

3GPP2 A.S0024-0 v1.0

March 2010



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Interoperability Specification (IOS) for Femtocell Access Points

© 2010, 3GPP2

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

Revision History

Date	Revision	Description
January 2010	A.S0024-0 v1.0	Initial revision. For features supported, refer to section 1.1

Table of Contents

1	Table of Contents		
2			
3	Foreword.....	vii	
4	1 Introduction.....	1-1	
5	1.1 Overview.....	1-1	
6	1.1.1 Purpose.....	1-1	
7	1.1.2 Scope.....	1-1	
8	1.1.3 Document Convention.....	1-1	
9	1.2 References.....	1-1	
10	1.2.1 Normative References.....	1-1	
11	1.2.2 Informative References.....	1-3	
12	1.3 Terminology.....	1-3	
13	1.3.1 Acronyms.....	1-3	
14	1.4 Architecture.....	1-4	
15	1.4.1 Femtocell 1x Voice Architecture.....	1-4	
16	1.4.1.1 Femtocell 1x RAN Network Entities.....	1-5	
17	1.4.1.2 Femtocell 1x RAN Interfaces.....	1-5	
18	1.4.2 Femtocell 1x and HRPD Packet Data.....	1-6	
19	1.4.2.1 Femtocell 1x and HRPD RAN Packet Data Network Entities.....	1-6	
20	1.4.2.2 Femtocell 1x and HRPD RAN Packet Data Interfaces.....	1-7	
21	1.4.3 HRPD LIPA.....	1-7	
22	1.4.3.1 Local IP Access Interfaces.....	1-8	
23	1.5 IOS Femtocell Assumptions.....	1-8	
24	1.6 Feature Descriptions.....	1-9	
25	1.6.1 Explicitly Supported Features.....	1-9	
26	1.6.1.1 1x Idle Handoff Between the Macro BS and the FAP.....	1-9	
27	1.6.1.2 1x Active Handoff Between the Macro BS and the FAP.....	1-9	
28	1.6.1.3 HRPD Dormant Handoff Between the Macro AN/PCF and the FAP.....	1-9	
29	1.6.1.4 Connected State Session Transfer from the FAP to Macro AN.....	1-9	
30	1.6.1.5 LIPA Session Establishment and Termination.....	1-9	
31	1.6.1.6 Femtocell Access Control.....	1-9	
32	2 Requirements and Procedures.....	2-1	
33	2.1 Femtocell Requirements.....	2-1	
34	2.1.1 Security Association for 1x and HRPD Packet Data Femtocells.....	2-1	
35	2.2 1x Packet Data Support.....	2-1	
36	2.3 Femtocell Access Control.....	2-1	

1	2.3.1	Access Control Enforcement Points	2-1
2	2.3.2	Access Control List.....	2-1
3	2.3.3	HRPD Femtocell Access Control	2-1
4	2.3.3.1	AN-AAA as HRPD Enforcement Point.....	2-2
5	2.4	A12 RADIUS Attribute Definition	2-2
6	2.4.1	Local-IP-Access-Authorized.....	2-2
7	2.4.2	Femtocell-Access-Control-Authorization.....	2-3
8	2.5	LIPA Requirements and Procedures	2-3
9	2.5.1	LIPA Protocol Reference Model	2-3
10	2.5.2	AN-PPP Session	2-4
11	2.5.2.1	Establishment.....	2-5
12	2.5.2.2	Authentication.....	2-5
13	2.5.2.3	Termination.....	2-5
14	2.5.2.4	AN-AAA Support	2-5
15	2.5.3	Addressing with IPCP.....	2-5
16	2.5.3.1	IPv4 Addressing.....	2-5
17	2.5.3.2	IPv6 Addressing.....	2-6
18	2.5.3.2.1	Stateless DHCPv6 Support.....	2-7
19	2.5.4	PPP Framing	2-8
20	2.5.5	Ingress Address Filtering at the FAP	2-8
21	2.5.6	Egress Address Filtering/Routing at the AT	2-8
22	3	Femtocell Interfaces.....	3-1
23	3.1	FGW and RAN Interfaces.....	3-1
24	3.2	FAP to Core Network Interface	3-1
25	3.2.1	A1 Formatted Messages Used on Fx2	3-1
26	3.2.1.1	Measurement Procedures	3-1
27	3.2.1.1.1	Measurement Request.....	3-1
28	3.2.1.1.1.1	Successful Operation	3-1
29	3.2.1.1.1.2	Failure Operation.....	3-2
30	3.2.1.1.2	Measurement Response	3-2
31	3.2.1.1.2.1	Successful Operation	3-2
32	3.2.1.1.2.2	Failure Operation.....	3-3
33	3.2.1.1.3	Femtocell Supplementary Info	3-3
34	3.2.1.1.3.1	Successful FCS Operation	3-3
35	3.2.1.1.3.2	Successful FAP Operation.....	3-3
36	3.2.1.1.3.3	Failure Operation.....	3-3

1	3.2.1.2	Message Formats	3-3
2	3.2.1.2.1	Measurement Request.....	3-3
3	3.2.1.2.2	Measurement Response	3-7
4	3.2.1.2.3	Femtocell Supplementary Info	3-9
5	3.2.1.3	Information Element Definitions	3-11
6	3.2.1.3.1	A1 Information Element Identifiers.....	3-11
7	3.2.1.3.2	Message Type	3-11
8	3.2.1.3.3	Long Code	3-12
9	3.2.1.3.4	Cause	3-12
10	3.2.1.3.5	Measurement Response Options	3-15
11	3.2.1.3.6	Measurement Report.....	3-15
12	3.2.1.3.7	Global RAND Key	3-16
13	3.2.1.3.8	Pilot List	3-16
14	3.2.1.3.9	Nonce.....	3-17
15	3.2.1.4	Timer Definitions.....	3-17
16	3.2.1.4.1	T _{mr-1}	3-18
17	3.3	FAP RAN Interfaces	3-18
18	3.3.1	A10/A11 (PCF - PDSN) Interface	3-18
19	3.3.2	A12 (AN/PCF - AN-AAA) Interface.....	3-18
20	3.3.3	A13 (AN/PCF – AN/PCF) Interface.....	3-18
21	3.3.3.1	HRPD Dormant Handoff from FAP to Macro AN/PCF.....	3-18
22	3.3.4	A16 (AN - AN) Interface	3-18
23	3.3.4.1	Connected-State Handoff from FAP to a Macro AN.....	3-18
24	3.3.5	A24 AN/PCF - AN/PCF (IP Tunneling) Interface.....	3-18
25	4	FAP Call Flows.....	4-1
26	4.1	FAP Operation	4-1
27	4.1.1	FAP Power-up.....	4-1
28	4.2	MS/AT Operation	4-1
29	4.2.1	MS/AT Power-up at the FAP.....	4-1
30	4.2.2	MS Registration and Paging at the FAP	4-2
31	4.2.3	1x Handoff	4-2
32	4.2.3.1	1x Macro BS to FAP Dormant Handoff (Intra-PDSN).....	4-2
33	4.2.3.2	1x Macro BS to FAP Dormant Handoff (Inter-PDSN).....	4-3
34	4.2.3.3	1x FAP to Macro BS Dormant Handoff	4-5
35	4.2.3.4	1x Macro BS to FAP Active Handoff.....	4-5
36	4.2.3.5	1x FAP to Macro BS Active Handoff.....	4-7

1	4.2.4	HRPD Handoff	4-9
2	4.2.4.1	HRPD Macro AN/PCF to FAP Dormant Handoff.....	4-9
3	4.2.4.2	HRPD FAP to Macro AN/PCF Dormant Handoff.....	4-9
4	4.2.4.3	HRPD Macro AN/PCF to FAP Connected State Session Transfer	4-11
5	4.2.4.4	HRPD FAP to Macro AN/PCF Connected State Session Transfer	4-11
6	4.3	LIPA Session Establishment between FAP and AT	4-11
7	4.3.1	Successful LIPA Session Establishment.....	4-11
8	4.3.2	LIPA not Supported at the AT	4-13
9	4.3.3	LIPA Terminated after Handoff.....	4-14
10			

Table of Figures

1		
2		
3	Figure 1.4.1-1	Femtocell 1x Voice Architecture.....1-5
4	Figure 1.4.2-1	Femtocell 1x Packet Data Architecture1-6
5	Figure 1.4.2-2	Femtocell HRPD Packet Data Architecture1-6
6	Figure 1.4.3-1	LIPA Bearer and Interfaces1-8
7	Figure 2.4-1	3GPP2 RADIUS Attribute Format2-2
8	Figure 2.5.1-1	HRPD LIPA Protocol Reference Model.....2-4
9	Figure 2.5.6-1	IPCP Vendor Specific Option.....2-8
10	Figure 2.5.6-2	Value(s) Field for the IPv4 Packet Filter Criteria.....2-9
11	Figure 2.5.6-3	Value(s) Field for the IPv6 Packet Filter Criteria.....2-9
12	Figure 4.1.1-1	FAP Power-up4-1
13	Figure 4.2.3.1-1	1x Macro BS to FAP Dormant Handoff (Intra-PDSN)4-2
14	Figure 4.2.3.2-1	1x Macro BS to FAP Dormant Handoff (Inter-PDSN)4-4
15	Figure 4.2.3.4-1	1x Macro BS to FAP Active Handoff.....4-6
16	Figure 4.2.3.5-1	1x FAP to Macro BS Active Handoff.....4-8
17	Figure 4.2.4.2-1	HRPD FAP to Macro AN/PCF Idle Handoff4-10
18	Figure 4.3.1-1	Successful LIPA Session Establishment4-12
19	Figure 4.3.2-1	LIPA not Supported by AT: Session Establishment Failure4-13
20	Figure 4.3.3-1	LIPA Terminated After Handoff4-14
21		

Table of Tables

1
2
3
4
5
6
7
8

Table 3.2.1.3.2-1 BSMAP Messages3-12
Table 3.2.1.3.4-1 Cause Class Values.....3-13
Table 3.2.1.3.4-2 Cause Values3-13
Table 3.2.1.4-1 Timer Values and Ranges Sorted by Name3-18

1 **Foreword**

2 The foreword is not part of this standard.

3 This document describes the protocols and procedures to support femtocell access points (FAPs) in the
4 Radio Access Network (RAN).

5

6

1
2
3
4

(This page intentionally left blank)

1 Introduction

This document contains the procedures, call flows and message descriptions associated with Femtocell Access Point (FAP) support in the access network.

1.1 Overview

This document includes a description of the interface protocols and procedures to support the following features and functions.

Features and functions explicitly supported in this standard:

- Femtocell power-up
- 1x dormant handoff between the macro AN and the FAP
- 1x active handoff between the macro AN and the FAP
- High Rate Packet Data (HRPD) idle handoff between the macro AN and the FAP
- HRPD connected state session transfer from the FAP to the macro AN
- Local IP Access (LIPA) for the HRPD FAP providing AT access to the local IP network.

1.1.1 Purpose

The purpose of this document is to provide a standard and call flows for the femtocell interfaces within the Radio Access Network (RAN).

1.1.2 Scope

This document provides an interoperability specification for a RAN that supports femtocell operation. This document contains message procedures and formats necessary to obtain this interoperability.

1.1.3 Document Convention

“Shall” and “shall not” identify requirements to be followed strictly to conform to the standard and from which no deviation is permitted. “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or (in the negative form) that a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the standard. “Can” and “cannot” are used for statements of possibility and capability, whether material, physical, or causal.

1.2 References

References are either normative or informative. A normative reference is used to include another document as a mandatory part of a 3GPP2 specification. Documents that provide additional non-essential information are included in the informative references section.

1.2.1 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based upon this document are encouraged to investigate the possibility of applying the most recent editions published by them.

- 1 [1] **3GPP2:** A.S0008-C v2.0, *Interoperability Specification (IOS) for High Rate Packet Data*
2 *(HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, January,
3 2009.
- 4 [2] **3GPP2:** A.S0009-C v2.0, *Interoperability Specification (IOS) for High Rate Packet Data*
5 *(HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function*,
6 January 2009.
- 7 [3] **3GPP2:** A.S0013-D v2.0, *Interoperability Specification (IOS) for cdma2000 Access Network*
8 *Interfaces - Part 3 Features*, August 2009.
- 9 [4] **3GPP2:** A.S0014-D v2.0, *Interoperability Specification (IOS) for cdma2000 Access Network*
10 *Interfaces – Part 4 (A1, A1p, A2, and A5 Interfaces)*, August 2009.
- 11 [5] **3GPP2:** A.S0017-D v2.0, *Interoperability Specification (IOS) for cdma2000 Access Network*
12 *Interfaces – Part 7 (A10 and A11 Interfaces)*, August 2009.
- 13 [6] **3GPP2:** C.S0005-E v1.0, *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread*
14 *Spectrum Systems*, June 2009.
- 15 [7] **3GPP2:** C.S0024-B v2.0, *cdma2000 High Rate Packet Data Air Interface Specification*, April
16 2007.
- 17 [8] **3GPP2:** S.S0132-0 v1.0, *Femtocell Security Framework*, December 2009.
- 18 [9] **3GPP2:** X.S0004-E v7.0, *Mobile Application Part (MAP)*, April 2008.
- 19 [10] **3GPP2:** X.S0011-E v1.0, *Wireless IP Network Standard*, November 2009.
- 20 [11] **3GPP2:** X.S0059-0-000 v1.0, *Femtocell Network Overview*, January 2010.
- 21 [12] **3GPP2:** X.S0059-0-100 v1.0, *Femtocell Network Specification*, January 2010.
- 22 [13] **3GPP2:** X.S0059-0-200 v1.0, *CDMA2000 1x/IMS Femtocell Network Specification*, January
23 2010.
- 24 [14] **IETF:** RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*, May 1992.
- 25 [15] **IETF:** RFC 1334, *PPP Authentication Protocols*, October 1992.
- 26 [16] **IETF:** RFC 1661, *Point-to-Point Protocol*, July 1994.
- 27 [17] **IETF:** RFC 1662, *PPP in HDLC-Like Framing*, July 1994.
- 28 [18] **IETF:** RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server*
29 *Addresses*, December 1995.
- 30 [19] **IETF:** RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, August 1996.
- 31 [20] **IETF:** RFC 2153, *PPP Vendor Extensions*, May 1997.
- 32 [21] **IETF:** RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, December 1998.
- 33 [22] **IETF:** RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*, December 1998.
- 34 [23] **IETF:** RFC 2462, *IPv6 Stateless Address Auto-configuration*, December 1998.
- 35 [24] **IETF:** RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol*
36 *Version 6 (IPv6) Specification RFC 2463*, December 1998.
- 37 [25] **IETF:** RFC 2472, *IP Version 6 over PPP*, December 1998.
- 38 [26] **IETF:** RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, June 2000.
- 39 [27] **IETF:** RFC 3513, *IP Version 6 Addressing Architecture*, April 2003.
- 40 [28] **IETF:** RFC 3587, *IPv6 Global Unicast Address Format*, August 2003.

1 [29] **IETF:** RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6*
 2 (*DHCPv6*), December 2003.

3 [30] **IETF:** RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*,
 4 April 2004.

5 **1.2.2 Informative References**

6 [I-1] **3GPP2:** X.R0063-0 v1.0, *3GPP2 Femtocell Configuration Parameters*.

8 **1.3 Terminology**

10 **1.3.1 Acronyms**

3GPP2	3 rd Generation Partnership Project 2
ACL	Access Control List
AN	Access Network
AAA	Authentication, Authorization and Accounting
AT	Access Terminal
BS	Base Station
BSMAP	Base Station Mobile Application Part
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
CVSE	Critical Vendor Specific Extension
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESN	Electronic Serial Number
FACDIR2	Facility Directive 2
FAP	Femtocell Access Point
FCS	Femtocell Convergence Server
FEID	Femtocell Equipment Identifier
FGW	Femtocell Gateway
FMS	Femtocell Management System
HDLC	High-Level Data Link Control
HRPD	High Rate Packet Data
IE	Information Element
IID	Interface-Identifier
IMS	IP Multimedia Subsystem
IOS	Interoperability Specification
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

kbps	kilobit per second
LCP	Link Control Protocol
LIPA	Local IP Access
MGW	Media Gateway
MS	Mobile Station
MSC	Mobile Switching Center
MSCe	Mobile Switching Center Emulation
NVSE	Normal Vendor Specific Extension
OUI	Organizationally Unique Identifier
PAP	Password Authentication Protocol
PCF	Packet Control Function
PCM	Pulse Code Modulation
PDSN	Packet Data Serving Node
PLCM	Public Long Code Mask
PPP	Point to Point Protocol
RA	Router Advertisement
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RFC	Request for Comments
RS	Router Solicitation
RTP	Real-time Transport Protocol
SC/MM	Session Control / Mobility Management
SeGW	Security Gateway
SIP	Session Initiation Protocol
UATI	Unicast Access Terminal Identifier
VSA	Vendor Specific Attribute
VoIP	Voice over IP

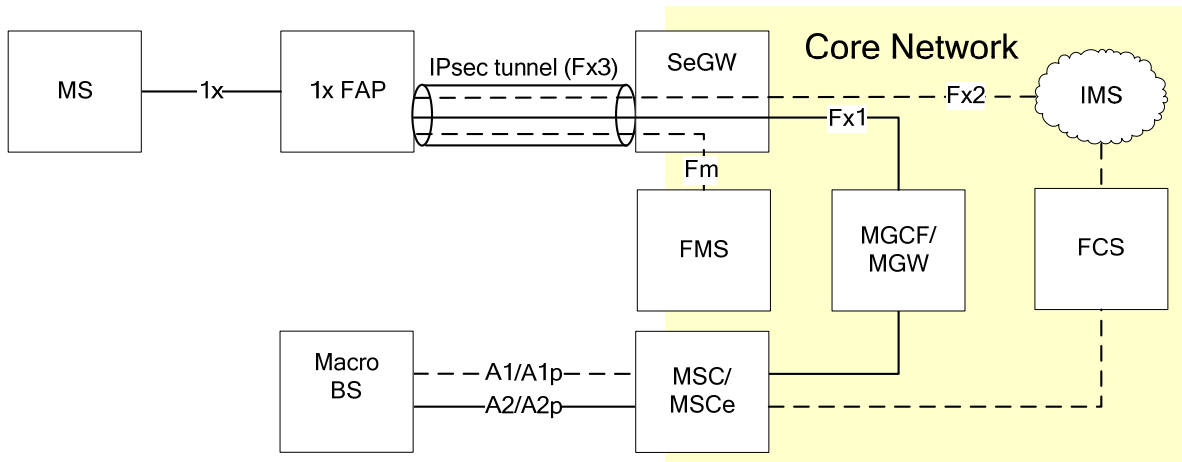
1

2 **1.4 Architecture**

3 1x and HRPD femtocell IOS and HRPD LIPA messaging and call flows are based on the architecture
4 reference models shown in this section. In the figures, solid lines indicate signaling and bearer and dashed
5 lines indicate only signaling.

6 **1.4.1 Femtocell 1x Voice Architecture**

7 Figure 1.4.1-1 shows the RAN reference architecture for 1x voice access from a FAP. For voice, the 1x
8 signaling and user plane packets are converted at the FAP to Session Initiation Protocol (SIP) and Voice
9 over IP (VoIP) traffic respectively.



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
26
27
28
29
30

Figure 1.4.1-1 Femtocell 1x Voice Architecture

1.4.1.1 Femtocell 1x RAN Network Entities

The entities identified in Figure 1.4.1-1 are defined as follows.

- BS The macro base station (BS) is an entity in the public radio telecommunications system used for radio telecommunications with MSs.
- FAP The Femtocell Access Point (FAP) is a wireless access point operating in licensed spectrum to connect a mobile station (MS) to the operator's network through the public Internet infrastructure. In 1x, this entity enables access to 1x voice users by providing a conversion function between 1x voice and IP Multimedia Subsystem (IMS)-based VoIP traffic and signaling.
- MS The mobile station (MS) is an entity in the public cellular radio telecommunications service intended to be used while in motion or during halts at unspecified points.
- MSC/MSCe The Mobile Switching Center (MSC) may be either a circuit-switched MSC or an IP based MSCe (emulation) and provides processing and control for calls and services. Refer also to X.S0004 [9].
- SeGW The Security Gateway (SeGW) is an entity residing in an operator's network that provides for secure access for the FAP to network operator services. Refer to X.S0059-000 [11].

Core network entities are defined in X.S0059-000 [11].

1.4.1.2 Femtocell 1x RAN Interfaces

The interfaces identified in Figure 1.4.1-1 are defined as follows.

- 1x For details on the air interface, refer to C.S0005 [6].
- A1 This interface carries signaling information between the mobility management functions of the circuit-switched MSC and the call control component of the macro BS.
- A1p This interface carries signaling information between the mobility management functions of the MSCe and the call control component of the macro BS.
- A2 This interface is used to provide a path for user traffic. The A2 interface carries 64/56 kbps PCM information (for circuit-oriented voice) or 64 kbps Unrestricted Digital Information (UDI, for ISDN) between the circuit-switched MSC and the BS.

- 1 A2p This interface provides a path for packet-based user traffic sessions. The A2p interface
- 2 carries voice information via IP packets between the Media Gateway (MGW) and the BS.
- 3 Fx1 For details on the bearer interface between the FAP and the MGW, refer to X.S0059-000
- 4 [11].
- 5 Fx2 For details on the signaling interface between the FAP and the IMS, refer to X.S0059-000
- 6 [11].
- 7 Fx3 IPsec tunnel between the FAP and the SeGW. Refer to X.S0059-000 [11].
- 8 Fm The Fm interface enables auto-configuration of the FAP by the FMS. Refer to X.R0063
- 9 [I-1] and X.S0059-000 [11].

1.4.2 Femtocell 1x and HRPD Packet Data

11 Figure 1.4.2-1 shows the reference architecture for 1x packet data access from a FAP. Figure 1.4.2-2

12 shows the reference architecture for HRPD packet data access from a FAP.

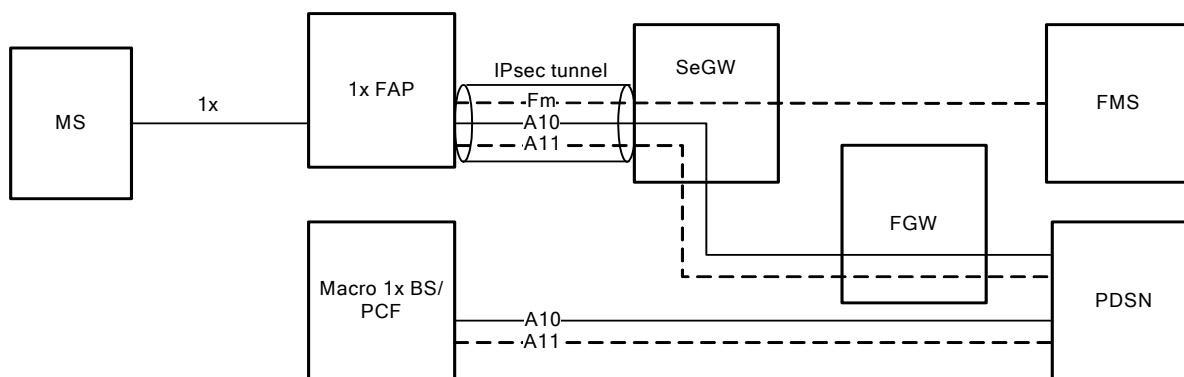


Figure 1.4.2-1 Femtocell 1x Packet Data Architecture

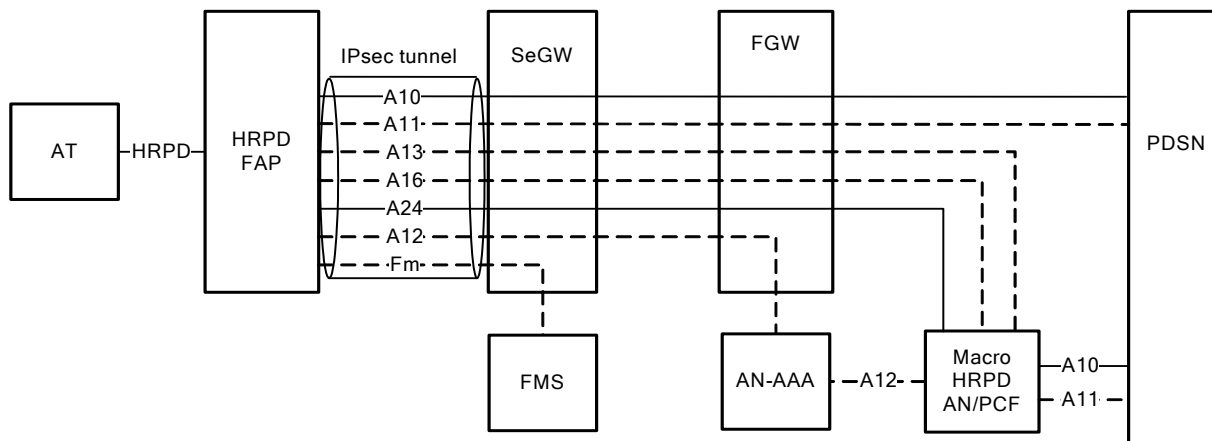


Figure 1.4.2-2 Femtocell HRPD Packet Data Architecture

1.4.2.1 Femtocell 1x and HRPD RAN Packet Data Network Entities

18 The entities identified in Figure 1.4.2-1 and Figure 1.4.2-2 are defined as follows.

- 19 AN The Access Network is a logical entity in the HRPD RAN used for radio communications
- 20 with the AT.
- 21 AN-AAA The AN Authentication, Authorization and Accounting server performs access
- 22 authentication and LIPA authorization functions for the RAN.

1	AT	The Access Terminal (AT) is a device providing data connectivity to a user.
2	BS	The macro base station is an entity in the public radio telecommunications system used
3		for radio telecommunications with MSs.
4	FAP	The Femtocell Access Point (FAP) is a wireless access point operating in licensed
5		spectrum to connect an AT to the operator's network through the public Internet
6		infrastructure.
7	FGW	The Femtocell Gateway (FGW) is an entity residing in an operator's network that
8		provides aggregation and proxy functions for the FAP to access network operator
9		services.
10	FMS	The Femtocell Management System (FMS) is a network entity residing in an operator's
11		network that aids in FAP auto-configuration before FAP can provide services.
12	MS	The mobile station is an entity in the public cellular radio telecommunications service
13		intended to be used while in motion or during halts at unspecified points.
14	PCF	The Packet Control Function (PCF) is an entity in the RAN that manages the relay of
15		packets between the BS or AN and the PDSN.
16	PDSN	The Packet Data Serving Node (PDSN) is an entity that routes MS/AT originated or
17		MS/AT terminated packet data traffic. A PDSN establishes, maintains and terminates link
18		layer sessions to MS/ATs.
19	SeGW	The Security Gateway (SeGW) is a network entity residing in an operator's network that
20		provides secure access for the FAP to the operator's network. Refer to X.S0059-000 [11].

21 **1.4.2.2 Femtocell 1x and HRPD RAN Packet Data Interfaces**

22 The interfaces identified in Figure 1.4.2-1 and Figure 1.4.2-2 are defined as follows.

23	1x	For details on the air interface, refer to C.S0005 [6].
24	A10	This interface carries user traffic between the FAP and the PDSN or between the PCF
25		and the PDSN.
26	A11	This interface carries signaling information between the FAP and the PDSN or between
27		the PCF and the PDSN.
28	A12	This interface carries signaling information related to access authentication between the
29		FAP or the AN/PCF and the AN-AAA.
30	A13	This interface carries signaling information between the Session Control / Mobility
31		Management (SC/MM) function in the macro AN/PCF and the SC/MM function in the
32		FAP for idle state session transfer and inter-AN paging when the AT is in idle state.
33	A16	This interface carries signaling information between the macro AN and the FAP for
34		HRPD inter-AN connected state session transfer (hard handoff).
35	A24	This interface carries buffered user data between the macro AN/PCF and the FAP for an
36		AT, during A13 session transfer.
37	Fm	The Fm interface enables auto-configuration of the FAP by the FMS. Refer to X.R0063
38		[I-1] and X.S0059-000 [11].
39	HRPD	For details on the air interface, refer to C.S0024 [7].

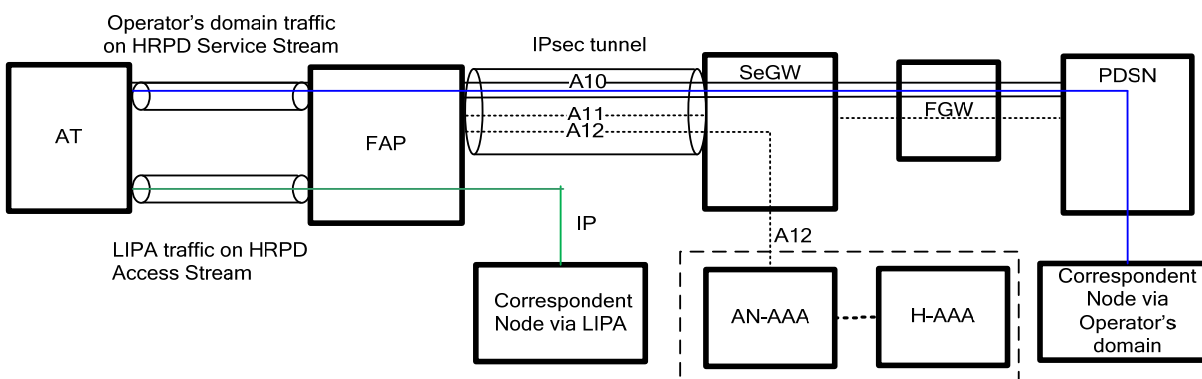
40 **1.4.3 HRPD LIPA**

41 LIPA at the HRPD FAP provides for IP connectivity to allow an AT to access either local IP networks or
42 Internet through the local interface. For LIPA, the AT connects through the FAP to the local network by

1 configuring an additional IP interface on the existing HRPD access stream. At the same time, the AT
 2 still have IP connectivity to the operator's IP domain via the PDSN. In this model, the AT can have
 3 connectivity with:

- 4 • Correspondent Node via LIPA in the same subnet with the FAP. LIPA to the home intranet allows an
 5 AT to communicate with local services (e.g., a local server).
- 6 • Correspondent Node via the operator's domain. Access to the private IP domain of the operator. The
 7 AT can still use the IP service provided by the PDSN. Therefore, the AT can access all services
 8 available on the macro network while simultaneously accessing the home intranet.
- 9 • Correspondent Node in the Internet. The Internet may be reached either on the local IP interface or
 10 through the PDSN IP interface. The operator may configure the FAP and the AT to use the local IP
 11 interface for internet communications.

12 Figure 1.4.3-1 shows the bearer and interfaces related to LIPA.



13
 14 **Figure 1.4.3-1 LIPA Bearer and Interfaces**

15 1.4.3.1 Local IP Access Interfaces

16 The AN-AAA may be used to authorize an AT for LIPA service during HRPD access or terminal
 17 authentication on the A12 interface. For LIPA authorization, the AN-AAA may access the Home AAA
 18 for authorization information; however this interface is outside the scope of this specification.

19 1.5 IOS Femtocell Assumptions

20 The following assumptions apply to this document.

- 21 1. The 1x voice FAP contains a SIP client that converts 1x signaling and user plane packets to/from SIP
 22 signaling and RTP traffic, respectively.
- 23 2. Each FAP connects to one and only one SeGW at a time.
- 24 3. Each FAP connects to one and only one FMS at a time.
- 25 4. Each 1x voice FAP is assigned a Cell_ID of type 07H (refer to A.S0014 [4]). The MSC_ID of the
 26 Cell_ID corresponds to the FCS (Femtocell Convergence Server) to which the FAP communicates.
 27 Refer to X.S0059-200 [13].
- 28 5. The 1x packet data/HRPD FAP contains PCF functionality.
- 29 6. Each FAP communicates with the core network entities in the operator's network through the SeGW.
- 30 7. Any AT that supports HRPD LIPA is capable of supporting multiple simultaneous IP addresses.
- 31 8. The PN offset broadcast by the 1x or HRPD FAP may not be unique; it is possible for multiple FAPs
 32 within the coverage area of a single macro BS/AN to have the same PN offset.
- 33 9. An AN-AAA acting as an enforcement point requires FEID support in the FAP.

1.6 Feature Descriptions

This section describes the features identified in the overview in section 1.1.

1.6.1 Explicitly Supported Features

1.6.1.1 1x Idle Handoff Between the Macro BS and the FAP

This feature supports handoff of an idle MS between the macro BS and the FAP.

1.6.1.2 1x Active Handoff Between the Macro BS and the FAP

This feature supports handoff of an active MS between the macro BS and the FAP.

1.6.1.3 HRPD Dormant Handoff Between the Macro AN/PCF and the FAP

This feature supports handoff of an idle AT between the macro AN/PCF and the FAP.

1.6.1.4 Connected State Session Transfer from the FAP to Macro AN

This feature supports handoff of an active AT from the FAP to macro AN.

1.6.1.5 LIPA Session Establishment and Termination

This feature supports the ability of an AT to perform session establishment with a FAP, establish an AN-PPP session, perform access authentication and then use the AN-PPP session to acquire a locally assigned IP address. The AT can have both a local IP address and an operator assigned IP address acquired over its AN-PPP session and PDSN-PPP session, respectively. The AT can simultaneously use the local IP address over the AN-PPP session and the operator assigned IP address over the PDSN-PPP session. Upon completion of the handoff out of the FAP, the AT and the FAP can each drop the AN-PPP session and release the locally assigned IP address.

1.6.1.6 Femtocell Access Control

This feature allows a FAP to be able to control the MS/ATs that can register or receive services from the FAP. A FAP can be configured to have one of following types of associations.

- Open Association: any MS/ATs can access and receive services from the FAP. However, LIPA service may be further controlled by AN-AAA.
- Signaling Association: any MS/ATs can access and register with the FAP, i.e., the MS/ATs are reachable/pageable. However, the MS/ATs that are not on the access control list (ACL) may be redirected to macro BS or AN when it attempts to establish a traffic connection.
- Restricted Association: only MS/ATs that are in the ACL are allowed to access or register. The FAP does not complete the registration process of any MS/ATs that are not on the access control list.

This specification explicitly supports the FAP being an enforcement point for 1x MS and HRPD AT where the ACL is provided by the FMS. This specification also explicitly supports the AN-AAA being an enforcement point for the HRPD FAP. Refer to section 2.5.

This specification transparently supports other core network entities being enforcement points for both 1x and HRPD.

Note that emergency services (e.g., global emergency call) may be exempt from femtocell access control, based on operator policy.

1
2
3
4

(This page intentionally left blank)

2 Requirements and Procedures

This section describes the requirements and procedures associated with this specification.

2.1 Femtocell Requirements

This section describes the requirements associated with this specification.

2.1.1 Security Association for 1x and HRPD Packet Data Femtocells

The 1x or HRPD packet data FAP shall maintain a security context for the PDSN to which it is attached. This context consists of an authentication algorithm and mode, a secret (shared key or appropriate public/private key pair), and a style of replay protection in use. This context is used to populate the Mobile-Home Authentication Extension and Registration Update Authentication Extension Information Elements (IEs). Refer to A.S0017 [5] for more information.

2.2 1x Packet Data Support

Upon receiving a 1x Origination or Enhance 1x Origination message from the MS with the service option set to 0x21H (i.e., SO 33), the FAP may acknowledge the message from the MS as described in C.S0005 [6]. If the FAP acknowledges the 1x origination and the MS is already 1x registered via the FAP, the FAP shall establish or perform service option negotiation procedures over the traffic channel (to support SO 33) with the MS directly and follow the BS procedures defined in A.S0017 [5] for setup of the A10 with the PDSN. Otherwise, if the MS is not registered via the FAP, the FAP shall perform the MS registration procedures as specified in X.S0059-200 [13] and after successful registration, establish the traffic channel (to support SO 33) with the MS directly and follow the BS procedures in A.S0017 [5] for setup of the A10 with the PDSN.

2.3 Femtocell Access Control

This section describes the requirements and procedures to support Femtocell Access Control (FAC).

2.3.1 Access Control Enforcement Points

The access control enforcement point performs a comparison between the identity of the MS/AT and the authorized identities in ACL and may subsequently deny services to MS/ATs not present on the ACL.

This specification explicitly supports the FAP being an enforcement point for 1x MS and HRPD AT where the ACL is provided by the FMS. This specification also explicitly supports the AN-AAA being an enforcement point for the HRPD FAP.

2.3.2 Access Control List

An ACL consists of the list of MSs or ATs that are allowed access on the FAP. Each entry in the ACL contains an identity of either an MS or an AT. For example, the identity can be one of the following IMSI, MEID, ESN, or NAI used in the CHAP response on the access stream. The FAP requirements and procedures when an MS or AT outside of the ACL tries to access the FAP are based on its association type described in section 1.6.1.6 and is outside the scope of this specification.

A FAP may be configured with the ACL and its association type by the FMS (refer to X.R0063 [I-1]).

2.3.3 HRPD Femtocell Access Control

For the HRPD FAP, the FAP, the AN-AAA, or both may be the FAC enforcement point.

2.3.3.1 AN-AAA as HRPD Enforcement Point

When the AN-AAA is to perform the FAC enforcement point function, it associates the ACL with the FAP through its Femtocell Equipment Identifier (FEID). If an FEID is supported in the FAP, then the FAP shall also include the FEID in the Access-Request message sent on the A12 interface.

When the AT returns a CHAP response message (refer to Section 3.1.1 in A.S0008 [1], or A.S0009 [2]), the FAP forwards the response along with its FEID in an Access-Request message to the AN-AAA on the A12 interface. Refer to section 3.3.2 for A12 interface procedures. The AN-AAA, in addition to performing access or terminal authentication, verifies through the HRPD ACL that the AT is authorized to receive services through the FAP. If the AT passes authentication and is allowed to receive services through the FAP, the AN-AAA returns an Access-Accept message on the A12 interface in accordance with RFC 2865 [26]. However if the AT passes authentication and is not allowed to receive services through the FAP (e.g., the AT is not in the FAP ACL), the AN-AAA returns an Access-Accept message on the A12 interface (in accordance with RFC 2865 [26]) including the Femtocell-Access-Control-Authorization attribute. Refer also to section 2.4.2. Otherwise, if the AT fails authentication, the AN-AAA sends an Access-Reject message on the A12 interface in accordance with RFC 2865 [26].

2.4 A12 RADIUS Attribute Definition

This section defines the 3GPP2 vendor specific attribute for FAP support in this specification. The general Vendor Specific Format is shown in Figure 2.4-1. The type and vendor ID are the same for every attribute. The vendor-ID of 5535 (159FH) is used to indicate 3GPP2. Note that all integers are in network byte order.

1												2												3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1				
Type												Length												Vendor-ID											
Vendor-ID (cont)												Vendor-Type												Vendor-Length											
Vendor-Value																																			

Figure 2.4-1 3GPP2 RADIUS Attribute Format

Values for the corresponding fields are defined in the following attribute sections.

2.4.1 Local-IP-Access-Authorized

The Local-IP-Access-Authorized VSA indicates if the AT is authorized to use LIPA (i.e., receive a local IP address from the FAP). This attribute, shown Figure 2.4-1, may be included in the RADIUS Access-Accept message sent from the AN-AAA to the FAP on the A12 interface.

Type: 26

Length: 12

Vendor ID: 5535

Vendor-Type: 208

Vendor-Length: 6

Vendor-Value:

0: AT is not authorized to be assigned a local IP address.

1: AT is authorized to be assigned a local IP address.

All other values are reserved.

2.4.2 Femtocell-Access-Control-Authorization

The Femtocell-Access-Control-Authorization VSA contains information related to femtocell access control authorization. This attribute, shown in Figure 2.4-1, may be included in the RADIUS Access-Accept message, sent from the AN-AAA to the FAP on the A12 interface.

Type: 26

Length: 12

Vendor ID: 5535

Vendor-Type: 217

Vendor-Length: 6

Vendor-Value:

0: AT is in the access control list of the femtocell.

1: AT is not in the access control list of the femtocell.

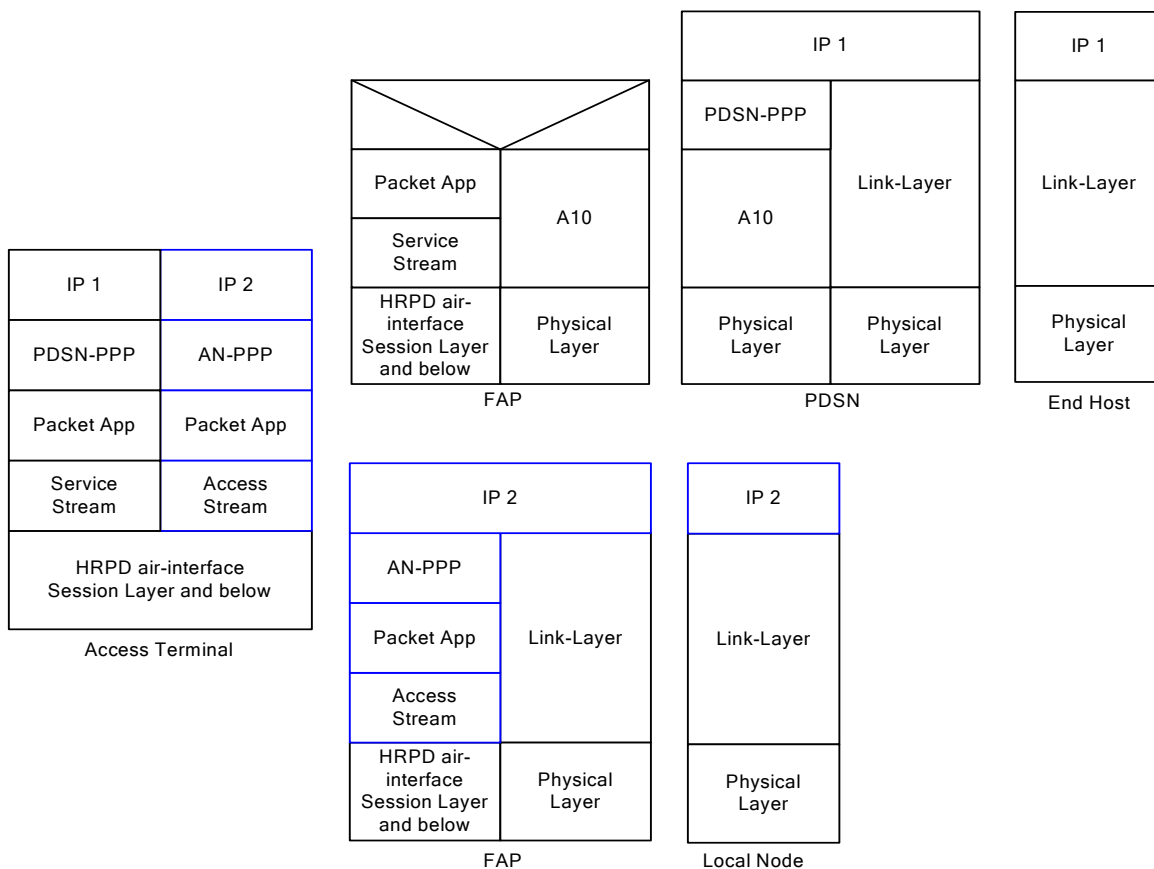
All other values are reserved.

2.5 LIPA Requirements and Procedures

This section describes the requirements and procedures for simple IP operation to support LIPA. In this context, simple IP refers to a service in which an AT is assigned either an IPv4 address or an IPv6 prefix and is provided IP routing service by the FAP. If LIPA is supported, the AT shall support two IP interfaces and the FAP shall support allocating an IP address to the AT. Note that an AT that only supports a single IP interface can still connect to a FAP that supports LIPA.

2.5.1 LIPA Protocol Reference Model

The following figure shows the protocol reference model for supporting LIPA at an HRPD FAP.



1
2
3
4
5
6
7
8
9

Figure 2.5.1-1 HRPD LIPA Protocol Reference Model

When LIPA is supported, there are two IP addresses allocated to the AT.

- The PDSN-PPP session (IP 1) for network operator connectivity is established on the service stream and the A10 interface carries user traffic between the FAP and the PDSN. Refer to A.S0008 [1] and A.S0009 [2].
- The AN-PPP session (IP 2) for LIPA connectivity is established on the access stream. Refer to section 2.5.2.

2.5.2 AN-PPP Session

PPP shall be the data link protocol between the AT and the FAP. This PPP session is referred to as AN-PPP. The AN-PPP session shall be established prior to any IP datagram being exchanged between the AT and the FAP. Only one AN-PPP session shall be supported between the AT and the FAP. If access authentication is performed, LIPA shall reuse the AN-PPP session that is established between the AT and the FAP for access authentication (refer to A.S0008 [1] and A.S0009 [2]). If access authentication is not performed, the FAP shall establish an AN-PPP session without specifying either CHAP or PAP as a PPP option in an initial LCP Configure-Request during the PPP establishment. PPP shall be supported as defined in the following standards with any limitations or extensions described in this document.

- Point to Point Protocol (RFC 1661 [16]);
 - PPP in HDLC-like Framing (RFC 1662 [17]);
 - IPCP (RFC 1332 [14]) for IPv4;
 - IPv6CP (RFC 2472 [25]) for IPv6;
 - CHAP (RFC 1994 [19]);
 - PAP (RFC 1334 [15]).
- 10
11
12
13
14
15
16
17
18
19
20
21
22
23

1 **2.5.2.1 Establishment**

2 After the AT indicates it is ready to exchange data on the access stream, the FAP shall initiate PPP
3 procedures according to RFC 1661 [16] by sending an LCP Configure-Request to the AT. PPP shall
4 support transparency in accordance with section 4.2 of RFC 1662 [17]. The FAP and AT shall attempt to
5 negotiate a control character mapping, with the minimum number of escape characters by proposing an
6 Async-Control-Character-Map (ACCM) of 0x00000000.

7 Additionally, the FAP may establish an AN-PPP session with the AT at any time (e.g., following session
8 transfer to the FAP).

9 **2.5.2.2 Authentication**

10 The AT shall support CHAP for the PPP instance on the access stream. If the FAP supports access
11 authentication, the FAP shall support CHAP for the PPP instance on the access stream. In this case, the
12 FAP shall always propose CHAP as a PPP option in an initial LCP Configure-Request during the PPP
13 establishment.

14 **2.5.2.3 Termination**

15 If the FAP does not support LIPA, the FAP may release the PPP connection after the access
16 authentication of the AT has been performed. If the FAP supports LIPA, then it proceeds to the IPCP
17 phase as described in section 2.5.3.

18 The FAP and the AT should support PPP link status determination as specified in Section 3.2.1.10 of
19 X.S0011-002 [10] on the AN-PPP. The FAP shall close the PPP session when the Max PPP Inactivity
20 Timer expires.

21 The FAP shall terminate the PPP session with the AT when the HRPD session for the AT is terminated.
22 The AT shall locally terminate its PPP session when the HRPD subnet changes or the HRPD session is
23 terminated.

24 **2.5.2.4 AN-AAA Support**

25 Upon successful access authentication the visited AN-AAA may include the RADIUS attribute “Local-IP
26 Access-Authorized” (refer to section 2.4.1) in an Access-Accept message to the FAP on the A12 interface.
27 The value of the attribute is based on operator policy.

28 **2.5.3 Addressing with IPCP**

29 A FAP shall not assign an IPv4 address or IPv6 Prefix to the AT if the RADIUS attribute, Local-IP-
30 Access-Authorized, from the AN-AAA in section 2.4.1 does not authorize the FAP to do so. A FAP may
31 assign an IPv4 address or IPv6 Prefix to the AT if the RADIUS attribute, Local-IP-Access-Authorized,
32 from the AN-AAA in section 2.4.1 authorizes the FAP to do so. If the RADIUS attribute Local-IP-
33 Access-Authorized is not received by the FAP, the FAP may allocate an IPv4 address or IPv6 prefix to
34 the AT based on its local policy.

35 **2.5.3.1 IPv4 Addressing**

36 The FAP assigns a local IPv4 address to the AT on the AN-PPP via IPCP negotiation by sending an IPCP
37 Configure-Request message. This message includes the FAP’s own IP address. If the AT supports LIPA,
38 the AT shall respond with an IPCP Configure-Ack message upon receipt of the IPCP Configure-Request
39 message.

40 If the AT does not support LIPA, the AT may send an IPCP Configure-Reject or ignore all IPCP packets.

1 Upon responding with an IPCP Configure-Ack to the IPCP Configure-Request from the FAP, the AT
2 may request a NULL or non-zero IPv4 address¹ in its IPCP Configure-Request message. The AT should
3 also include the request for egress packet filter criteria from the FAP in its IPCP Configure-Request
4 message as described in section 2.5.6.

5 If the AT requests a NULL or non-zero IPv4 address, the FAP should assign an IPv4 address to the AT
6 with an IPCP Configure-Nak message. This message shall also include the egress packet filter criteria the
7 AT should use to determine for each IP packet whether it should traverse through the LIPA interface as
8 defined in section 2.5.6.

9 If the AT requests a non-zero IPv4 address during the IPCP phase, and if the FAP is unable to assign the
10 requested address, the FAP shall send an IPCP Configure-Nak containing the new IPv4 address. This
11 message shall also include the egress packet filter criteria the AT should use to determine for each IP
12 packet whether it should traverse through the LIPA interface.

13 The AT should acknowledge the IPv4 address assigned to it and the egress packet filter criteria it should
14 use, in the subsequent IPCP Configure-Request message.

15 If the AT fails to accept the assigned IPv4 address, the FAP shall send an LCP Terminate-Request.

16 The FAP shall implement IPCP configuration options as defined in RFC 1877 [18] for the Domain Name
17 System (DNS) server address negotiation.

18 The FAP shall remove the binding created for this IPv4 address assigned to the AT if either the HRPD
19 session or the AN-PPP session for the AT is terminated.

20 **2.5.3.2 IPv6 Addressing**

21 If IPv6 addressing is supported, both the AT and the FAP shall support the MS-PDSN Version Capability
22 Indication (refer to X.S0011 [10]).

23 If FAP supports IPv6 addressing, the MS-PDSN Version Capability Indication (refer to X.S0011 [10]) is
24 used, and the AT signaled that it does not support Simple IPv6, then the FAP shall not negotiate IPv6CP
25 with the AT and shall not send IPv6 Router Advertisements to the AT.

26 If the MS-PDSN Version Feature Indication is used, and the AT signaled that it supports Simple IPv6 (C2
27 bit set to 1), then the FAP shall provide Simple IPv6 service to the AT as described in the remainder of
28 this section.

29 When IPv6 addressing is being used, the FAP shall be the PPP termination point.

30 If the FAP supports IPv6 addressing, the FAP shall support the following RFCs, with exceptions as noted
31 in this document:

- 32 • An IPv6 Aggregatable Global Unicast Address Format RFC 3587 [28];
- 33 • Internet Protocol, Version 6 (IPv6) Specification RFC 2460 [21];
- 34 • Neighbor Discovery for IP Version 6 (IPv6) RFC 2461 [22];
- 35 • IPv6 Stateless Address Auto-configuration RFC 2462 [23];
- 36 • Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
37 RFC 2463 [24];
- 38 • IP Version 6 over PPP RFC 2472 [25];
- 39 • IP Version 6 Addressing Architecture RFC 3513 [27].

40 The FAP shall perform Interface-Identifier negotiation as described in RFC 2472 [25]. Interface-
41 Identifiers used by the FAP and the AT are configured via IPv6CP. The FAP shall provide to the AT a
42 valid non-zero Interface-Identifier of the FAP in the IPv6CP Configure-Request. The FAP shall provide a

¹ The AT can request a non-zero IP address in case the AT wants to retain the existing local IP address.

1 valid non-zero Interface-Identifier for the AT in IPv6CP Configure-NAK if the AT's proposed IID is not
 2 acceptable to the FAP. While communicating with the AT, the FAP shall use only the link local address
 3 that it constructed with its Interface-Identifier that it provided to the AT (i.e. FAP's Interface-Identifier)
 4 during IPv6CP phase. Because the Interface-Identifier negotiated in the IPv6CP phase of the PPP
 5 connection setup is unique for the AN-PPP connection, it is not required to perform duplicate address
 6 detection for the link local address formed as part of IPv6 stateless address auto-configuration RFC 2462
 7 [23].

8 Following successful IPv6CP negotiation and the establishment of a unique link-local address for both the
 9 FAP and the AT, the FAP shall immediately² transmit initial unsolicited Router Advertisement (RA)
 10 messages on the AN-PPP link using its link-local address as a source address. The FAP shall include a
 11 prefix in the RA message to the AT. The AT uses this prefix to configure its global IPv6 addresses.

12 The FAP shall send unsolicited RA messages for an operator configurable number of times. Also, the
 13 FAP shall set the interval between initial RA messages to an operator configurable value, which may be
 14 less than MAX_INITIAL_RTR_ADVERT_INTERVAL. After the configurable number of initial
 15 unsolicited RA messages has been transmitted, the interval between the periodic transmissions of
 16 unsolicited RA messages shall be controlled by the router configurable parameters MaxRtrAdvInterval
 17 and MinRtrAdvInterval as defined in RFC 2461 [22]. The FAP may set MaxRtrAdvInterval to a value
 18 greater than 1800 seconds and less than 1/3 of the AdvDefaultLifetime. The FAP shall set
 19 MinRtrAdvInterval³ to a fraction of MaxRtrAdvInterval as per RFC 2461 [22].

20 The FAP shall send a RA message in response to a Router Solicitation (RS) message received from the
 21 AT. The FAP may set the delay between consecutive (solicited RA) or (solicited /unsolicited RA)
 22 messages sent to the all-nodes multicast address to a value less⁴ than that specified by the constant
 23 MIN_DELAY_BETWEEN_RAS, contrary to the specification in Section 6.2.6 of RFC 2461 [22].

24 The advertised prefix⁵ identifies the subnet associated with the AN-PPP link. The prefix advertised by the
 25 FAP shall be exclusive to the AN-PPP session.

26 The FAP shall set:

- 27 • the M-flag = 0 in the RA message header;
- 28 • the L-flag = 0 and the A-flag = 1 in the RA message Prefix Information Option.

29 The FAP shall set the Router Lifetime value in the RA message to a value of 216-1 (18.2 hrs).

30 The FAP shall not send any redirect messages to the AT over the AN-PPP interface.

31 2.5.3.2.1 Stateless DHCPv6 Support

32 The FAP shall support Stateless DHCPv6 as specified in RFC 3736 [30], and shall set the O bit to 1 in the
 33 RA messages sent to the AT.

34 Upon receiving a DHCPv6 Information-Request packet from the AT, the FAP shall respond with
 35 Dynamic Host Configuration Protocol (DHCP) Reply message. The FAP should include DNS
 36 configuration options as specified in RFC 3646 [29]).

2 This is an exception to RFC 2461 necessary to optimize applicability over the cdma2000 wireless air-interface.

3 This may cause an exception to RFC 2461 as it may put the interval outside the normal range. This exception is allowed by
 this document to optimize IPv6 RA over the cdma2000 wireless links.

4 This exception is allowed by this document to optimize IPv6 RA over the cdma2000 wireless links.

5 If the network operator desires to reduce frequent unsolicited RA for the prefix, they should set the 32-bit Valid Lifetime
 and Preferred Lifetime fields for the advertised prefix in the RA message Prefix Information Option to a very high value
 (i.e., 0xFFFFFFFF to indicate prefix validity for the lifetime of the PPP session).

2.5.4 PPP Framing

The FAP shall frame PPP packets sent on the PPP link layer using the octet synchronous framing protocol defined in RFC 1662 [17], except that there shall be no inter-frame time fill (refer to Section 4.4.1 of RFC 1662 [17]). I.e., no flag octets shall be sent between a flag octet that ends one PPP frame and the flag octet that begins the subsequent PPP frame. For IPv6, the FAP shall set the MTU size as specified in RFC 2460 [21].

2.5.5 Ingress Address Filtering at the FAP

For each IP packet received from the AT, the FAP should check whether the source IP address of the IP packet matches with the local IP address assigned to the AT. If the source IP address differs from the local IP address assigned to the AT, the FAP shall discard the packets.

2.5.6 Egress Address Filtering/Routing at the AT

For each IP packet, the AT determines the interface through which the packet will be transmitted based on a packet filtering criteria.

During the IPCP negotiation phase, the FAP shall send an IPCP Configure-Nak message to assign an IP address to the AT and to update the AT with the criteria to be applied for packet filtering. Figure 2.5.6-1 defines the format of the vendor specific option that includes the packet filter criteria.

This vendor specific option should be appended to the IPCP Configure-Nak message from the FAP when assigning a local IP address to the AT and should also be appended to the IPCP Configure-Request message from the AT acknowledging the IP address it received from the FAP.

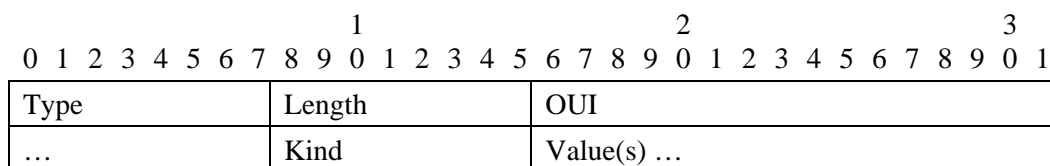


Figure 2.5.6-1 IPCP Vendor Specific Option

- 21 Type: Type shall be set to zero to indicate vendor specific option (RFC 2153 [20]).
- 22 Length: Length of the vendor specific option in bytes (from Type field through Value(s) field).
- 23 OUI: The Organizationally Unique Identifier (OUI) field shall be set to “CF0002H” indicating
24 3GPP2 vendor specific option.
- 25 Kind: 01H value indicates that the IPv4 egress packet filter criteria to be used by AT is
26 contained in the Value(s) field.
- 27 02H value indicates that the IPv6 egress packet filter criteria to be used by AT is
28 contained in the Value(s) field.
- 29 All other values are reserved.
- 30 Value(s): If the Kind field is set to 01H, then the Value(s) field is coded as shown in Figure 2.5.6-2.

										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Count										Subnet 1																			
Subnet 1 (cont)																				Subnet Mask 1																			
Subnet Mask 1 (cont)																				Subnet 2																			
Subnet 2 (cont)																				Subnet Mask 2																			
Subnet Mask 2 (cont)																				...																			

Figure 2.5.6-2 Value(s) Field for the IPv4 Packet Filter Criteria

- 2 Type: A Type of 0 identifies the range of subnets that are accessible through the LIPA interface.
- 3 A Type of 1 identifies the range of subnets that are not accessible through the LIPA inter-
- 4 face.
- 5 Count: This field indicates the number of subnets and subnet masks (each) associated with this
- 6 type.
- 7 Subnet: This field contains a 32-bit value in IPv4 format.
- 8 Subnet Mask: This field contains a 32 bit subnet mask applied to the IP address to yield the non-host
- 9 portion of the address.

10 If the Kind field is set to 02H, then the Value(s) field is as shown in Figure 2.5.6-3.

										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Count										Reserved										Subnet Length 1									
Subnet 1																																							
Subnet 1 (cont)																																							
Subnet 1 (cont)																																							
Subnet 1 (cont)																																							
Reserved										Subnet Length 2										Subnet 2																			
Subnet 2 (cont) ...																																							

Figure 2.5.6-3 Value(s) Field for the IPv6 Packet Filter Criteria

- 12 Type: A Type of 0 identifies the range of subnets that are accessible through the LIPA interface.
- 13 A Type of 1 identifies the range of subnets that are not accessible through the LIPA inter-
- 14 face.
- 15 Count: This field indicates the number of subnet length and subnet (each) associated with this
- 16 type.
- 17 Subnet Length: This field contains the number of valid leading bits in the following subnet. The bits in
- 18 the subnet after the length are reserved and shall be set to zero.
- 19 Subnet: This field contains a 128 bit value in IPv6 format.

1
2
3
4
5

(This page intentionally left blank)

3 Femtocell Interfaces

This section describes the interface requirements for the FAP.

3.1 FGW and RAN Interfaces

Messages from all interfaces in section 1.4.2 that pass through the FGW (i.e., A10, A11, A12, A13, A16, A24) may:

1. be intercepted and regenerated,
2. be passed through without modification, or
3. bypass the FGW.

Whether this occurs is implementation-specific except where it is explicitly indicated.

3.2 FAP to Core Network Interface

The FAP communicates with the core network using the Fm, Fx1 and Fx2 interfaces. Refer to X.S0059-100 [12], part 200. The Fx2 signaling interface is based on IEs defined for the A1 interface. New messages are defined in A1 format in this specification to support the Fx2 interface. The new messages defined in this specification are not sent or received by the macro BS. Instead, the Fx2 interface uses the Message Type and IEs defined in these messages (refer to section 3.2.1.2) according to the procedures in X.S0059-200 [13] to support 1x active hand-in.

3.2.1 A1 Formatted Messages Used on Fx2

3.2.1.1 Measurement Procedures

3.2.1.1.1 Measurement Request

This Base Station Mobile Application Part (BSMAP) message allows the FCS to request potential target FAPs (e.g., FAPs with the same PN offset reported by an MS) to provide signal strength measurements for determining the target FAP for handoff of the existing MS connection.

Note: FAP measurement requests are not supported for IS-95 or 3x IS-2000 channels.

3.2.1.1.1.1 Successful Operation

If a handoff is required and the FCS can not uniquely identify the FAP, the FCS may send a Measurement Request message to candidate target FAPs for handoff measurement requests. The FCS determines the candidate FAPs from the information in the Facility Directive 2 (FACDIR2) message. Refer to X.S0059-200 [13].

The IS-2000 Channel Identity IE shall be included to provide MS physical channel information.

The Long Code IE shall be included in the Measurement Request message and based on the FACDIR2 message, set to the received Public Long Code Mask (PLCM), the Electronic Serial Number (ESN) derived PLCM or the received Private Longcode value.

The FCS shall include the Downlink Radio Environment, CDMA Serving One Way Delay and MS Measured Channel Identity IEs if received in the FACDIR2 message.

The Mobile Identity IE should be included if the FAP is the access control enforcement point. When the FAP receives a Measurement Request message from the FCS, the FAP verifies that the MS identifier is on the ACL. If the MS is not on the ACL, then the FAP includes the requested measurement if possible and returns a Measurement Response message with the cause value 'MS not allowed'.

1 Upon sending this message to one or multiple FAPs, the FCS starts one instance of timer T_{mr-1} to await
2 the arrival of the corresponding Measurement Response message(s). Note that if Measurement Request
3 messages are sent to multiple FAPs, the FCS should consider the responses from multiple FAPs before
4 selecting the target FAP for handoff. The duration that the FCS should wait for responses from FAPs
5 should be large enough to account for the round-trip delay between the FCS and any of the candidate
6 FAPs plus the value of Measurement Response Timer field in the Measurement Response Options IE.

7 Refer also to section 3.2.1.2.1.

8 *3.2.1.1.1.2 Failure Operation*

9 If timer T_{mr-1} expires and the FCS did not set either the Low Signal Report Suppression bit or the Error
10 Report Suppression bit in the Measurement Response Options IE for a non responsive FAP, the FCS may
11 re-determine the candidate FAPs and repeat the measurement request procedure. If the Measurement
12 Response message is not received, the FCS shall terminate the measurement request procedure with the
13 FAP. Note that T_{mr-1} should be larger than the Measurement Response Timer field in the Measurement
14 Response Options IE.

15 Refer also to X.S0059-200 [13].

16 *3.2.1.1.2 Measurement Response*

17 This BSMAP message allows the target FAP to respond to the FCS for a Measurement Request message.
18 Upon receipt of a Measurement Request message, the candidate FAP shall perform the requested
19 measurement procedures if possible, and shall respond to the FCS with a Measurement Response message
20 if any of the following conditions are true:

- 21 • The measurement is successful and the result is above the operator's configurable threshold.
- 22 • The measurement is successful, the result is below the operator's configurable threshold and the Low
23 Signal Report Suppression bit in the Measurement Request message is set to '0'.
- 24 • The measurement is not successful (i.e., cause value of the Measurement Response message is not
25 'Measurement successful') and the Error Report Suppression bit in the Measurement Request
26 message is set to '0'.

27 Note: The definition of the operator's configurable threshold is outside the scope of this specification.

28 *3.2.1.1.2.1 Successful Operation*

29 This message is sent by the FAP to the FCS in response to a Measurement Request message, and shall
30 include the Long Code IE set to the value received in the corresponding Measurement Request message,
31 the cause value and a measurement report, if available.

- 32 • If a measurement is successfully made, the FAP shall respond with a 'Measurement successful' Cause
33 value and the measurement report.
- 34 • If a measurement is attempted and the MS is not detected, the FAP shall respond with an 'MS not
35 detected' Cause value.
- 36 • If the MS is not allowed to utilize FAP resources, the FAP shall make and include the requested
37 measurement if possible and respond with the Cause value set to 'MS not allowed'.
- 38 • If the FAP determines there is not sufficient time to make a satisfactory measurement before
39 expiration of the measurement response timer, the FAP shall set the Cause value to 'Measurement
40 procedure time-out' and may include a measurement report.
- 41 • If the FAP is not capable of providing signal strength measurements, the FAP shall respond with the
42 Cause value, 'BS not equipped'.
- 43 • If the FAP is unable to provide measurements at this time due to other on-going procedures, the FAP
44 shall respond with the Cause value 'BS busy'.

- For equipment and/or interface failure, resource availability or OAM&P intervention, the FAP shall include the appropriate Cause value.

Upon receipt of this message for all corresponding Measurement Request messages sent, the FCS stops timer T_{mr-1} . Refer also to section 3.2.1.2.2.

3.2.1.1.2.2 Failure Operation

None.

3.2.1.1.3 Femtocell Supplementary Info

This BSMAP message allows the FCS and FAP to exchange femtocell related information in support of IOS messaging.

3.2.1.1.3.1 Successful FCS Operation

When the FCS chooses to update the Global RAND key at the FAP, it shall send this message with the new key contained in the Global RAND Key IE. The IE contains the Global RAND key that the FAP shall use to generate and broadcast the Global Challenge. Refer to S.S0132 [8].

When the FCS sends a Location Updating Accept message to the FAP (i.e., the MS successfully registers via the FAP), the FCS shall also send a Femtocell Supplementary Info message with the Called Party BCD Number IE included and set to the Mobile Directory Number (MDN) of the MS, with the Type of Number field set to "Unknown".

3.2.1.1.3.2 Successful FAP Operation

When the FAP successfully performs IMS registration, it shall send this message with the list of IS-41 Cell Global Identifier for neighboring cells in the Cell Identifier List IE. This message should also be sent any time the FAP determines that the neighboring cell information has changed.

When the FAP successfully performs IMS registration, it shall send this message with its Pilot PN information in the Pilot List IE. This message shall also be sent any time the FAP's PN information is changed.

When the FAP generates a Global Challenge Broadcast and returns the MS response in the Authentication Response Parameter IE of an IOS message (refer to A.S0014 [4]), the FAP shall also send a Femtocell Supplementary Info message with the Nonce IE set to the NONCE used by the FAP to generate the Global Challenge Broadcast (refer to S.S0132 [8]) and the Authentication Response Parameter IE.

3.2.1.1.3.3 Failure Operation

None.

3.2.1.2 Message Formats

3.2.1.2.1 Measurement Request

The BSMAP Measurement Request message is sent from the FCS to a target FAP to request that the FAP provide measurement information for an MS to be potentially handed off to that FAP.

Information Element	Section Reference	Element Direction	Type
Message Type	3.2.1.3.2	FCS → FAP	M
Classmark Information Type 2	[4]	FCS → FAP	M ^a
Cell Identifier List (Target)	[4]	FCS → FAP	M ^b

Information Element	Section Reference	Element Direction	Type	
Downlink Radio Environment	[4]	FCS → FAP	O ^{c,d}	C
CDMA Serving One Way Delay	[4]	FCS → FAP	O ^d	C
MS Measured Channel Identity	[4]	FCS → FAP	O ^d	C
<i>IS-2000</i> Channel Identity	[4]	FCS → FAP	O ^e	R
Long Code	3.2.1.3.3	FCS → FAP	O ^f	R
Measurement Response Options	3.2.1.3.5	FCS → FAP	O	R
Mobile Identity	[4]	FCS → FAP	O ^g	C

- 1 a. This IE provides the signaling types and band classes that the MS is permitted to use. More than
2 one is permitted. If an MS is capable of supporting multiple band classes, and this information was
3 included in the Handoff Required message, it shall be indicated in the band class entry field as
4 shown in [4], Section 4.2.12.
- 5 b. If more than one cell is specified, then they shall be in order of selection preference. Only
6 discriminator types '0000 0010' and '0000 0111' are used.
- 7 c. This IE provides information for each cell in the Cell Identifier List (target) IE.
- 8 d. This IE shall be included if received by the FCS.
- 9 e. This IE specifies the *IS-2000* physical channels intended for the Code Division Multiple Access
10 (CDMA) to CDMA hard handoff request and shall be included.
- 11 f. This IE shall be included and set to the Public or Private Long Code in use by the MS.
- 12 g. This IE is included if the FAP is the access control enforcement point.
- 13 The following table shows the bitmap layout for the Measurement Request message.

3.2.1.2.1 Measurement Request

7	6	5	4	3	2	1	0	Octet
⇒ BSMAP Header: Message Discrimination = [00H]								1
Length Indicator (LI) = <variable>								2
⇒ Message Type = [71H]								1
⇒ Classmark Information Type 2: A1 Element Identifier = [12H]								1
Length = <variable>								2
MOB_P_REV = [000 – 111]		Reserved = [0]		See List of Entries = [0, 1]	RF Power Capability = [000-010]			3
Reserved = [00H]								4
NAR_ AN_ CAP = [0,1]	IS-95 = [1]	Slotted = [0,1]	Reserved = [00]		DTX = [0,1]	Mobile Term = [0,1]	TIA/ EIA-553 = [0,1]	5
Reserved = [00H]								6
Reserved = [0000 00]					Mobile Term = [0,1]	PSI = [0,1]		7

3.2.1.2.1 Measurement Request

7	6	5	4	3	2	1	0	Octet
SCM Length = [01H]								8
Station Class Mark = [00H – FFH]								9
Count of Band Class Entries = [01H-20H]								10
Band Class Entry Length = [03H]								11
Mobile Band Class Capability Entry {1+:								
Reserved = [000]				Band Class n = [00000-11111]				k
Band Class n Air Interfaces Supported = [00H-FFH]								k+1
Band Class n MOB_P_REV = [00H-FFH]								k+2
} Mobile Band Class Capability Entry								
⇒ Cell Identifier List (Target): A1 Element Identifier = [1AH]								1
Length = <variable>								2
Cell Identification Discriminator = [02H,07H]								3
IF (Discriminator = 02H), Cell Identification {1+:								
(MSB)	Cell = [001H-FFFH]						j	
						Sector = [0H-FH] (0H = Omni)	(LSB)	j+1
} OR IF (Discriminator = 07H), Cell Identification {1+:								
(MSB)	MSCID = <any value>						j	
								j+1
						(LSB)	j+2	
(MSB)	Cell = [001H-FFFH]						j+3	
						Sector = [0H-FH] (0H = Omni)	(LSB)	j+4
} Cell Identification								
⇒ Downlink Radio Environment: A1 Element Identifier = [29H]								1
Length = <variable>								2
Number of Cells = <variable>								3
Cell Identification Discriminator = [02H,07H]								4
Downlink Radio Environment entry {1+:								
IF (Discriminator = 02H), Cell Identification {1								
(MSB)	Cell = [001H-FFFH]						j	
						Sector = [0H-FH] (0H = Omni)	(LSB)	j+1
} OR IF (Discriminator = 07H), Cell Identification {1:								
(MSB)	MSCID = <any value>						j	
								j+1
						(LSB)	j+2	
(MSB)	Cell = [001H-FFFH]						j+3	
						Sector = [0H-FH] (0H = Omni)	(LSB)	j+4
} Cell Identification								

3.2.1.2.1 Measurement Request

7	6	5	4	3	2	1	0	Octet
Reserved = [00]		Downlink Signal Strength Raw = [000000-111111]						k
(MSB)	CDMA Target One Way Delay = [0000H-FFFFH] (x100ns)						(LSB)	k+1
							(LSB)	k+2
} Downlink Radio Environment entry								
⇒		CDMA Serving One Way Delay: A1 Element Identifier = [0CH]						1
		Length = [08H, 0BH]						2
		Cell Identification Discriminator = [02H, 07H]						3
IF (Discriminator = 02H), Cell Identification {1:								
(MSB)	Cell = [001H-FFFH]						(LSB)	j
							(LSB)	j+1
} OR IF (Discriminator = 07H), Cell Identification {1:								
(MSB)	MSCID = <any value>						(LSB)	j
							(LSB)	j+1
							(LSB)	j+2
(MSB)	Cell = [001H-FFFH]						(LSB)	j+3
			(LSB)	Sector = [0H-FH] (0H = Omni)			(LSB)	j+4
} Cell Identification								
(MSB)	CDMA Serving One Way Delay = [0000H-FFFFH]						(LSB)	k
							(LSB)	k+1
Reserved = [0000 00]				Resolution = [00, 01, 10]			(LSB)	k+2
(MSB)	CDMA Serving One Way Delay Time Stamp = [00 00H – FF FFH]						(LSB)	k+3
							(LSB)	k+4
⇒		MS Measured Channel Identity: A1 Element Identifier = [64H]						1
		Length = [02H]						2
Band Class = [00000 – 11111]			ARFCN (high part) = [000-111]					3
		ARFCN (low part) = [00H – FFH]						4
⇒		IS-2000 Channel Identity: A1 Element Identifier = [09H]						1
		Length = <variable>						2
OTD= [0] (Ignored)	Physical Channel Count = [001, 010]		Frame Offset = [0H-FH]				(LSB)	3
The following 6 octets are repeated once for each physical channel {1...2:								
Physical Channel Type = [01H (Fundamental Channel – FCH – IS-2000), 02H (Dedicated Control Channel – DCCCH – IS-2000)]							(LSB)	n
Rev_ FCH_ Gating	Reverse Pilot Gating Rate = [00, 01, 10]	QOF Mask = <any value> (ignored)	Walsh Code Channel Index (high part) = <any value> (Ignored)				(LSB)	n+1

3.2.1.2.1 Measurement Request

7	6	5	4	3	2	1	0	Octet	
Walsh Code Channel Index (low part) = <any value> (Ignored)								n+2	
Pilot PN Code (low part) = <any value> (Ignored)								n+3	
Pilot PN Code (high part) = <any value> (Ignored)	Reserved = [00]		Power Combined = [0]	Freq. included = [1]	ARFCN (high part) = [000-111]			n+4	
ARFCN (low part) = [00H-FFH]								n+5	
} Channel Information									
⇒ Long Code: A1 Element Identifier = [50H]								1	
Length = [06H]								2	
Reserved = [00 0000]						(MSB)		3	
Long Code = <any value>								4	
.....								5	
.....								6	
.....								7	
						(LSB)		8	
⇒ Measurement Response Options: A1 Element Identifier [51H]								1	
Length = 02H								2	
Reserved = [0000 00]						Error Report Suppression = [0,1]	Low Signal Report Suppression = [0,1]	3	
(MSB)	Measurement Response Timer = <any value>						(LSB)		4
⇒ Mobile Identity (MN ID): A1 Element Identifier [0DH]								1	
Length = [06H - 08H] (10 - 15 digits)								2	
Identity Digit 1 = [0H-9H] (BCD)			Odd/even Indicator = [1,0]	Type of Identity = [001 (MEID – Hex Digits), 110 (IMSI – BCD Digits)]				3	
Identity Digit 3 = [0H-9H] (BCD)			Identity Digit 2 = [0H-9H] (BCD)				4		
...				
Identity Digit N+1 = [0H-9H] (BCD)			Identity Digit N = [0H-9H] (BCD)				n		
= [1111] (if even number of digits)			Identity Digit N+2 = [0H-9H] (BCD)				n+1		

1 3.2.1.2.2 Measurement Response

- 2 This BSMAP message is sent from the target FAP to the FCS to indicate whether or not the MS has been
3 located and to provide link signal strength measurement information if available. This message is sent in
4 response to a Measurement Request message.

Information Element	Section Reference	Element Direction	Type	
Message Type	3.2.1.3.2	FAP → FCS	M	
Long Code	3.2.1.3.3	FAP → FCS	O ^a	R
Cause	3.2.1.3.4	FAP → FCS	O ^b	R
Measurement Report	3.2.1.3.6	FAP → FCS	O ^c	C

- 1 a. This IE shall be included and set to the Long Code received in the corresponding Measurement
- 2 Request message.
- 3 b. This IE shall be included and indicates a successful measurement, the reason why measurement
- 4 information could not be provided or a condition related to the included measurement information.
- 5 c. This IE is included to provide the requested signal strength information, when available.
- 6 The following table shows the bitmap layout for the Measurement Response message.

3.2.1.2.2 Measurement Response

7	6	5	4	3	2	1	0	Octet
⇒ BSMAP Header: Message Discrimination = [00H]								1
Length Indicator (LI) = <variable>								2
⇒ Message Type = [72H]								1
⇒ Long Code: A1 Element Identifier = [50H]								1
Length = [06H]								2
Reserved = [00 0000]						(MSB)		3
Long Code = <any value>								4
								5
								6
								7
							(LSB)	8
⇒ Cause: A1 Element Identifier = [04H]								1
Length = [01H]								2
ext = [0]	Cause Value = [01H (Radio interface failure), 07H (OAM&P intervention), 20H (Equipment failure), 21H (No radio resource available), 25H (BS not equipped), 60H (Protocol error between BS and MSC), 70H (Measurement successful), 72H (MS not detected), 73H (MS not allowed), 74H (BS busy), 75H (Terrestrial resources are not available), 76H (Measurement procedure time-out)]							3
⇒ Measurement Report: A1 Element Identifier = [52H]								1

3.2.1.2.2 Measurement Response

7	6	5	4	3	2	1	0	Octet
Length = [12H]								2
(MSB)	BS Tx Pilot Power						(LSB)	3
(MSB)	MS Rx Pilot Strength						(LSB)	4
(MSB)	Measurement Start Timestamp = <any value>							5
...								...
							(LSB)	12
(MSB)	Measurement End Timestamp = <any value>							13
...								...
							(LSB)	20

1

2 3.2.1.2.3 Femtocell Supplementary Info

3 The BSMAP Femtocell Supplementary Info message is sent between the FCS and the FAP to provide
4 additional femtocell related information.

Information Element	Section Reference	Element Direction	Type	
Message Type	3.2.1.3.2	FCS ↔ FAP	M	
Global RAND Key	3.2.1.3.7	FCS → FAP	O ^a	C
Called Party BCD Number	[4]	FCS → FAP	O ^b	C
Cell Identifier List	[4]	FCS ← FAP	O ^c	C
Pilot List	3.2.1.3.8	FCS ← FAP	O ^d	C
Nonce	3.2.1.3.9	FCS ← FAP	O ^e	C
Authentication Response Parameter	[4]	FCS ← FAP	O ^e	C

- 5 a. This IE is sent to the FAP when the FCS chooses to update the Global RAND key at the FAP.
6 Refer to S.S0132 [8].
- 7 b. This IE is sent to the FAP when the MS successfully registers via the FAP. The IE shall contain the
8 MDN of the MS registered via the FAP, sent in Called Party BCD format with the Type of Number
9 field set to “Unknown”.
- 10 c. This IE is sent to the FCS after the FAP successfully performs IMS registration (or its neighboring
11 cell information changes) to provide the list of IS-41 Cell Global Identifier for neighboring cells.
- 12 d. This IE is sent to the FCS after the FAP successfully performs IMS registration (or its PN
13 information changes).
- 14 e. This IE is sent to the FCS when the FAP performs a Global Challenge Broadcast and sends the
15 response from the MS to the FCS (in an Authentication Response Parameter IE in an associated
16 IOS message), refer to A.S0014 [4].

17 The following table shows the bitmap layout for the Femtocell Supplementary Info message.

3.2.1.2.3 Femtocell Supplementary Info

7	6	5	4	3	2	1	0	Octet
⇒ BSMAP Header: Message Discrimination = [00H]								1

3.2.1.2.3 Femtocell Supplementary Info

7	6	5	4	3	2	1	0	Octet
Length Indicator (LI) = <variable>								2
⇒ Message Type = [73H]								1
⇒ Global RAND Key: A1 Element Identifier = [53H]								1
Length = <variable>								2
(MSB)	Global RAND Key Value = <any value>							3
...								...
							(LSB)	n
⇒ Called Party BCD Number: A1 Element Identifier = [5EH]								1
Length = <variable>								2
= [1]	Type of Number = [000]			Number Plan Identification = [0000-1111]				3
Number Digit/End Mark 2 = [0000-1111]				Number Digit/End Mark 1 = [0000-1111]				4
Number Digit/End Mark 4 = [0000-1111]				Number Digit/End Mark 3 = [0000-1111]				5
...								...
Number Digit/End Mark m+1 = [0000-1111]				Number Digit/End Mark m = [0000-1111]				n
⇒ Cell Identifier List: A1 Element Identifier = [1AH]								1
Length = <variable>								2
Cell Identification Discriminator = [07H]								3
} Cell Identification {1+:								
(MSB)	MSCID = <any value>							j
							j+1	
						(LSB)	j+2	
(MSB)	Cell = [001H-FFFH]							j+3
					Sector = [0H-FH] (0H = Omni)	(LSB)	j+4	
} Cell Identification								
⇒ Pilot List: A1 Element Identifier = [54H]								1
Length = <variable>								2
Number of Pilots = [01H-10H]								3
} Pilot Entry { Number of Pilots: {1+:								
Channel Record Length = <variable>								j
(MSB)	Channel Record = <any value>							j+1
...								...
						(LSB)	k	
Reserved	(MSB)	Pilot PN Information = <any value>					k+1	
						(LSB)	k+2	
} Pilot Entry								
⇒ Nonce: A1 Element Identifier = [55H]								1

3.2.1.2.3 Femtocell Supplementary Info

7	6	5	4	3	2	1	0	Octet
Length = <variable>								2
(MSB)	NONCE Value = <any value>							3
...								...
							(LSB)	n
⇒ Authentication Response Parameter: A1 Element Identifier = [42H]								1
Length = 04H								2
Reserved = [0000]				Auth Signature Type = [0001] (AUTHR) [0010] (AUTHU)				3
[0]	[0]	[0]	[0]	[0]	[0]	(MSB)		4
Auth Signature = <any value>								5
							(LSB)	6

1

3.2.1.3 Information Element Definitions

3.2.1.3.1 A1 Information Element Identifiers

The following table lists all femtocell specific IEs included in the messages defined in section 3.2.1.2. The table includes the Information Element Identifier (IEI) coding which distinguishes one IE from another. The table also includes a section reference indicating where the IE coding can be found.

Element Name	IEI (Hex)	Reference
Cause	04H	3.2.1.3.4
Cell Identifier List	1AH	[4]
Authentication Response Parameter	42H	[4]
Long Code	50H	3.2.1.3.3
Measurement Response Options	51H	3.2.1.3.5
Measurement Report	52H	3.2.1.3.6
Global RAND Key	53H	3.2.1.3.7
Pilot List	54H	3.2.1.3.8
Nonce	55H	3.2.1.3.9
Called Party BCD Number	5EH	[4]

Refer to [4] for additional IEIs used on the A1 interface.

3.2.1.3.2 Message Type

The A1 Message Type IE is used to indicate the type of message on the A1 interface.

3.2.1.3.2 Message Type

7	6	5	4	3	2	1	0	Octet
Message Type								1

- 1 Message Type This octet is coded as shown in Table 3.2.1.3.2-1.

Table 3.2.1.3.2-1 BSMAP Messages

BSMAP Message Name	Message Type Value	Message Category	Section Reference
Measurement Request	71H	Radio Resource Mgmt.	3.2.1.2.1
Measurement Response	72H	Radio Resource Mgmt.	3.2.1.2.2
Femtocell Supplementary Info	73H	Radio Resource Mgmt.	3.2.1.2.3

- 2 BSMAP messages are used to perform functions at the MSC or BS. Refer to [4] for additional Message
3 Types used on the A1 interface.

4 3.2.1.3.3 Long Code

- 5 This IE is used to provide either the Public Long Code Mask or the Private Long Code in use by the MS,
6 to the FAP.

3.2.1.3.3 Long Code

7	6	5	4	3	2	1	0	Octet	
A1 Element Identifier								1	
Length								2	
Reserved						(MSB)		3	
Long Code								4	
								5	
								6	
								7	
								(LSB)	8

- 7 Length This field is defined as the number of octets following the Length field.
- 8 Long Code This field 42-bit shall be set to the Public Long Code if any of the following
9 conditions are true:
- 10 • Public Long Code is received by the FCS in the FACDIR2 message, or
 - 11 • if the Public Long Code Mask is not included and the received Encryption
12 Information does not include the Encryption Parameter Identifier field with
13 the value set to '00100' (Private Longcode) and the corresponding Status bit
14 set to '1' (active), i.e., then the Public Long Code is derived from the Mobile
15 Identity (ESN) IE.
- 16 Otherwise this field shall be set to the received Private Long Code value.

17 3.2.1.3.4 Cause

- 18 This IE is used to indicate the reason for occurrence of a particular event and is coded as follows.

3.2.1.3.4 Cause

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2

3.2.1.3.4 Cause

7	6	5	4	3	2	1	0	Octet
0/1	Cause Value							3

- 1 Length This field is defined as the number of octets following the Length field.
- 2 Cause Value The Cause Value field is a single octet field if the extension bit (bit 7) is set to
 3 '0'. If bit 7 of octet 3 is set to '1' then the cause value is a two octet field. If the
 4 value of the first octet of the cause field is '1XXX 0000' then the second octet is
 5 reserved for national applications, where 'XXX' indicates the Cause Class as
 6 indicated in Table 3.2.1.3.4-1. Otherwise, the Cause values are defined in Table
 7 3.2.1.3.4-2.

Table 3.2.1.3.4-1 Cause Class Values

Binary Values	Meaning
000	Normal event
001	Normal event
010	Resource unavailable
011	Service or option not available
100	Service or option not implemented
101	Invalid message (e.g., parameter out of range)
110	Protocol error
111	Interworking

9

Table 3.2.1.3.4-2 Cause Values

6	5	4	3	2	1	0	Hex Value	Cause
Normal Event Class (000 xxxx and 001 xxxx)								
0	0	0	0	0	0	0	00	Radio interface message failure
0	0	0	0	0	0	1	01	Radio interface failure
0	0	0	0	0	1	0	02	Uplink quality
0	0	0	0	0	1	1	03	Uplink strength
0	0	0	0	1	0	0	04	Downlink quality
0	0	0	0	1	0	1	05	Downlink strength
0	0	0	0	1	1	0	06	Distance
0	0	0	0	1	1	1	07	OAM&P intervention
0	0	0	1	0	0	0	08	MS busy
0	0	0	1	0	0	1	09	Call processing
0	0	0	1	0	1	0	0A	Reversion to old channel
0	0	0	1	0	1	1	0B	Handoff successful
0	0	0	1	1	0	0	0C	No response from MS
0	0	0	1	1	0	1	0D	Timer expired
0	0	0	1	1	1	0	0E	Better cell (power budget)
0	0	0	1	1	1	1	0F	Interference
0	0	1	0	0	0	0	10	Packet call going dormant
0	0	1	0	0	0	1	11	Service option not available
0	0	1	0	1	0	1	15	Short data burst authentication failure
0	0	1	0	1	1	1	17	Time critical relocation/handoff
0	0	1	1	0	0	0	18	Network optimization
0	0	1	1	0	0	1	19	Power down from dormant state

Table 3.2.1.3.4-2 Cause Values

6	5	4	3	2	1	0	Hex Value	Cause
0	0	1	1	0	1	0	1A	Authentication failure
0	0	1	1	0	1	1	1B	Inter-BS soft handoff drop target
0	0	1	1	1	0	1	1D	Intra-BS soft handoff drop target
0	0	1	1	1	1	0	1E	Autonomous Registration by the Network
Resource Unavailable Class (010 xxxx)								
0	1	0	0	0	0	0	20	Equipment failure
0	1	0	0	0	0	1	21	No radio resource available
0	1	0	0	0	1	0	22	Requested terrestrial resource unavailable
0	1	0	0	0	1	1	23	A2p RTP Payload Type not available
0	1	0	0	1	0	0	24	A2p Bearer Format Address Type not available
0	1	0	0	1	0	1	25	BS not equipped
0	1	0	0	1	1	0	26	MS not equipped (or incapable)
0	1	0	0	1	1	1	27	2G only sector
0	1	0	1	0	0	0	28	2G only carrier
0	1	0	1	0	0	1	29	PACA call queued
0	1	0	1	0	1	0	2A	Handoff blocked
0	1	0	1	0	1	1	2B	Alternate signaling type reject
0	1	0	1	1	0	0	2C	A2p Resource not available
0	1	0	1	1	0	1	2D	PACA queue overflow
0	1	0	1	1	1	0	2E	PACA cancel request rejected
Service or Option Not Available Class (011 xxxx)								
0	1	1	0	0	0	0	30	Requested transcoding/rate adaptation unavailable
0	1	1	0	0	0	1	31	Lower priority radio resources not available
0	1	1	0	0	1	0	32	PCF resources are not available
0	1	1	0	0	1	1	33	TFO control request failed
0	1	1	0	1	0	0	34	MS rejected order
Service or Option Not Implemented Class (100 xxxx)								
1	0	0	0	1	0	1	45	PDS-related capability not available or not supported)
Invalid Message Class (101 xxxx)								
1	0	1	0	0	0	0	50	Terrestrial circuit already allocated
Protocol Error (110 xxxx)								
1	1	0	0	0	0	0	60	Protocol error between BS and MSC
Interworking (111 xxxx)								
1	1	1	0	0	0	0	70	Measurement successful
1	1	1	0	0	0	1	71	ADDS message too long for delivery on the paging channel
1	1	1	0	0	1	0	72	MS not detected
1	1	1	0	0	1	1	73	MS not allowed
1	1	1	0	1	0	0	74	BS busy
1	1	1	0	1	0	1	75	Terrestrial resources are not available
1	1	1	0	1	1	0	76	Measurement procedure time-out
1	1	1	0	1	1	1	77	PPP session closed by the MS
1	1	1	1	0	0	0	78	Do not notify MS
1	1	1	1	0	0	1	79	PDSN resources are not available
1	1	1	1	0	1	1	7B	Concurrent authentication
1	1	1	1	1	0	0	7C	MS incorrect integrity info
1	1	1	1	1	1	1	7F	Handoff procedure time-out
All other values								Reserved for future use.

3.2.1.3.5 Measurement Response Options

This IE is used to provide options related to the Measurement Response message.

3.2.1.3.5 Measurement Response Options

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2
Reserved						Error Report Suppression	Low Signal Report Suppression	3
(MSB)	Measurement Response Timer						(LSB)	4

Length This field indicates the number of octets in this IE following the Length field.

Error Report Suppression This bit shall be set to '1' if the FAP may omit responding with a Measurement Response message when the cause value is not Measurement successful. Otherwise, this bit shall be set to '0'.

Low Signal Report Suppression This bit shall be set to '1' if the FAP may omit responding with a Measurement Response message when the MS measurement result is below the operator's configurable threshold. Otherwise, this bit shall be set to '0'.

Measurement Response Timer This field is an 8-bit binary number, in units of 80 ms., which indicates the duration of the timer, starting at the receipt of the Measurement Request message, in which the FAP should respond with a Measurement Response message.

3.2.1.3.6 Measurement Report

This IE is used to provide FAP transmit pilot power and receive pilot signal strength for the requested MS.

3.2.1.3.6 Measurement Report

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2
(MSB)	BS Tx Pilot Power						(LSB)	3
(MSB)	MS Rx Pilot Strength						(LSB)	4
(MSB)	Measurement Start Timestamp							5
...								...
							(LSB)	12
(MSB)	Measurement End Timestamp							13
...								...
							(LSB)	20

Length This field indicates the number of octets in this IE following the Length field.

1	BS Tx Pilot Power	This field indicates the FAP's pilot power. If the FAP's pilot power is within the range of -128 to 127 dBm, the FAP shall set this field to the two's complement representation of its Pilot Channel Power (in dBm). Otherwise, if the pilot power is below -128 or above 127 dBm, the FAP shall set this field to the two's complement representation of -128 or 127, respectively.
2		
3		
4		
5		
6		
7	MS Rx Pilot Strength	This field indicates the received power of the MS pilot channel measured at the FAP RF input ports. If the received power is in the range of -127.5 to 0 dBm, the FAP shall set this field to the nearest integer value of $-2 \times$ the received power (in dBm). For example, if the received power is -20.25 dBm this field is set to 41. Otherwise if the received power is below -127.5 or above 0 dBm, the FAP shall set this field to 255 or 0, respectively.
8		
9		
10		
11		
12		
13		
14	Measurement Start Timestamp	This field is a 64-bit binary number set to the CDMA System Time at the time that the MS Rx Pilot measurement in this IE is started. The time stamp is in units of 80 ms.
15		
16		
17	Measurement End Timestamp	This field is a 64-bit binary number set to the CDMA System Time at the time that the MS Rx Pilot measurement in this IE is finished. The time stamp is in units of 80 ms.
18		
19		

20 3.2.1.3.7 Global RAND Key

21 This IE is used to update the FAP with the Global RAND key used to generate and broadcast the Global
22 Challenge.

3.2.1.3.7 Global RAND Key

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2
(MSB)	Global RAND Key Value							3
...								...
							(LSB)	n

23 **Length** This field indicates the number of octets in this IE following the Length
24 field.

25 **Global RAND Key Value** This field contains the Global RAND key to be used by the FAP to
26 generate and broadcast the Global Challenge. Refer to S.S0132 [8].

27 3.2.1.3.8 Pilot List

28 This IE is used to update the FCS with the FAP's Pilot List information, after successful IMS registration
29 or when the FAPs PN information changes.

3.2.1.3.8 Pilot List

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2
Number of Pilots								3
Channel Record Length								j
(MSB)	Channel Record							j+1

3.2.1.3.8 Pilot List

7	6	5	4	3	2	1	0	Octet	
...								...	
							(LSB)	k	
Reserved	(MSB)	Pilot PN Information							k+1
							(LSB)	k+2	

- 1 Length This field indicates the number of octets in this IE following the Length
2 field.
- 3 Number of Pilots This field indicates the number of pilots represented by this IE. The
4 Channel Record and Pilot PN Phase are indicated for each pilot.
- 5 Channel Record Length This field contains the numbers of octets in the Channel Record field as a
6 binary number.
- 7 Channel Record This field contains a channel record as defined in C.S0024 [7]. The
8 information contained in a channel record include the system type, band
9 class, and channel number.
- 10 Pilot PN Information This field contains the Pilot PN Phase of the pilot. Refer to C.S0024 [7].

3.2.1.3.9 Nonce

- 11 This IE is used to update the FCS with the NONCE used by the FAP to generate the Global Challenge
12 Broadcast.
13

3.2.1.3.9 Nonce

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2
(MSB)	Nonce Value							3
...								...
							(LSB)	n

- 14 Length This field indicates the number of octets in this IE following the Length
15 field.
- 16 Nonce Value This field contains the NONCE used by the FAP to generate the Global
17 Challenge Broadcast. Refer to S.S0132 [8].
18

3.2.1.4 Timer Definitions

- 19 This section describes the timers associated with the Femtocell IOS.
20

Table 3.2.1.4-1 Timer Values and Ranges Sorted by Name

Timer Name	Default Value (seconds)	Range of Values (seconds)	Granularity (seconds)	Section Reference	Classification
T _{mr-1}	5	0-10	0.1	3.2.1.4.1	Handoff

3.2.1.4.1 T_{mr-1}

This FCS timer is started when one or more Measurement Request messages are sent, and stopped when all the corresponding Measurement Response messages are received.

3.3 FAP RAN Interfaces

This section describes the RAN interfaces associated with this specification.

3.3.1 A10/A11 (PCF - PDSN) Interface

Refer to A.S0008 [1], A.S0009 [2] and A.S0017 [5].

3.3.2 A12 (AN/PCF - AN-AAA) Interface

If supported by the FAP and by operator policy (policy configured via FMS, refer to X.R0063 [I-1]), the FAP shall include the FEID RADIUS attribute X.S0059-100 [12] in the Access Request message sent on the A12 interface.

Refer also to A.S0008 [1] and A.S0009 [2].

3.3.3 A13 (AN/PCF – AN/PCF) Interface

3.3.3.1 HRPD Dormant Handoff from FAP to Macro AN/PCF

When an HRPD AT performs a dormant handoff from a FAP to a macro AN/PCF, the macro AN/PCF sends an A13-Session Information Request message to retrieve the HRPD session from the source FAP. The destination IP address of the A13-Session Information Request message may be the source FAP or the FGW. The macro AN/PCF may receive the A13-Session Information Response message either from the source FAP or the FGW. This specification assumes that the FGW can be supported without any additional interface or modification to A13 interface at both FAP and macro AN/PCF.

Upon receipt of the session information, the macro AN/PCF completes session establishment with the AT and selects the PDSN to set up an A10 connection for each service connection. Refer to A.S0008 [1] and A.S0009 [2], section 4.2.4.2.

3.3.4 A16 (AN - AN) Interface

3.3.4.1 Connected-State Handoff from FAP to a Macro AN

When an AT with an active HRPD connection hands off from a FAP to a macro AN, the FAP uses the A16 interface to request transfer of the HRPD session to the target AN/PCF and the A11 interface to release the associated A10 connections (after the A16 release indication). In the A16-Session Transfer Request message, the FAP shall include the Target Sector ID IE to assist the target AN in determining the sector to which the resource should be allocated.

Refer also to A.S0008 [1] and A.S0009 [2], Section 3.12.

3.3.5 A24 AN/PCF - AN/PCF (IP Tunneling) Interface

Refer to A.S0008 [1] and A.S0009 [2].

4 FAP Call Flows

This section describes the call flows associated with FAP and AT operation.

4.1 FAP Operation

This section describes the call flows associated with femtocell operation.

4.1.1 FAP Power-up

This scenario describes the call flow associated with FAP power-up and initialization, including neighborhood discovery, network discovery and configuration.

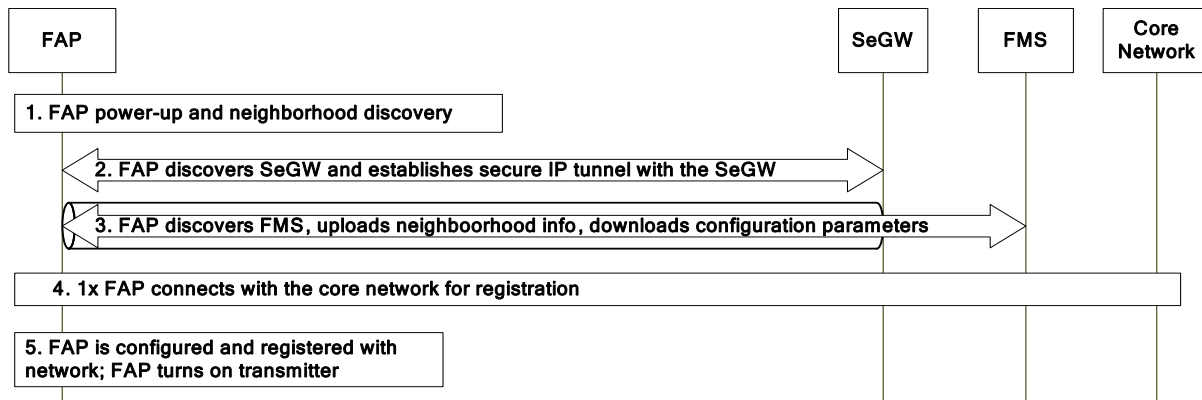


Figure 4.1.1-1 FAP Power-up

1. The FAP powers-up and initiates neighborhood discovery (refer to X.R0063-0 [I-1]). The FAP scans its neighboring cells and obtains its radio neighborhood information. Note this step should complete prior to step 3.
2. The FAP discovers the IP address of the SeGW by DNS lookup or by other means and establishes a secure IP tunnel with the SeGW. Refer to X.S0059-100 [12].
3. The FAP discovers the FMS through the secure IP tunnel and uploads the information it obtained during neighborhood discovery to the FMS. The FMS configures the FAP with air-interface and network parameters (including those required for 1x FAP operation). Refer to X.R0063-0 [I-1].
4. If the FAP is to provide 1x services, it also connects to and registers with the IMS core network. Refer to X.S0059-100 [12].
5. The FAP, once authorized and configured by the serving FMS, may start transmitting on the assigned frequency.

4.2 MS/AT Operation

This section describes the call flows associated with MS/AT operation.

4.2.1 MS/AT Power-up at the FAP

Refer to the registration call flow in X.S0059-200 [13].

4.2.2 MS Registration and Paging at the FAP

For registration and paging call flows, refer to X.S0059-200 [13].

4.2.3 1x Handoff

This section describes the call flows associated with handoff between 1x macro and femtocell systems.

4.2.3.1 1x Macro BS to FAP Dormant Handoff (Intra-PDSN)

This scenario describes the call flow when an MS with a dormant packet data session hands off from a macro BS to a FAP under the same PDSN. From the perspective of the source macro BS, these procedures are identical to those for a dormant handoff of a packet data service instance. Refer to A.S0013 [3], Section 3.17.4.13.1).

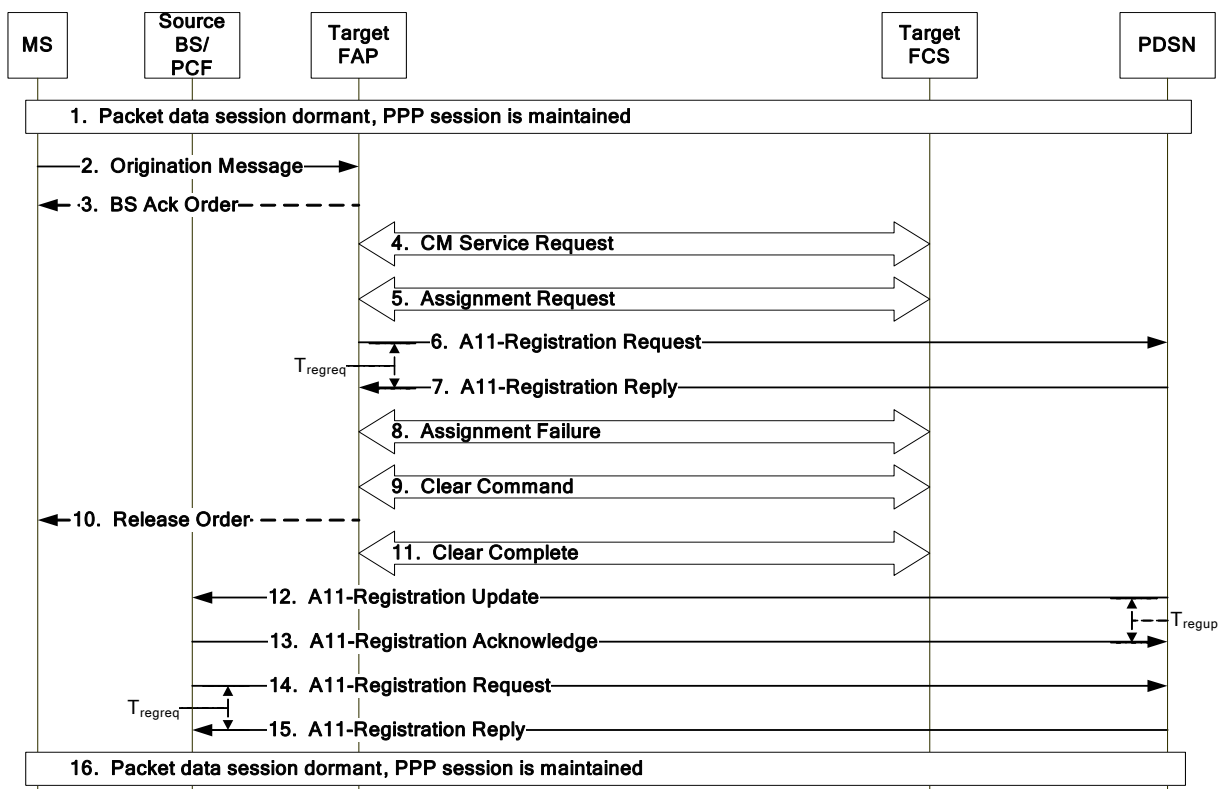


Figure 4.2.3.1-1 1x Macro BS to FAP Dormant Handoff (Intra-PDSN)

1. It is assumed that the MS has performed a MIP registration (if required) and established a PPP connection with the PDSN however the packet data session is now dormant. The MS does not have an active voice call in progress.
2. On detection of a new PZID, SID or NID, the MS sends an Origination Message with DRS set to '0' to the target FAP.
3. The target FAP acknowledges the receipt of the Origination Message with a BS Ack Order to the MS.
4. The target FAP constructs a CM Service Request message, places it in the Complete Layer 3 Information message and sends it to the target FCS via Fx2 signaling. Refer to X.S0059-200 [13] for the messaging format between the FAP and the FCS.

1 Note: Step 4 is optional. If step '4' is not performed, steps '5', '8', '9' and '11' are omitted.

2 5. The target FCS sends an Assignment Request message to the target FAP via Fx2 signaling to request
3 assignment of radio resources.

4 6. The target FAP sends an A11-Registration Request message to the PDSN. This message includes the
5 Mobility Event Indicator within the Critical Vendor Specific Extension (CVSE) and a non-zero Life-
6 time. This message also includes Accounting Data (A10 Connection Setup Airlink Record) and
7 ANID information (CANID/PANID). The target FAP starts timer T_{regreq} .

8 7. The A11-Registration Request message is validated and the PDSN accepts the connection by
9 returning an A11-Registration Reply message with an accept indication. If the PDSN has data to send,
10 it includes the Data Available Indicator within the CVSE. The A10 connection binding information at
11 the PDSN is updated to point to the target FAP. The target FAP stops timer T_{regreq} .

12 If the PDSN responds to the target FAP with the Data Available Indicator, the target FAP establishes
13 traffic channels. In this case, steps 8-11 and 16 are omitted.

14 8. The target FAP sends the Assignment Failure message to the target FCS via Fx2 signaling, with the
15 cause value indicating Packet Call Going Dormant.

16 9. After the target FCS has successfully authenticated the MS, it sends a Clear Command message to the
17 target FAP via Fx2 signaling with the cause value 'Do not notify mobile'.

18 10. The target FAP may send a Release Order to the MS. This allows the MS to send Origination
19 Messages for any remaining PDSIs sooner.

20 11. The target FAP sends a Clear Complete message to the target FCS via Fx2 signaling.

21 12. The PDSN initiates release of the A10 connection with the source BS/PCF by sending an A11-
22 Registration Update message. The PDSN starts timer T_{regupd} .

23 13. The source BS/PCF responds with an A11-Registration Acknowledge message. The PDSN stops
24 timer T_{regupd} .

25 14. The source BS/PCF sends an A11-Registration Request message with Lifetime set to zero to the
26 PDSN. The source BS/PCF starts timer T_{regreq} .

27 15. The PDSN sends the A11-Registration Reply message with an accept indication to the source
28 BS/PCF. The source BS/PCF releases the A10 connection for the MS. The source PCF stops timer
29 T_{regreq} .

30 If the MS sends an Origination Message with $\text{DRS} = 0$ for additional dormant service instances (this
31 may occur any time after step '10' or when timer T_{42m} expires for the last dormant service instance
32 handed off), this procedure is repeated for each such service instance.

33 16. The packet data session remains dormant.

34 **4.2.3.2 1x Macro BS to FAP Dormant Handoff (Inter-PDSN)**

35 This scenario describes the call flow when an MS with a dormant packet data session hands off from a
36 macro BS to a FAP under a different PDSN. From the perspective of the source macro BS, these
37 procedures are identical to those for a dormant handoff of a packet data service instance. Refer to
38 A.S0013 [3], Section 3.17.4.14).

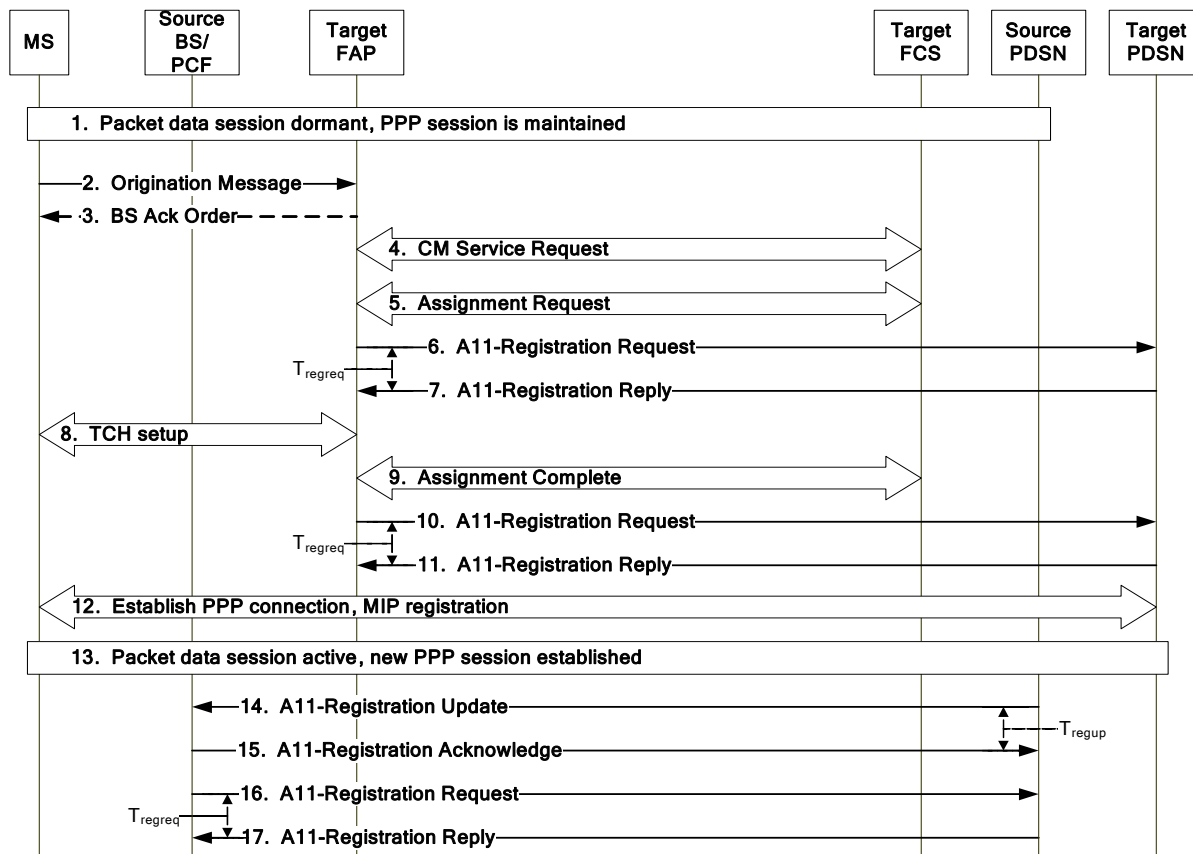


Figure 4.2.3.2-1 1x Macro BS to FAP Dormant Handoff (Inter-PDSN)

1. It is assumed that the MS has performed a MIP registration (if required) and established a PPP connection with the PDSN however the packet data session is now dormant. The MS does not have an active voice call in progress.
 2. On detection of a new PZID, SID or NID, the MS sends an Origination Message with DRS set to '0' to the target FAP.
 3. The target FAP acknowledges the receipt of the Origination Message with a BS Ack Order to the MS.
 4. The target FAP constructs a CM Service Request message, places it in the Complete Layer 3 Information message and sends it to the target FCS via Fx2 signaling. Refer to X.S0059-200 [13] for the messaging format between the FAP and the FCS.
- Note: Step 4 is optional. If step '4' is not performed, steps '5' and '9' are omitted.
5. The target FCS sends an Assignment Request message to the target FAP via Fx2 signaling to request assignment of radio resources.
 6. The target FAP initiates establishment of the A10 connection by sending an A11-Registration Request message with non-zero Lifetime value to the target PDSN. The message includes the Mobility Event Indicator within a CVSE and a non-zero Lifetime. This message also includes Accounting Data (A10 Connection Setup Airlink Record) and ANID information (CANID/PANID). The target FAP starts timer T_{reqreq} .
 7. The A11-Registration Request message is validated and the target PDSN accepts the connection by returning an A11-Registration Reply message with an accept indication and Data Available Indicator within a CVSE. If the PDSN supports fast handoff the Anchor P-P Address is included. If the target

- 1 FAP does not support fast handoff it ignores the Anchor P-P Address. The target FAP stops timer
2 T_{regreq} .
- 3 8. The target FAP initiates setup of the traffic channel with the MS.
- 4 9. The target FAP sends the Assignment Complete message to the target FCS.
- 5 10. The target FAP sends an A11-Registration Request message to the target PDSN containing an Airlink
6 Start accounting record. The target FAP starts timer T_{regreq} .
- 7 11. The target PDSN updates the accounting data and returns an A11-Registration Reply message with an
8 accept indication back to the target FAP. The target FAP stops timer T_{regreq} .
- 9 12. The MS and the target PDSN establish the link layer (PPP) connection and perform MIP registration
10 procedures (if required) over the link layer (PPP) connection, thereby creating a mobility binding for
11 the MS.
- 12 13. The packet data session is active and a new PPP session has been established.
- 13 14. On expiration of the PPP timer or other events internal to the source PDSN, the source PDSN initiates
14 release of the A10 connection with the source BS/PCF by sending an A11-Registration Update
15 message. The source PDSN starts timer T_{regupd} .
- 16 15. The source BS/PCF responds with an A11-Registration Acknowledge message. The source PDSN
17 stops timer T_{regupd} .
- 18 16. The source BS/PCF sends an A11-Registration Request message with Lifetime set to zero. The source
19 PCF starts timer T_{regreq} .
- 20 17. The source PDSN stores the accounting related information for further processing before returning an
21 A11-Registration Reply message with an accept indication. The source BS/PCF releases the A10
22 connection. The source BS/PCF stops timer T_{regreq} .

23 **4.2.3.3 1x FAP to Macro BS Dormant Handoff**

24 For the scenario when a MS with a dormant packet data session hands off from FAP to a macro BS, from
25 the perspective of the target BS and the source FAP, these procedures are identical to those for a dormant
26 handoff of a packet data service instance. Refer to A.S0013 [3], Section 3.17.4.13.1) for details.

27

28 **4.2.3.4 1x Macro BS to FAP Active Handoff**

29 This scenario describes the call flow when an MS with a 1x active voice call hands off from a macro BS
30 to a FAP. From the perspective of the source macro BS, these procedures are similar to those for a hard
31 handoff via the MSC using the A1/A2 or A1p/A2p interfaces (refer to A.S0013 [3], Section 3.19.3.1).

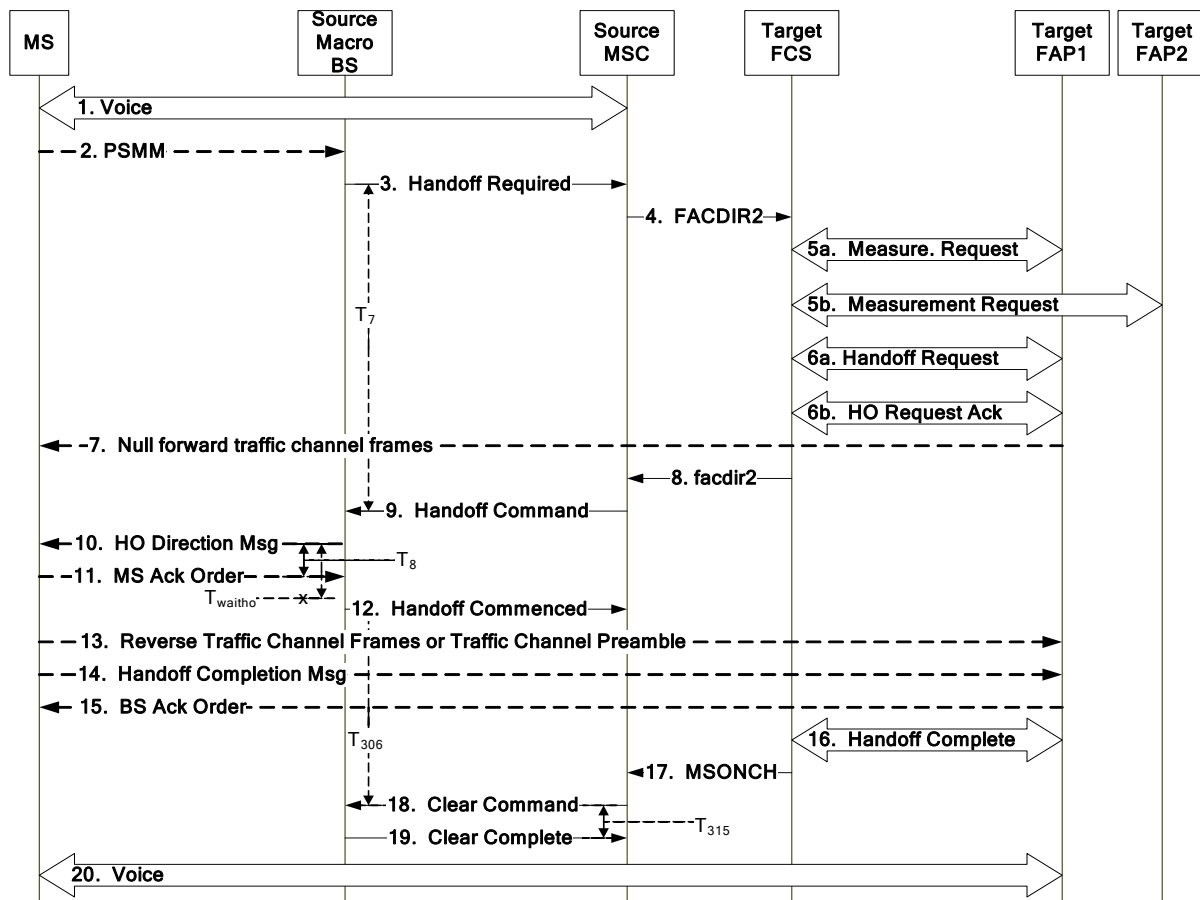


Figure 4.2.3.4-1 1x Macro BS to FAP Active Handoff

1. The MS is in a voice call via the source macro BS and the source MSC.
2. The MS sends a Pilot Strength Measurement Message (PSMM), refer to C.S0005 [6], to the source macro BS that includes the PN offset of the FAP as the strongest neighboring cell.
3. Based on the PSMM, the source macro BS decides to perform a hard handoff. The source macro BS sends a Handoff Required message to the source MSC and starts timer T_7 . The message contains the Cell ID value that maps to PN offset of the FAP and the MSC_ID of the target FCS.
4. The source MSC sends a FACDIR2 message to the target FCS via core network messaging, directing the target FCS to initiate the handoff. Refer to X.S0004 [9].
5. If the target FCS can not determine the FAP corresponding to the Cell ID reported in step 4 (i.e., there are multiple FAPs that have the same PN offset), the target FCS sends a measurement request message via Fx2 signaling to all FAPs that have the same PN offset (steps 5a and 5b). All FAPs that receive this message verify that the MS is allowed 1x cdma2000^{®6} circuit switched services through the FAP, and attempt to detect the MS and measure the signal strength of the reverse link of the MS (refer to C.S0005 [6]). Each FAP responds to the FCS providing the signal strength measured on the reverse link of the MS and the transmit power of the FAP.

⁶ cdma2000[®] is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000[®] is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

- 1 6. Based on the results of the measurement request or other means, the target FCS uniquely determines
2 the target FAP, allocates bearer resources and sends a handoff request to target FAP 1. Target FAP 1
3 allocates the appropriate radio resources and responds with a handoff request acknowledge via Fx2
4 signaling. Refer to X.S0059-200 [13].
- 5 7. Target FAP 1 sends null forward traffic channel frames to the MS.
- 6 8. The target FCS, having completed the Handoff Request procedure, sends a facdir2 message to the
7 source MSC via core network messaging. Refer to X.S0004 [9].
- 8 9. The source MSC prepares to switch the MS from the source macro BS to target FAP 1 and sends a
9 Handoff Command message to the source macro BS. The source MSC shall include in the Handoff
10 Command message the service configuration records contained in the handoff request ack message
11 and received in the facdir2 message. Refer to X.S0059-200 [13]. The source macro BS stops timer T₇.
- 12 10. The source macro BS sends a handoff direction message to the MS and starts timer T₈. If the MS is
13 allowed to return to the source macro BS, timer T_{wait_{tho}} is also started by the source macro BS.
- 14 11. The MS may acknowledge the handoff direction message by sending an MS Ack Order to the source
15 macro BS. The source macro BS stops timer T₈ upon receipt of this message.
- 16 12. The source macro BS sends a Handoff Commenced message to the source MSC to notify it that the
17 MS has been ordered to move to the target FAP 1 channel. If timer T_{wait_{tho}} has been started, the
18 source BS shall wait for that timer to expire before sending the Handoff Commenced message.
- 19 13. The MS sends reverse traffic channel frames or the traffic channel preamble to the target cell.
- 20 14. The MS sends a Handoff Completion Message to target FAP 1.
- 21 15. Target FAP 1 sends a BS Ack Order to the MS over the air interface.
- 22 16. Target FAP 1 sends a Handoff Complete message to the target FCS via Fx2 signaling to notify it that
23 the MS has successfully completed the hard handoff.
- 24 17. The target FCS sends the MSONCH message to the source MSC via core network messaging to
25 notify it that the MS has successfully completed the hard handoff.
- 26 18. The source MSC sends a Clear Command message to the source macro BS.
- 27 19. The source macro BS sends a Clear Complete message to the source MSC to notify it that clearing
28 has been accomplished.
- 29 20. The MS is in a voice call via target FAP 1 and the target FCS.

30 **4.2.3.5 1x FAP to Macro BS Active Handoff**

31 This scenario describes the call flow when an MS with a 1x active voice call hands off from a FAP to a
32 macro BS. From the perspective of the target macro BS, these procedures are similar to those for a hard
33 handoff via the MSC using the A1/A2 or A1p/A2p interfaces (refer to A.S0013 [3], Section 3.19.3.1).

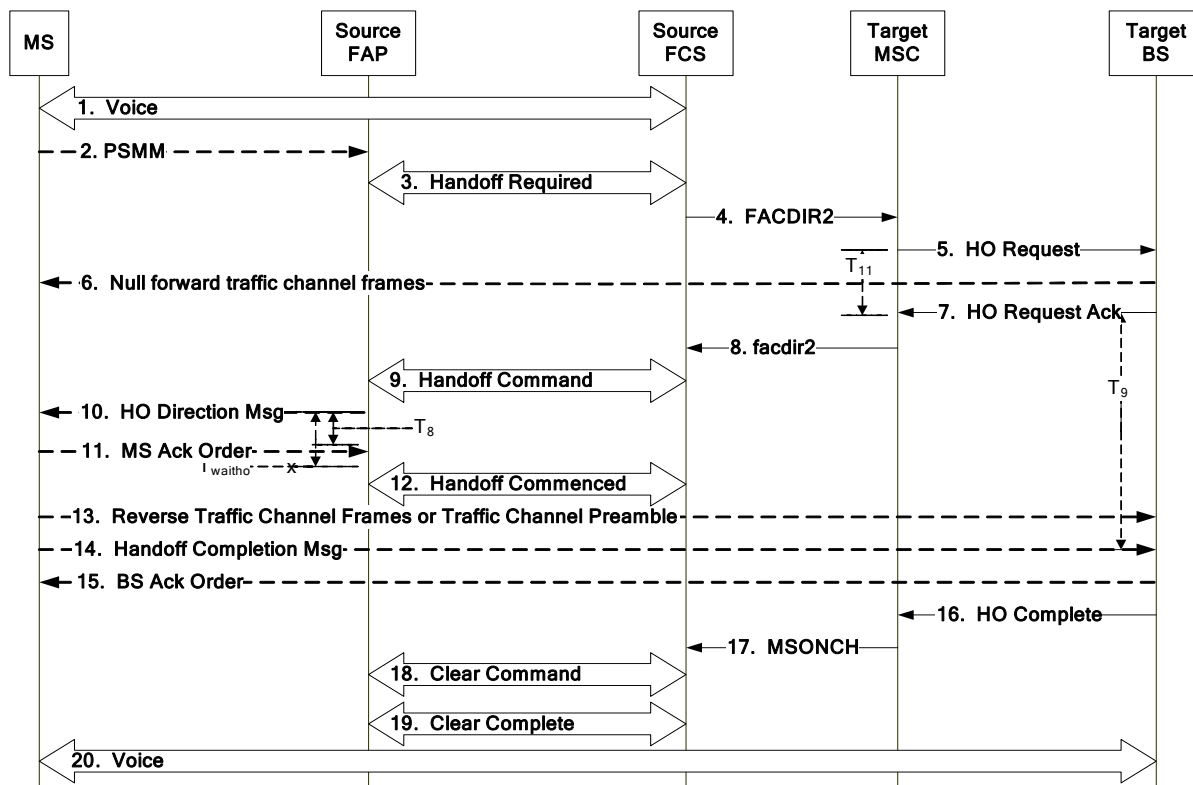


Figure 4.2.3.5-1 1x FAP to Macro BS Active Handoff

1. The MS is in a voice call via the source FAP and the source FCS.
2. The MS sends a PSMM message C.S0005 [6] to the source FAP.
3. Based on the PSMM, the source FAP decides to perform a hard handoff to the target BS. The source FAP sends a Handoff Required message with the list of target cells to the source FCS via Fx2 signaling. Refer to X.S0059-200 [13] for the messaging format between the FAP and the FCS.
4. The source FCS sends a FACDIR2 message to the target MSC via core network messaging. Refer to X.S0004 [9].
5. The target MSC sends a Handoff Request message to the target BS and starts timer T_{11} .
6. Upon receipt of the Handoff Request message from the target MSC, the target BS allocates the appropriate radio resources as specified in the message and connects the call. The target BS sends null forward traffic channel frames to the MS.
7. The target BS sends a Handoff Request Acknowledge message to the target MSC and starts timer T_9 to wait for arrival of the MS on its radio channel. The target MSC stops timer T_{11} upon the receipt of this message. The cell identifier list contains the BS Cell ID.
8. The target MSC sends the facdir2 message to the source FCS via core network messaging. Refer to X.S0004 [9].
9. The source FCS prepares to switch the MS from the source FAP to the target BS and sends a Handoff Command message to the source FAP via Fx2 signaling. The source FCS shall include in the Handoff Command message the service configuration records it received in the Handoff Request Ack message. Refer to X.S0059-200 [13].
10. The source FAP sends a handoff direction message to the MS and starts timer T_8 . If the MS is allowed to return to the source FAP, timer $T_{wait\ho}$ is also started by the source FAP.

- 1 11. The MS may acknowledge the handoff direction message by sending an MS Ack Order to the source
2 FAP. The source FAP stops timer T_8 upon receipt of this message.
- 3 12. The source FAP sends a Handoff Commenced message to the source FCS via Fx2 signaling to notify
4 it that the MS has been ordered to move to the target BS channel. If timer T_{wait} has been started, the
5 source BS shall wait for that timer to expire before sending the Handoff Commenced message.
- 6 13. The MS sends reverse traffic channel frames or the traffic channel preamble to the target cell(s).
- 7 14. The MS sends a Handoff Completion Message to the target BS. The target BS stops timer T_9 .
- 8 15. The target BS sends the BS Ack Order to the MS over the air interface.
- 9 16. The target BS sends a Handoff Complete message to the target MSC to notify it that the MS has
10 successfully completed the hard handoff.
- 11 17. The target MSC sends the MSONCH message to the source FCS via core network messaging to
12 notify it that the MS has successfully completed the hard handoff.
- 13 18. The source FCS sends a Clear Command message to the source FAP via Fx2 signaling.
- 14 19. The source FAP sends a Clear Complete message to the source FCS via Fx2 signaling to notify it that
15 clearing has been accomplished.
- 16 20. The MS is in a voice call via the target BS and the target MSC.

17 **4.2.4 HRPD Handoff**

18 This section describes the call flows associated with handoff between HRPD macro and femtocell
19 systems.

20 **4.2.4.1 HRPD Macro AN/PCF to FAP Dormant Handoff**

21 For the scenario when an HRPD AT performs a dormant handoff from a macro AN/PCF to a FAP, from
22 the perspective of the source AN/PCF these procedures are identical to those for a dormant handoff using
23 the A13 interface to retrieve session information. From the perspective of the target FAP, the
24 configuration of the handoff source appears as an AN/PCF and the handoff procedure occurs after
25 performing femtocell access control procedures. Refer to A.S0008 [1] and A.S0009 [2], Section 3.7 for
26 details and section 1.6.1.6 for femtocell access control procedures.

27 **4.2.4.2 HRPD FAP to Macro AN/PCF Dormant Handoff**

28 This scenario describes the call flow when an HRPD AT performs a dormant handoff from a FAP to a
29 macro AN/PCF. It is assumed that the AT has crossed a mobility boundary and that based on the UATI,
30 the AN/PCF sends the A13-Session Information Request message to the FGW instead of the FAP. This
31 call flow also assumes that the A13-Session Information Response and the A13-Session Information
32 Confirm messages are exchanged directly between the source FAP and the target AN/PCF.

33 Otherwise, if the AN/PCF is able to send the session request message directly to the FAP, then from the
34 perspective of the target AN/PCF these procedures are identical to those for a dormant handoff using the
35 A13 interface to retrieve session information. Refer to A.S0008 [1] and A.S0009 [2], Section 3.7 for
36 details.

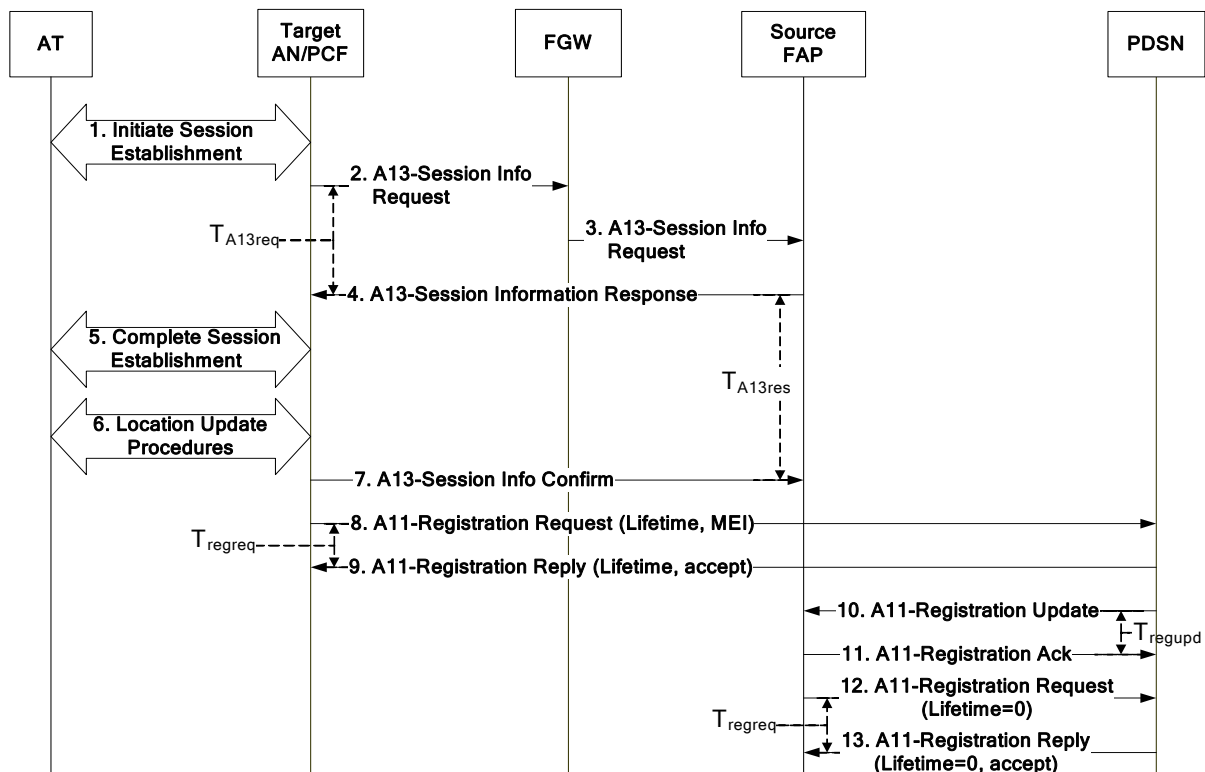


Figure 4.2.4.2-1 HRPD FAP to Macro AN/PCF Idle Handoff

1. After the AT crosses a mobility boundary (e.g., the macro AN pilot is the strongest pilot), the AT requests an HRPD connection. Subsequently, the AT and the macro target AN/PCF initiate HRPD session establishment. During this procedure, the target AN/PCF receives the UATI of an existing HRPD session (if available). The UATI can be used as an identifier for the existing HRPD session and based on the UATI, the target AN/PCF attempts to retrieve the existing HRPD session state information from the source FAP, via the FGW.
2. The target AN/PCF sends an A13-Session Information Request message to the FGW. The A13-Session Information Request message includes the received UATI, the Security Layer Packet and (target) Sector ID. The target AN/PCF starts timer T_{A13req} .
3. The FGW determines the address of the source FAP, through means outside the scope of this specification, and forwards the A13-Session Information Request message to the source FAP, to request the HRPD session information for the AT.
4. The source FAP validates the A13-Session Information Request and sends the requested HRPD session information of the AT to the target AN/PCF in an A13-Session Information Response message. The message may be sent directly to the target AN/PCF or through the FGW. The source FAP starts timer T_{A13res} . The target AN/PCF stops timer T_{A13req} .
5. The AT and the target AN/PCF complete the establishment of the HRPD session. Depending on the state of the AT and the target AN/PCF, either an existing HRPD session may be re-established, or a new HRPD session may be initiated if required. This step may be omitted if no further over-the-air signaling is required.
6. If the target AN/PCF supports the Location Update procedure, the target AN/PCF updates the ANID in the AT using the Location Update procedure. The target AN/PCF may also retrieve the PANID from the AT if necessary (e.g., the Session Configuration retrieved in step '4' indicates that the source FAP does not support the Location Update procedure).

- 1 7. The target AN/PCF sends an A13-Session Information Confirm message to the source FAP to
 2 indicate that the target AN/PCF has received the HRPD session information. The message may be
 3 sent directly to the source AN/PCF or through the FGW. Upon receipt of the A13-Session
 4 Information Confirm message, the source FAP deletes the associated AT HRPD session information
 5 and stops timer T_{A13res} .
- 6 8. The target AN/PCF selects the PDSN (refer to A.S0013 [3]), and sends an A11-Registration Request
 7 message to the PDSN to set up an A10 connection for each service connection. The A11-Registration
 8 Request message includes the MEI within the CVSE and a non-zero Lifetime. This message also
 9 includes a CVSE containing Accounting Data (A10 Connection Setup Airlink Record), if new A10
 10 connections are being established, and an Normal Vendor Specific Extension (NVSE) including
 11 ANID information (CANID/PANID). The target AN/PCF starts timer T_{regreq} .
- 12 9. The A11-Registration Request message is validated and the PDSN accepts the A10 connections by
 13 returning an A11-Registration Reply message with an accept indication and the Lifetime set to the
 14 configured T_{rp} value. If the PDSN has data to send, it includes the Data Available Indicator within the
 15 CVSE. If the subscriber has a Subscriber QoS Profile, the PDSN includes it in an NVSE. The A10
 16 connection binding information at the PDSN is updated to point to the target AN/PCF. The target
 17 AN/PCF stops timer T_{regreq} .
- 18 10. If the PDSN has A10 connections to another AN/PCF (e.g., the source FAP), it initiates closure of the
 19 A10 connections with that AN/PCF by sending an A11-Registration Update message. The PDSN
 20 starts timer T_{regupd} .
- 21 11. The source FAP responds with an A11-Registration Acknowledge message. The PDSN stops timer
 22 T_{regupd} .
- 23 12. The source FAP sends an A11-Registration Request message with Lifetime set to zero, to the PDSN.
 24 The source FAP starts timer T_{regreq} .
- 25 13. The PDSN sends an A11-Registration Reply message to the source FAP. The source FAP closes the
 26 A10 connections for the AT and stops timer T_{regreq} .

27 **4.2.4.3 HRPD Macro AN/PCF to FAP Connected State Session Transfer**

28 This section is for further study.

29 **4.2.4.4 HRPD FAP to Macro AN/PCF Connected State Session Transfer**

30 For the scenario when an AT with an active HRPD connection hands off from a FAP to a macro AN,
 31 from the perspective of the target AN/PCF these procedures are identical to those for a connected state
 32 handoff using the A16 interface to request a session transfer. From the perspective of the source FAP, the
 33 configuration of the handoff target appears as an AN/PCF. Refer to section 3.3.4 for details.

34 **4.3 LIPA Session Establishment between FAP and AT**

35 This section describes the call flows associated with bringing up the LIPA interface at the AT.

36 **4.3.1 Successful LIPA Session Establishment**

37 This scenario describes the call flow associated with session establishment for an AT that supports LIPA.

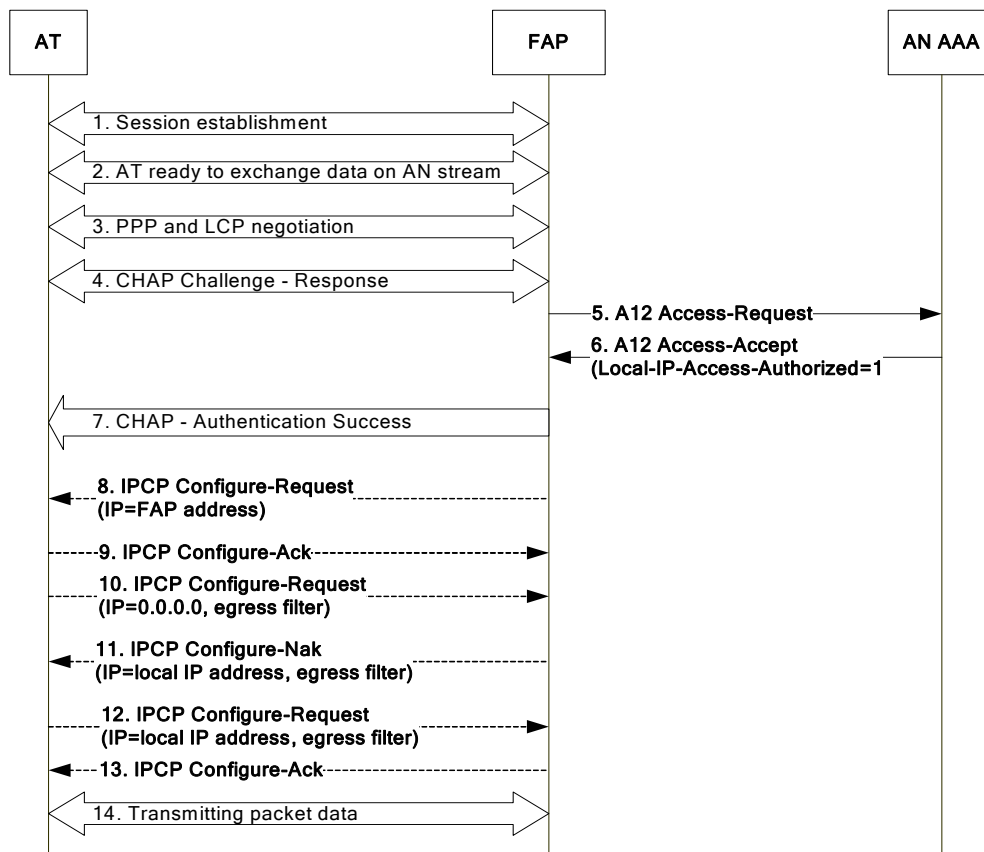


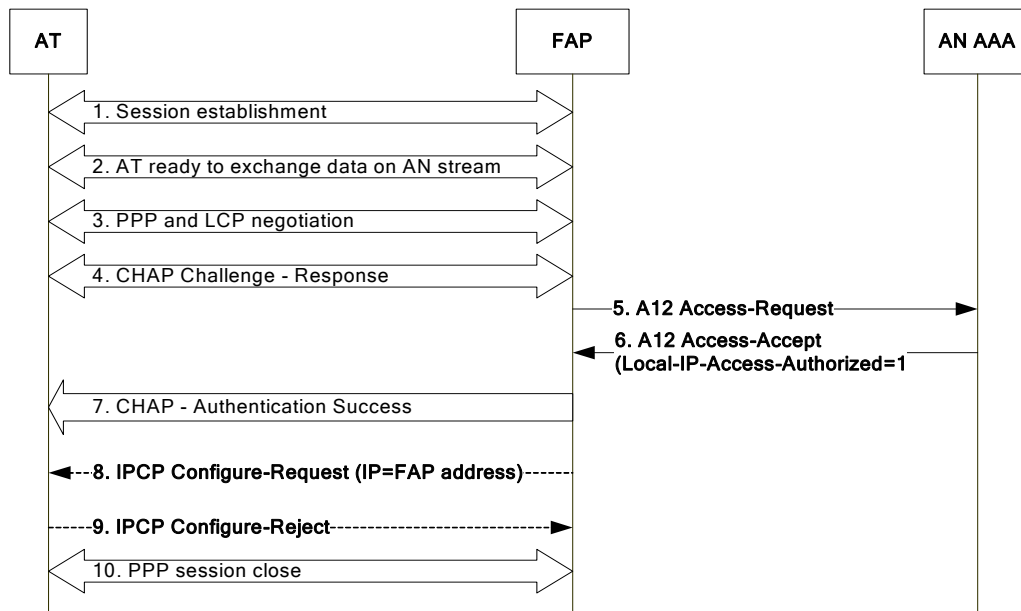
Figure 4.3.1-1 Successful LIPA Session Establishment

1. The AT and the FAP initiate HRPD session establishment. During this procedure, the FAP does not receive a UATI for an existing HRPD session. Since no session exists between the AT and the FAP, a session is established where protocols and protocol configurations are negotiated, stored and used for communications between the AT and the FAP. Refer to C.S0024 [7], Session Layer.
2. The AT indicates that it is ready to exchange data on the access stream (e.g., the flow control protocol for the default packet application bound to the FAP is in the open state).
3. The AT and the FAP initiate Point-to-Point Protocol (PPP) and LCP negotiations for access authentication for the architecture specified in A.S0008 (or terminal authentication for the architecture specified in A.S0009). Refer to RFC 1661 [16].
4. If the FAP supports access/terminal authentication and the A12 interface, the FAP generates a random challenge and sends it to the AT in a CHAP Challenge message in accordance with RFC 1994 [19].
5. When the FAP receives the CHAP response message from the AT, it sends an Access-Request message on the A12 interface to the AN-AAA, which acts as a RADIUS server in accordance with RFC 2865 [26]).
6. The AN-AAA looks up a password based on the User-name attribute in the Access-Request message and if the access/terminal authentication passes (as specified in RFC 1994 [19] and RFC 2865 [26]), the AN-AAA sends an Access-Accept message on the A12 interface in accordance with RFC 2865 [26]. The Access-Accept message contains a RADIUS attribute with Type set to 20 (Callback-Id), which is set to the MN ID of the AT. The Access-Accept message also includes a RADIUS attribute Local-IP-Access-Authorized indicating the AT is authorized to be assigned a local IP address.

- 1 7. The FAP returns an indication of CHAP access/terminal authentication success to the AT. Refer
2 to RFC 1994 [19].
- 3 8. The FAP sends an IPCP Configure-Request message including its IP address.
- 4 9. The LIPA-capable AT sends an IPCP Configure-Ack message.
- 5 10. The AT sends an IPCP Configure-Request message to the FAP to request a local IP address. The
6 AT may include either a NULL IP address or the non-zero IP address it wants to use for the LIPA
7 interface. The AT also includes a vendor specific option indicating it currently has no egress
8 packet filter criteria.
- 9 11. The FAP assigns a local IP address for the AT and sends it to the AT in an IPCP Configure-Nak
10 message. The FAP also includes a vendor specific option that includes the egress packet filter
11 criteria that the AT should use to determine for each packet whether it should traverse through the
12 LIPA interface.
- 13 12. The AT sends an IPCP Configure-Request message with the local IP address assigned to it and
14 the vendor specific option indicating the egress packet filter criteria to be use.
- 15 13. The FAP sends an IPCP Configure-Ack message in acknowledgement to the IPCP Configure-
16 Request message received in step '12'.
- 17 14. At this point, the main connection is established and packet data can flow from the AT to the
18 local intranet and internet through the LIPA interface at the AT without using the operator's
19 network resources.

20 4.3.2 LIPA not Supported at the AT

21 This scenario describes the call flow associated with session establishment for an AT that does not
22 support LIPA.



23
24 **Figure 4.3.2-1 LIPA not Supported by AT: Session Establishment Failure**

- 25 1. The AT and the FAP initiate HRPD session establishment. During this procedure, the FAP does
26 not receive a UATI for an existing HRPD session. Since no session exists between the AT and the
27 FAP, a session is established where protocols and protocol configurations are negotiated, stored
28 and used for communications between the AT and the FAP. Refer to C.S0024 [7], Session Layer.

2. The AT indicates that it is ready to exchange data on the access stream (e.g., the flow control protocol for the default packet application bound to the FAP is in the open state).
3. The AT and the FAP initiate PPP and LCP negotiations for access authentication for the architecture specified in A.S0008 (or terminal authentication for the architecture specified in A.S0009). Refer to RFC 1661 [16].
4. If the FAP supports access/terminal authentication and the A12 interface, the FAP generates a random challenge and sends it to the AT in a CHAP Challenge message in accordance with RFC 1994 [19].
5. When the FAP receives the CHAP response message from the AT, it sends an Access-Request message on the A12 interface to the AN-AAA which acts as a RADIUS server in accordance with RFC 2865 [26]).
6. The AN-AAA looks up a password based on the User-name attribute in the Access-Request message and if the access/terminal authentication passes (as specified in RFC 1994 [19] and RFC 2865 [26]), the AN-AAA sends an Access-Accept message on the A12 interface in accordance with RFC 2865 [26]. The Access-Accept message contains a RADIUS attribute with Type set to 20 (Callback-Id), which is set to the MN ID of the AT. The Access-Accept message also includes a RADIUS attribute Local-IP-Access-Authorized indicating the AT is authorized to be assigned a local IP address.
7. The FAP returns an indication of CHAP access/terminal authentication success to the AT. Refer to RFC 1994 [19].
8. The FAP sends an IPCP Configure-Request message including its IP address.
9. The AT sends an IPCP Configure-Reject message back to the FAP. The AT may also drop the IPCP packet received from the FAP over the AN-PPP stream. In this case, the FAP may repeat sending the IPCP Configure-Request message multiple times.
10. The FAP terminates the AN-PPP session.

4.3.3 LIPA Terminated after Handoff

This scenario describes the call flow associated with termination of LIPA upon completion of handoff from the source FAP.

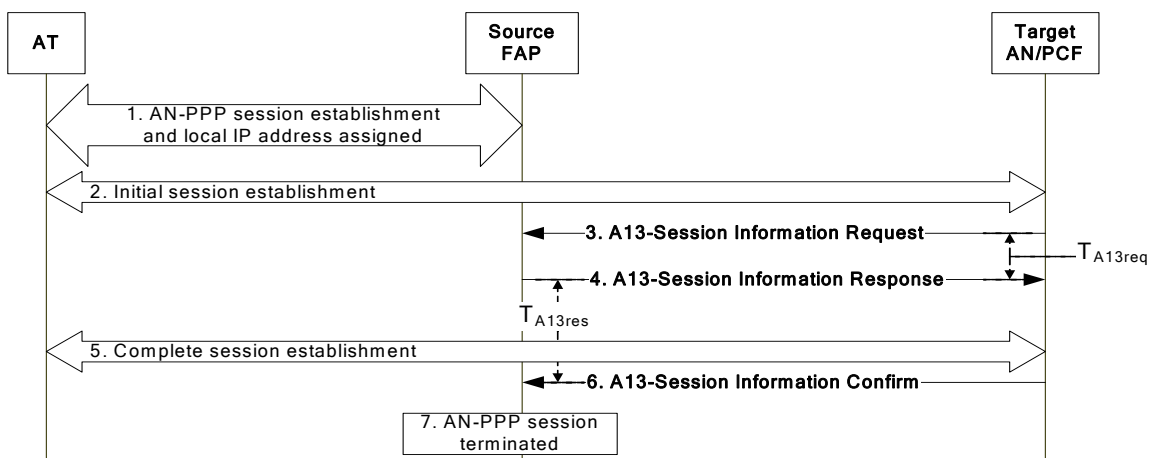


Figure 4.3.3-1 LIPA Terminated After Handoff

1. The source FAP and the AT establish an AN-PPP session and the AT is also assigned a local IP address.

- 1 2. Upon the AT crossing a mobility boundary, the AT and the target AN/PCF initiate HRPD session
2 establishment. During this procedure, the target AN/PCF receives the UATI of an existing HRPD
3 session. The AT terminates its AN-PPP session as it crosses the HRPD subnet boundary.
4
5 Note: The target AN/PCF can send the A13-Session Information Request message to the source
6 FAP via the FGW, based on the destination IP address provided for the A13-Session Information
7 Request message. Refer to section 3.3.3.1.
8
9 3. The target AN/PCF sends an A13-Session Information Request message to the source FAP to
10 request the HRPD session information for the AT. The A13-Session Information Request
11 message shall include the received UATI, the Security Layer Packet and Sector ID. The target
12 AN/PCF starts timer T_{A13req} .
13
14 4. The source FAP validates the A13-Session Information Request and sends the requested HRPD
15 session information of the AT to the target AN/PCF in an A13-Session Information Response
16 message. The source FAP starts timer T_{A13res} . The target AN/PCF stops timer T_{A13req} .
17
18 5. The AT and the target AN/PCF complete the establishment of the HRPD session.
19
20 6. The target AN/PCF sends an A13-Session Information Confirm message to the source FAP to
 indicate that the target AN/PCF has received the HRPD session information. Upon receipt of the
 A13-Session Information Confirm message, the source FAP deletes the associated AT HRPD
 session information. The source FAP stops timer T_{A13res} .

 7. Upon receipt of the A13-Session Information Confirm message, the source FAP also deletes the
 AN-PPP session.

1
2
3

(This page intentionally left blank)