termination Request/Answer command	48
51	6.3.2.5	WiMAX® Femtocell Accounting Request/Answer command	49
52	6.4	TLV Definitions	52
53	6.4.1	Backoff Timer	52
54	6.4.2	Failure Indication	52

Femto-Core

1 6.4.3 *Failure Cause* 52

2 6.4.4 *De-Registration Cause* 52

3 6.4.5 *Femto-GW ID* 53

4 6.4.6 *WFAP IP Address* 53

5 6.4.7 *WFAP ID* 53

6 6.5 *RADIUS Attributes* 54

7 6.5.1 *R6-ID* 54

8 6.6 *Diameter Attributes* 54

9 6.6.1 *R6-ID* 54

10 6.7 *DHCP Vendor Specific Option* 55

11 6.7.1 *Vendor-Identifying Vendor Class Option* 55

12 6.7.2 *Vendor-Identifying Vendor Specific Information Option* 56

13 7. *DATA PLANE* 57

14 7.1 *Secure Tunnel Management* 57

15 7.1.1 *IP-Sec Encapsulation* 57

16 7.2 *User Data Delivery over R6-F* 57

17

18

1 List of Figures

2	FIGURE 4-1 FEMTOCELL NETWORK REFERENCE MODEL	14
3	FIGURE 5-1: WFAP INITIALIZATION PROCEDURE	18
4	FIGURE 5-2: DISCOVERY OF BOOTSTRAP SERVER	20
5	FIGURE 5-3: FEMTO IKE AUTHENTICATION AND IPSEC TUNNEL SETUP CALL FLOW	25
6	FIGURE 5-4: WFAP REGISTRATION	28
7	FIGURE 5-5: WFAP TRIGGERED WFAP NETWORK EXIT	29
8	FIGURE 5-6: NETWORK TRIGGERED WFAP NETWORK EXIT (GRACEFUL)	30
9	FIGURE 5-7 FE-GW TRIGGERED WFAP NETWORK EXIT (UNGRACEFUL)	31
10	FIGURE 5-8: WFAP DE-REGISTRATION (WFAP INITIATED)	32
11	FIGURE 5-9: RANGING PROCEDURE OF CSG-CLOSED WFAP DURING MS NETWORK ENTRY	33
12	FIGURE 5-10: RANGING PROCEDURE OF CSG-CLOSED WFAP FOR EMERGENCY CALL DURING MS	
13	NETWORK ENTRY	34
14	FIGURE 7-1: DATA PLANE PROTOCOL STACK OVER R6-F	57
15		

1 **List of Tables**

2 TABLE 5-1: BOOTSTRAP MESSAGE ENCODING21

3 TABLE 6-1: WFAP_REGISTER_REQUEST38

4 TABLE 6-2: WFAP_DE-REGISTER_REQUEST38

5 TABLE 6-3: WFAP_DE-REGISTER_RESPONSE38

6 TABLE 6-4:WFAP_REGISTER_RESPONSE38

7 TABLE 6-5: RADIUS MESSAGES BETWEEN SE-GW AND FEMTOCELL AAA39

8 TABLE 6-6: RADIUS ACCOUNTING MESSAGES BETWEEN SE-GW AND FEMTOCELL AAA40

9 TABLE 6-7: RADIUS DISCONNECT MESSAGES BETWEEN SE-GW AND FEMTOCELL AAA41

10 TABLE 6-8: RADIUS CHANGE OF AUTHORIZATION MESSAGES BETWEEN SE-GW AND FEMTO-CELL

11 AAA.....42

12

1. Introduction and Scope

2 The WiMAX® Femtocell specification comprises three documents:

- 3 • Femtocell Core Specification, WMF-T33-118
- 4 • Femtocell Management Specification, WMF-T33-119
- 5 • Femtocell Self-Organizing Networks (SON), WMF-T33-120

6 This document, the Femtocell Core Specification, describes the architecture reference model, reference points, and
7 protocols and procedures for WiMAX® Femtocell Networks.

8 1.1 Document Scope

9 The scope of WiMAX® Femtocell specification in WiMAX Forum® Network Architecture Rel. 1.6 is limited to
10 *basic* femtocell features which can be provided with no changes in the underlying air reference point as specified in
11 [4] and the WiMAX system profile [28]. This specification includes the following support for Femto:

- 12 a) Femto system NRM and associated interface definitions
- 13 b) Femto E2E QoS
- 14 c) Femto active mode mobility aspects
 - 15 1) Hand in/out between Femto BS and macro BS
 - 16 2) Hand in/out between Femto BS and Femto BS
- 17 d) Femto idle mode mobility aspects and power saving
 - 18 1) Rove in/out between Femto BS and macro BS
 - 19 2) Rove in/out between Femto BS and Femto BS
- 20 e) Authentication, Authorization and Provisioning for WiMAX Femtocell Access Point (WFAP).
- 21 f) Emergency services
- 22 g) E2E security for Femtocell
- 23

2. Definitions and Conventions

2.1 Definitions

2.1.1 Broadband Connection

The Broadband Connection is a high throughput physical link, e.g., DSL, Cable Modem, Fiber, Ethernet, etc. supporting IP traffic between a customer premise and the network of an Internet Service Provider.

2.1.2 WiMAX® Femto Access Point

A WiMAX® Femto Access point (WFAP) is a low-power WiMAX Base Station, operating in licensed band, intended to:

- a) Be end user installed without service provider manual configuration (plug and play).
- b) Provide service for a limited number of concurrent users over small areas such as the home and SOHO (small office, home office) environment.
- c) Use a shared broadband connection for backhaul that may be operated by a different Service Provider.
- d) Support limited user mobility (low speed, infrequent need for handover).

In the case where one Service Provider operates both the broadband network and WFAP, additional features and control options may be enabled that leverage the additional network control when possible.

2.1.3 Exclusion Zone

Exclusion zone is an area around the WFAP where the service may not be available due to air interface limitations (i.e., exceeding maximum RF input threshold due to the ability of the end-user to use a MS very near the WFAP).

2.1.4 WiMAX® Femtocell

A WiMAX® Femtocell is a system comprising of a WFAP and other additional network functions that may be necessary to provide service through that WFAP. WFAP backhaul is not controlled by the WFAP, but may be cooperatively managed as in the case of participation in quality of service management. WiMAX Femtocell operation is managed by a WiMAX Network Access Provider (NAP). The backhaul service provider may be different from NAP.

Note: In the case where one Service Provider operates both the broadband network and WFAP, additional features and control options may be enabled that leverage the additional network controls.

Note: The term “femtocell” in this document implies WiMAX Femtocell, unless explicitly stated.

2.1.5 WiMAX® Macro-network

A WiMAX® Macro-network is the part of a WiMAX access network that does not include WiMAX Femtocells. The WiMAX Macro-network may interoperate with a WiMAX Femtocell-network.

2.1.6 Closed Subscriber Group (CSG)

A Closed Subscriber Group is a set of users authorized by the FemtoCell subscriber and/or WFAP service provider to have reserved/privileged access to WiMAX services through a particular WFAP.

2.1.7 Non-CSG Authorized User

A Non-CSG Authorized User is any user not included in the CSG who may, or may not be granted access to the WiMAX Femtocell based on operator and/or subscriber controlled configuration.

1 **2.1.8 FemtoCell Subscriber**

2 A FemtoCell Subscriber is the person, enterprise, or public entity that subscribes to the Femtocell service provided
3 to the WFAP, has physical control over the WFAP, and may be responsible for a portion of the management of the
4 Femtocell.

5 **2.1.9 Self-Organizing Networks**

6 Self-Organizing Networks (SON) is a process that involves Network Elements (NEs) in Radio Access Networks
7 (RAN) and Core networks to enable automatic configuration, to measure / analyze performance data, and to fine
8 tune network attributes in order to achieve optimal performance.

9 **2.1.10 CSG white list**

10 List of CSG WFAP IDs configured on the MS, that the MS is allowed to access.

11 **2.1.11 Femto Gateway**

12 An ASN Gateway for a Femto network which interfaces to a Femto Access Point and includes support for all femto
13 specific gateway functionality in addition to existing WiMAX ASN-GW functions.

14 **2.1.12 Security Gateway**

15 A network entity which provides an IPsec tunnel interface to the WFAP in order to secure intra-ASN
16 communication between the WFAP and other ASN entities.

17

18 **2.2 Conventions**

19 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
20 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below,
21 taken from IETF RFC 2119.

22 Note that the force of these words is modified by the requirement level of the document in which they are used.

- 23 • MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement
24 of the specification.
- 25 • MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of
26 the specification.
- 27 • SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in
28 particular circumstances to ignore a particular item, but the full implications must be understood and carefully
29 weighed before choosing a different course.
- 30 • SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons
31 in particular circumstances when the particular behavior is acceptable or even useful, but the full implications
32 should be understood and the case carefully weighed before implementing any behavior described with this
33 label.

3. References

- 1 [1] WMF-T32-001-R016, WiMAX Forum® Network Architecture - Architecture Tenets, Reference Model
2 and Reference Points – Base Specification
- 3 [2] WMF-T33-001-R016, WiMAX Forum® Network Architecture – Detailed Protocols and Procedures Base
4 Specification
- 5 [3] WMF-T31-123-R016, WiMAX Forum® Requirements for WiMAX® Femtocell Systems
- 6 [4] IEEE Std 802.16-2009, IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface
7 for Broadband Wireless Access Systems
- 8 [5] WMF-T31-123-R016, WiMAX Forum® Requirements for WiMAX® Femtocell Systems
- 9 [6] WMF-T33-110-R015, WiMAX Forum® Network Architecture – Protocols and Procedures for Location
10 Based Services
- 11 [7] WMF-T33-119-R016, WiMAX Forum® Network Architecture- Architecture, detailed Protocols and
12 Procedures, Femtocell Management Specification
- 13 [8] WMF-T33-120-R016, WiMAX Forum® Network Architecture – Architecture, detailed Protocols and
14 Procedures Self-Organizing Networks
- 15 [9] WMF-T33-117-R016, WiMAX Forum® Network Architecture- Architecture, detailed Protocols and
16 Procedures
- 17 [10] RFC 2401, available at <http://www.ietf.org/rfc/rfc2401.txt>
- 18 [11] RFC 2131, available at <http://www.ietf.org/rfc/rfc2131.txt>
- 19 [12] RFC 3315, available at <http://www.ietf.org/rfc/rfc3315.txt>
- 20 [13] RFC 3361, available at <http://www.ietf.org/rfc/rfc3361.txt>
- 21 [14] RFC 3646, available at <http://www.ietf.org/rfc/rfc3646.txt>
- 22 [15] RFC 2616, available at <http://www.ietf.org/rfc/rfc2616.txt>
- 23 [16] RFC 4306, available at <http://www.ietf.org/rfc/rfc4306.txt>
- 24 [17] RFC 2818, available at <http://www.ietf.org/rfc/rfc2818.txt>
- 25 [18] RFC 5280, available at <http://www.ietf.org/rfc/rfc5280.txt>
- 26 [19] RFC 2486, available at <http://www.ietf.org/rfc/rfc2486.txt>
- 27 [20] RFC 4282, available at <http://www.ietf.org/rfc/rfc4282.txt>
- 28 [21] RFC 2865, available at <http://www.ietf.org/rfc/rfc2865.txt>
- 29 [22] RFC 2866, available at <http://www.ietf.org/rfc/rfc2866.txt>
- 30 [23] RFC 3588, available at <http://www.ietf.org/rfc/rfc3588.txt>
- 31 [24] RFC 4005, available at <http://www.ietf.org/rfc/rfc4005.txt>
- 32 [25] RFC 2869, available at <http://www.ietf.org/rfc/rfc2869.txt>
- 33 [26] RFC 5176, available at <http://www.ietf.org/rfc/rfc5176.txt>
- 34 [27] RFC 3925, available at <http://www.ietf.org/rfc/rfc3925.txt>
- 35 [28] WMF-T23-001-R015, WiMAX Forum®, Mobile System Profile Specification
- 36
- 37

4. Network Reference Model

4.1 Overview

Figure 4-1 describes the overall WiMAX® Femtocell architecture.

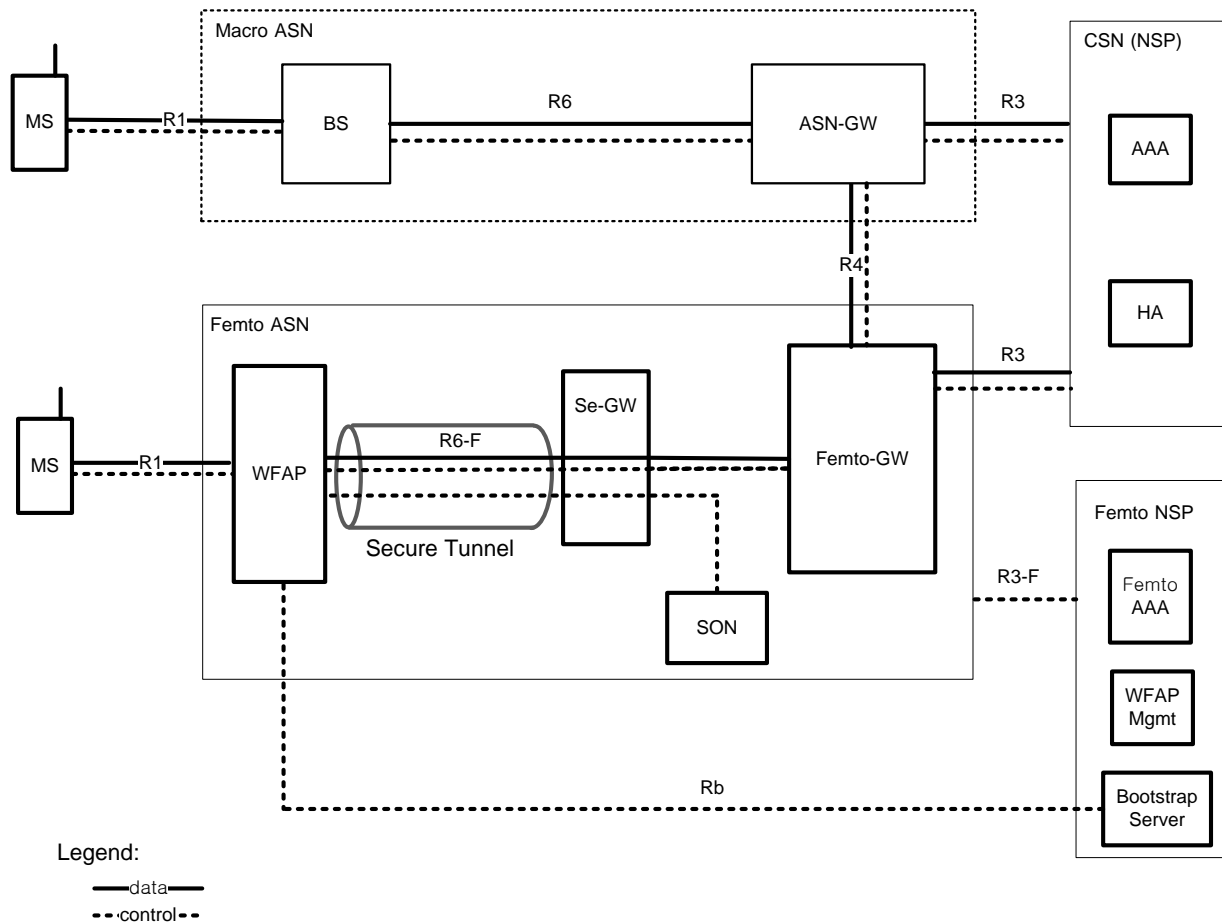
In addition to traditional business entities such as NAP and NSP, a new entity called the Femto NSP is introduced for Femtocell business. Femto NSP is responsible for the operation, authentication and management of the Femto Access Point (WFAP). The Femto-AAA in the Femto NSP performs the authentication and accounting of the WFAP. The NSP is the operator responsible for the MS user's subscription.

The WFAP resides at a user's home, SOHO or enterprise and is operated over the IP broadband connection. The WFAP is connected to Femto Gateway (Fe-GW) and other functional entities in the network through an IP Security (IPsec) tunnel provided by Security Gateway (Se-GW). The Se-GW is a mandatory functional entity which provides IPsec tunnels for WFAP and is responsible for authentication of the WFAP. The Fe-GW controls WFAP(s) and performs transmission of user data packets to CSN.

In addition to the femto features and traditional human involved network management functions, SON provides the ability to perform certain functions [8] automatically with minimum human/manual intervention, and it is expected to have dynamic and real time behavior. Those functions deals with the management functions related to the air interface aspects of the WFAP.

Note: With the exception of SON server discovery, SON functionality for WiMAX Femtocell operation is not in the scope of this document and is covered by [8].

1 **4.2 Reference Model**



2
3 **Figure 4-1 Femtocell Network Reference Model**

4 Note: Se-GW may be implemented as a separate physical box or integrated together with other functional entities in
 5 a single physical box, for example, with a Fe-GW.

6 **4.2.1 WiMAX® Femto Access Points (WFAP)**

7 The main features supported by the Femto Access Point are:

- 8 - Provide Access Connectivity to a user over R1RP
 9 - Access Control with Closed Subscriber Group (CSG) management
 10 - Support Closed Subscriber Group (CSG) configuration
 11 - Control of Radio Resources
 12 - Bootstrap Server, SON Server, WFAP Management System, Femto Gateway and Security Gateway
 13 Discovery
 14 - Support MS Mobility within the WFAP(s) or/and between a WFAP and Macro BS
 15 - Auto-Configuration

16 **4.2.2 Femto Gateway (Fe-GW)**

17 The main features supported by the Femto Gateway are:

Femto-Core

- 1 - Terminate R6-F starting from the WFAP
- 2 - Support all the existing functionalities of Release 1.5 ASN-GW

3 **4.2.3 Security Gateway (Se-GW)**

4 The main features supported by the Security Gateway are:

- 5 - Terminate IPsec Tunneling for Femtocell
- 6 - Filter out unauthorized traffic on the links between the Security Gateway and the WFAP
- 7 - Access Control of WFAP to the Network
- 8 - Inspection of data packets from WFAP over R6 to verify the correct source ID.
- 9 - Encryption of the data between WFAP and Se-GW (optional)
- 10 - Integrity protection
- 11 - NAT traversal

12 **4.2.4 SON**

13 The main features supported by the SON functions are:

- 14 - Support SON functions specified by [8]

15

16 **4.2.5 WFAP Management System**

17 The main features supported by the Femto Management System are:

- 18 - Support O&M features of the WFAP based on SNMP, TR069 or DOCSIS standards.

19 **4.2.6 Bootstrap server**

20 This server supports the initial bootstrap of the WFAP and the redirection of the WFAP to the right Se-GW in the
21 Femto ASN.

22 **4.2.7 Femto-AAA server**

23 The Femto-AAA server maintains the WFAP subscription information. It is involved in the authentication of the
24 WFAP.

25 **4.3 Reference Points**

26 The Reference Points shown in Figure 4-1 terminates at the Network Elements which support the WiMAX
27 Femtocell network.

28 **4.3.1 Reference Point R1**

29 Reference Point R1 consists of the protocols and procedures between MS, and WFAP and macro BS per the air
30 interface (PHY and MAC) specifications [4]. For this release of Femtocell specification, no femto specific
31 requirements are specified by [4].

32 **4.3.2 Reference Point R3**

33 The Reference Point R3 consists of the set of Control Plane protocols and Bearer Plane protocols to support AAA
34 and also to transfer of user data between the Femto ASN and the CSN. AAA is responsible for subscriber
35 authentication and charging.

1 **4.3.3 Reference Point R4**

2 The Reference Point R4 consists of the set of Control Plane protocols and Bearer Plane protocols
3 originating/terminating in various functions entities of an ASN that coordinates MS mobility between different
4 ASNs and Fe-GW as well as between Fe-GWs. The Fe-GW may also be connected to Macro ASN-GW through R4
5 if the interoperability with Macro network is required.

6 **4.3.4 Reference Point R6-F**

7 The Reference Point R6-F consists of the set of Control Plane and Bearer Plane for communication between the
8 WFAP and the Fe-GW. It is mainly defined for the purpose of supporting Femto specific features and the existing
9 features of R6. All control and bearer plane traffic over the Reference Point R6-F will be sent through an IPsec
10 tunnel between the WFAP and the Se-GW.

11 **4.3.4.1 R6-F control plane**

12 This SHALL be based on the R6 control plane in the baseline scenario [2], with the following differences as detailed
13 in this specification as well as in [7], [8].

14 R6-F control plane has 2 parts:

- 15 a) From WFAP to Se-GW: R6-F over secure tunnel: This SHALL use WiMAX header [2] over UDP over IP
16 over IPsec
- 17 b) From Se-GW to Fe-GW: R6-F: This SHALL use WiMAX header over UDP over IP

18 WiMAX® header format shall be the same as baseline scenario [2].

19 **4.3.4.2 R6-F bearer plane**

20 R6-F data plane has 2 parts:

- 21 a) From WFAP to Se-GW: R6-F over secure tunnel: This SHALL use GRE over IP over IPsec
- 22 b) From Se-GW to Fe-GW: R6-F: This SHALL use GRE over IP

23 The GRE tunnel format shall be the same as the baseline scenario [2].

24 **4.3.5 Reference Point R3-F**

25 The Reference Point R3-F consists of the set of Control Plane protocols based on the protocols for R3 in the macro
26 WiMAX network [2], to support the authorization, authentication and accounting of the WFAP between Femto ASN
27 and Femto NSP.

28 R3-F also consists of management plane protocols between the Management server and WFAP, and Management
29 system and SON server as defined in [7] and [8].

30 **4.3.6 Reference Point Rb**

31 The Reference Point Rb consists of the set of the initial bootstrapping protocol between WFAP and the bootstrap
32 server. This Reference Point is for control plane only. Rb SHALL use the Femto related WiMAX Initial Bootstrap
33 (Femto-WIB) protocol as specified in [9].

34

35

5. Control Plane Protocols and Procedures

This section specifies control plane protocols and procedures for WiMAX® Femtocell Networks.

5.1 WFAP Initialization and authentication

The pre-provisioned parameters on the WFAP are as follows:

- a) WFAP credential: An X.509 certificate which will be used with IKEv2 [16] for authenticating the WFAP to the Se-GW. There is no mandatory-to-implement certificate profile specification in this release. It is expected that the Se-GW can recognize the WFAP certificate profile and its root CA to perform validation. [Note: The certificate profile and the root CA(s) will be specified in the future version of this specification for retail WFAP support] The certificate identifier is used for uniquely identifying the WFAP in the Femto ASN. This identifier shall be compliant with [20] and it may include realm information.
- b) Public Keys for Root CAs: A root CA public key for validating the Se-GW's X.509 certificate, and another root CA public key for verifying the bootstrap server's X.509 certificate. The two public keys may be the same.
- c) FQDN of the bootstrap sever in the Femto NSP. This is optional.
- d) WFAP R6 identifier: If the R6 identifier is a MAC address, then it is pre-provisioned on the WFAP (hence this is an optional parameter). Absence of a pre-provisioned R6 identifier means the identifier is an IP address and it will be dynamically assigned by the Se-GW during IKEv2 procedure.

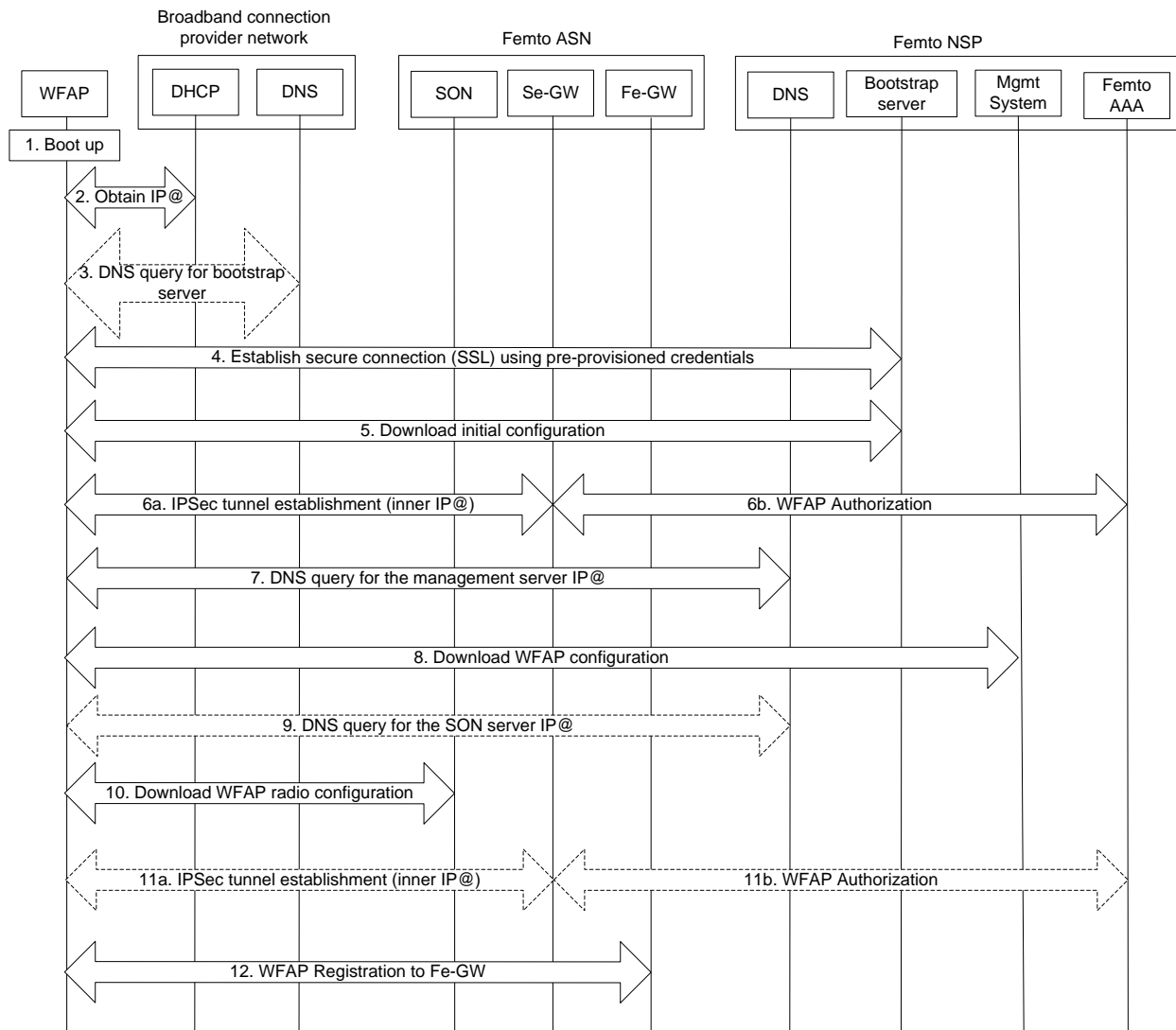
The WFAP SHALL discover the bootstrap server to download the initial configuration, and SHALL start the WFAP attachment procedure to associate with the Femto ASN.

If the FQDN of the bootstrap server is pre-provisioned at the WFAP, the bootstrap server IP address SHALL be discovered via DNS lookup. In the event that FQDN of the bootstrap server is not pre-provisioned at the WFAP, the bootstrap server IP address MAY be discovered via DHCP options.

5.1.1 WFAP Initialization

The procedure for the WFAP initialization is as shown in the figure below.

1



2

3

Figure 5-1: WFAP Initialization procedure

4

Step 1: The WFAP is booted up

5

Step 2: The WFAP obtains the (outer) IP address from the backhaul network (e.g.: DSL, Cable) via DHCP. If the WFAP does not have a pre-provisioned FQDN of the bootstrap server, the IP address of this bootstrap server MAY be provided as a DHCP option.

6

Step 3: If the WFAP is pre-provisioned with the FQDN of the bootstrap server, the WFAP does a DNS query for the IP address of the bootstrap server in the Femto NSP

7

Step 4: Once the IP address of the bootstrap server is determined by the WFAP in either step2 or step3, the WFAP establishes secure connection with the bootstrap server using HTTPS [17]. The WFAP does not provide its certificate to the server. Only the bootstrap server is authenticated.

8

Step 5: The WFAP connects to the bootstrap server and requests initial configuration information. The WFAP provides its IP address and may also provide other location information (e.g. GPS info) so that the appropriate Se-GW can be selected for the WFAP by the bootstrap server. The bootstrap server may contact the external Location Server for the location determination of the WFAP which is out of the scope of this specification. WFAP obtains the

9

10

11

12

13

14

15

16

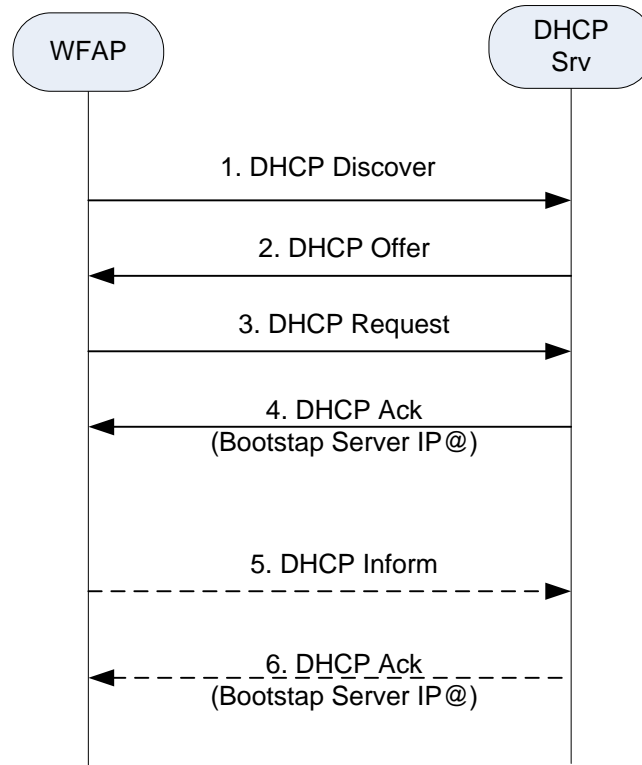
Femto-Core

- 1 IP address of Se-GW from the bootstrap server. In addition the WFAP also obtains the FQDN of the management
2 server.
- 3 Step 6: WFAP and Se-GW perform IKEv2 to authenticate each other, and establish an IPsec tunnel between the two.
4 The Se-GW communicates with the Femto-AAA via the Femto-GW for the authorization of the WFAP. How the
5 Se-GW selects a default Femto-GW for WFAP is out of scope of this specification. The inner IP address is also
6 assigned to WFAP by the Se-GW.
- 7 Step 7: WFAP does a DNS query to obtain the IP address of the management server from the FQDN obtained in
8 step 5.
- 9 Step 8: The WFAP connects to the management server. The WFAP sends its local information to the management
10 server such as the IP address of WFAP, HW S/N, S/W version, location information etc. Based on the provided
11 information by WFAP, the management server provides the higher layer configuration parameters to the WFAP.
12 Along with these parameters, either the FQDN or the IP address of the SON server is returned to the WFAP.
- 13 Step 9: If the FQDN of the SON server is obtained in Step 8, then a DNS query is executed to obtain the IP address
14 of the SON server. This is an optional step. This step is not executed if the IP address of the SON server is directly
15 returned in Step 8.
- 16 Step 10: The WFAP connects to SON server and the WFAP sends its local information to the SON server. The
17 location of the WFAP is authorized by the SON server as detailed in section 5.1.5. This is a regulatory requirement
18 and cannot be skipped. Based on the provided information by WFAP, the SON server provides the PHY/MAC
19 configuration parameters to the WFAP and authorizes the WFAP to turn on the radio transmission. Based on the
20 location information, the SON server also provides the ID of the preferred Fe-GW, R6-ID of the WFAP, and the ID
21 of Se-GW, which associates with the Fe-GW, to the WFAP.
- 22 Step 11: Optionally, if the Se-GW is not the same as the serving Se-GW selected by bootstrap server in Step 5, the
23 WFAP shall repeat Step 6 to release the existing IPsec tunnel with the serving Se-GW and to establish IPsec tunnel
24 with the new Se-GW
- 25 Step 12: After the WFAP finishes the Initial configuration which is defined in [8]. WFAP registers with the Fe-GW.

26 **5.1.2 Discovery of Bootstrap Server by WFAP using DHCP**

27 Figure 5-2 describes DHCP procedure to retrieve IP address of the WFAP and to obtain IP address or the FQDN of
28 Bootstrap server by DHCP option. This corresponds to step-2 of Figure 5-1.

29



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Figure 5-2: Discovery of Bootstrap server

Steps 1-4: The WFAP retrieves its IP address as defined in RFC 2131 [11] for IPv4 or RFC 3315 [12] for IPv6 and Domain Name as defined in RFC 3361 [13] for IPv4 and in RFC 3646 [14] for IPv6. The WFAP may indicate DHCP server with V-I Vendor Class option [27] that it wants the address of Bootstrap server in the DHCP Discover message or Request message. According to the indication, DHCP server may optionally include the address of Bootstrap server in the DHCP ACK with V-I Vendor-specific information option [27].

Note: The Step 5-6 are not required if WFAP implement DHCP with V-I Vendor Class option in step 1-4.

Step 5: The WFAP sends a DHCP Inform message with V-I Vendor Class option to the DHCP server in order to receive Bootstrap server address.

Step 6: The DHCP server returns the address of the Bootstrap server in the DHCP ACK with V-I Vendor-specific information option.

5.1.3 WFAP Bootstrapping over Rb

The WFAP SHALL use Femto-WIB for bootstrapping over Rb based on WIB defined in [9]. The WFAP shall include a Femto-WIB client that will use this defined protocol to obtain the initial configuration from the bootstrap server. This corresponds to step-5 of Figure 5-1.

The Femto-WIB client shall perform the required protocol steps based on the pre-provisioned information. In particular, if the WFAP is preprovisioned with the bootstrap server IP address it will perform only the HTTPS exchange to obtain the IP address of the Se-GW and the FQDN of the management server.

5.1.3.1 Femto-WIB Protocol Requirements

1. The WFAP SHALL open a HTTPS (HTTP/TLS) session, according to RFC2618 [17] to the Bootstrap server. Only the bootstrap server certificate is presented during the authentication, no WFAP certificate is used. In other words the WFAP authenticates the Bootstrap server. This session will be used by the WFAP to inform the

Femto-Core

- 1 Bootstrap server of its IP address and location information and retrieve the Se-GW IP address and the FQDN of
2 the management server.
- 3 2. The WFAP SHALL use the HTTP GET method with the Request-URI
4 “/femto.bootstrap.wib?version=VERSION&ip_address=IP_ADDRESS&location=LOCATION”.
- 5 3. The WFAP SHALL provide the IP address in the URI and SHALL indicate the Femto-WIB HTTP protocol
6 version in the URI using the “version” parameter.
- 7 4. The WFAP MAY provide its location
- 8 For example, when assuming the following parameters;
- 9 VERSION = 0
- 10 IP = 10.1.3.5
- 11 LOCATION = XXXX
- 12 Femto-WIB Server Domain = wibserver.foo.com
- 13 The URI will be “http://wibserver.foo.com/femto.bootstrap.wib?version=0&ip=10.1.3.5&location=XXXX”
- 14 5. The WFAP SHALL provide an Accept Header [15] containing the media type defined for the femto bootstrap
15 (application/vnd.wmf.femto_bootstrap).
- 16 6. Bootstrap server SHALL respond to the WFAP with one of the following HTTP responses:
- 17 a. 200 OK. If the Bootstrap server can provide the bootstrap information for the WFAP identified with
18 the IP address, the Bootstrap server SHALL reply with an HTTP 200 OK message containing the
19 initial configuration information in the response body encoded as specified in section 5.1.3.2. The
20 Content-Type of the reply SHALL be “application/vnd.wmf.femto_bootstrap”.
- 21 b. 302 Found. If the Bootstrap server does not support bootstrap information delivery but can redirect the
22 WFAP to another server that can provide the bootstrap information, the Bootstrap server SHALL reply
23 with an HTTP 302 Found message containing the URI to the location of the bootstrap information.
24 Upon receiving the redirect the WFAP SHALL open an HTTP session to the indicated URL and
25 SHALL use the HTTP GET method with the new server. The Bootstrap server SHALL only redirect to
26 the new servers that support the Femto-WIB HTTP query with the parameters and responses specified
27 in this chapter.
- 28 c. 400 Bad Request. If the Bootstrap server does not understand the request due to malformed syntax,
29 corrupted packet, decode error, unsupported Femto-WIB protocol revision, etc., it SHALL reply with
30 an 400 Bad Request message which indicates the failure of the OTA provisioning procedure.
- 31 d. 404 Not Found. If the server cannot provide the bootstrap information or redirect the WFAP to another
32 server, it SHALL reply with an HTTP 404 Not Found message which indicates the failure of the Femto
33 provisioning procedure.

34 **5.1.3.2 Bootstrap message encoding**

35 The bootstrap information SHALL be provided to the WFAP using the format defined for the bootstrap, i.e.,
36 application/vnd.wmf.bootstrap. The bootstrap information consists of a fixed size header followed by a variable size
37 data as described below.

38 **Table 5-1: Bootstrap Message Encoding**

Field	Version	IP Address version	IP Address	FQDN length	FQDN value
Number of Octets	2	1	4 for IPv4 16 for IPv6	1	Variable (0 – 255)

Octet Significance	MSB	LSB	MSB	LSB	MSB	LSB	MSB	LSB	MSB	LSB
Value	0		0 - for IPv4		The IP address of the Se-GW		Length as number of octets of the FQDN of the management sever		FQDN of the management sever	
	1 – 65535 = Reserved		1 – for IPv6							
			2-255= reserved							

1

2 5.1.4 WFAP-Se-GW Authentication and IPsec Tunnel Management

3 This section describes the Authentication, Authorization, and Accounting procedures, and IPsec tunnel management
4 procedures between WFAP and Se-GW.

5 5.1.4.1 Authentication and Tunnel Setup

6 IKEv2 is used for mutual authentication, establishment of security association, and setup of IPsec tunnel between
7 the WFAP and the Se-GW. The X.509 certificates possessed by WFAP and the Se-GW are utilized as the
8 credentials. Even though the Se-GW can authenticate the WFAP without any 3rd party help, it still needs to
9 communicate with the Femto-AAA server for the authorization and accounting of the WFAP.

10 5.1.4.1.1 WFAP R6 Identifier

11 The WFAP's R6 identifier is either a MAC address or an IP address. This specification does not describe where the
12 value comes from when R6 identifier is a MAC address (e.g. from a LAN or WAN interface, BSID, or X.509
13 certificate identifier, etc.). R6 identifier does not have to be same value as the WFAP X.509 certificate identifier
14 even when both are MAC addresses. The Femto GW needs to learn that value as the termination point of R6 for all
15 WFAPs that are authorized to join the Femto ASN. The Se-GW also needs to learn that value for performing
16 integrity checks on the R6 control packets. The Se-GW may perform a deep packet inspection of all R6 control
17 messages passing through it towards Femto GW in order to ensure that each WFAP is using its assigned R6
18 identifier.

19 When the R6 identifier is a MAC address, its value is preconfigured on both the WFAP and the Femto-AAA server.
20 The value is sent to the Femto GW and the Se-GW from Femto-AAA server as part of the authorization procedure.

21 When the R6 identifier is an IP address, its value is dynamically assigned by the Se-GW to the WFAP as the IPsec
22 tunnel inner IP address. The value is sent to the Femto GW from Se-GW as part of the accounting procedure.

23 5.1.4.1.2 WFAP Requirements

24 WFAP shall use certificate-based mutual authentication with IKEv2.

25 The WFAP shall be provisioned with an X.509 certificate that is compliant to [18]. This certificate may be installed
26 on the WFAP during the manufacturing or at a later time. There is no mandatory-to-implement certificate profile in
27 this release of the specification. Until such a profile is defined in a future release, the choice of X.509 certificate
28 profile is left to the Femto ASN provider.

29 The WFAP certificate shall be identified by a value that is supplied in IKEv2 identification payload (IDi field). This
30 identifier shall be known to the Femto-AAA server for authorization and accounting purposes. The Se-GW shall
31 send this identifier to the Femto-AAA in the username attribute of AAA messages. Therefore, the identifier format
32 shall be compliant with the NAI format [20].

33 Additionally, the WFAP shall be provisioned with one or more root CA public keys for validating the X.509
34 certificate of the Se-GWs. Which root CA public key(s) to use is not specified in this release of the specification and
35 it is left to the Femto ASN provider to decide.

36 WFAP shall use IKEv2 for setting up IPsec security associations and tunnels with the Se-GW. The WFAP shall
37 support NAT traversal per IKEv2 and UDP encapsulation of IPsec ESP in tunnel mode [19]. It shall also support
38 both IPv4 and IPv6 for inner IP address. Upon completion of IKEv2 procedure, WFAP shall establish an IPsec ESP
39 tunnel between itself and the Se-GW.

40 If the WFAP is not pre-provisioned with its R6 identifier, then it shall use the IPsec tunnel inner IP address assigned
41 by the Se-GW as its R6 identifier.

1 **5.1.4.1.3 Se-GW Requirements**

2 Se-GW shall use certificate-based mutual authentication with IKEv2.

3 The Se-GW shall be compliant with RADIUS protocols as defined by [21][22][25][26]. The Se-GW may support
4 Diameter protocol as defined by [23].

5 In the case of supporting Diameter, the Se-GW shall advertise support for the WiMAX Femtocell Diameter
6 Application id and WiMAX Femtocell Accounting Diameter Application during Diameter capability exchange as
7 defined by in [23]. The Se-GW shall include the Vendor-Specific-Application-Id in the Capability-Exchange
8 Request (CER) command. The Vendor-Id attribute shall be set to the WiMAX Forums private enterprise number
9 (24757) assigned by IANA, the Auth-Application-Id attribute shall be set to TBDWFDA assigned by IANA, and the
10 Acct-Application-Id shall be set to TBDWFADA assigned by IANA. The Se-GW shall comply with the commands
11 defined by this specification for the WiMAX Femtocell Application. These commands are derived from the
12 Diameter Network Access Server Application specified by [24].

13 The Se-GW shall be provisioned with an X.509 certificate that is compliant to [19]. This certificate may be installed
14 on the Se-GW during the manufacturing or at a later time. There is no mandatory-to-implement certificate profile in
15 this release of the specification. Until such a profile is defined in a future release, the choice of X.509 certificate
16 profile is left to the Femto ASN provider.

17 Additionally, the Se-GW shall be provisioned with one or more root CA public keys for validating the X.509
18 certificate of the WFAPs. Which root CA public key(s) to use is not specified in this release of the specification and
19 it is left to the Femto ASN provider to decide.

20 Upon successfully verifying the WFAP certificate, the Se-GW shall send a RADIUS Access-Request or Diameter
21 WFAAR message to the Femto-AAA server. The AAA message shall include the WFAP identifier (which was
22 received in the IDi payload of IKEv2) in the username attribute. If the Se-GW receives a RADIUS Access-Accept
23 or Diameter WFAAA indicating successful operation, then Se-GW shall complete IKEv2 authentication
24 successfully; otherwise the Se-GW shall send a rejection with notify payload containing
25 AUTHENTICATION_FAILED status type.

26 Se-GW shall use IKEv2 for setting up IPsec security associations and tunnels with the WFAPs. The Se-GW shall
27 support NAT traversal per IKEv2 and UDP encapsulation of IPsec ESP in tunnel mode [19]. It shall also support
28 both IPv4 and IPv6 for inner IP address. Upon completion of IKEv2 procedure, Se-GW shall establish an IPsec ESP
29 tunnel between itself and the WFAP.

30 Upon successfully completing the IKEv2 procedure, the Se-GW SHALL send a RADIUS Accounting-Request Start
31 or Diameter WFACR message to the Femto-AAA server on behalf of the WFAP.

32 When the tunnel for the Se-GW and the WFAP terminates, the Se-GW SHALL send a RADIUS Accounting-
33 Request Stop or Diameter WFSTR and WFACR messages to the Femto-AAA Server on behalf of the WFAP.

34 All AAA messages shall be routed by the Se-GW through the Femto GW. This Se-GW shall select a default Femto-
35 GW for the WFAP during the authentication of WFAP.

36 If the Se-GW receives R6-ID attribute in AAA message that authorized the WFAP to join the Femto ASN, then the
37 Se-GW shall store the attribute value as the R6 identifier of the WFAP. If that attribute is absent, then the Se-GW
38 shall store the IPsec tunnel inner IP address as the R6 identifier value.

39 Se-GW should perform deep packet inspection (DPI) on all R6 control messages passing through it towards Femto
40 GW in order to ensure WFAPs are using their assigned R6 identifiers. Upon receiving a R6 control message from a
41 WFAP, the Se-GW performing DPI shall drop the message and should log the event if the Source Identifier TLV in
42 the R6 header carries a value different than the R6 identifier of the WFAP known to the Se-GW.

43 **5.1.4.1.4 Femtocell GW Requirements**

44 The Femtocell GW acts as a AAA proxy between the Se-GW and the Femtocell AAA Server. The Femtocell GW
45 shall be compliant with RADIUS protocols as defined by [21][22][25][26]. The Femtocell GW may optionally
46 support Diameter protocol as defined by [23].

47 If Diameter is supported, the Femtocell GW shall advertise support for the WiMAX Femtocell Diameter Application
48 identifier and the WiMAX Femtocell Accounting Diameter Application during Diameter capability exchange as

Femto-Core

1 defined by in [23]. The Femtocell GW shall include the Vendor-Specific-Application-Id in the Capability-Exchange
2 Request (CER) command. The Vendor-Id attribute shall be set to the WiMAX Forums private enterprise number
3 (24757) assigned by IANA, the Auth-Application-Id attribute shall be set to TBDWFDA assigned by IANA, and the
4 Acct-Application-Id shall be set to TBDWFADA assigned by IANA. The Femtocell GW shall comply with the
5 commands defined by this specification for the WiMAX Femtocell Application. These commands are derive from
6 the Diameter Network Access Server Application specified by [24].

7 Femtocell GW shall learn the R6 identifier of a WFAP from R6-ID attribute of the AAA message that authorized the
8 WFAP to join the Femto ASN, when that attribute is present. In case the attribute is absent, then the Femtocell GW
9 shall learn the value from the accounting start message. It is an IPv4 address carried in the Framed-IP-Address
10 attribute if present, or the IPv6 address generated from the Framed-Interface-Id and Framed-IPv6-Prefix attributes
11 otherwise.

12 **5.1.4.1.5 Femto-AAA Server Requirements**

13 Femto-AAA server is in charge of authorization and accounting of the WFAPs. It shall manage a list of authorized
14 WFAP identifiers, and perform authorization procedure in response to the Se-GW requests. Provisioning of Femto-
15 AAA servers with WFAP identifiers is outside the scope of this specification.

16 The Femto-AAA server shall be compliant with RADIUS protocols as defined by [21][22][25][26]. The Femto-
17 AAA server may optionally support Diameter protocol as defined by [23].

18 In the case of supporting Diameter, the Femto-AAA server shall advertise support for the WiMAX Femtocell
19 Diameter Application identifier and WiMAX Femtocell Accounting Diameter Application id during Diameter
20 capability exchange as defined by in [23]. The Femto-AAA server shall include the Vendor-Specific-Application-Id
21 in the Capability-Exchange Request (CER) command. The Vendor-Id attribute shall be set to the WiMAX Forums
22 private enterprise number (24757) assigned by IANA, the Auth-Application-Id attribute shall be set to TBDWFDA
23 assigned by IANA, and the Acct-Application-Id shall be set to TBDWFADA assigned by IANA. The Femto-AAA
24 server shall comply with the commands defined by this specification for the WiMAX Femtocell Application. These
25 commands are derived from the Diameter Network Access Server Application specified by [24].

26 When the Femto-AAA server receives a RADIUS Access-Request or Diameter WFAAR, it shall check to see if the
27 WFAP whose identifier is supplied in the username attribute is authorized to connect to the Se-GW. If WFAP is
28 authorized, then the Femto-AAA server shall send a RADIUS Access-Accept or Diameter WFAAA indicating
29 success; otherwise it shall send a RADIUS Access-Reject or Diameter WFAAR indicating failure to authorize to
30 the Se-GW.

31 If the R6 identifier of WFAP is a pre-provisioned value, then Femto-AAA server shall include an R6-ID attribute
32 with that value in the RADIUS Access-Accept or Diameter WFAAA indicating success.

33 Upon receiving a RADIUS Accounting-Request Start or Diameter WFACR from the Se-GW, the Femto-AAA
34 server shall respond with a RADIUS Accounting-Response or Diameter WFACA.

35 Upon receiving a Diameter WFSTR message indicating that the Se-GW has terminated the tunnel then the Se-GW
36 shall respond back with a Diameter WFSTA message and release the Diameter session.

37 **5.1.4.1.6 Call Flow**

38 Figure 5-3. depicts the call flow for IKEv2 authentication and IPsec tunnel establishment between the WFAP and
39 the Se-GW.

40

Femto-Core

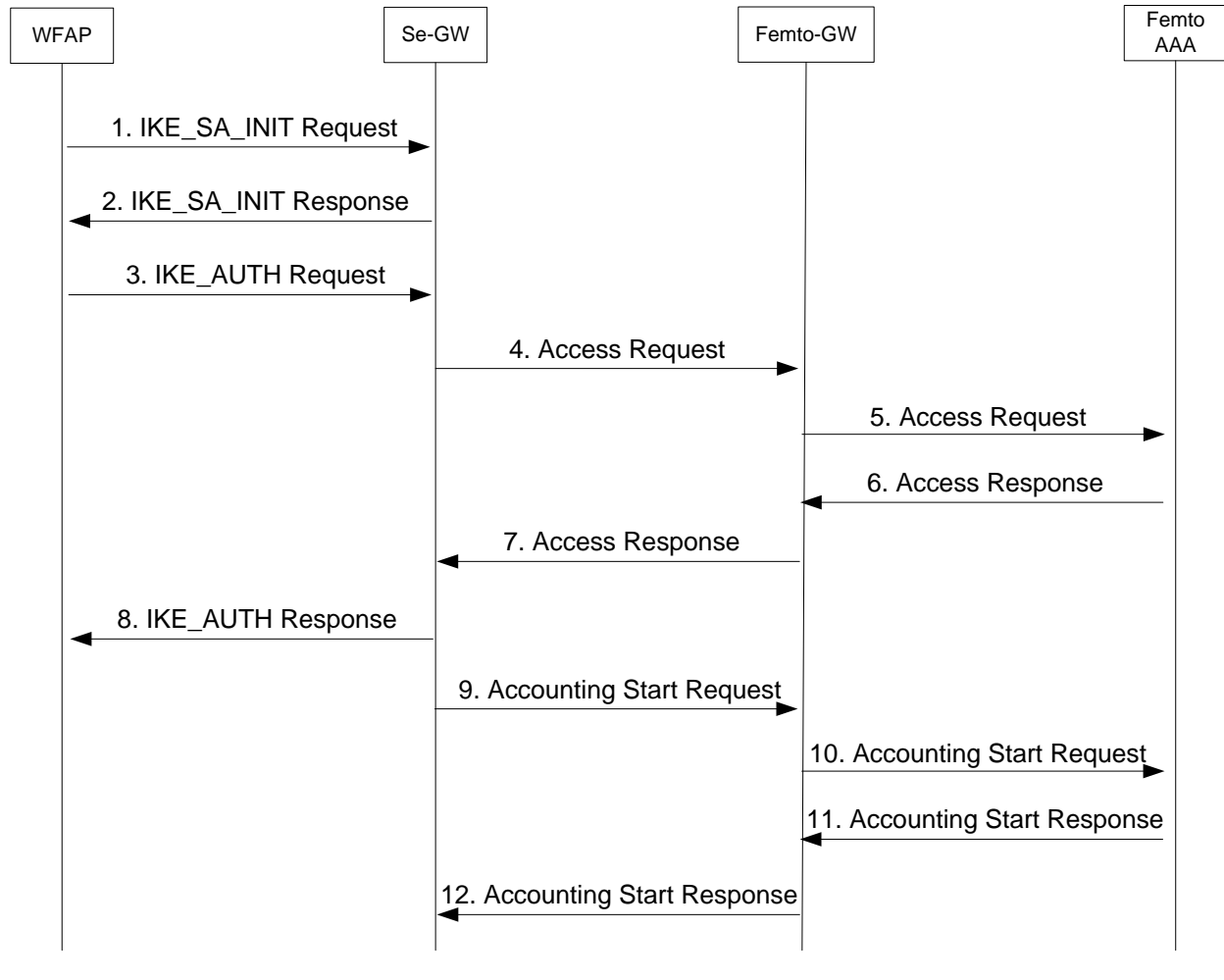


Figure 5-3: Femto IKE authentication and IPsec tunnel setup call flow.

Note that in the following call flow descriptions, only the payloads that have significance to this specification are mentioned. Other standard payloads that are already described in [16] are omitted.

1. The WFAP initiates the IKEv2 procedure by sending a IKE_SA_INIT request to the Se-GW. In addition to the mandatory payloads defined in [16], the WFAP also includes NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP payloads in order to negotiate support for UDP encapsulation.

2. The Se-GW responds with a IKE_SA_INIT response. This message completes the IKE_SA_INIT exchange.

3. The WFAP initiates the IKE_AUTH exchange by sending a IKE_AUTH request. The IDi payload carries the WFAP identifier, CERT payload carries the matching WFAP certificate.

When the Se-GW receives the IKE_AUTH request, it verifies that the CERT payload is not modified and the identifier included in the IDi matches the identifier in the WFAP certificate. If the verification is successful, then the Se-GW verifies the AUTH payload using the WFAP certificate. If this verification succeeds, then the authentication is successful. Otherwise, the Se-GW sends IKEv2 notification message to the WFAP indicating authentication failure.

4. Se-GW sends a RADIUS Access-Request or Diameter WFAAR message to the Femtocell AAA server via the Femtocell GW for the authorization of the WFAP. The username attribute includes the WFAP identifier as received in IDi payload.

Femto-Core

- 1 5. Femtocell GW sends the received RADIUS Access-Request or Diameter WFAAR message to the Femtocell
- 2 AAA.
- 3 6. Femtocell AAA server performs authorization and sends the result back to the Femtocell GW.
- 4 7. If the indicated result is success and the AAA message includes R6-ID attribute, then the Femto GW learns the
- 5 WFAP's R6 identifier from that attribute. Femto GW sends the result to the Se-GW.
- 6 8. If the Se-GW received a RADIUS Access-Reject or Diameter WFAAA with failure indication, then it sends an
- 7 IKEv2 Notification message to the WFAP indicating failure. Otherwise, the Se-GW sends an IKE_AUTH response
- 8 to the WFAP. The IDr payload contains Se-GW identifier, and the CERT payload carries the matching Se-GW
- 9 certificate.
- 10 When the WFAP receives the IKE_AUTH response, it verifies that the CERT payload is not modified and the
- 11 identifier included in the IDr matches the identifier in the Se-GW certificate. If the verification is successful, then
- 12 the WFAP verifies the AUTH payload using the Se-GW certificate. If this verification succeeds, then the
- 13 authentication is successful. This completes the IKE_AUTH exchange and an IPsec SA is established between the
- 14 WFAP and the Se-GW.
- 15 9. Upon successful completion of IKEv2 authentication, the Se-GW sends a RADIUS Accounting-Request Start or
- 16 Diameter WFACR message to the Femtocell AAA server via the Femtocell GW.
- 17 10. If the R6 identifier was not already received from the Femto-AAA at step 7, then the Femto GW learns that
- 18 identifier from the incoming accounting message. R6 identifier is set to the IPv4 address stored in Framed-IP-
- 19 Address attribute if present, and to the IPv6 address generated from the Framed-Interface-Id and Framed-IPv6-
- 20 Prefix attributes otherwise.
- 21 11. Femtocell AAA server responds to the Femtocell GW with a RADIUS Accounting-Response or Diameter
- 22 WFACA message.
- 23 12. Femto GW sends the AAA response to the Se-GW.

24 5.1.4.2 Tunnel Tear Down

25 The IPsec tunnel between the WFAP and the Se-GW is torn down either by the WFAP or the Se-GW based on IKE

26 SA lifetime timeout or by the Se-GW based on a request received from the Femto-AAA server

27 5.1.4.2.1 WFAP Requirements

28 The WFAP shall use the procedures defined in IKEv2 [16] to tear down IPsec tunnels.

29 5.1.4.2.2 Se-GW Requirements

30 The Se-GW shall use the procedures defined in IKEv2 [16] to tear down IPsec tunnels.

31 When the Se-GW receives a RADIUS Disconnect-Request or Diameter WFASR from the Femto-AAA server via

32 the Femtocell GW, it shall first check if the target WFAP has any active security associations. If they exist, the Se-

33 GW shall perform tunnel tear down by sending IKEv2 Informational request message with Protocol ID set to 1 in

34 the Delete payload to the WFAP and send a RADIUS Disconnect-Ack or Diameter WFASA message indicating

35 success to the Femtocell AAA server via the Femtocell GW. If there is no active security association, then the Se-

36 GW shall respond to the Femto-AAA server via the Femtocell GW with a RADIUS Disconnect-Nak or Diameter

37 WFASA message indicating failure.

38 Upon successfully tearing down the IPsec tunnel in either case, the Se-GW shall send a RADIUS Accounting-

39 Request Stop or Diameter WFACR and Diameter WFSTR message to the Femto-AAA server via the Femtocell

40 GW.

41 5.1.4.2.3 Femto-AAA Requirements

42 When the Femto-AAA server desires to disconnect a WFAP from the Femto ASN, it shall send a RADIUS

43 Disconnect-Request or Diameter WFASR to the associated Se-GW via the Femtocell GW.

Femto-Core

1 Upon receiving a RADIUS Accounting-Request Stop or Diameter WFACR and Diameter WFSTR from the Se-GW,
2 the Femto-AAA server shall reply to the Se-GW via the Femtocell GW with a RADIUS Accounting-Response or
3 Diameter WFACA and Diameter WFSTA message.

4 **5.1.5 WFAP Location authorization**

5 This is performed as part of step-10 in Figure 5-1. WFAP needs to get its location authorized before it can start
6 transmitting on the licensed spectrum. This is a mandatory regulatory requirement. However, reception of WiMAX
7 radio signal may happen prior to the location authorization.

8 In order to do this, the WFAP provides the following info to the SON server.

9 a) Mandatory info:

10 a. WFAP public IP address.

11 b) Optional info:

12 a. GPS info

13 b. Neighbor WiMAX (Macro and Femto) BS info

14 c. Wi-Fi/3G/2G cell info

15 *WFAP Public IP address:* The SON server can use the public IP address and contact the backhaul service provider
16 (e.g. cable, DSL) for the civic location (e.g. street name or locality) of the user.

17 *GPS info:* If GPS is present on the WFAP and coverage is available, the WFAP can provide the GPS location or the
18 GPS pseudo-ranges [6] to the SON server. GPS however does not work indoors and WFAPs may often be deployed
19 indoors and can't provide such GPS information. The SON server can accurately pin point the location to the order
20 of 10s of meters if the GPS capability is available. The SON server may talk to the location server (LS) [6] in order
21 to obtain the WFAP location.

22 *Neighbor WiMAX (Macro and Femto) BS info:* Obtained by WFAP scanning procedure e.g.: BSID, RSSI and
23 relative delay of 2 nearby BSs. If the BSID of a neighbor WFAP is provided by the current WFAP, the SON server
24 can use this as the approximate location of the current WFAP. The SON server talks to the WiMAX Location server
25 to determine the location of the WFAP if the WFAP provides the neighboring WiMAX macro BS info such as
26 BSID, RSSI and relative delay.

27 *Wi-Fi/3G/2G cell info:* The WFAP may provide the cellular (2G/3G) cell ids or a Wi-Fi® AP MAC addresses, if
28 such air interfaces are supported on the WFAP and the corresponding coverage is available. The SON server may
29 need to talk to the location servers of these technologies in order to obtain the location of the WFAP.

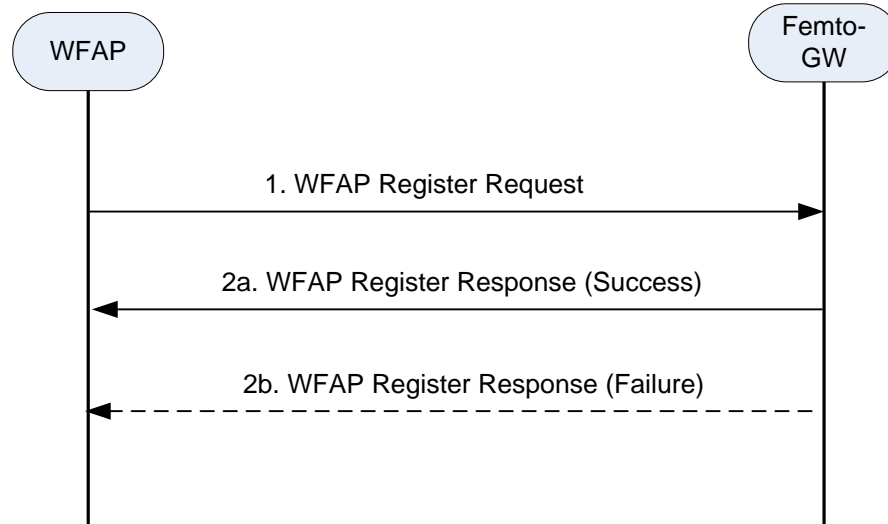
30 *Manual intervention:* If all of the above fails and location cannot be authorized using the WFAP provided info,
31 manual intervention may be triggered by the SON server to the operations center. The Femto cell subscriber will be
32 asked to provide and verify his current civic location (e.g. zip code/street address, etc) via a web interface or phone
33 call.

34 *Dynamic Movement of WFAP:* In this specification, a WFAP is expected to be a stationary and static node,
35 maintaining a connection to the Se-GW and Femto-GW in order to provide service to connected mobiles. Movement
36 of a WFAP or a dynamic change of its location, or an operating WFAP within a continuously moving environment
37 such as within a vehicle, is not anticipated and not addressed. Operating a WFAP in this fashion is not supported in
38 this specification and will have many repercussions on the femto and the overlaid macro networks.

39 **5.1.6 WFAP Registration to Fe-GW**

40 This corresponds to step-11 of Figure 5-1. The WFAP shall initiate this procedure across R6-F by sending WFAP
41 Register Request message whenever it needs to require femtocell service from Fe-GW. The purpose of this
42 registration is for WFAP to inform the Fe-GW that a WFAP is now available at a particular IP address. Figure 5-4
43 describes WFAP Registration procedure.

44



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Figure 5-4: WFAP Registration

Step-1: The WFAP registers with the serving Fe-GW via a WFAP Register Request message.

Step 2a: If the Fe-GW accepts the registration attempt it shall respond with a WFAP Register Response (Success) message.

Step 2b: Alternatively, the Fe-GW may reject the registration request. In this case, the Fe-GW shall respond with a WFAP Register Response (Failure). In this case, the WFAP may request SON server to re-select another FeGW as defined in [8] and shall not retry registration to the same Fe-GW for at least the duration indicated in the Backoff Timer TLV.

5.2 WFAP Network Exit

The WFAP network exit procedure may be triggered either by the WFAP or the other network entities (Fe-GW or the Femto-AAA) in the WiMAX Femtocell. The Fe-GW may trigger the network exit because of the loss of the backhaul keepalive exchange with the WFAP or for other reasons. The Femto-AAA may trigger a WFAP network exit procedure due to the expiry of the WFAP subscription.

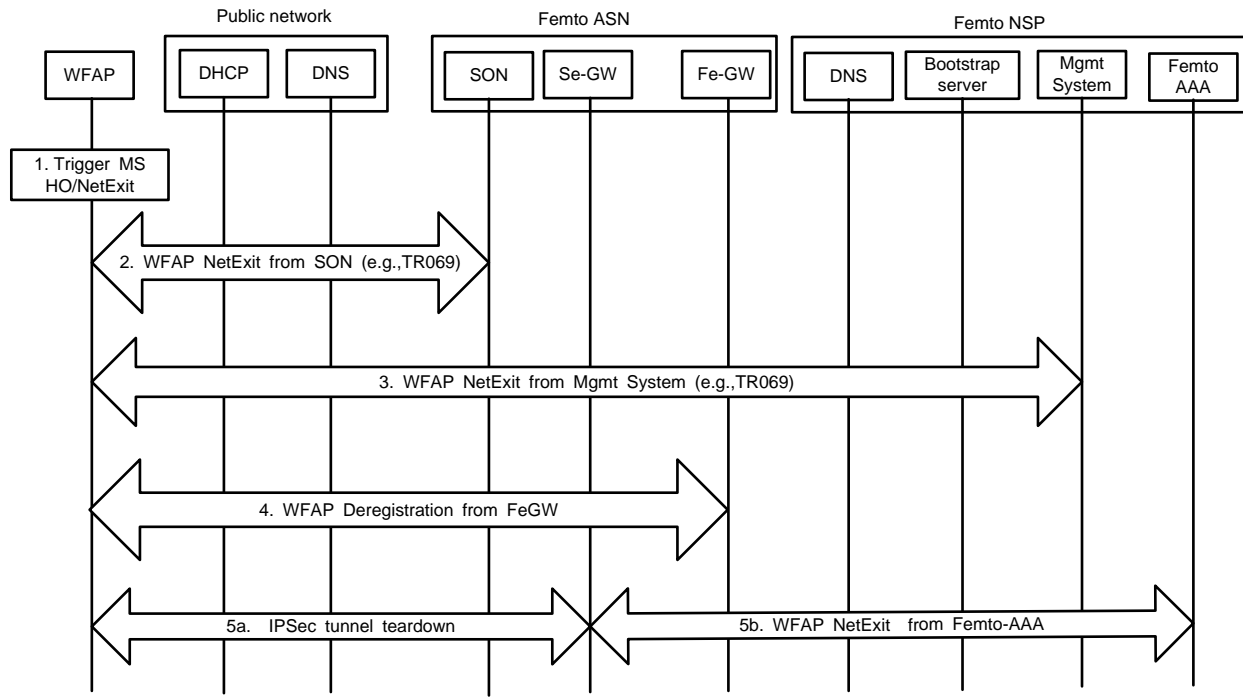
During the WFAP network exit, the corresponding network entities (e.g., Se-GW, Femto-GW, SON Server, WFAP Mgmt System, and Femto-AAA) shall release the associated resources (e.g. WFAP context, etc.) that are dedicated for the given WFAP.

5.2.1 WFAP triggered WFAP network exit

This is the basic scenario of WFAP network exit. Prior to the WFAP network exit, WFAP may first trigger its attached MS(s), if any, to handover to the neighbor BS(s) (Macro BS or WFAP), if feasible, or to proceed with MS network exit procedure. Which of the two procedures for MS (Handover or MS Network Exit) the WFAP should trigger before WFAP Network Exit depends on the network policy decision which out of scope of this specification.

The procedure described above is shown in Figure 5-5.

Femto-Core



1
2
3
4
5
6
7
8
9
10
11
12
13
14

Figure 5-5: WFAP triggered WFAP network exit

Step-1: WFAP triggers WFAP network exit, prior to which it initiates handover or network exit for its attached MS(s) based on network policy.

Step-2: WFAP performs network exit from the SON server as specified in [8].

Step-3: WFAP performs network exit from the WFAP management server as specified in [7].

Step-4: WFAP performs deregistration from the Fe-GW as detailed in section 5.2.4.1.

Step-5a: WFAP tears down IPSec tunnel with the Se-GW.

Step-5b: Se-GW performs WFAP network exit from Femto-AAA on behalf of the WFAP.

5.2.2 Network triggered WFAP exit (Graceful)

This scenario of graceful WFAP network exit occurs when WFAP still has backhaul connectivity with the Femto ASN, and can be triggered by either the Fe-GW or Femto-AAA.

The procedure is shown in **Error! Reference source not found..**

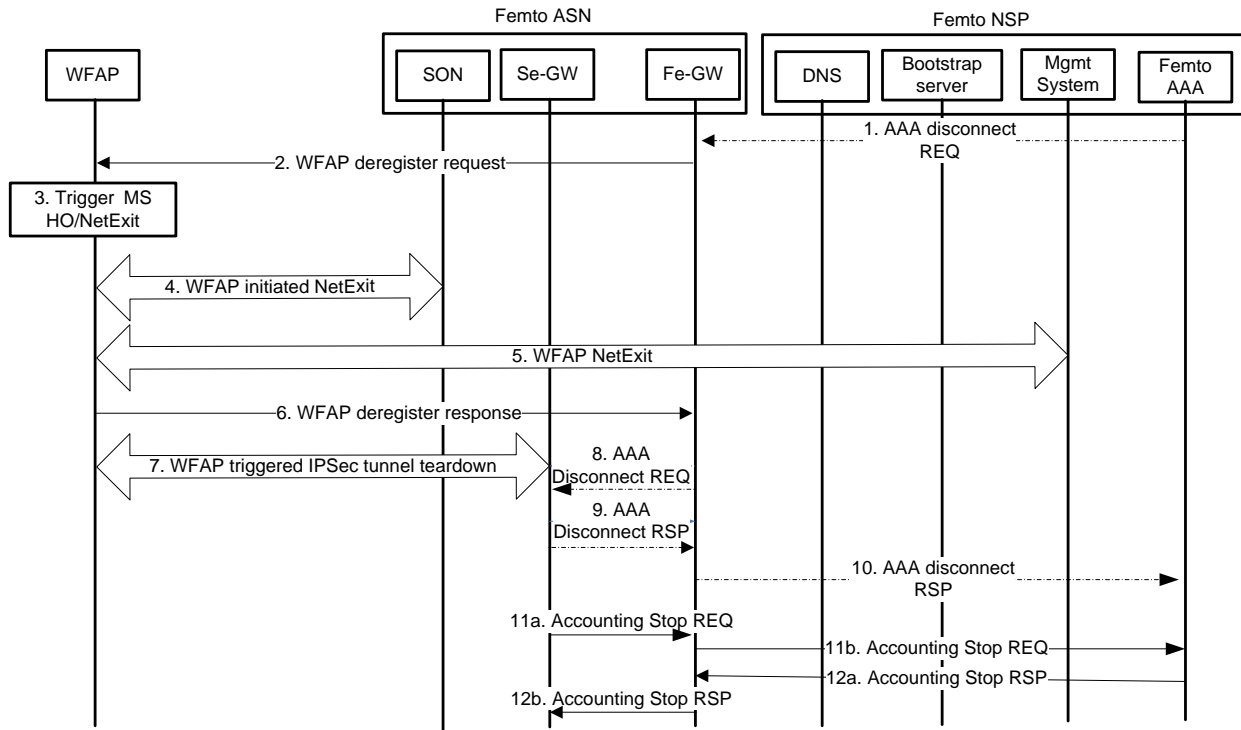


Figure 5-6: Network triggered WFAP Network Exit (Graceful)

Step-1: If the WFAP subscription has expired the Femto-AAA shall trigger the network triggered WFAP exit. This step is only limited to Femto-AAA triggered scenario so it is not required in Fe-GW triggered scenario.

Step-2: The Fe-GW triggers the WFAP network exit by sending the WFAP de-register request to the WFAP.

Step-3: WFAP initiates handover or network exit for its attached MS(s), dependent on the network policy.

Step-4: WFAP performs network exit from the SON server as specified in [8].

Step-5: WFAP performs network exit from the WFAP management server as specified in [7].

Step-6: WFAP responds back to the Fe-GW with WFAP de-registration response after all the MS's detachment(s) are completed, if any.

Step-7: WFAP shall initiate and tear down the IPsec tunnel towards the Se-GW.

Steps-8,9,10: If the network exit was triggered by the Femto-AAA (as in step-1), the Fe-GW relays the AAA Disconnect Request message to the Se-GW. These steps happen right after Step-6. Se-GW responds back with AAA disconnect response which the Fe-GW relays back to the Femto-AAA. These steps are only limited to Femto-AAA triggered scenario and they are not required in Fe-GW triggered scenarios.

Steps-11,12: After the IPsec tunnel is successfully terminated, the Se-GW sends accounting stop request to the Femto-AAA via the Fe-GW and the Femto-AAA responds back with accounting stop response to the Se-GW via the Fe-GW.

5.2.3 Fe-GW triggered WFAP Network Exit (Ungraceful)

This scenario of ungraceful WFAP network exit occurs when the WFAP has lost its connectivity to the Femto-ASN. The Fe-GW detects the loss of backhaul connectivity (i.e., via R6 keepalive) and triggers the WFAP network exit.

The procedure is shown in **Error! Reference source not found.**

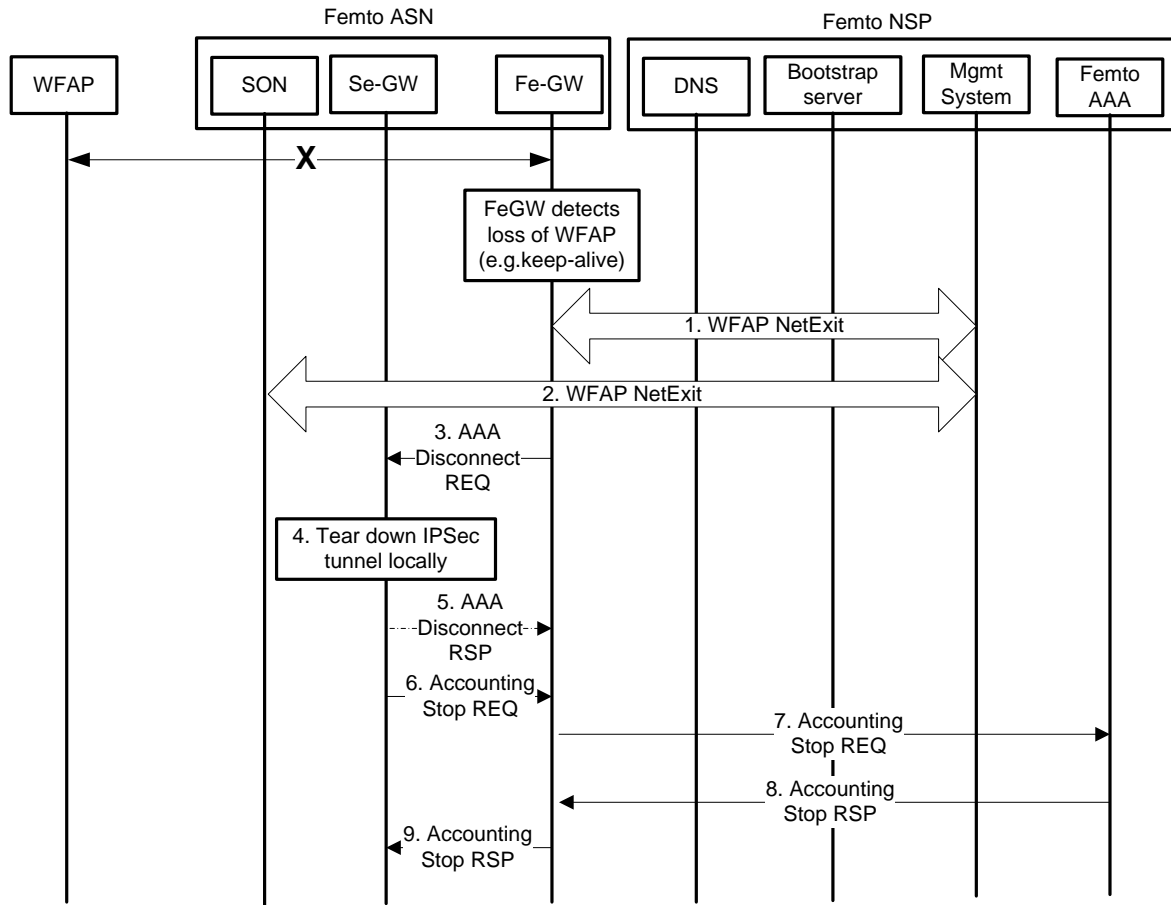


Figure 5-7 Fe-GW triggered WFAP Network Exit (Ungraceful)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

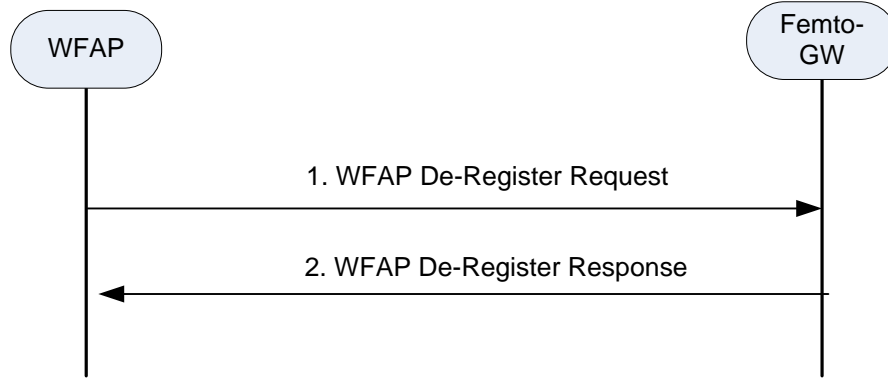
- Step-1: Fe-GW detects the loss of WFAP connectivity and triggers WFAP network exit to the management system .
- Step-2: Management system indicates the WFAP network exit to the SON server.
- Step-3: Fe-GW sends a AAA disconnect request to the Se-GW to indicate the loss of WFAP.
- Step-4: Se-GW tears down the IPsec tunnel locally.
- Step-5: Se-GW responds back to the Fe-GW with a AAA disconnect response.
- Steps-6~Step-9: the Se-GW indicates the loss of WFAP to the Femto-AAA via the Fe-GW and the Femto-AAA responds back to the Se-GW via the Fe-GW.

5.2.4 WFAP De-registration with Fe-GW

This section describes WFAP’s deregistration procedure triggered by either WFAP or Fe-GW. The Fe-GW and the WFAP will clear all related resources.

5.2.4.1 WFAP initiated De-registration

Figure 5-8 describes WFAP initiated De-registration procedure. The WFAP will initiate this procedure whenever it needs to terminate its operation.



1
2
3
4
5
6

Figure 5-8: WFAP De-Registration (WFAP Initiated)

Step-1: The WFAP sends WFAP De-register Request to the serving Fe-GW.

Step 2: The Fe-GW responds with the WFAP De-register Response.

1 5.3 CSG White-list on the MS

2 If the MS implementation supports CSG white list, the MS MAY store the relevant information regarding the
 3 WFAPs that include the MS in their respective CSGs, such as the BSID of WFAP, BSID of the overlay macro BS (if
 4 applicable), GPS location of the WFAP (if available), carrier frequency, cell type and preamble index. The MS may
 5 use such information in its CSG white list to perform initial network entry as well as trigger MS initiated scanning
 6 and handover from the Macro BS to the CSG WFAP(s) that the MS is member of.

7 OTA or ND&S MAY be used for MS acquiring and updating its CSG white list, i.e. the provisioning server defined
 8 in OTA method could acquire and deliver the CSG white list to the MS. Using manual selection, an MS may attempt
 9 to access a WFAP(s) not contained in the CSG white-list. Based on the feedback from the network, the MS's CSG
 10 white-list may be updated.

11 The support of CSG whitelist on the MS is applicable to TWG Rel 1.5 and beyond MSs.

12 5.4 MS Network entry and exit

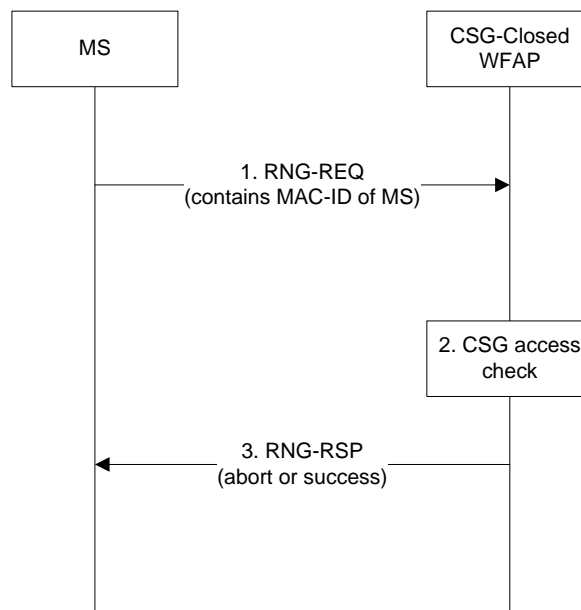
13 The MS network entry into a CSG (open or closed) WFAP is described below. The MS network entry into an Open
 14 WFAP is the same as the baseline scenario [2].

15 5.4.1 MS Network entry into CSG WFAP

16 5.4.1.1 MS Network entry into CSG-Closed WFAP

17 For the CSG-Closed WFAP, the MS Initial Network Entry into the WFAP is exactly the same as regular Macro
 18 Initial Network Entry with one extra step. During MS initial ranging, and there is no emergency indication issued by
 19 the MS, the CSG-Closed WFAP SHALL examine the MAC-ID of the MS to validate the MAC-ID against the CSG
 20 list of the WFAP. If the MS MAC-ID is not part of the CSG-list of the WFAP, the MS Initial Network Entry should
 21 be rejected by this WFAP. If the MS MAC-ID is part of the CSG-list of WFAP, the MS Initial Network Entry
 22 proceeds as normal Initial Network Entry from this point onward as described in [2]. Figure 5-9 describes the
 23 ranging procedure for the MS initial network entry into CSG-Closed WFAP.

24 For Emergency Service Initial Network Entry at CSG-closed WFAP, Sec.5.4.1.3 shall be referred.



25

26 **Figure 5-9: Ranging Procedure of CSG-closed WFAP during MS network entry**

Femto-Core

- 1 Step-1: The MS performing initial network entry shall perform CDMA ranging followed by RNG-REQ message
 2 transmission (as specified in [4] section 6.3.2.3.5). The MS shall include its MAC-ID as part of this RNG-REQ
 3 message.
- 4 Step-2: The CSG-closed WFAP checks if the MAC-ID included in RNG-REQ message is a part of CSG list stored
 5 on the WFAP.
- 6 Step-3: If the MAC-ID is a part of CSG list, the CSG-closed WFAP sends RNG-RSP message including Ranging
 7 Status TLV with a value of “success”. If the MAC-ID is not a part of CSG list, the CSG-closed WFAP sends RNG-
 8 RSP message including Ranging Status TLV with a value of “abort”. If the Ranging Status value is “abort”, the
 9 WFAP may redirect the MS to different BS by using Downlink frequency override TLV and Preamble Index
 10 Override TLV.

11 **5.4.1.2 MS Network entry into CSG-Open WFAP**

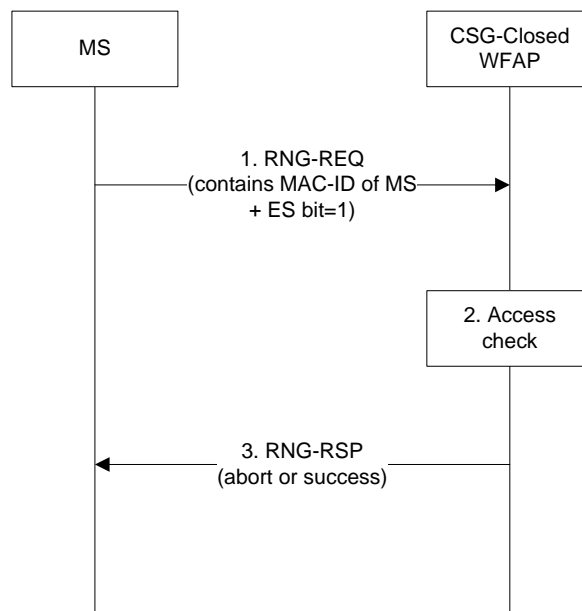
12 For the CSG-Open WFAP, MS Initial Network Entry into the WFAP is exactly the same as the baseline scenario [2]
 13 and no filtering is done provided there is no congestion at the WFAP. Under WFAP congestion scenarios, priority is
 14 given to access and/or traffic from the MSs present in the CSG list of the WFAP

15 **5.4.1.3 MS Network entry for Emergency access**

16 For the CSG-Closed WFAP, MS may perform Initial Network Entry for the sake of emergency calling even if the
 17 MS does not belong to the CSG of the WFAP. The MS shall include the emergency indication in the initial ranging
 18 message [4] to the CSG-Closed WFAP. This will signal the emergency call to the CSG-Closed WFAP which will
 19 subsequently allow the MS access even if the MS MAC-ID is not part of the CSG list of the WFAP.

20 Whether the WFAP allows or rejects emergency access for non-CSG MSes SHALL be configurable via the
 21 management plane. It is an operator policy decision that also depends on regional regulatory requirements.

22 Figure 5-10 describes ranging procedures for an MS initial network entry, focusing on emergency access for a non-
 23 member CSG WFAP.



24

25 **Figure 5-10: Ranging Procedure of CSG-closed WFAP for emergency call during MS network entry**

26

27 Step-1: The MS performing initial network entry for emergency access will perform CDMA ranging and will
 28 subsequently send RNG-REQ message (as specified in [4] section 6.3.2.3.5). The MS shall include the MAC-ID
 29 and set the emergency indication (ES bit) for emergency access.

Femto-Core

1 Step-2: If the WFAP is configured to support emergency network access, the WFAP checks for the ES bit. If the ES
2 bit has been set by the MS, then the WFAP ignores any CSG-closed configuration and allow emergency network
3 entry for this MS. If the WFAP is configured not to support emergency network access, the WFAP rejects the MS
4 for emergency network access.

5 Step-3: If emergency network entry is granted as a result of step 2, the CSG-closed WFAP sends a RNG-RSP
6 message including the Ranging Status TLV with a value of "success". For rejection case in step 2, the WFAP may
7 redirect the MS to a different BS which supporting emergency network access by the way as described in step 3 of
8 section 5.4.1.1.

9 **5.4.2 MS Network exit**

10 The MS network exit procedure is same as baseline scenario [2].

11 If the MS is currently attached to the WFAP, then the MS network exit may be triggered by WFAP based on the
12 removal of the MS from the CSG membership list of the WFAP. The removal of the MS from the CSG membership
13 list of the WFAP may happen locally at WFAP or may be triggered by the WFAP Management System. How the
14 WFAP becomes aware which neighbor base stations support the emergency service is out of the scope of this
15 specification.

16 **5.5 Mobility Management**

17 The Fe-GW plays the role of the ASN-GW in the baseline mobility management [2], [5].

18 Only Intra-NAP handovers are supported in this release of the specification.

19 Three mobility scenarios are considered for the MS.

- 20 a) WFAP to Macro-BS mobility: also called hand-out
- 21 b) Macro-BS to WFAP mobility: also called hand-in
- 22 c) WFAP to WFAP mobility

23 **5.5.1 WFAP to Macro-BS mobility**

24 WFAP SHALL advertise all the overlay Macro-BSs in its NBR-ADV broadcast [4]. No specific enhancements are
25 needed to support this mobility scenario when compared to the baseline mobility scenario [5].

26 The WFAP to Macro-BS mobility may be initiated either by the MS or the WFAP.

27 If the MS is currently attached to the WFAP, then the MS handover from WFAP may be triggered by the WFAP
28 based on the removal of the MS from the CSG membership list of the WFAP. The removal of the MS from the CSG
29 membership list of the WFAP may happen locally at WFAP or may be triggered by the management server.

30 **5.5.2 Macro-BS to WFAP mobility**

31 Macro-BS MAY advertise some of the WFAPs in its NBR-ADV broadcast.

32 The handover procedures are the same as the baseline mobility scenario [5] with the following enhancements:

- 33 a) For network initiated handovers, Serving Macro-BS may become aware of the list of viable target CSG
34 WFAPs for the MS upon the entry of the MS into the serving BS (taking into account CSG memberships of
35 the MS) through its management plane and may store this information as a part of MS context. The exact
36 mechanism for doing this is outside the scope of the current specification. The serving BS may use this
37 information to trigger BS initiated scanning and handover to the appropriate CSG WFAP. The BS initiated
38 SCAN-RSP SHALL contain the full 48bit BSID of the WFAP [4].
- 39 b) For MS initiated handovers, the MS may use its CSG white-list to trigger MS initiated scanning and
40 handover from the Macro BS to the CSG WFAP(s) that the MS is member of.

41 **5.5.3 WFAP to WFAP mobility**

42 WFAP MAY advertise some of the neighbor WFAPs in its NBR-ADV broadcast.

1 The WFAP to WFAP mobility may be initiated either by the MS or the WFAP.

2 If the MS is currently attached to the WFAP, then the MS handover from WFAP may be triggered by the WFAP
3 based on the removal of the MS from the CSG member list of the WFAP. The removal of the MS from the CSG
4 member list of the WFAP may happen locally at WFAP or may be triggered by the management server.

5 **5.6 Idle-Mode and Paging**

6 The Fe-GW contains the PC function. PGID allocation is a deployment choice. Depending on the deployment
7 configurations and/or NAP sharing configurations, each CSG-Closed WFAP may have a shared PGID with the rest
8 of the network or may have a dedicated PGID of its own.

9 **5.6.1 Location Update at WFAP**

10 The MS SHALL perform the Location Update procedure when it meets the LU conditions as specified in [4]. The
11 MS SHALL use one of two processes for Location Update: Secure Location Update or Unsecure Location Update.
12 An Un-Secure Location Update process is performed when MS and BS do not share a valid security context which
13 means that BS is not able to receive a valid AK (e.g., MS crossed Mobility Domain boundaries or PMK has expired)
14 or when the BS otherwise elects to direct the MS to proceed with network re-entry. Un-Secure Location Update
15 results in MS network re-entry from Idle Mode. It is performed in the same way as a regular MS network entry
16 process.

17 An MS should be able to perform location update at a CSG-Closed WFAP via Secure Location Update or Unsecure
18 Location Update dependent on the success of the retrieval of the MS security context and the validation of the
19 CMAC key, if the MS is the member of CSG of the target WFAP. When the MS has selected the preferred target
20 WFAP of which the MS is not the member of its CSG, the MS Location Update SHALL be rejected and this will
21 lead to the MS to proceed with the re-entry procedures as described in the section 4.10.2 of [2].

22 **5.6.1.1 Secure Location Update Failure**

23 In case of secure location update failure, if the MS is not a member of the CSG of the target WFAP, the WFAP may
24 provide redirection to the MS to other target WFAPs/BSs in the RNG-RSP message during the network re-entry.
25 Otherwise, the network will re-authenticate the MS during the network re-entry from Idle Mode.

26 **5.6.2 Paging**

27 The CSG-Closed WFAP shall not page the non-member MSs. The Paging procedure is the same as baseline
28 scenario[2]. (see section 4.10.3)

29 **5.6.3 Idle-mode Exit in WFAP**

30 An MS shall be able to perform idle mode exit only in a CSG-Closed WFAP to which it is a member. In this case,
31 the idle mode exit procedure is the same as baseline scenario[2]. (see section 4.10.4). If the MS is not a member of
32 the CSG-Closed WFAP, then the WFAP may provide redirection to the MS to other WFAPs/BSs in the RNG-RSP
33 message. The WFAP determines CSG-membership of the MS based on MAC ID of the MS.

34 **5.6.4 Idle-mode Entry in WFAP**

35 MS idle mode entry in Femtocell is same as baseline scenario[2](see section 4.10.5)

36 **5.7 QoS Control**

37 The QoS control is aligned with the baseline specification [5]. The SFM shall reside in the WFAP and the SFA shall
38 reside in the Fe-GW. In addition, the WFAP and Fe-GW shall support QoS class mapping to DSCP code points
39 based on operator policy. The WFAP may reuse the uplink DSCP marking that may be already done by the MS or
40 alternatively the WFAP may apply its own DSCP marking for the uplink traffic. Any additional QoS mechanisms
41 that the backhaul link may provide (e.g.: DOCSIS) can be utilized to further improve QoS on the R6-F interface.
42 This is not in scope of the current specification.

1 **5.8 Radio Resource Management**

2 RRM is an optional feature to be supported by WFAPs. The existing WiMAX Forum® Network Architecture RRM
3 framework is re-used in the case of WFAPs. WFAPs when supporting the RRM, SHALL implement both RRC and
4 RRA functions. No new RRM messages are defined specifically for WFAPs.

5 *Note-1:* WFAPs overlaid with Macro BS network: In this scenario, under a given Macro cell coverage, there may be
6 potentially large number of WFAPs. Configuring all of these WFAPs as neighbors to the Macro BS and running
7 RRM exchanges, will create that many RRM instances in the macro BS. This may consume lot of resources in the
8 Macro BS.

9 *Note-2:* WFAPs with non-overlay Macro BS: In this scenario, RRM makes sense only in the case where different
10 WFAPs are grouped to serve a CSG of MSs (e.g.: within an enterprise environment), deployed with WFAPs. If the
11 WFAPs are deployed with no shared CSG MSs like in a neighborhood of independent homes, implementing RRM
12 between them may not yield any benefit.

13 **5.9 Accounting**

14 **5.9.1 Accounting of the MS session**

15 For accounting of MS session, the Fe-GW functionality is equivalent to the ASN GW functionality and the WFAP
16 functionality is equivalent to the Macro BS functionality

17 **5.9.2 Accounting of the WFAP session**

18 The accounting agent and client function for WFAP session shall be located at Se-GW. Details of accounting
19 messages are defined in section 6.3.

20 **5.10 WFAP backhaul fault detection and mitigation**

21 The operation of Femtocell BS relies greatly on broadband backhaul in order to provide services to subscribers. A
22 backhaul fault detection and mitigation function shall be supported to enable the detection and mitigation of
23 backhaul faults automatically by sending the keep alive messages between WFAP and Fe-GW. The details of the
24 backhaul fault detection and mitigation function are described in the SON specification [8].

25

6. Message and Parameter Definitions

6.1 Constants and Counters

6.2 Message Definitions

Table 6-1: WFAP_Register_Request

IE	Reference	M/O	Notes
WFAP ID	6.4.7	M	WFAP MAC ID indicating the WFAP performing Register operation.
WFAP inner IP address	6.4.6	O	WFAP inner IP address, indicating the WFAP performing Register operation.

Table 6-2: WFAP_De-Register_Request

IE	Reference	M/O	Notes
WFAP ID	6.4.7	M	
Femto-GW ID	6.4.5	M	
De-Registration Cause	6.4.4	O	

Table 6-3: WFAP_De-Register_Response

IE	Reference	M/O	Notes
Failure Indication	6.4.2	O	Reference to WiMAX Forum® Network Architecture Release 1.5 spec:
WFAP ID	6.4.7	O	
Femto-GW ID	6.4.5	O	

Table 6-4: WFAP_Register_Response

IE	Reference	M/O	Notes
Failure Indication	6.4.2	O	Reference to WiMAX Forum® Network Architecture Release 1.5 spec:
Failure Cause	6.4.3	O	Provide the failure cause for this message
Backoff Timer	6.4.1	O	This TLV SHALL be included if Failure Cause is "Overload".

6.3 AAA Exchanges between Se-GW, Femtocell GW and Femtocell AAA Server

This section specifies the RADIUS and Diameter messages and attributes exchanged between the Se-GW and the Femtocell AAA server via Fe-WG.

6.3.1 RADIUS exchanges between Se-GW, Femtocell GW and Femtocell AAA Server

The following tables define the RADIUS messages exchanged between the Se-GW and the Femtocell AAA Servers. Only attributes that are specific to this interface are documented. The tables are in addition to other requirements defined by the other RADIUS RFCs specifically RFC2865, RFC2866, RFC2869 and RFC5176 as appropriate.

It is not anticipated that Access-Challenge packets will be exchanged between the Se-GW and the Femtocell AAA and thus the column are marked as Not Applicable (N/A) in this specification. Should a Femtocell AAA require to send an Access-Challenge then the requirements of the various RADIUS RFCs should be followed.

Table 6-5: RADIUS Messages between Se-GW and Femtocell AAA

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
User-Name	1	NAI obtained from the IDi attribute received by the Se-GW during IKEv2 procedures.	1	N/A	0-1	0
Service-Type	6	MUST be set to "Authorize Only"	1	N/A	0-1	0
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [52].	1	N/A	1	1
NAS-Identifier	32	This attribute contains a string identifying the Se-GW. The format SHALL be the fully qualified domain name of the NAS.	1[A]	N/A	0	0
NAS-Port-Type	61	Set to Femtocell	1	N/A	0	0
NAS-IP-Address	4	NAS IP Address.	0-1[A]	N/A	0	0
NAS-IPv6-Address	95	NAS-IPv6 address.	0-1[A]	N/A	0	0
Error-Cause	101	Error Codes generated during access authentication [51].	0	N/A	0	0-1
Class	25	Opaque value set by the Server used to bind authentication to accounting.	0	N/A	0-1[B]	0
Session-Timeout	27	The time remaining before the Se-GW needs to re-authorize.	0	N/A	0-1[C]	0
Termination-Action	29	Indicates what action the NAS should take when service is completed.	0	N/A	0-1[C]	0
R6-ID	26/236	The R6-ID in case when the R6-ID is assigned by the Femtocell AAA server. The attribute is opaque.	0	N/A	0-1[D]	0

Femto-Core

1 **Notes:**

- [A] NAS-ID SHALL appear in the Access-Request. One of NAS-IP-Address or NAS-IPv6 address MAY also appear.
- [B] If more than one Class attribute is found in an Access-Accept packet, the NAS SHALL only store the first one and discard the rest.
- [C] Both Session-Timeout and Termination-Action SHALL be present. Termination-Action SHALL be set to "RADIUS-Request"(1). This causes the Se-GW to re-authenticate when the Session-Timeout expires.
- [D] Shall be included in Access-Accept when the R6-ID is not an IP address. Otherwise, this attribute MUST NOT be present.

2

3 The following table describes the Accounting messages sent by the Se-GW to the Femtocell AAA server. Upon
 4 receiving the Accounting messages the Femtocell AAA server shall respond back in accordance with RFC 2866 and
 5 RFC 2869..

6

Table 6-6: RADIUS Accounting Messages between Se-GW and Femtocell AAA

7

Attribute	TYPE	Description	Accounting-Request Start	Accounting-Request Interim	Accounting-Request Stop
User-Name	1	NAI obtained from the IDi attribute received by the Se-GW during IKEv2 procedures or must be set to the User-Name attribute if received in the Access-Accept in response to the Access-Request.	1	1	1
Acct-Session-Id	44		1	1	1
Framed-IP-Address	8	The IPv4 address assigned to the WFAP	0-1[a]	0-1[a]	0-1[a]
Framed-Interface-Id	96	The IPv6 interface identifier used by the WFAP in case of IPv6 assignment.	0-1[a]	0-1[a]	0-1[a]
Framed-IPv6-Prefix	97	The IPv6 prefix used by the WFAP in case of IPv6 assignment.	0-1[a]	0-1[a]	0-1[a]
Acct-Session-Time	46	The number of seconds the session was active.	0	0-1	0-1
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the Se-GW.	0-1	0-1	0-1
Event-Timestamp	55	The time the event occurred.	1	1	1

Acct-Delay-Time	41	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.	0-1	0-1	0-1
Acct-Input-Octets	42	The total number of octets in IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1	0-1
Acct-Output-Octets	43	The total number of octets in IP packets sent to the user, as received at the accounting agent from the IP network (i.e., prior to any compression and/or fragmentation).	0	0-1	0-1
Acct-Input-Packets	47	The total number of IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1	0-1
Acct-Output-Packets	48	The total number of IP packets sent to the user, as received at the accounting agent from the IP network (i.e., prior to any compression and/or fragmentation).	0	0-1	0-1
Acct- Input - Gigawords	52	Incremented when attribute 42 overflows.	0	0-1	0-1

1
 2 Other attributes may be included in the Accounting packets exchanged between the Se-GW and the Femtocell AAA
 3 server.

4 **Notes:**

[a] In the case of IPv4 address assignment to the WFAP, Framed-IP-Address is required. In the case of IPv6
 address assignment to the WFAP Framed-Interface-Id and Framed-IPv6-Prefix as per RFC3162 are required.

5
 6 The Femtocell AAA server may send a Change of Authorization (COA) packet or Disconnect Packets as per RFC
 7 5176.

8 **Table 6-7: RADIUS Disconnect Messages between Se-GW and Femtocell AAA**

Attribute	TYPE	Description	DM	DM-ACK	DM-NAK
User-Name	1	The NAI received from the Se-GW in the Access-	1	0	0

Attribute	TYPE	Description	DM	DM-ACK	DM-NAK
		Request during authorization procedures			
NAS-Identifier	32	The NAS identifier received from the Se-GW in the Access-Request during the authorization procedures	1	0	0
NAS-IP-Address	4	The IPv4 address of the Se-GW if received in the Access-Request during the authorization procedures	0-1	0	0
NAS-IPv6-Address	95	The IPv4 address of the Se-GW if received in the Access-Request during the authorization procedures	0-1	0	0
Framed-IP-Address	8	The IPv4 address assigned to the WFAP	0-1[a]	0	0
Framed-Interface-Id	96	The IPv6 interface identifier used by the WFAP in case of IPv6 assignment.	0-1[a]	0	0
Framed-IPv6-Prefix	97	The IPv6 prefix used by the WFAP in case of IPv6 assignment.	0-1[a]	0	0
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [52]	1	1	1
Error-Cause	101	Error Codes generated during access authentication [51]	0	0	0-1

1 **Notes:**

[a] This attributes must match the corresponding attributes received in the Accounting Request packets.

2

3

Table 6-8: RADIUS Change of Authorization Messages between Se-GW and Femto-cell AAA

Attribute	TYPE	Description	DM	DM-ACK	DM-NAK
User-Name	1	The NAI received from the Se-GW in the Access-Request during authorization procedures	1	0	0
NAS-Identifier	32	The NAS identifier received from the Se-GW in the Access-Request	1	0	0

Attribute	TYPE	Description	DM	DM-ACK	DM-NAK
		during the authorization procedures			
NAS-IP-Address	4	The IPv4 address of the Se-GW if received in the Access-Request during the authorization procedures	0-1	0	0
NAS-IPv6-Address	95	The IPv4 address of the Se-GW if received in the Access-Request during the authorization procedures	0-1	0	0
Framed-IP-Address	8	The IPv4 address assigned to the WFAP	0-1[a]	0	0
Framed-Interface-Id	96	The IPv6 interface identifier used by the WFAP in case of IPv6 assignment.	0-1[a]	0	0
Framed-IPv6-Prefix	97	The IPv6 prefix used by the WFAP in case of IPv6 assignment.	0-1[a]	0	0
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [52]	1	1	1
Error-Cause	101	Error Codes generated during access authentication [51]	0	0	0-1

1 **Notes:**

[a] This attributes must match the corresponding attributes received in the Accounting Request packets.

2

3 **6.3.2 Diameter exchanges between Se-GW, Femtocell GW and Femtocell AAA Server**

4 The Se-GW, Femtocell GW and Femtocell AAA Server shall advertise support for this application by including the
5 value of TBDWFDA (WiMAX® Femtocell Diameter Application ID) in the Diameter Capability Exchange
6 procedure, as well as all the commands specified in this document.

7 For Accounting support, the Se-GW, Femtocell GW and Femto-AAA Server shall advertise support for this
8 application as per [23].

9 The Femtocell AAA server SHALL maintain Diameter state and thus the Se-GW must inform the Femtocell AAA
10 server when the IPsec session has terminated.

11 The commands supported by the WiMAX® Femtocell Application are listed below:

Code	Command Name	Abbreviation
TBDWFAA	WiMAX Femtocell Authentication Authorization Request / Answer	WFAAR/A
TBDWFRA	WiMAX Femtocell Re-Auth-Request /Answer	WFRAR/A

TBDWFAS	WiMAX® Femtocell Abort Session Request / Answer	WFASR/A
TBDWFST	WiMAX® Femtocell Session Termination Request / Answer	WFSTR/A
TBDWFAC	WiMAX® Femtocell Accounting Request/ Answer	WFACR/A

- 1
- 2 The specification of the commands in this document only highlight the WiMAX specific usage. The Se-GW,
3 Femtocell GW and the Femtocell AAA server shall comply with [23][24].
- 4 The Diameter AVP appearing in these commands are defined in [23][24].
- 5 **6.3.2.1 WiMAX® Femtocell Authentication-Authorization Request/Answer (WFAAR/A) command**

6 The following represents the subset of the WFAAR and WFAAA command.

7 <WFAA-Request> ::= < Diameter Header: TBDWFAA, REQ, PXY >

```

< Session-Id >
  { Auth-Application-Id }
  { Origin-Host }
  { Origin-Realm }
  { Destination-Realm }
  { Auth-Request-Type }           Set to Authorize Only
  { User-Name }                  NAI from the IKEv2 IDi attribute.
  { NAS-Identifier }             Set to the domain name of the Se-GW
  { Service-Type }              Set to Authorize-Only.
  { NAS-Port-Type }
  [ Destination-Host ]
  [ NAS-IP-Address ]             May also be included.
  [ NAS-IPv6-Address ]          May also be included.
  [ Origin-AAA-Protocol ]
  [ Origin-State-Id ]
  * [ Proxy-Info ]
  * [ Route-Record ]
  * [ AVP ]

```

8

9 <WFAA-Answer> ::= < Diameter Header: TBDWFAA, PXY >

```

< Session-Id >
  { Auth-Application-Id }
  { Auth-Request-Type }
  { Result-Code }
  { Origin-Host }
  { Origin-Realm }
  [ User-Name ]
  [ R6-ID ]
  [ Service-Type ]
  * [ Class ]
  [ Acct-Interim-Interval ]
  [ Error-Message ]
  [ Error-Reporting-Host ]

```

* [Failed-AVP]
 [Idle-Timeout]
 [Authorization-Lifetime]
 [Auth-Grace-Period]
 [Auth-Session-State]
 [Re-Auth-Request-Type]
 [Multi-Round-Time-Out]
 [Session-Timeout]
 [State]
 * [Redirect-Host]
 [Redirect-Host-Usage]
 [Redirect-Max-Cache-Time]
 * [Proxy-Info]
 * [AVP]

1
 2

3 6.3.2.2 WiMAX® Femtocell Re-Auth-Request/Re-Auth-Answer command

4 Note that Diameter does not support Change of Authorization procedures as defined by RADIUS. Instead,
 5 WFRAR/A is used to trigger the Se-GW to Re-authorize (send an WFAAR command to the Femtocell AAA server).
 6 During the Re-authorization phase the Femtocell AAA server can provide the updated authorization attributes (in
 7 WFAAA command).

8 <WFRA-Request> ::= < Diameter Header: TBDWFRA, REQ, PXY >

< Session-Id >
 { Origin-Host }
 { Origin-Realm }
 { Destination-Realm }
 { Destination-Host }
 { Auth-Application-Id }
 { Re-Auth-Request-Type }
 { User-Name } Set to the value received in WFAAR.
 { NAS-Identifier }
 { NAS-Port-Type }
 [Service-Type]

 [Origin-AAA-Protocol]
 [Origin-State-Id]
 [NAS-IP-Address]
 [NAS-IPv6-Address]

[NAS-Port]
[NAS-Port-Id]
[Framed-IP-Address] Set to the value received in the ACR command
[Framed-IPv6-Prefix] Set to the value received in the ACR command
[Framed-Interface-Id] Set to the value received in the ACR command
[Called-Station-Id]
[Acct-Session-Id]
[Acct-Multi-Session-Id]
[State]
* [Class]
[Reply-Message]
* [Proxy-Info]
* [Route-Record]
* [AVP]

1

2 <WFRA-Answer> ::= < Diameter Header: TBDWFRA, PXY >

< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Origin-AAA-Protocol]
[Origin-State-Id]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
* [Redirected-Host]
[Redirected-Host-Usage]
[Redirected-Host-Cache-Time]
[Service-Type]
* [Configuration-Token]
[Idle-Timeout]
[Authorization-Lifetime]
[Auth-Grace-Period]
[Re-Auth-Request-Type]
[State]
* [Class]

* [Reply-Message]

[Prompt]

* [Proxy-Info]

* [AVP]

1

2 6.3.2.3 WiMAX® Femtocell Abort Session Request/ Answer command

3 This command is used by the Femtocell AAA server to request the Se-GW to terminate the WFAP IPsec session.

4 The command is defined as per RFC4005.

5 <WFAS-Request> ::= < Diameter Header: TBDWFAS, REQ, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Destination-Host }

{ Auth-Application-Id }

{ User-Name }

[Origin-AAA-Protocol]

[Origin-State-Id]

{ NAS-Identifier }

[NAS-IP-Address]

[NAS-IPv6-Address]

[NAS-Port]

[NAS-Port-Id]

[NAS-Port-Type]

[Service-Type]

[Framed-IP-Address]

[Framed-IPv6-Prefix]

[Framed-Interface-Id]

[Called-Station-Id]

[Calling-Station-Id]

[Originating-Line-Info]

[Acct-Session-Id]

[Acct-Multi-Session-Id]

[State]

* [Class]

* [Reply-Message]

* [Proxy-Info]

* [Route-Record]

* [AVP]

1

2

3 <WFAS-Answer> ::= < Diameter Header: TBDWFAS, PXY >

< Session-Id >

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

[User-Name]

[Origin-AAA-Protocol]

[Origin-State-Id]

[State]

[Error-Message]

[Error-Reporting-Host]

* [Failed-AVP]

* [Redirected-Host]

[Redirected-Host-Usage]

[Redirected-Max-Cache-Time]

* [Proxy-Info]

* [AVP]

4

5 6.3.2.4 WiMAX® Femtocell Session Termination Request/Answer command

6 This command is used by the Se-GW to inform the Femtocell AAA server when the session (IPsec session) has been
7 terminated.

8

9 <WFST-Request> ::= < Diameter Header: TBDWFST, REQ, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Auth-Application-Id }

{ Termination-Cause }

{ User-Name }

[Destination-Host]

* [Class]

[Origin-AAA-Protocol]

1 [Origin-State-Id]
2 * [Proxy-Info]
3 * [Route-Record]
4 * [AVP]
5
6
7 <WFST-Answer> ::= < Diameter Header: TBDWFST, PXY >
8 < Session-Id >
9 { Result-Code }
10 { Origin-Host }
11 { Origin-Realm }
12 [User-Name]
13 * [Class]
14 [Error-Message]
15 [Error-Reporting-Host]
16 * [Failed-AVP]
17 [Origin-AAA-Protocol]
18 [Origin-State-Id]
19 * [Redirect-Host]
20 [Redirect-Host-Usase]
21 [Redirect-Max-Cache-Time]
22 * [Proxy-Info]
23 * [AVP]

4
5 **6.3.2.5 WiMAX® Femtocell Accounting Request/Answer command**

6
7 <WFAC-Request> ::= < Diameter Header: TBDWFAC, REQ, PXY >
8 < Session-Id >
9 { Origin-Host }
10 { Origin-Realm }
11 { Destination-Realm }
12 { Accounting-Record-Type }
13 { Accounting-Record-Number }
14 { Vendor-Specific-Application-Id }
15 { User-Name }
16 { NAS-Port-Type } ????

Femto-Core

{ NAS-Identifier }	Mandatory
[Accounting-Sub-Session-Id]	
[Acct-Session-Id]	
[Acct-Multi-Session-Id]	
[Origin-AAA-Protocol]	
[Origin-State-Id]	
[Destination-Host]	
[Event-Timestamp]	
[Acct-Delay-Time]	
[NAS-IP-Address]	
[NAS-IPv6-Address]	
[NAS-Port]	
[NAS-Port-Id]	
* [Class]	
[Service-Type]	
[Termination-Cause]	
[Accounting-Input-Octets]	Required if performing accounting on a per WFAP
[Accounting-Input-Packets]	Required if performing accounting on a per WFAP
[Accounting-Output-Octets]	Required if performing accounting on a per WFAP
[Accounting-Output-Packets]	Required if performing accounting on a per WFAP
[Acct-Authentic]	
[Accounting-Auth-Method]	
[Acct-Link-Count]	
[Acct-Session-Time]	
[Acct-Tunnel-Connection]	
[Acct-Tunnel-Packets-Lost]	
* [Connection-Info]	
[Originating-Line-Info]	
[Authorization-Lifetime]	
[Session-Timeout]	
[Idle-Timeout]	
[Port-Limit]	
[Accounting-Realtime-Required]	
[Acct-Interim-Interval]	
[Framed-Interface-Id]	If IPv6 then Mandatory
[Framed-IP-Address]	If IPv4 then Mandatory.
* [Framed-IPv6-Prefix]	If IPv6 then Mandatory

Femto-Core

- * [Tunneling]
- * [Proxy-Info]
- * [Route-Record]
- * [AVP]

1

2

3 <WFAC-Answer> ::= < Diameter Header: TBDWFAC, PXY >

- < Session-Id >
- { Result-Code }
- { Origin-Host }
- { Origin-Realm }
- { Accounting-Record-Type }
- { Accounting-Record-Number }
- [Acct-Application-Id]
- [Vendor-Specific-Application-Id]
- [User-Name]
- [Accounting-Sub-Session-Id]
- [Acct-Session-Id]
- [Acct-Multi-Session-Id]
- [Event-Timestamp]
- [Error-Message]
- [Error-Reporting-Host]
- * [Failed-AVP]
- [Origin-AAA-Protocol]
- [Origin-State-Id]
- [NAS-Identifier]
- [NAS-IP-Address]
- [NAS-IPv6-Address]
- [NAS-Port]
- [NAS-Port-Id]
- [NAS-Port-Type]
- [Service-Type]
- [Termination-Cause]
- [Accounting-Realtime-Required]
- [Acct-Interim-Interval]
- * [Class]
- * [Proxy-Info]

* [Route-Record]

* [AVP]

1

2 **6.4 TLV Definitions**3 **6.4.1 Backoff Timer**

Type	590
Length in octets	2
Value	16-bit unsigned integer, in units of 10 sec.
Description	Used by the WFAP as Backoff timer for re-registration with Femto-GW.
Message Primitives That Use This TLV	WFAP_Register_Response

4

5 **6.4.2 Failure Indication**

Type	69
Length in octets	1 byte
Value	Note : For WFAP registration, new two codes are added in section 5.3.2.69 [2] Error Codes: 0x30-0x7F Message-specific Failure Codes <ul style="list-style-type: none"> • 0x3D = WFAP Registration Failure • 0x3E = WFAP De-Registration Failure
Description	Boolean that indicates the result of the WFAP registration operation.
Message Primitives That Use This TLV	Any message on R6/R4/R8 that is used for failure reporting

6

7 **6.4.3 Failure Cause**

Type	591
Length in octets	1
Value	Enumerator. The values are: <ul style="list-style-type: none"> • 0x01 = Overload • 0x02 = Unspecified All other values are Reserved.
Description	
Message Primitives That Use This TLV	WFAP_Register_Response

8

9 **6.4.4 De-Registration Cause**

Type	592
Length in octets	1

Femto-Core

Value	Enumerator. The values are: <ul style="list-style-type: none"> • 0x01 = Normal • 0x02 = Overload • 0x03 = Unspecified All other values are Reserved.
Description	
Message Primitives That Use This TLV	WFAP_De-Register_Req

1

2 **6.4.5 Femto-GW ID**

Type	593
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Femto-GW Identifier.
Message Primitives That Use This TLV	WFAP_Register_Response, WFAP_De-Register_Request, WFAP_De-Register_Response

3

4 **6.4.6 WFAP IP Address**

Type	594
Length in octets	Variable (could be of three fixed sized: 4 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, or 16-octet IPv6 Address. The length defines also the format of the Identifier. This is the IPsec tunnel inner IP Address assigned to WFAP by the Se-GW.
Description	WFAP IP address.
Message Primitives That Use This TLV	WFAP_Register_Req

5

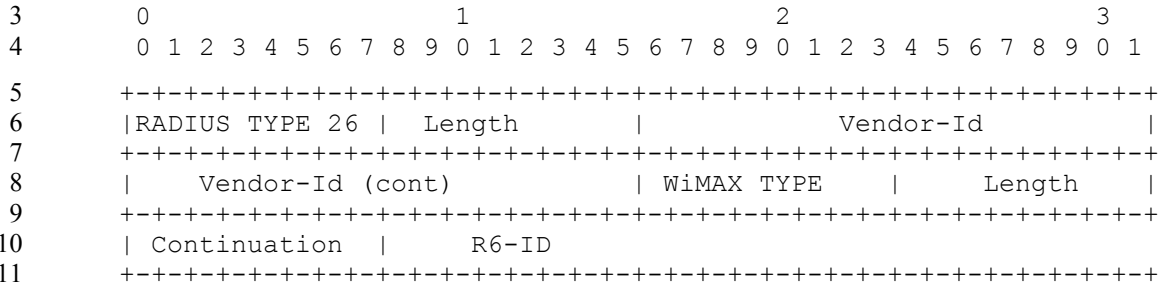
6 **6.4.7 WFAP ID**

Type	595
Length in octets	6 octets
Value	The Identifier SHALL be in format of 6-octet IEEE 802.16 BS ID.
Description	Unique WFAP Identifier, referring to a single sector with a single frequency assignment.
Message Primitives That Use This TLV	WFAP_Register_Request, WFAP_De-Register_Request, WFAP_De-Register_Response

7

1 **6.5 RADIUS Attributes**

2 **6.5.1 R6-ID**



WType-ID	236 for R6-ID
Description	The R6-ID for the R6 communication between the WFAP and the Femtocell GW. The Femtocell AAA server may send this attribute in an Access-Accept.
Length	6 + 3 + length of R6-ID value in octets
Continuation	C-bit = 0
Value	Octet-String containing the value of the R6-ID configured in the WFAP and the Femtocell AAA server. The value may be the MAC address of the WFAP. The value must match on a bit per bit basis with the value configured in the WFAP.

14

15 **6.6 Diameter Attributes**

16 **6.6.1 R6-ID**

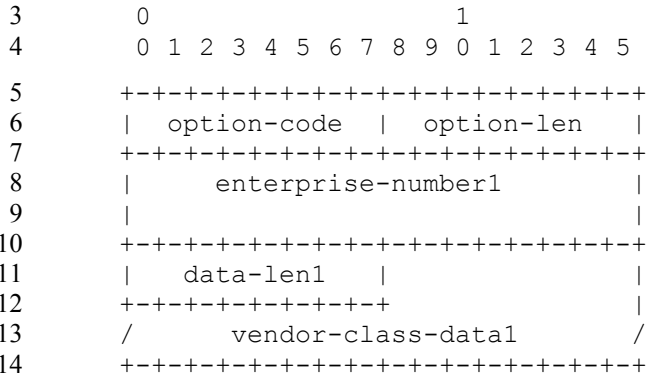
17

WType-ID	236 for R6-ID
Description	The R6-ID for the R6 communication between the WFAP and the Femtocell GW. The Femtocell AAA server may send this attribute in a WFAAA.
Value-Type	OctetString
Value	Octet-String containing the value of the R6-ID configured in the WFAP and the Femtocell AAA server. The value may be the MAC address of the WFAP. The value must match on a bit per bit basis with the value configured in the WFAP.

18

1 **6.7 DHCP Vendor Specific Option**

2 **6.7.1 Vendor-Identifying Vendor Class Option**



17 option-code

18 OPTION_V-I_VENDOR_CLASS (124)

19 option-len

20 total length of all following option data in octets

21 enterprise-numberN

22 24757 is the WiMAX Forum IANA entry. The value is a four-byte integer in network byte-order.

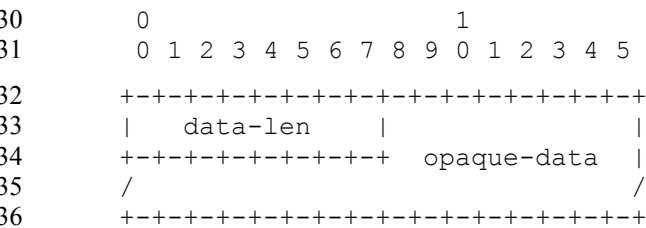
23 data-lenN

24 Length of vendor-class-data field, in bytes

25 vendor-class-dataN

26 Details of the hardware configuration of the host on which the client is running

29 Each instance of the vendor-class-data is formatted as follows:

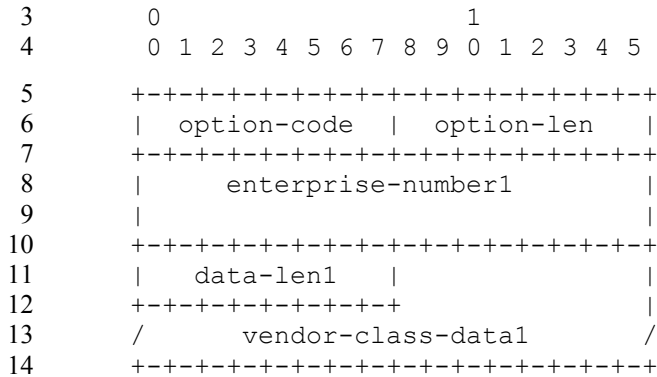


data-lenN	vendor-class-dataN
1	0x01= R1.6 WFAP

39

6.7.2 Vendor-Identifying Vendor Specific Information Option

The format of the V-I Vendor Specific Information option is as follows:



option-code:

OPTION_V-I_VENDOR_OPTS (125)

option-len:

total length of all following option data in octets

enterprise-numberN

24757 is the WiMAX Forum IANA entry. The value is a four-byte integer in network byte-order.

data-lenN

Length of option-data field

option-dataN

Vendor-specific options, described below

The encapsulated vendor-specific option-data field MUST be encoded as a sequence of code/length/value fields.

subopt-code

The code for the encapsulated option

subopt-len

An unsigned integer giving the length of the option-data field in this encapsulated option in octets

sub-option-data

Data area for the encapsulated option

subopt-code	subopt-len	sub-option-data	description
0x01	Variable (either 4 or 16)	IP address of Bootstrap server	Subopt-len will be either 4-octet for IPv4 Address, or 16-octet for IPv6 Address of Bootstrap Server.

7. Data Plane

Convergence sublayer for R1 shall be located in the Fe-GW. This is the same as the case with the ASN-GW in the baseline scenario [2]. The DL Classification SHALL be done in the Fe-GW. The Classification SHALL be done per SF granularity. Fe-GW obtains the Data Path ID of the incoming packet and maps it to the GRE key of the GRE tunnel. The WFAP simply maps this GRE key to the SFID of the MS.

On the UL, classification and PHS/ROHC (if enabled) SHALL be done in the MS. The WFAP simply maps SFID of the MS to GRE key.

7.1 Secure Tunnel Management

7.1.1 IP-Sec Encapsulation

IPsec encapsulation SHALL be applied for transport of user payload on the secure tunnel over the path between WFAP and Se-GW. The encapsulation SHALL be done in accordance to IPsec ESP tunnel [10].

7.2 User Data Delivery over R6-F

The data plane protocol stack is shown in Figure 7-1. In the event that the DP goes over an inter-NAP R4 reference point, a secure R4 transport is expected. However, this is not supported and out of scope of this specification.

The R6-F data plane has two parts:

- a) From WFAP to Se-GW: R6-F over secure tunnel: This uses GRE over IPsec
- b) From Se-GW to Fe-GW: R6-F: This uses GRE over IP

The GRE tunnel format same as the baseline scenario [2].

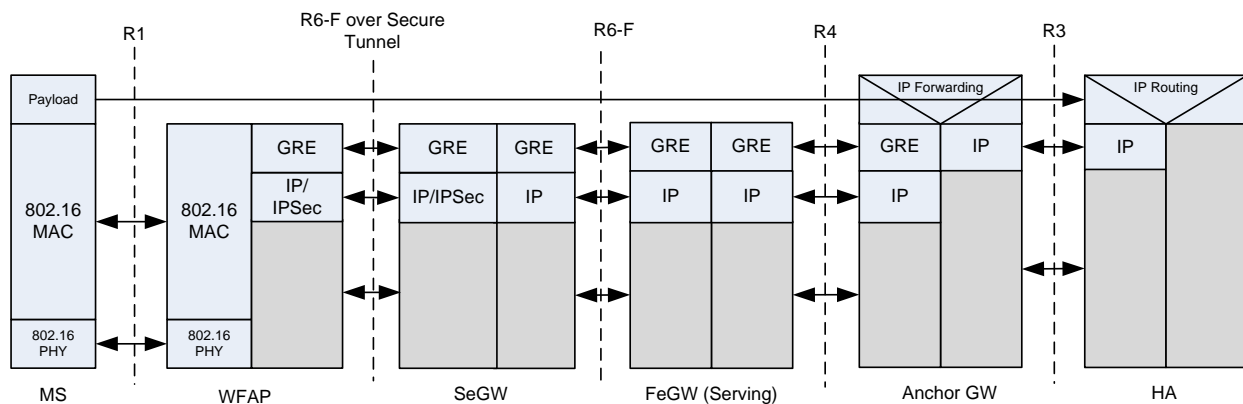


Figure 7-1: Data plane protocol stack over R6-F