

3GPP2 X.S0034-0

Version 1.0

Date: April 2005



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

cdma2000/GPRS Roaming

COPYRIGHT

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.

Foreword

(This foreword is not part of this document)

This document was prepared by 3GPP2 TSG-X.

This document is a new specification.

Revision History

Revision		Date
Rev.0	Initial Publication	April 2005

1		
2	Table of Contents	
3	Revision History	iii
4	Table of Contents.....	i
5	List of Figures.....	iii
6	List of Tables	iv
7	1 Introduction.....	1
8	1.1 Scope	1
9	2 References.....	2
10	2.1 Normative References	2
11	2.2 Informative References.....	3
12	3 Goals and Assumptions.....	4
13	4 Definitions and Abbreviations	5
14	4.1 Definitions	5
15	4.2 Abbreviations	5
16	5 Reference Model	7
17	5.1 IIF Description.....	7
18	5.2 Reference Points	8
19	6 General Requirements.....	9
20	6.1 Roaming Directions	9
21	6.2 Authentication and Authorization.....	9
22	6.3 Roaming Connectivity.....	9
23	6.4 Data Integrity and Privacy	9
24	6.5 Accounting	9
25	7 Roaming Scenarios & Description	10
26	7.1 GPRS Foreign Mode with Mobile IPv4	10
27	7.2 GPRS Foreign Mode with Simple IPv4.....	11
28	7.3 cdma2000 Packet Data Foreign Mode with Mobile IPv4.....	12
29	7.4 cdma2000 Packet Data Foreign Mode with Simple IPv4.....	13
30	8 Functional & Interface Requirements	16
31	8.1 GPRS Foreign Mode with Mobile IPv4	16
32	8.1.1 HLR/ VLR Requirements for IIF.....	16
33	8.1.2 GGSN/FA Requirements for IIF.....	16
34	8.1.2.1 PDP Context Establishment	16
35	8.1.2.2 Mobile IP Registration	16
36	8.1.2.3 PDP Context Deactivation and Mobile IP De-registration.....	17
37	8.1.2.4 IPsec Support	17
38	8.1.2.5 Transport	17
39	8.1.3 RADIUS Client Requirements for IIF	17
40	8.1.3.1 IETF Standard RADIUS Attributes	18
41	8.1.3.2 3GPP2 Vendor Specific Attributes.....	18
42	8.1.4 MS Requirements	19
43	8.1.4.1 PDP Context Activation.....	19
44	8.1.4.2 Mobile IP Registration	20
45	8.1.4.3 Termination	20
46	8.1.5 Reverse Tunneling support between the IIF and the HA.....	20
47	8.2 GPRS Foreign Mode with Simple IPv4.....	20
48	8.2.1 HLR/VLR Requirements for IIF.....	20
49	8.2.2 GGSN/LAC Requirements for IIF.....	20
50	8.2.2.1 PDP Context Activation and Address Assignment	20
51	8.2.2.2 L2TP Support	21
52	8.2.2.2.1 L2TP Tunnel/Session Establishment with Pre-Configured LNS Address	21

1	8.2.2.2.2	L2TP Tunnel/Session Establishment without Pre-Configured LNS Address.....	21
2	8.2.2.2.3	IPsec Support.....	22
3	8.2.2.2.4	L2TP session termination	22
4	8.2.2.2.5	Transport.....	22
5	8.2.3	RADIUS Client Requirements for IIF	22
6	8.2.4	MS Requirements	23
7	8.2.5	LNS Requirements for the Home cdma2000 Packet Data System	23
8	8.2.5.1	PPP Negotiation	23
9	8.2.5.1.1	PPP Authentication.....	23
10	8.2.5.1.2	IPCP.....	24
11	8.2.5.2	IPsec support.....	24
12	8.2.6	HAAA Requirements.....	24
13	8.3	cdma2000 Packet Data Foreign Mode with Mobile IPv4.....	24
14	8.3.1	HLR/VLR Requirements for IIF.....	24
15	8.3.2	AAA Requirements for IIF.....	24
16	8.3.2.1	RADIUS Access-Request.....	24
17	8.3.2.2	RADIUS Access-Accept.....	25
18	8.3.2.3	RADIUS Accounting-Request START.....	25
19	8.3.2.4	RADIUS Accounting-Request INTERIM.....	25
20	8.3.2.5	RADIUS Accounting-Request STOP.....	26
21	8.3.3	HA/SGSN Requirements for IIF.....	26
22	8.3.3.1	Mobile IP Authentication	26
23	8.3.3.2	PDP Context Management	26
24	8.3.3.3	IPsec Support	28
25	8.3.3.4	Transport Requirements for IIF.....	28
26	8.3.4	MS Requirements	28
27	8.4	cdma2000 Packet Data Foreign Mode with Simple IPv4.....	28
28	8.4.1	HLR/VLR Requirements for IIF.....	28
29	8.4.2	AAA Requirements for IIF.....	28
30	8.4.2.1	RADIUS Access-Request.....	29
31	8.4.2.2	RADIUS Access-Accept.....	29
32	8.4.2.3	RADIUS Accounting-Request START.....	29
33	8.4.2.4	RADIUS Accounting-Request INTERIM.....	29
34	8.4.2.5	RADIUS Accounting-Request STOP.....	29
35	8.4.3	LNS/SGSN Requirements for IIF.....	29
36	8.4.3.1	L2TP Tunnel/Session Establishment.....	29
37	8.4.3.2	PPP Authentication	30
38	8.4.3.3	PDP Context Establishment	30
39	8.4.3.4	IPCP Negotiation	31
40	8.4.3.5	Transport	31
41	8.4.3.6	Termination	31
42	8.4.4	PDSN Requirements	31
43	8.4.4.1	PPP LCP Negotiation and Authentication.....	32
44	8.4.4.2	L2TP Tunnel/Session Establishment.....	32
45	8.4.4.3	IPsec Support	32
46	8.4.4.4	Transport	32
47	8.4.4.5	Termination	32
48	8.4.5	MS Requirements	32
49	9	Call Flow Examples	33
50	9.1	GPRS Foreign Mode with Mobile IPv4	33
51	9.2	GPRS Foreign Mode with Simple IP.....	36
52	9.3	cdma2000 Packet Data Foreign Mode with Mobile IPv4.....	38
53	9.4	cdma2000 Packet Data Foreign Mode with Simple IP.....	40
54			

1 List of Figures

2	Figure 1	cdma2000/GPRS roaming reference model	7
3	Figure 2	GPRS foreign mode with Mobile IPv4	10
4	Figure 3	GPRS foreign mode with Simple IPv4.....	11
5	Figure 4	cdma2000 packet data foreign mode with Mobile IPv4 with bearer connectivity between the visited and home systems	12
6			
7	Figure 5	cdma2000 packet data foreign mode with Mobile IPv4 without bearer connectivity between the visited and home systems	13
8			
9	Figure 6	cdma2000 packet data foreign mode with Simple IPv4 with bearer connectivity between the visited and home systems	14
10			
11	Figure 7	cdma2000 packet data foreign mode with Simple IPv4 without bearer connectivity between the visited and home systems	15
12			
13	Figure 8	Mobile IPv4 operation in the GPRS foreign mode.....	34
14	Figure 9	Simple IP operation in the GPRS foreign mode.....	37
15	Figure 10	Mobile IPv4 operation in the cdma2000 packet data foreign mode	39
16	Figure 11	Simple IP operation in the cdma2000 packet data foreign mode	41
17			
18			

1 **List of Tables**

2

3

No table is specified in this document.

1 Introduction

When a subscriber to one data network type (e.g., cdma2000^{®1} packet data) roams to a network of another type (e.g., GPRS), inter-working and interoperability functions are required to support packet data roaming. This document describes an Interworking and Interoperability Function (IIF) to support cross-technology roaming between a cdma2000 packet data system and a GPRS system.

“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 that (in the negative form) 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.

1.1 Scope

The scope of this document includes the roaming of a subscriber homed in a cdma2000 packet data system to a GPRS system and vice versa. The roaming between cdma2000 packet data systems is outside the scope of this document.

¹ “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.”

2 References

This section provides references to other specifications and standards that are necessary to implement the specifications in this document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP2 document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

2.1 Normative References

- [1] **3GPP2:** X.S0023-B v1.0, Network Interworking Between GSM MAP and TIA-41 MAP – cdma2000 Support, July 2004
- [2] **3GPP2:** P.S0001-A v3.0, Wireless IP Network Standard, July 2001
- [3] **IETF:** RFC 2661, Townsley, et al, ‘Layer Two Tunneling Protocol “L2TP” ’, August 1999
- [4] **3GPP:** TS 29.002, Mobile Application Part (MAP) specification, June 2004
- [5] **3GPP:** TS 29.060, General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp interface, March 2004
- [6] **3GPP:** TS 29.061, Interworking between the Public Land Mobile Network (PLMN) supporting packet based service and Packet Data Networks (PDN), January 2004
- [7] **IETF:** RFC 2794, Calhoun, et al, ‘Mobile IP Network Access Identifier Extension for IPv4’, March 2000
- [8] **IETF:** RFC 2002, Perkins, ‘IP Mobility Support’, October 1996
- [9] **IETF:** RFC 3012, Perkins, et al, ‘Mobile IPv4 Challenge/Response Extensions’, November 2000
- [10] **3GPP:** TS 23.003, Numbering, addressing and identification, January 2004
- [11] **3GPP:** TS 23.060, General Packet Radio Service (GPRS); Service description; Stage 2, December 2003
- [12] **IETF:** RFC 2809, Aboba, et al, ‘Implementation of L2TP Compulsory Tunneling via RADIUS’, April 2000
- [13] **IETF:** RFC 2868, Zorn, et al, ‘RADIUS Attributes for Tunnel Protocol Support’, June 2000
- [14] **3GPP:** TS 44.065, Mobile Station (MS) – Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDP), September 2004

- 1 [15] **3GPP**: TS 24.008, Mobile radio interface layer 3 specification; Core Network Protocols;
2 Stage 3, June 2004
- 3 [16] **IETF**: RFC 1144, Jacobson, 'Compressing TCP/IP Headers for Low-Speed Serial
4 Links', February 1990
- 5 [17] **IETF**: RFC 1962, Rand, 'The PPP Compression Control Protocol (CCP)', June 1996
- 6 [18] **IETF**: RFC 1974, Friend, et al, 'PPP Stac LZS Compression Protocol', August 1996
- 7 [19] **IETF**: RFC 2118, Pall, 'Microsoft Point-To-Point Compression (MPPC) Protocol',
8 March 1997
- 9 [20] **3GPP2**: A.S0001, 3GPP2 Access Network Interfaces Interoperability Specification (3G-
10 IOS v4.0.0) Release A (1999) Revision 0, January 2000

11 **2.2 Informative References**

12 No informative reference is specified.

1 **3 Goals and Assumptions**

2 This section provides the goals and assumptions for cdma2000/GPRS roaming:

- 3 1. This document supports roaming between cdma2000 packet data systems (based on [2])
4 and GPRS systems (based on Release 97, 98, 99).
- 5 2. There is a goal to minimize additional requirements on the cdma2000 packet data system
6 for supporting cdma2000/GPRS roaming.
- 7 3. No changes are to be required for 3GPP documents.
- 8 4. This document does not support the handoff of packet data sessions between a cdma2000
9 packet data system and a GPRS system.

4 Definitions and Abbreviations

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

4.1 Definitions

cdma2000 Packet Data Native Subscriber describes an end user whose primary or home subscription resides in a cdma2000 packet data system.

GPRS Native Subscriber describes an end user whose primary or home subscription resides in a GPRS system. **cdma2000 Packet Data Foreign Mode** indicates the condition or state of a GPRS native subscriber accessing a cdma2000 packet data system.

GPRS Foreign Mode indicates the condition or state of a cdma2000 packet data native subscriber accessing a GPRS system.

Roaming Exchange describes 3rd-party facilities providing connectivity and transport of signaling and/or bearer data exchanged between a cdma2000 packet data system and a GPRS system.

4.2 Abbreviations

AAA	Authentication, Authorization, and Accounting
ANSI	American National Standards Institute
APN	Access Point Name
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
DNS	Domain Name System
FA	Foreign Agent
FAC	Foreign Agent Challenge
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRX	GPRS Roaming exchange
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
HA	Home Agent
HLR	Home Location Register
IIF	Interworking and Interoperability Function
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol

1	IPCP	Internet Protocol Control Protocol
2	IRM	International Roaming MIN
3	LAC	L2TP Access Concentrator
4	LCP	Link Control Protocol
5	LNS	L2TP Network Server
6	L2TP	Layer Two Tunneling Protocol
7	MCC	Mobile Country Code
8	MIN	Mobile Identification Number
9	MNC	Mobile Network Code
10	MS	Mobile Station
11	NAI	Network Access Identifier
12	NSAPI	Network Layer Service Access Point Identifier
13	PAP	Password Authentication Protocol
14	PDP	Packet Data Protocol
15	PDSN	Packet Data Serving Node
16	PPP	Point to Point Protocol
17	RADIUS	Remote Authentication Dial In User Service
18	RRP	Registration Reply
19	RRQ	Registration Request
20	SGSN	Serving GPRS Support Node
21	SO	Service Option
22	TEID	Tunnel Endpoint ID
23	VLR	Visited Location Register
24		

5 Reference Model

The Interworking and Interoperability Function (IIF) provides signaling control and bearer interfaces between cdma2000 packet data systems and GPRS systems. The IIF enables service access when a subscriber operates in a visited network whose signaling and network protocols are different from the home network's protocols. Figure 1 depicts the family of network interfaces provided by the IIF in interconnecting networks. Bold lines are the bearer paths, non-bold lines indicate signaling paths.

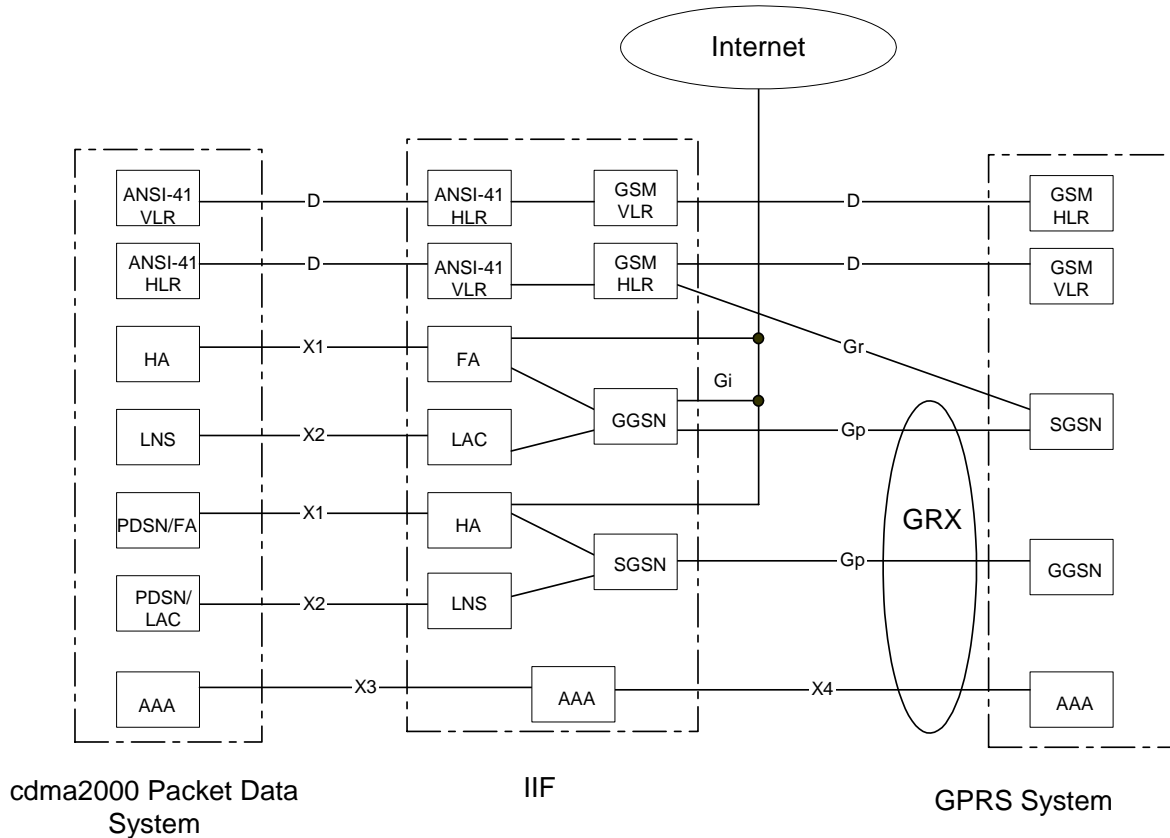


Figure 1 cdma2000/GPRS roaming reference model

5.1 IIF Description

The Interworking and Interoperability Function (IIF) supports the following functions:

- ANSI-41 VLR and/or HLR
- GSM VLR and/or HLR
- Mobile IP Foreign Agent (FA) and/or Home Agent (HA)
- L2TP Access Concentrator (LAC) and/or L2TP Network Server (LNS) for L2TP tunnel management (i.e., establishment, maintenance, and termination)

- 1 • GGSN and/or SGSN for GTP tunnel management
- 2 • RADIUS protocols for interacting with AAA server in the cdma2000
- 3 system and/or GPRS system

4 **5.2 Reference Points**

5 Reference D is the interface between HLR and VLR. This interface is specified in [1].

6 Reference X1 is the interface between Mobile IP HA and FA. This interface is specified in [2].

7 Reference X2 is the interface between LAC and LNS. This interface is specified in [3].

8 Reference X3 is the interface between IIF and AAA server in the cdma2000 system for exchanging
9 cdma2000 packet data authentication, authorization, and accounting information. This interface is
10 based on [2] with enhancements to support L2TP tunneling.

11 Reference X4 is the interface between an IIF and a AAA server in the GPRS system for exchanging
12 3GPP packet data authentication, authorization, and accounting information based on RADIUS. This
13 interface is specified in [6].

14 Reference Gr is the interface between IIF and SGSN for the authentication of a GPRS attach. This
15 interface is specified in [1] and [4].

16 Reference Gp is the interface between SGSN and GGSN. This interface is specified in [5][11].

17 Reference Gi is the interface between the GGSN and Internet. This interface is specified in [6].

6 General Requirements

This section provides general requirements for cdma2000/GPRS roaming.

6.1 Roaming Directions

- It shall be possible to support cdma2000 packet data foreign mode.
- It shall be possible to support GPRS foreign mode.

6.2 Authentication and Authorization

- Authentication and authorization for packet data access of a subscriber operating in foreign mode (i.e., cdma2000 packet data foreign mode or GPRS foreign mode) should be performed by the home network of the subscriber.

6.3 Roaming Connectivity

- It shall be possible for the roaming MS to establish connectivity to the Internet through the serving system directly, or through the serving and home systems.
- If the GPRS system has connectivity through a roaming exchange (e.g., GRX), it shall be possible to support connectivity between the cdma2000 packet data system and GPRS system through the roaming exchange.
- cdma2000 packet data systems shall support the cdma2000 foreign mode for MS using:
 - a. Mobile IPv4
 - b. Simple IPv4
 - c. Simultaneous Mobile IPv4 and Simple IPv4

6.4 Data Integrity and Privacy

- The integrity of signaling data exchanged between the cdma2000 packet data system and GPRS system shall be possible.
- The privacy of signaling and bearer data exchanged between the cdma2000 packet data system and GPRS system shall be possible.

6.5 Accounting

- The accounting information for the MS's roaming access shall be made available to the home system.
- A set of accounting record types shall be defined for cdma2000/GPRS data roaming. The intention of this requirement is to maximize compatibility with existing accounting documents in 3GPP and 3GPP2.

7 Roaming Scenarios & Description

This section describes the architectures for four cdma2000/GPRS roaming scenarios:

- GPRS foreign mode with Mobile IPv4,
- GPRS foreign mode with Simple IPv4,
- cdma2000 packet data foreign mode with Mobile IPv4,
- cdma2000 packet data foreign mode with Simple IPv4.

7.1 GPRS Foreign Mode with Mobile IPv4

This section describes the roaming scenario where a cdma2000 packet data native subscriber operates a terminal supporting Mobile IPv4 [2] in GPRS foreign mode. Figure 2 depicts the functions and control interface associated with the IIF that provides signaling and bearer connectivity between the CDMA packet data system and the GPRS system.

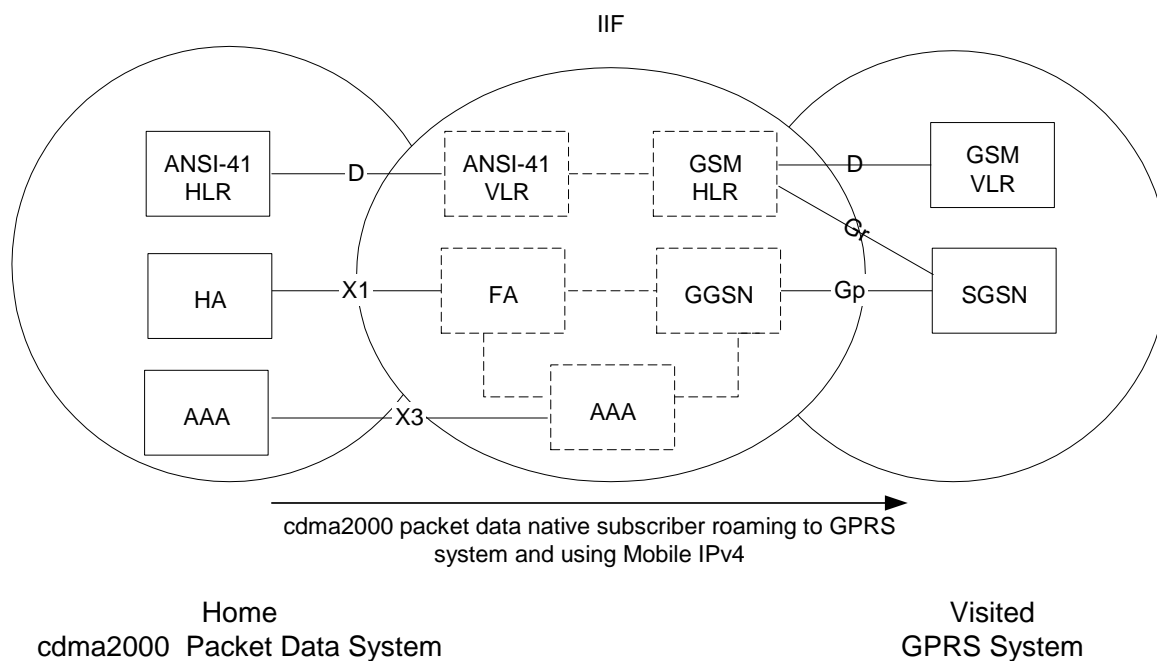


Figure 2 GPRS foreign mode with Mobile IPv4

The IIF provides both GSM HLR and ANSI-41 VLR emulation to allow the subscriber to register. This interworking is provided over the interface references “Gr” and “D”. The Gr and D interfaces are specified in [1].

The IIF provides GGSN and FA emulation to support bearer connectivity between the visited and home networks via the IIF. This interworking is provided over the interface references “Gp” and

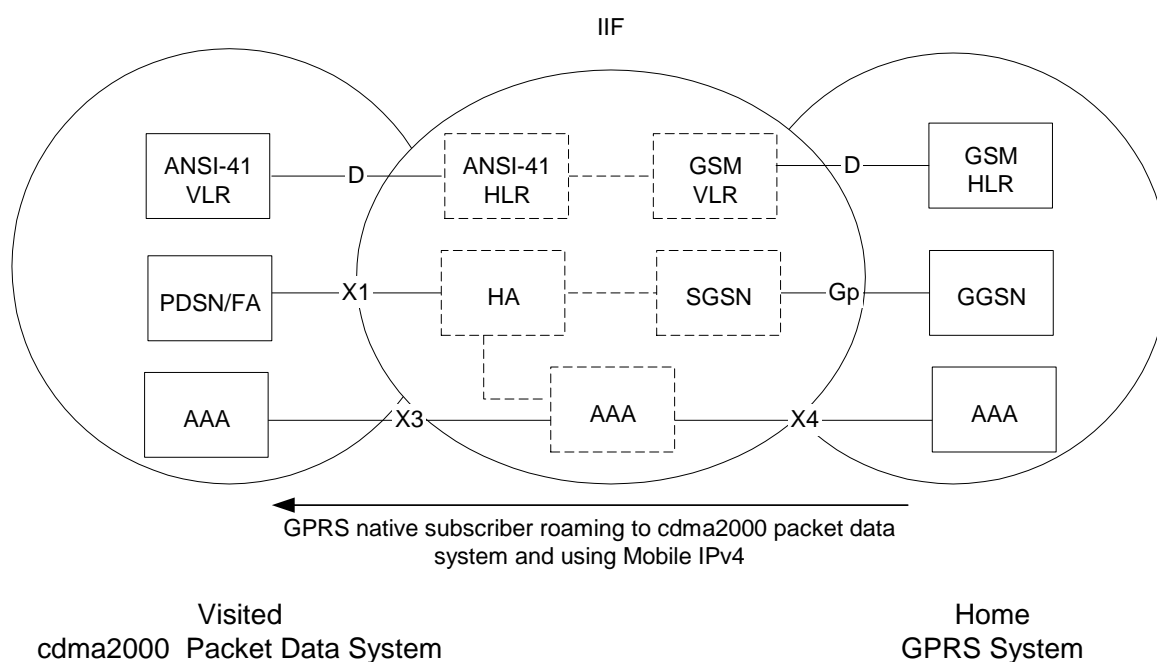
1 (GRX). If the IIF is in the home cdma2000 packet data system, X2 is not required. The X2 and Gp
2 interfaces are specified in [3] and [5][11], respectively.

3 The IIF provides AAA emulation to interact with the home network's AAA for supporting Simple IP
4 authentication/authorization and 3GPP2 packet data accounting. This interworking is provided over
5 the interface reference "X3". The X3 interface is specified in [2].

6 If bearer connectivity between the cdma2000 packet data system and GPRS system is not required,
7 then the X2 interfaces is not required for the IIF in Figure 3. The IIF still supports the Gp interface to
8 the SGSN and provides the Internet access via the Gi interface (not shown in the figure).

9 **7.3 cdma2000 Packet Data Foreign Mode with Mobile IPv4**

10 This section describes the roaming scenario where a GPRS native subscriber operates a terminal
11 supporting Mobile IPv4 [2] in the cdma2000 packet data foreign mode. Figure 4 depicts the functions
12 and control interface associated with the IIF that provides signaling and bearer connectivity between
13 the cdma2000 packet data system and the GPRS system.



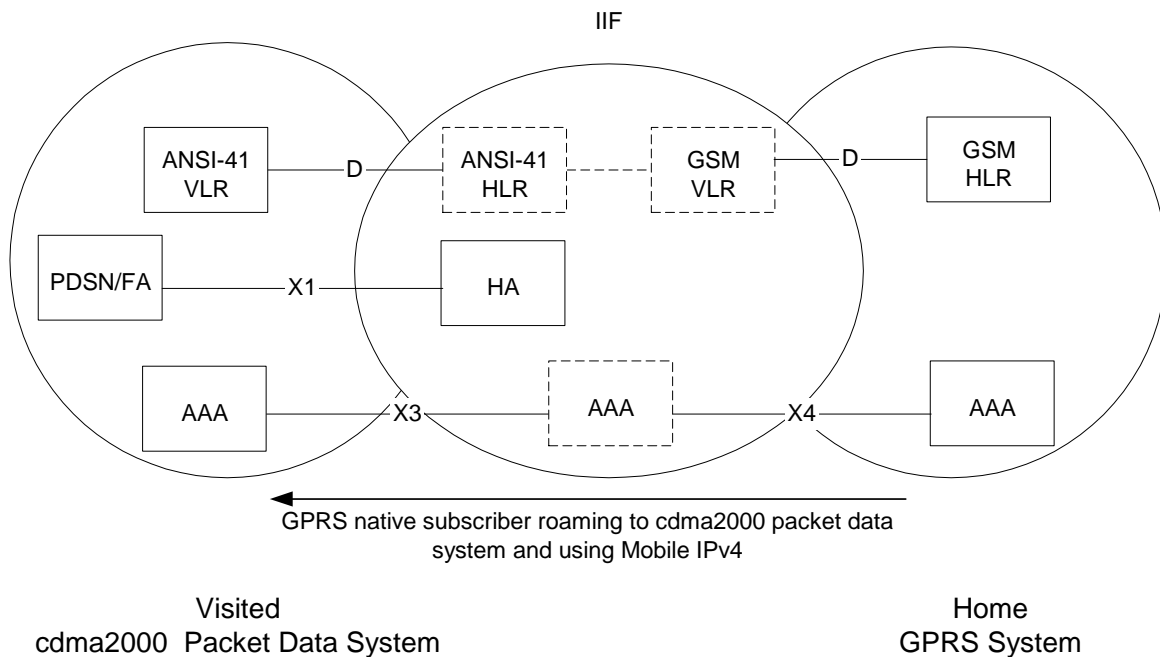
14
15 **Figure 4 cdma2000 packet data foreign mode with Mobile IPv4 with bearer connectivity**
16 **between the visited and home systems**

17 The IIF provides both GSM VLR and ANSI-41 HLR emulation to allow the subscriber to register.
18 This interworking is provided over the interface reference "D". The D interface is specified in [1].

19 The IIF provides HA and SGSN emulation to support bearer connectivity between the visited and
20 home networks via the IIF. This interworking is provided over the interface reference "X1" and "Gp".
21 The Gp interface connectivity may be provided by GPRS Roaming eXchange (GRX). The X1 and
22 Gp interfaces are specified in [2] and [5][11], respectively.

1 The IIF provides AAA emulation to interact with the visited network's AAA and home network's
 2 AAA over the interface reference "X3" and "X4", respectively, for supporting Mobile IP FAC
 3 authentication/authorization, cdma2000 packet data accounting, and GPRS packet data accounting.
 4 The X3 and X4 interfaces are specified in [2] and [6], respectively.

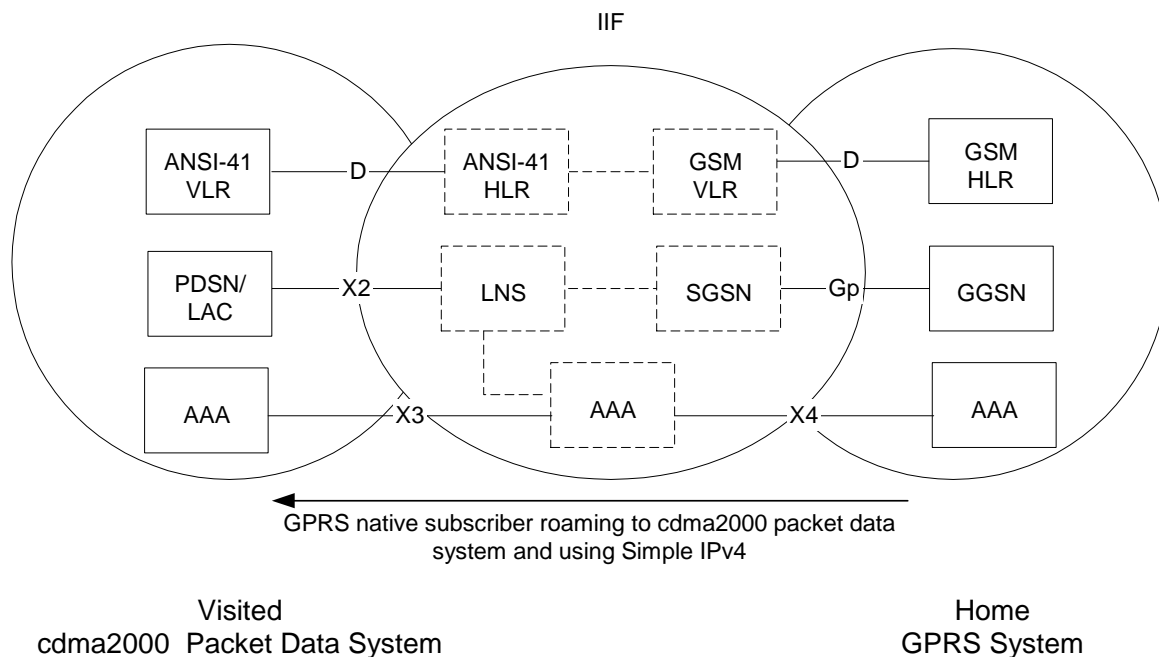
5 Figure 5 depicts the functions and control interface associated with the IIF if bearer connectivity
 6 between the visited cdma2000 packet data system and home GPRS system is not required. In this
 7 case, the MS gains access to the Internet directly from the IIF. The X1, X3 and X4 interfaces are still
 8 required.



9
 10 **Figure 5 cdma2000 packet data foreign mode with Mobile IPv4 without bearer connectivity**
 11 **between the visited and home systems**

12 **7.4 cdma2000 Packet Data Foreign Mode with Simple IPv4**

13 This section describes the roaming scenario where a GPRS native subscriber operates a terminal
 14 supporting Simple IPv4 in the cdma2000 packet data foreign mode. Figure 6 depicts the functions
 15 and control interface associated with the IIF that provides signaling and bearer connectivity between
 16 the cdma2000 packet data system and the GPRS system.



1

2

Figure 6 cdma2000 packet data foreign mode with Simple IPv4 with bearer connectivity between the visited and home systems

3

4

The IIF provides both GSM VLR and ANSI-41 HLR emulation to allow the subscriber to register. This interworking is provided over the interface reference “D”. The D interface is specified in [1].

5

6

The IIF provides LNS and SGSN emulation to support bearer connectivity between the visited and home networks via the IIF. This interworking is provided over the interface reference “X2” and “Gp”. The Gp interface connectivity may be provided by GPRS Roaming eXchange (GRX). The X2 interface does not maintain the same MS’s packet data session across PDSNs; in other words, if the MS changes PDSN, the MS and LNS establish a new PPP session via the new PDSN/LAC. The X2 and Gp interfaces are specified in [3] and [5][11], respectively.

7

8

9

10

11

12

The IIF provides AAA emulation to interact with the visited network’s AAA and home network’s AAA over the interface reference “X3” and “X4”, respectively, for supporting Simple IP authentication/authorization, cdma2000 packet data accounting, and GPRS packet data accounting. The X3 and X4 interfaces are specified in [2] and [6], respectively.

13

14

15

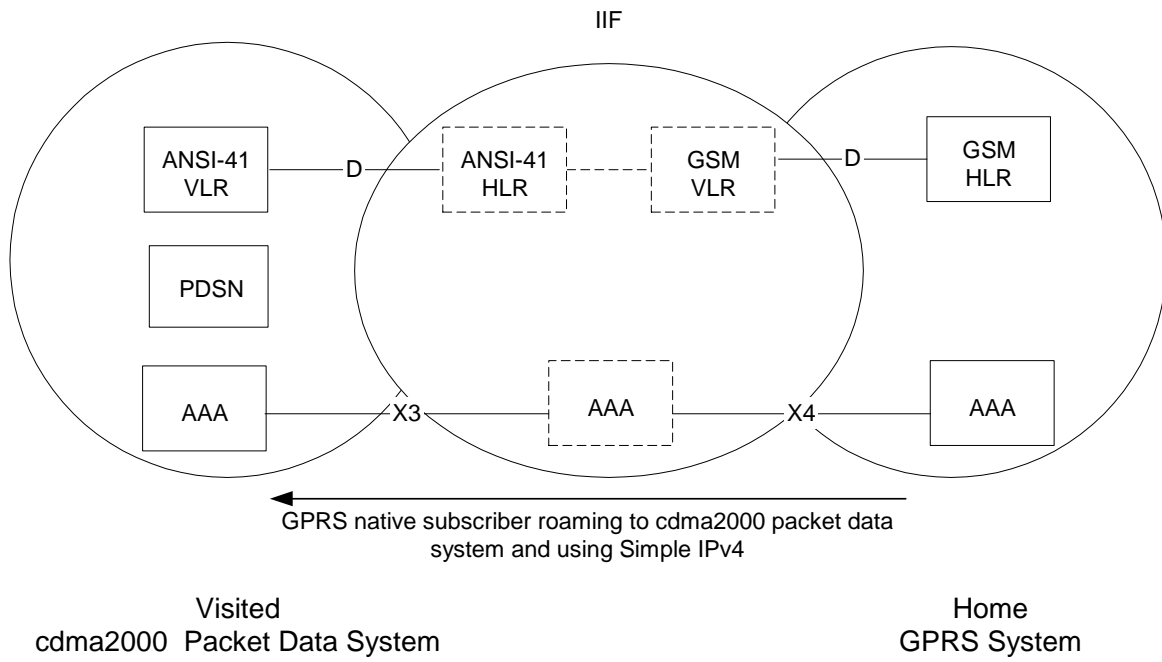
16

Figure 7 depicts the functions and control interface associated with the IIF if bearer connectivity between the visited cdma2000 packet data system and home GPRS system is not required. In this case, the MS gains access to the Internet directly from the visited system. The X3 and X4 interfaces are still required.

17

18

19



- 1
- 2
- 3
- 4

Figure 7 cdma2000 packet data foreign mode with Simple IPv4 without bearer connectivity between the visited and home systems

8 Functional & Interface Requirements

This section specifies the functional and interface requirements for four cdma2000/GPRS roaming scenarios:

- GPRS foreign mode with Mobile IPv4,
- GPRS foreign mode with Simple IPv4,
- cdma2000 packet data foreign mode with Mobile IPv4,
- cdma2000 packet data foreign mode with Simple IPv4.

8.1 GPRS Foreign Mode with Mobile IPv4

This section specifies the requirements for the roaming scenario where the roaming MS is a cdma2000 native subscriber and uses Mobile IPv4 to access a visited GPRS system.

If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to traverse through the home cdma2000 packet data system via the IIF, section 8.1.5 is applicable in addition to sections from 8.1.1 to 8.1.4. If the roaming MS's data traffic is not required to traverse through the home cdma2000 packet data system via the IIF, only sections from 8.1.1 to 8.1.4 are applicable.

8.1.1 HLR/ VLR Requirements for IIF

The IIF shall support the GSM HLR functions for authenticating the MS GPRS attach in accordance with [1]. The IIF shall also support the ANSI-41 VLR functions for the MS registration with the HLR in the home cdma2000 packet data system [1].

8.1.2 GGSN/FA Requirements for IIF

The IIF shall follow the requirements for Gp interface specified in [5][11] and the FA requirements specified in [2].

8.1.2.1 PDP Context Establishment

If the APN received from the MS via the SGSN during PDP context activation begins with 'MIPv4', the IIF considers that the MS uses the Mobile IPv4 to access its home cdma2000 packet data system. The IIF shall create the PDP context by setting PDP address to 0.0.0.0 in the Create PDP Context Response indicating that the PDP address will be assigned after the Mobile IP registration is completed [6].

After the Mobile IP registration is completed successfully, the IIF shall perform the PDP context update by setting the PDP address to the MS's home address.

8.1.2.2 Mobile IP Registration

After PDP context with 0.0.0.0 PDP address is activated, the IIF shall send the Mobile IP Agent Advertisement to the MS over the established PDP context. The IIF shall include the FA Challenge in the Agent Advertisement.

1 Upon receiving the Mobile IP Registration Request from the MS, the IIF requests the Home AAA to
 2 verify the MN-AAA authenticator (section 8.1.3). If the IIF receives the RADIUS Access-Accept
 3 message from the home AAA, the IIF shall forward the Mobile IP RRQ message to the HA in the
 4 home cdma2000 packet data system. If the IIF receives the RADIUS Access-Reject message from the
 5 Home AAA, the IIF shall discard the RRQ and send an RRP with the error value 67 indicating Bad
 6 Authentication.

7 Upon receiving the Mobile IP Registration Reply from the HA, the IIF shall forward it to the MS over
 8 the established PDP context.

9 **8.1.2.3 PDP Context Deactivation and Mobile IP De-registration**

10 If the PDP context is deactivated by either the MS or the network (IIF or SGSN), the IIF shall remove
 11 the MS's entry from the FA visitor list in the IIF.

12 If the MS performs a Mobile IP de-registration, the IIF shall deactivate the PDP context and remove
 13 the MS's entry from the FA visitor list in the IIF.

14 **8.1.2.4 IPsec Support**

15 IPsec may be used to protect the control and data packets exchanged in the Mobile IP tunnel between
 16 the IIF and HA. If IPsec is used, the IIF shall use the procedure in [2] to establish security
 17 associations with the HA.

18 **8.1.2.5 Transport**

19 For MS-terminated data packets received from the MS's HA, the IIF shall route the packets to the
 20 MS's GTP tunnel destined for the SGSN in the visited GPRS system.

21 For MS-originated data packets received from the MS's GTP tunnel, if Mobile IP reverse tunneling is
 22 used, the IIF shall route the packets to the Mobile IP reverse tunnel destined for the MS's HA in the
 23 home cdma2000 packet data system. If the Mobile IP reverse tunneling is not used, the IIF shall route
 24 the packets to the Internet.

25 **8.1.3 RADIUS Client Requirements for IIF**

26 Upon receiving a Mobile IP RRQ from the MS, the IIF shall send the RADIUS Access-Request
 27 message to the home AAA to verify the Foreign Agent challenge response according to [2].

28 The IIF shall send the RADIUS Accounting Request (Start) message to the home AAA after the IIF
 29 completes the update PDP context by setting the PDP address to the MS's home address.

30 The IIF may send the RADIUS Accounting Request (Interim) message to the home AAA when the
 31 MS changes SGSN.

32 The IIF shall send the RADIUS Accounting Request (Stop) message to the home AAA if the PDP
 33 context is deactivated or the Mobile IP re-registration fails.

34 The following two sections describe IIF requirements for supporting the IETF standard RADIUS
 35 attributes and 3GPP2 Vendor Specific Attributes (VSAs).

1 **8.1.3.1 IETF Standard RADIUS Attributes**

2 The IIF shall support the standard RADIUS attributes specified in [2].

3 **8.1.3.2 3GPP2 Vendor Specific Attributes**

4 3GPP2 VSAs are defined in [2]. Some attributes are mandatory. The IIF shall support the mandatory
5 3GPP2 VSAs using the following guidelines:

6

- Correlation ID

7 The IIF shall send a Correlation ID VSA in the RADIUS Access Request and
8 Accounting Request (Start, Stop and Interim) messages. It is optionally included in the
9 RADIUS Access Accept message. The IIF shall maintain the same value for the
10 lifetime of the PDP context.

11

- Session Continue

12 The IIF shall send the Session Continue VSA in the RADIUS Accounting Request
13 (Stop) message with the value 0 (False) set if the PDP context is deactivated. The IIF
14 may send the Session Continue VSA in the RADIUS Accounting Request (Interim)
15 message with the value 1 (True) set if the PDP context is updated.

16

- Serving PCF

17 Since the PCF address is not applicable in the GPRS system, the IIF shall send the
18 Serving PCF VSA with the value 0.0.0.0 in the RADIUS Accounting Request (Start,
19 Stop, and Interim).

20

- BS ID

21 The IIF shall send the BS ID VSA in the RADIUS Accounting Request (Start, Stop,
22 and Interim). If the IIF receives the GPRS location information consisting of Mobile
23 Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC),
24 and Routing Area Code (RAC)[10], the IIF shall convey the GPRS location
25 information in the 3GPP2 BS ID attribute. The value of the BS ID attribute shall be
26 formed from the concatenation of MCC, MNC, LAC, and RAC, where each item is
27 encoded using hexadecimal upper case ASCII characters. The MSB value of the BS
28 ID formed from the concatenation of MCC, MNC, LAC, and RAC shall be aligned
29 with the MSB of the BS ID field. The remaining Least Significant Bits (LSB) of the
30 BS ID field shall be set to '0'. Otherwise, the IIF shall set the BS ID value to all 1s in
31 this attribute.

32

- Service Option

33 The IIF shall send the Service Option VSA in the RADIUS Accounting Request (Start,
34 Stop and Interim) messages with the value 65 set. This VSA indicates that the MS is
35 roaming in a GPRS system. The IIF should include this VSA in the RADIUS Access
36 Request message.

37

- IP Technology

38 The IIF shall send the IP Technology VSA with the value 2 (Mobile IP) set in the
39 RADIUS Accounting Request (Start, Stop and Interim) messages. The IIF may send
40 this VSA in the RADIUS Access Request message.

41

- Release Indicator

- 1 The IIF shall send the Release Indicator VSA in the RADIUS Accounting Request
2 (Stop) message. The value shall be determined as follows:
- 3 – Although the IIF does not establish PPP with the MS in the GPRS Foreign Mode,
4 the IIF shall use the value 3 (PPP Termination) when the PDP context is
5 deactivated.
 - 6 – If the Mobile IP re-registration fails, the IIF shall use the value 4 (Mobile IP re-
7 registration failure).
 - 8 – If the PDP Context update fails, the IIF shall use the value 0 (unknown).
9
 - Number of Active Transitions
- 10 The IIF shall send the Number of Active Transitions VSA with the value 1 in the
11 RADIUS Accounting Request (Start, Stop, and Interim). (Note: The home AAA that
12 receives SO 65 should not use this VSA for accounting.)
- 13 • Home Agent
- 14 The IIF shall send the HA Address VSA in the RADIUS Accounting Request (Start,
15 Stop, and Interim). The IIF shall set the HA Address VSA with the value obtained
16 from the Mobile IP Registration Request.
- 17 The IIF shall not use other 3GPP2 VSAs in this release. If the IIF receives VSAs that are not specified
18 in this document, it shall silently discard them.

19 **8.1.4 MS Requirements**

20 This section specifies requirements for the MS.

21 **8.1.4.1 PDP Context Activation**

22 The MS shall support GPRS Attach, Authentication and PDP functions as required in [5][11].

23 After GPRS Attach and Authentication are completed, the MS shall perform the PDP Context
24 Activation with the SGSN in the visited GPRS system. The MS shall leave PDP address empty (i.e.,
25 the value of octet 2 equals 2) in Packet data protocol address IE [15] and set PDP Type to IPv4 in the
26 Activate PDP Context Request. If the MS wants to establish multiple Mobile IP sessions, it shall
27 activate one primary PDP Context for each Mobile IP session.

28 The MS shall include the APN information element in the Activate PDP context request. The MS
29 shall construct the APN according to [10].

30 APN =<APN Network ID>.mnc<MNC>.mcc<MCC>.gprs

31 The APN Network ID shall begin with MIPv4. 'MIPv4' is an indication to the IIF that the MS wants
32 to use Mobile IPv4 to access its home network. If 'MIPv4' is not included in the APN Network ID, it
33 is an indication that the MS wants to use Simple IPv4 (see section 8.2). The <APN Network ID> is the
34 concatenation of 'MIPv4' and the realm of the MS's NAI used for Mobile IP registration. The
35 <MNC> and <MCC> are the IMSI digits that are used for the Mobile Network Code (MNC) and
36 Mobile Country Code (MCC), respectively.

1 **8.1.4.2 Mobile IP Registration**

2 After PDP Activation is completed with the MS having received an Activate PDP Context Accept with
3 PDP address 0.0.0.0, the MS waits for the Mobile IP Agent Advertisement from the IIF or may send a
4 Mobile IP Agent Solicitation to the IIF. The MS shall support the Mobile IPv4 operations as required
5 in [2]. The PDP context update is performed after the Mobile IP Registration is completed.

6 The MS shall set the T bit in the Mobile IP Registration Request, if the policy of the home cdma2000
7 packet data system requires the roaming MS's data traffic to traverse through the home cdma2000
8 packet data system via the IIF.

9 **8.1.4.3 Termination**

10 If the MS receives the Deactivate PDP context request from the network, it shall consider the Mobile
11 IP session associated with the deactivated PDP context is terminated (i.e., removing Mobile IP state
12 information).

13 **8.1.5 Reverse Tunneling support between the IIF and the HA**

14 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
15 traverse through the home cdma2000 packet data system via the IIF, the IIF shall follow the
16 guidelines specified in section 6.2.2.5 of [2] for Reverse Tunneling.

17 **8.2 GPRS Foreign Mode with Simple IPv4**

18 This section specifies the requirements for the roaming scenario where the roaming MS is a
19 cdma2000 native subscriber and uses Simple IPv4 to access a visited GPRS system.

20 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
21 traverse through the home cdma2000 packet data system via the IIF, and the IIF is not in the home
22 cdma2000 packet data system, L2TP tunnel/session is required between the IIF and the home network.
23 If the IIF is located in the home cdma2000 packet data system, or the roaming MS's data traffic is not
24 required to traverse through the home cdma2000 packet data system via the IIF, L2TP tunnel/session
25 is not required, and the MS simply establishes a PDP context with the GGSN in the IIF.

26 **8.2.1 HLR/VLR Requirements for IIF**

27 See section 8.1.1.

28 **8.2.2 GGSN/LAC Requirements for IIF**

29 This section specifies IIF requirements to support the GGSN and LAC functionalities.

30 **8.2.2.1 PDP Context Activation and Address Assignment**

31 The IIF shall support the requirements of Gp interface specified in [5][11].

32 If the APN received from the MS during PDP context activation does not include 'MIPv4', the IIF
33 shall consider that the MS uses Simple IP to access its home cdma2000 packet data system.

1 If the policy of the home cdma2000 packet data system does not require the roaming MS's data traffic
2 to traverse through the home cdma2000 packet data system via IIF, or the IIF is in the home
3 cdma2000 packet data system, the IIF shall assign a PDP address to the MS in the Activate PDP
4 Context Response.

5 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
6 traverse through the home cdma2000 packet data system via IIF, and the IIF is not in the home
7 cdma2000 packet data system, the IIF shall set PDP address to 0.0.0.0 indicating that the PDP address
8 will be assigned after the PPP negotiation is completed with the LNS in the home cdma2000 packet
9 data network. After the PDP context is established, the IIF may send an LCP Configure-Request to
10 the MS over the PDP context. During the IPCP negotiation between the MS and LNS, the IIF shall
11 monitor for the assigned IP address. After the IPCP negotiation is completed, the IIF shall perform
12 the PDP context update by setting the PDP address to the MS's IP address.

13 **8.2.2.2 L2TP Support**

14 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
15 traverse through the home cdma2000 packet data system via IIF, and the IIF is not in the home
16 cdma2000 packet data system, the IIF shall support the functionality for LAC specified in [3][12].

17 **8.2.2.2.1 L2TP Tunnel/Session Establishment with Pre-Configured LNS Address**

18 During LCP negotiation with the MS, if the IIF is pre-configured with the address information of the
19 LNS in the MS's home cdma2000 packet data system, the IIF shall establish an L2TP tunnel/session
20 with the LNS in the home cdma2000 packet data network. If there is no existing L2TP tunnel to the
21 LNS, the IIF shall initiate the control connection establishment procedure [3] to establish an L2TP
22 tunnel with the LNS and initiate the incoming call establishment procedure [3] to establish an L2TP
23 session with the LNS. If an L2TP tunnel to the LNS exists already, the IIF shall initiate the incoming
24 call establishment procedure [3] to establish an L2TP session with the LNS. The L2TP tunnel
25 identified by a Tunnel ID is used to transport multiple L2TP sessions, where each L2TP session
26 corresponds to a PPP session. After the L2TP tunnel/session is established, the IIF shall forward all
27 PPP control packets between the LNS and MS.

28 **8.2.2.2.2 L2TP Tunnel/Session Establishment without Pre-Configured LNS Address**

29 During LCP negotiation with the MS, if the IIF doesn't know the address information of the LNS in
30 the MS's home cdma2000 packet data system, the IIF shall propose CHAP in an initial LCP
31 Configure-Request message sent to the MS. If the MS is not configured to use CHAP but to use PAP
32 instead, and the MS proposes PAP in an LCP Configure-NAK, the IIF shall accept PAP by sending an
33 LCP Configure-Request message with PAP.

34 During PPP authentication, if the IIF receives Tunnel-Server-Endpoint (conveying the address of an
35 LNS in the MS's home cdma2000 packet data network), Tunnel-Type, and Tunnel-Medium-Type
36 attributes [13] in the RADIUS Access-Accept message from the home AAA, and there is no L2TP
37 tunnel between the IIF and the LNS, the IIF shall perform the control connection establishment
38 procedure [3] to establish an L2TP tunnel with the LNS and initiate the incoming call establishment
39 procedure [3] to establish an L2TP session with the LNS. If an L2TP tunnel to the LNS exists already,
40 the IIF shall initiate the incoming call establishment procedure [3] to establish an L2TP session with
41 the LNS. After the L2TP tunnel/session is established, the IIF may forward LCP messages to the
42 LNS using the Proxy LCP AVPs specified in [3].

1 8.2.2.2.3 IPsec Support

2 IPsec may be used to protect the control and data packets exchanged in the L2TP tunnel. If IPsec is
3 used, the IIF shall use IKE to establish security associations with the LNS, before the L2TP control
4 connection establishment procedures.

5 8.2.2.2.4 L2TP session termination

6 When the PDP context is deactivated, the IIF shall initiate the L2TP session termination procedure as
7 specified in [3].

8 8.2.2.2.5 Transport

9 For MS-originated PPP frames received from the MS's GTP tunnel, the IIF shall route the packets to
10 the MS's L2TP tunnel/session destined for the LNS in the home cdma2000 packet data system.

11 For MS-terminated PPP frames received from the MS's L2TP tunnel/session, the IIF shall route the
12 PPP frames to the MS's GTP tunnel destined for the SGSN in the visited GPRS system.

13 8.2.3 RADIUS Client Requirements for IIF

14 The IIF shall support [13] if the policy of the home cdma2000 packet data system requires the
15 roaming MS's data traffic to traverse through the home system via the IIF.

16 If PPP authentication is required at the IIF, upon receiving the MS's NAI and credential (PAP
17 password or CHAP challenge response), the IIF shall send a RADIUS Access-Request message to the
18 home AAA to verify the MS's credential.

19 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
20 traverse through the home cdma2000 packet data system via IIF, and the IIF is not in the home
21 cdma2000 packet data system, the IIF shall send the RADIUS Accounting Request (Start) message to
22 the home AAA after the IIF completes the update PDP context by setting the PDP address to the MS's
23 home address. This requires the IIF to monitor for the NAI in the CHAP Response or PAP
24 Authenticate-Request if the IIF does not perform PPP authentication.

25 If the policy of the home cdma2000 packet data system does not require the roaming MS's data traffic
26 to traverse through the home cdma2000 packet data system via IIF, or the IIF is in the home
27 cdma2000 packet data system, the IIF shall send the RADIUS Accounting Request (Start) message to
28 the home AAA after the IIF completes the PDP context activation. If the IIF doesn't have the MS's
29 NAI, the IIF shall use the MS's IMSI and APN Network ID to construct the NAI as IMSI@<APN
30 Network ID>.

31 The IIF may send the RADIUS Accounting Request (Interim) message to the home AAA when the
32 MS changes SGSN.

33 The IIF shall send the RADIUS Accounting Request (Stop) message to the home AAA if the PDP
34 context is deactivated.

35 See section 8.1.3.1 and 8.1.3.2 for the IETF standard RADIUS attributes and 3GPP2 VSA,
36 respectively. The Home Agent VSA is not applicable in the GPRS Foreign Mode with Simple IP
37 operation. IP Technology shall be set to 1 (Simple IP).

1 **8.2.4 MS Requirements**

2 The MS shall support GPRS Attach, Authentication and PDP procedures as required in [5][11].

3 After GPRS Attach and Authentication are completed, the MS shall perform the PDP Context
4 Activation with the SGSN in the visited GPRS system. The MS shall leave PDP address empty (the
5 value of octet 2 equals 2) in Packet data protocol address IE [15] and set PDP Type to IPv4 in the
6 Activate PDP Context Request.

7 The MS shall include the APN information element in the Activate PDP context request. The MS
8 shall construct the APN according to [10].

9 If 0.0.0.0 PDP address is included in the Activate PDP Context Response, the MS shall perform the
10 PPP negotiation as specified in [2]. The MS shall perform PPP authentication (PAP or CHAP). The
11 PDP context update is performed after PPP negotiation is completed.

12 If a non-zero PDP address is included in the Activate PDP Context Response, the MS shall not
13 perform PPP negotiation.

14 **8.2.5 LNS Requirements for the Home cdma2000 Packet Data System**

15 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
16 traverse through the home cdma2000 packet data system via IIF, and the IIF is not in the home
17 cdma2000 packet data system, the home cdma2000 network shall support the LNS as per [3].

18 **8.2.5.1 PPP Negotiation**

19

20 **8.2.5.1.1 PPP Authentication**

21 This section is applicable only if PPP authentication is required at the LNS.

22 If IIF doesn't perform PPP authentication and relays the initial LCP Configure-Request message from
23 the MS to the LNS, the LNS shall continue the LCP negotiation with the MS via the IIF and perform
24 PPP authentication.

25 If the IIF has performed PPP authentication and forwards LCP messages to the LNS via the Proxy
26 LCP AVPs, the LNS shall perform one of the following behaviors:

- 27
- 28 • If the LNS agreed with the forwarded LCP parameters, then the LNS shall
proceed to the PPP authentication phase.
 - 29 • Otherwise, the LNS shall perform LCP negotiation and then proceed to the
30 PPP authentication phase.

31 If IIF has performed PPP authentication and doesn't forward LCP messages to the LNS via the Proxy
32 LCP AVPs, the LNS shall send an LCP Configure-Request proposing CHAP as the authentication
33 protocol. If the MS responds with an LCP Configure Ack, the PDSN shall send a CHAP challenge to
34 the MS. If the MS responds with an LCP Configure Nak proposing PAP, the PDSN shall accept the
35 proposal by sending an LCP Configure-Request proposing PAP and wait for the MS's PAP credential.

1 If the LNS receives the MS's credential (PAP password or CHAP challenge response), the LNS shall
2 request the Home RADIUS server to verify the MS's credential.

3 **8.2.5.1.2 IPCP**

4 If PPP authentication is successful, or PPP authentication is not required by the LNS, the LNS shall
5 perform IPCP negotiation with the MS. The LNS shall assign an IP address to the MS during IPCP
6 negotiation.

7 **8.2.5.2 IPsec support**

8 IPsec may be used to protect the control and data packets exchanged in the L2TP tunnel. If IPsec is
9 used, the LNS shall use IKE to establish security associations with the IIF, before the L2TP control
10 connection establishment procedures.

11 **8.2.6 HAAA Requirements**

12 If the policy of the home cdma2000 packet data system requires the roaming MS's data traffic to
13 traverse through the home cdma2000 packet data system via IIF, and the IIF is not in the home
14 cdma2000 packet data system, the HAAA in the cdma2000 network shall support [13].

15 **8.3 cdma2000 Packet Data Foreign Mode with Mobile IPv4**

16 This section specifies the requirements for the roaming scenario where the roaming MS is a GPRS
17 native subscriber and uses Mobile IPv4 to access a visited cdma2000 packet data system.

18 The policy of the home GPRS system determines whether the roaming MS's data traffic is required to
19 traverse through the home GPRS system via the IIF. If it is required, the IIF routes the MS's data
20 traffic between a PDSN/FA in the visited cdma2000 packet data system and a GGSN in the home
21 GPRS system.

22 **8.3.1 HLR/VLR Requirements for IIF**

23 The IIF shall support the ANSI-41 HLR functions for the CAVE-based access authentication in
24 accordance with[1]. The IIF shall also support the GSM VLR functions for the MS registration with
25 the GSM HLR in the home GPRS system [1].

26 **8.3.2 AAA Requirements for IIF**

27 This section specifies the IIF requirements to interwork RADIUS messages between the visited
28 cdma2000 packet data system and the home GPRS system.

29 **8.3.2.1 RADIUS Access-Request**

30 This section specifies the IIF requirements to process the RADIUS Access-Request received from the
31 visited cdma2000 packet data system.

32 The IIF shall proxy all IETF RADIUS attributes without modification, except the Calling-Station-ID
33 attribute, Called-Station-ID attribute, and Framed-Protocol attribute. The processing of these three
34 attributes is described below.

1 If the Calling-Station-ID attribute in the received RADIUS Access-Request contains IMSI, the IIF
2 shall copy the IMSI into the 3GPP-IMSI attribute [6] and include it in the RADIUS Access-Request
3 destined for the MS's home GPRS system. The IIF shall not include the Calling-Station-ID attribute
4 in the RADIUS Access-Request sent to the home AAA in the GPRS system.

5 If the Calling-Station-ID attribute in the received RADIUS Access-Request contains MIN or IRM, the
6 IIF shall map it to the MS's IMSI used in the home GPRS system and include it in the 3GPP-IMSI
7 attribute of the RADIUS Access-Request destined for the home GPRS system. The IIF shall not
8 include the Calling-Station-ID attribute in the RADIUS Access-Request sent to the home AAA in the
9 GPRS system.

10 The IIF shall include the Called-Station-ID attribute in the RADIUS Access-Request destined for the
11 MS's home GPRS system. The Value field of the Called-Station-ID attribute shall be set to the APN
12 (see section 8.3.3.2).

13 If the Framed-Protocol attribute is included in the received RADIUS Access-Request, the IIF shall
14 override the value to 7 (GPRS PDP Context) [6].

15 The IIF shall remove all 3GPP2 VSAs from the received RADIUS Access-Request. The IIF is not
16 required to include any 3GPP VSAs, except the 3GPP-IMSI attribute, in the transmitted RADIUS
17 Access-Request destined for the MS's home GPRS system.

18 **8.3.2.2 RADIUS Access-Accept**

19 This section specifies the IIF requirements to process the RADIUS Access-Accept received from the
20 MS's home GPRS system.

21 The IIF shall proxy all IETF RADIUS attributes without modification.

22 The IIF shall remove all 3GPP VSAs from the received RADIUS Access-Accept, before transmitting
23 the RADIUS Access-Accept to the visited cdma2000 packet data system.

24 If the policy of the home GPRS system requires the roaming MS's data traffic to traverse through the
25 home GPRS system via the IIF, and the HA-Address VSA was included in the corresponding
26 RADIUS Access-Request received earlier from the visited cdma2000 packet data system, the IIF shall
27 include the Reverse-Tunnel-Specification VSA in the transmitted RADIUS Access-Accept destined
28 for the visited cdma2000 packet data system. The Value field of the VSA shall be set to 1 indicating
29 that reverse tunneling is required.

30 **8.3.2.3 RADIUS Accounting-Request START**

31 The IIF requirements to process the RADIUS Accounting-Request (Start) message received from the
32 visited cdma2000 packet data system are the same as in section 8.3.2.1.

33 **8.3.2.4 RADIUS Accounting-Request INTERIM**

34 The IIF requirements to process the RADIUS Accounting-Request (Interim) message received from
35 the visited cdma2000 packet data system are the same as in section 8.3.2.1.

1 **8.3.2.5 RADIUS Accounting-Request STOP**

2 The IIF requirements to process the RADIUS Accounting-Request (Stop) message received from the
3 visited cdma2000 packet data system are the same as in section 8.3.2.1, with the additional
4 requirements herein.

5 If the Session-Continue VSA is set to FALSE in the received RADIUS Accounting-Request STOP,
6 and if the IIF has not previously received an Accounting-Request (Start) from another PDSN with the
7 same IP Address (for the case of inter-PDSN handoff with Mobile IP), the IIF shall insert the 3GPP-
8 Session-Stop-Indicator VSA to indicate that the PDP session has been terminated.

9 **8.3.3 HA/SGSN Requirements for IIF**

10

11 **8.3.3.1 Mobile IP Authentication**

12 Upon receiving the Mobile IP RRQ from the visited cdma2000 packet data system, the IIF shall verify
13 the MN-HA authenticator. The IIF is configured with the MN-HA shared secret indexed by the MS's
14 NAI. If local policy requires the IIF to process the MN-AAA authenticator, the IIF shall request the
15 Home RADIUS server to verify the MN-AAA authenticator. In this case, the IIF shall send a
16 RADIUS Access-Request to the home AAA in the GPRS system in accordance with [2] (except
17 3GPP2 VSAs) and additionally include the Called-Station-ID attribute to convey the APN.

18 If the roaming MS's traffic is not required to traverse through the home GPRS system via the IIF,
19 after the Mobile IP RRQ is authenticated successfully, the IIF shall respond to it with a Mobile IP
20 RRP as specified in [2].

21 If the roaming MS's traffic is required to traverse through the home GPRS system via the IIF, after
22 the Mobile IP RRQ is authenticated successfully, the IIF establishes a PDP context with a GGSN in
23 the MS's home GPRS system, as specified in section 8.3.3.2.

24 The IIF shall support MIPv4 operation as specified in [2].

25 **8.3.3.2 PDP Context Management**

26 This section is applicable only if the roaming MS's traffic is required to traverse through the home
27 GPRS system via the IIF. In this case, the IIF shall support the SGSN requirements for the Gp
28 interface [5][11].

29 If the Mobile IP RRQ is authenticated successfully, the IIF shall construct the APN as follows [10]:

30
$$\text{APN} = \langle \text{APN Network ID} \rangle . \text{mnc} \langle \text{MNC} \rangle . \text{mcc} \langle \text{MCC} \rangle . \text{gprs}$$

31 The $\langle \text{APN Network ID} \rangle$ is the realm of the MS's NAI. The NAI is available in the Mobile IP RRQ.
32 The $\langle \text{MNC} \rangle$ and $\langle \text{MCC} \rangle$ are the IMSI digits that are used for the Mobile Network Code (MNC) and
33 Mobile Country Code (MCC), respectively. The IMSI may be available in the Calling-Station-ID
34 attribute of the RADIUS Access Request received from the visited cdma2000 packet data system. If
35 the Calling-Station-ID attribute contains MIN or IRM, the IIF shall map it to the MS's IMSI used in
36 the home GPRS system.

1 The IIF shall resolve the APN to the GGSN IP address(es) as specified in [5][11].

2 After the IIF selects a GGSN in the MS's home GPRS system, the IIF shall establish a PDP context
3 with that GGSN according to [5][11]. The IIF shall initiate a Create PDP Context Request that
4 includes the following information elements:

- 5 • IMSI
- 6 • NSAPI
- 7 • TEID
- 8 • APN
- 9 • Selection Mode
- 10 • SGSN Address for Signaling
- 11 • SGSN Address for User Traffic
- 12 • End User Address
- 13 • QoS Profile

14 The IIF shall generate a 4-bit NSAPI value, as specified in [14], for the MS's PDP context. The IIF
15 shall generate a 32-bit TEID value, as specified in [5][11], for each pair of IMSI and NSAPI. The
16 TEID uniquely identifies a GTP tunnel between the IIF and GGSN. If the Home Address field of the
17 received Mobile IP RRQ is zero, the MS shall leave PDP address empty (i.e., the value of octet 2
18 equals 2) in the End User Address information element[5][11] and set PPP Type to IPv4, which is an
19 indication to request the GGSN to assign an IP address. If the Home Address field of the received
20 Mobile IP RRQ is non-zero, it shall be included in the PDP Address field of the End User Address
21 information element. The QoS Profile specifies the requested QoS parameters for the PDP context.
22 The content of the QoS Profile information element may be coded with values based on local policy
23 or user profile made available to the IIF. The coding of the QoS Profile is specified in [15].

24 The IIF may include in the Create PDP Context Request other information elements specified by
25 [5][11].

26 After the PDP context is established, the IIF shall send the Mobile IP RRP, as specified in [2], to the
27 MS via the serving PDSN. If the IIF receives a Create PDP Context Response that contains a PDP
28 address assigned by the GGSN, the IIF shall include it in the Home Address field of the Mobile IP
29 RRP with the Code value 0 indicating "registration accepted". If the IIF receives a Create PDP
30 Context Response with the Cause value 220 indicating that the MS's requested static IP address is
31 unknown to the GGSN, the IIF shall send the Mobile IP RRP with the Code value 129 indicating
32 "administratively prohibited".

33 If the MS performs registration for multiple Mobile IP sessions, the IIF shall establish one primary
34 PDP Context for each Mobile IP session.

35 If the PDP context is deactivated by the GGSN in the home GPRS system, the IIF shall remove the
36 MS's Mobile IP mobility binding.

37 If the MS performs Mobile IP de-registration, the MS's Mobile IP mobility binding has expired, or
38 the Mobile IP re-registration has failed, the IIF shall deactivate the PDP context.

1 **8.3.3.3 IPsec Support**

2 IPsec may be used to protect the control and data packets exchanged in the Mobile IP tunnel between
3 the IIF and FA. If IPsec is used, the IIF shall use the procedure in [2] to establish security
4 associations with the FA.

5 **8.3.3.4 Transport Requirements for IIF**

6 If the roaming MS's traffic is required to traverse through the home GPRS system via the IIF, the IIF
7 shall route the packets received from the Mobile IP reverse tunnel to the MS's GTP tunnel destined
8 for the GGSN in the home GPRS system. The IIF shall route the packets received from the MS's
9 GTP tunnel to the Mobile IP tunnel destined for the PDSN serving the MS in the visited cdma2000
10 packet data system.

11 If the roaming MS's traffic is not required to traverse through the home GPRS system via the IIF, the
12 IIF shall route packets received from the Internet to the Mobile IP tunnel destined for a PDSN serving
13 the MS in the visited cdma2000 packet data system. If the Mobile IP reverse tunnel is enabled for the
14 MS, the IIF shall route packets received from the Mobile IP reverse tunnel to the Internet.

15 **8.3.4 MS Requirements**

16 The MS shall support the Mobile IPv4 operations described in [2]. The MS shall use the NAI whose
17 realm corresponds to the MS's home GPRS system. The MS shall use the IIF address as the static
18 HA address.

19 If the roaming MS's traffic is required to traverse through the home GPRS system via the IIF, the MS
20 shall enable the T-bit in the Mobile IP RRQ. If the roaming MS's traffic is not required to traverse
21 through the home GPRS system via the IIF, the MS may enable the T-bit in the Mobile IP RRQ.

22 **8.4 cdma2000 Packet Data Foreign Mode with Simple IPv4**

23 This section specifies the requirements for the roaming scenario where the roaming MS is a GPRS
24 native subscriber and uses Simple IPv4 to access a visited cdma2000 packet data system.

25 If the roaming MS's data traffic is not required to traverse through the home GPRS system via the IIF,
26 only sections 8.4.1, 8.4.2, and 8.4.5 are applicable. If the policy of the home GPRS system requires
27 the roaming MS's data traffic to traverse through the home GPRS system via the IIF, sections 8.4.3
28 and 8.4.4 are applicable in addition to sections 8.4.1, 8.4.2, and 8.4.5.

29 **8.4.1 HLR/VLR Requirements for IIF**

30 See section 8.3.1.

31 **8.4.2 AAA Requirements for IIF**

32 This section specifies the IIF requirements to interwork RADIUS messages between the visited
33 cdma2000 packet data system and the home GPRS system.

- 1 **8.4.2.1 RADIUS Access-Request**

- 2 The IIF requirements to process the RADIUS Access-Request received from the visited cdma2000
3 packet data system are the same as in section 8.3.2.1.
- 4 **8.4.2.2 RADIUS Access-Accept**

- 5 The IIF requirements to process the RADIUS Access-Accept received from the MS's home GPRS
6 system are the same as in section 8.3.2.2, except the following requirement. The IIF shall support [13].
- 7 If the policy of the home GPRS system requires the roaming MS's data traffic to traverse through the
8 home GPRS system via the IIF, and the HA-Address VSA was not included in the corresponding
9 RADIUS Access-Request received earlier from the visited cdma2000 packet data system, the IIF shall
10 insert the Tunnel-Server-Endpoint, Tunnel-Type, and Tunnel-Medium-Type attributes in the
11 transmitted RADIUS Access-Accept destined for the visited cdma2000 packet data system. The
12 Tunnel-Server-Endpoint attribute shall indicate the LNS address in the IIF. The Tunnel-Type
13 attribute shall indicate L2TP. The Tunnel-Medium-Type attribute shall indicate IPv4.
- 14 **8.4.2.3 RADIUS Accounting-Request START**

- 15 The IIF requirements to process the RADIUS Accounting-Request (Start) message received from the
16 visited cdma2000 packet data system are the same as in section 8.3.2.3.
- 17 **8.4.2.4 RADIUS Accounting-Request INTERIM**

- 18 The IIF requirements to process the RADIUS Accounting-Request (Interim) message received from
19 the visited cdma2000 packet data system are the same as in section 8.3.2.4.
- 20 **8.4.2.5 RADIUS Accounting-Request STOP**

- 21 The IIF requirements to process the RADIUS Accounting-Request (Stop) message received from the
22 visited cdma2000 packet data system are the same as in section 8.3.2.5, except the following
23 requirement.
- 24 If the Session-Continue VSA is set to FALSE in the received RADIUS Accounting-Request (Stop)
25 message, and the IP-Technology VSA indicates Simple IP, the IIF shall insert the 3GPP-Session-
26 Stop-Indicator VSA to indicate that the PDP session has been terminated.
- 27 **8.4.3 LNS/SGSN Requirements for IIF**

- 28 Based on the policy of the home GPRS system, if the roaming MS's traffic is required to traverse
29 through the home GPRS system via the IIF, the IIF shall support the LNS functions [3] and the SGSN
30 requirements for the Gp interface [5][11].
- 31 **8.4.3.1 L2TP Tunnel/Session Establishment**

- 32 Upon receiving the Start-Control-Connection-Request (SCCRQ) from a PDSN in the visited
33 cdma2000 packet data system, the IIF shall perform the control connection establishment procedure
34 [3] to establish an L2TP tunnel with the PDSN. The L2TP tunnel identified by a Tunnel ID is used to
35 transport multiple L2TP sessions, where each L2TP session corresponds to a PPP session. IPsec may
36 be used to protect the control and data packets exchanged in the L2TP tunnel.

1 Upon receiving the Incoming-Call-Request (ICRQ) within an existing L2TP tunnel, the IIF shall
2 perform the incoming call establishment procedure [3] to establish an L2TP session for the MS. Each
3 L2TP session is identified by a session ID. The L2TP tunnel ID and session ID uniquely identify a
4 PPP session in the IIF.

5 **8.4.3.2 PPP Authentication**

6 After the L2TP session establishment, the IIF may request the MS to perform PPP authentication
7 (CHAP or PAP).

8 If PPP authentication is required at the IIF, and the PDSN forwards LCP messages to the IIF via the
9 Proxy LCP AVPs, the IIF shall perform one of the following behaviors:

- 10 • If the IIF agreed with the forwarded LCP parameters, then the IIF shall
11 proceed to the PPP authentication phase.
- 12 • Otherwise, the IIF shall perform LCP negotiation and then proceed to the
13 PPP authentication phase.

14 If PPP authentication is required at the IIF, and the PDSN doesn't forward LCP messages to the IIF
15 via the Proxy LCP AVPs, the IIF shall send an LCP Configure-Request proposing CHAP as the
16 authentication protocol. If the MS responds with an LCP Configure Ack, the IIF shall send a CHAP
17 challenge to the MS. If the MS responds with an LCP Configure Nak proposing PAP, the IIF shall
18 accept the proposal by sending an LCP Configure-Request proposing PAP and wait for the MS's PAP
19 credential.

20 If the IIF receives the MS's credential (PAP password or CHAP challenge response), the IIF shall
21 request the Home RADIUS server to verify the MS's credential [6] and additionally include the
22 Called-Station-ID attribute to convey the APN (see section 8.3.3.2).

23 **8.4.3.3 PDP Context Establishment**

24 If PPP authentication is successful or not required, the IIF shall establish a PDP context with a GGSN
25 in the MS's home GPRS system. The IIF shall construct the APN (see section 8.3.3.2). The IIF shall
26 resolve the APN to the GGSN IP address(es) as specified in [5][11].

27 The IIF shall establish GTP tunnels with a selected GGSN in the home GPRS system according to
28 [5][11]. The IIF shall initiate a Create PDP Context Request that shall include the following
29 information elements:

- 30 • IMSI
- 31 • NSAPI
- 32 • TEID
- 33 • APN
- 34 • Selection Mode
- 35 • SGSN Address for Signaling
- 36 • SGSN Address for User Traffic

- 1 • End User Address
- 2 • Quality of Service Profile

3 The IIF shall generate a 4-bit NSAPI value, as specified in [14], for the MS's PDP context. The IIF
 4 shall generate a 32-bit TEID value for each pair of IMSI and NSAPI. The TEID uniquely identifies a
 5 GTP tunnel between the IIF and GGSN. The MS shall leave PDP address empty (i.e., the value of
 6 octet 2 equals 2) in the End User Address information element [5][11] and set PDP Type to IPv4,
 7 which is an indication to request the GGSN to assign an IP address. The QoS Profile specifies the
 8 requested QoS parameters for the PDP context. The content of the QoS Profile information element
 9 may be coded with values based on local policy or user profile made available to the IIF. The coding
 10 of the QoS Profile is specified in [15].

11 The IIF may include in the Create PDP Context Request other information elements specified by
 12 [5][11].

13 **8.4.3.4 IPCP Negotiation**

14 After the GTP tunnels are established, the IIF shall perform IPCP negotiation with the MS. Upon
 15 receiving a Create PDP Context Response that contains a PDP address assigned by the GGSN, the IIF
 16 shall assign the same IP address to the MS via IPCP. The IIF shall support Van Jacobson TCP/IP
 17 header compression [16]. The IIF shall support CCP [17] for the negotiation of PPP compression.
 18 The IIF shall support the following types of PPP compression: Stac-LZS [18] and Microsoft Point-To-
 19 Point Compression Protocol [19] compression. The IIF may support other PPP payload compression
 20 algorithms.

21 **8.4.3.5 Transport**

22 For MS-originated PPP frames received from the MS's L2TP tunnel/session, the IIF shall perform
 23 header decompression (if negotiated during IPCP) and route the packets to the MS's GTP tunnel
 24 destined for the GGSN in the home GPRS system. For MS-terminated data packets received from the
 25 MS's GTP tunnel, the IIF shall perform header compression (if negotiated during IPCP) and route the
 26 PPP frames to the MS's L2TP tunnel/session destined for the serving PDSN in the visited cdma2000
 27 packet data system.

28 **8.4.3.6 Termination**

29 The IIF shall support a PPP inactivity timer for each PPP session. If the inactivity timer for an MS
 30 expires, the IIF shall close the MS's PPP session, tear down the MS's L2TP session [RFC 2661], and
 31 deactivate the MS's PDP context.

32 If the GGSN in the home GPRS system deactivates the MS's PDP context, the IIF shall close the
 33 MS's PPP session and tear down the MS's L2TP session.

34 If the PDSN in the visited cdma2000 packet data system tears down the MS's L2TP session, the IIF
 35 shall close the MS's PPP session and deactivate the MS's PDP context.

36 **8.4.4 PDSN Requirements**

37 If the PDSN supports the roaming MS's data traffic to traverse through the home GPRS system via
 38 the IIF, the PDSN shall support [3] and [13].

1 8.4.4.1 PPP LCP Negotiation and Authentication

2 The PDSN performs LCP negotiation with the MS as specified [2].

3 If the PDSN receives a RADIUS Access-Accept originated from the Home RADIUS server [6], the
4 PDSN shall send the Success message for CHAP or PAP to the MS after the L2TP tunnel/session
5 establishment (see section 8.4.4.2).

6 8.4.4.2 L2TP Tunnel/Session Establishment

7 If the PDSN receives Tunnel-Server-Endpoint (conveying the IIF address), Tunnel-Type, and Tunnel-
8 Medium-Type attributes in the RADIUS Access-Accept, and there is no L2TP tunnel between the
9 PDSN and the IIF, the PDSN shall perform the control connection establishment procedure [3] to
10 establish an L2TP tunnel with the IIF and initiate the incoming call establishment procedure [3] to
11 establish an L2TP session with the IIF. If an L2TP tunnel already exists between the PDSN and the
12 IIF, the PDSN shall perform the incoming call establishment procedure [3] with the IIF to establish an
13 L2TP session for the MS. The PDSN shall request that sequence number is used in transporting
14 packets in the L2TP session. The PDSN may forward to the IIF the LCP parameters negotiated
15 between the MS and PDSN.

16 8.4.4.3 IPsec Support

17 IPsec may be used to protect the control and data packets exchanged in the L2TP tunnel. If IPsec is
18 used, the PDSN shall use IKE to establish security associations with the IIF, before the L2TP control
19 connection establishment procedures.

20 8.4.4.4 Transport

21 For MS-originated PPP/HDLC frames (control and data) received from the MS's A10 connection, the
22 PDSN shall perform HDLC de-framing [2] and forward the PPP frames to the MS's L2TP
23 tunnel/session destined for the IIF. For MS-terminated PPP frames (control and data) received from
24 the MS's L2TP tunnel/session, the PDSN shall perform HDLC framing and forward the PPP/HDLC
25 frames to the MS's A10 connection.

26 8.4.4.5 Termination

27 If the MS's A10 connection is terminated, the PDSN shall tear down the MS's L2TP session. If the
28 IIF tears down the MS's L2TP session, the PDSN shall request the PCF to terminate the MS's A10
29 connection [20].

30 8.4.5 MS Requirements

31 The MS shall support the Simple IP operations described in [2]. If the policy of the home GPRS
32 system requires the roaming MS's data traffic to traverse through the home GPRS system via the IIF,
33 the MS shall perform PPP authentication (PAP or CHAP).

1 **9 Call Flow Examples**

2 This section illustrates some call flow examples for four cdma2000/GPRS roaming scenarios:

- 3 ▪ GPRS foreign mode with Mobile IPv4,
- 4 ▪ GPRS foreign mode with Simple IPv4,
- 5 ▪ cdma2000 packet data foreign mode with Mobile IPv4,
- 6 ▪ cdma2000 packet data foreign mode with Simple IPv4.

7 **9.1 GPRS Foreign Mode with Mobile IPv4**

8 Figure 8 depicts a call flow example for the roaming scenario where a cdma2000 packet data native
9 subscriber operates a terminal supporting Mobile IPv4 [2] in GPRS foreign mode. In this example,
10 the MS has shared secrets with the home cdma2000 system for Mobile IP authentication. The MS
11 may request the home cdma2000 system to assign an IP address. In this example, reverse tunneling is
12 enabled so that all data traffic (MS-originated and –terminated) traverses through the IIF and home
13 cdma2000 system. The IIF generates 3GPP2 packet data accounting records and sends it to the home
14 cdma2000 system via RADIUS.

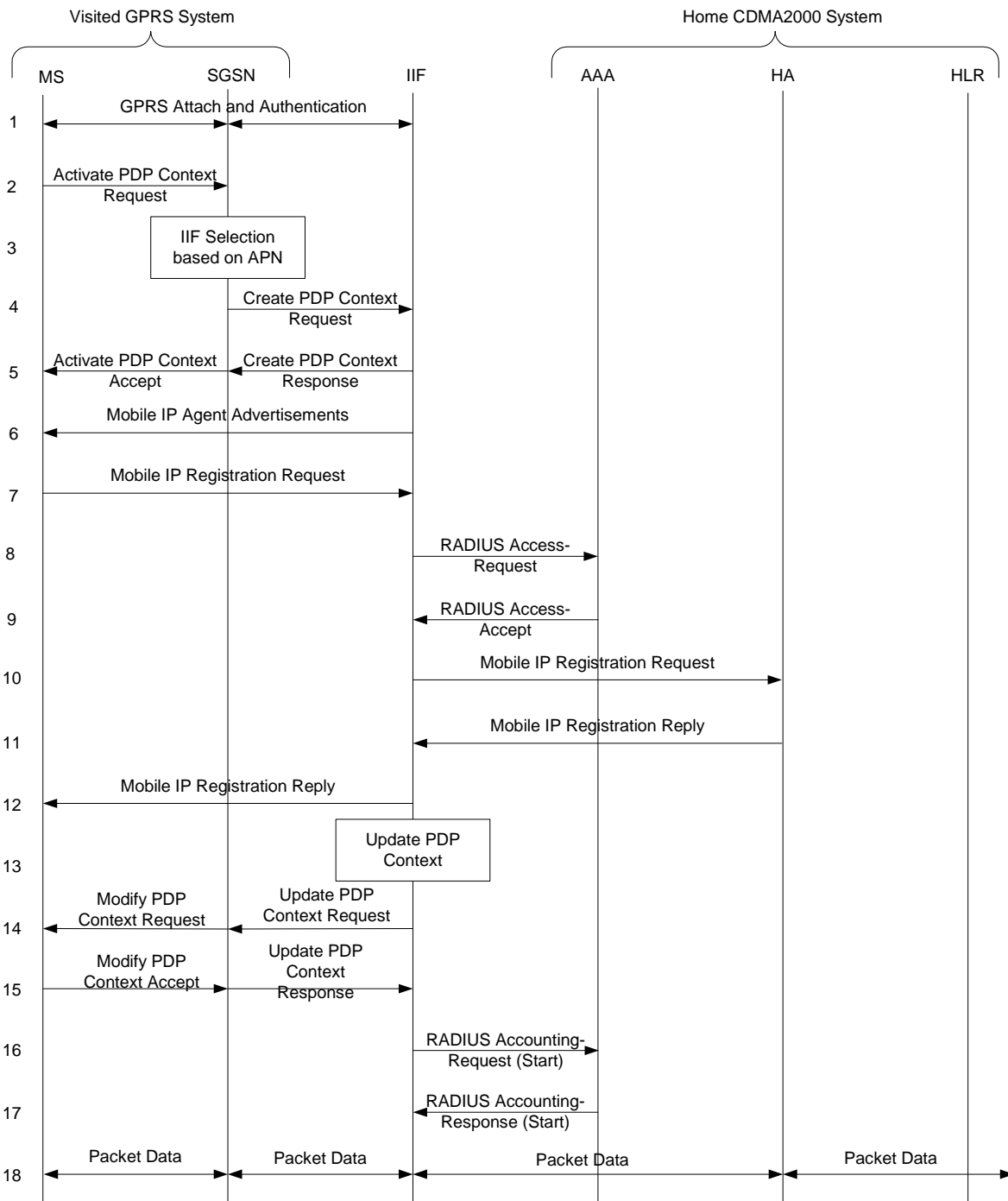


Figure 8 Mobile IPv4 operation in the GPRS foreign mode

1. The MS performs GPRS attach with a SGSN. The authentication associated with the GPRS attach is a SIM-based authentication requiring the Ki secret. The IIF supports the GSM HLR functionality and is configured with the Ki secret. The IIF is not required to communicate with the HLR in the home cdma2000 system for the authentication.

- 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
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
2. The MS sends the Activate PDP Context Request to the SGSN. The message includes the APN (Access Point Name). The APN has the format <Network ID>.mnc<MNC>.mcc<MCC>.gprs. The <Network ID> (e.g., MIPv4FA.cdma2000carrier.com) indicates that the MS wants connectivity to its home cdma2000 system via Mobile IPv4. The <MNC> and <MCC> are derived from the MS's IMSI. The Requested PDP Address is left empty (see section 8.1.4.1) in the message whether the MS has a static Mobile IP home address or wishes to obtain a new Mobile IP home address.
3. The SGSN selects a GGSN based on the APN. To do so, the SGSN uses the APN as the lookup name to query a DNS server (not shown in the figure) and obtains the IP address of the GGSN in the IIF.
4. The SGSN sends the Create PDP Context Request to the GGSN functionality in the IIF to set up a PDP context for the MS. The message includes the APN Network ID, but the PDP Address is left empty (see section 8.1.4.1).
5. The GGSN functionality in the IIF sends the Create PDP Context Response to the SGSN that in turn sends the Activate PDP Context Accept to the MS. The PDP Address in both messages is set to 0.0.0.0 to indicate that the PDP address will be assigned later after successful Mobile IP registration.
6. Because the requested APN Network ID indicates MIPv4FA, the FA functionality in the IIF is invoked and sends one or more Mobile IP Agent Advertisements to the MS over the established PDP context. The Agent Advertisement contains the FA Care-of Address and the FA Challenge (FAC).
7. The MS sends the Mobile IP Registration Request to the FA functionality in the IIF over the PDP context. The following information is contained in the Registration Request:
 - MS's NAI [7] has the format <username>@<domain_name>, where the domain_name identifies the MS's home cdma2000 system.
 - MN-HA authenticator is computed based on the content of the Registration Request and the secret shared between the MS and HA [7].
 - MN-AAA authenticator is computed based on the FAC and the secret shared between the MS and home AAA server [9].
 - HA Address field is set to the permanent HA of the MS.
 - Home Address field is set to a known value if the MS uses a permanent address, or to 0.0.0.0 if the MS wants a new address assigned by the HA.
 - T-bit is set to one to enable a reverse tunnel from the IIF to the MS's HA.
8. The IIF RADIUS client functionality sends a RADIUS Access-Request to the home AAA server. The RADIUS Access-Request conveys MS's NAI, FAC authenticator, FAC, HA address, etc. [2].
9. If the authentication is successful, the home AAA server responds with the RADIUS Access-Accept.
10. The IIF FA functionality forwards the Mobile IP Registration Request to the HA.
11. The HA verifies the MN-HA authenticator in the Mobile IP Registration Request. The HA responds to the Mobile IP Registration Request with the Mobile IP Registration Reply containing a registration result (e.g., successful or an error code). If the MS requests a new home address, a new address is returned in the Registration Reply; otherwise, the MS's permanent address is returned.

- 1 12. The IIF FA functionality forwards the Mobile IP Registration Reply to the MS over the
2 appropriate PDP context. The IIF FA functionality notes the assigned MS IP Address and
3 shares that address with the IIF GGSN functionality.
- 4 13. The IIF GGSN functionality updates its PDP context by setting the PDP address to the
5 MS's home address (as indicated in the Mobile IP Registration Reply and shared by the
6 FA functionality). The PDP address (hence the MS's home address) is associated with a
7 GTP tunnel identified by the Tunnel Endpoint ID (TEID).
- 8 14. The IIF GGSN functionality triggers the GGSN-initiated PDP Context modification
9 procedure in order to update the PDP address in the SGSN and MS [6]. The IIF GGSN
10 functionality sends the Update PDP Context Request to the SGSN which in turn sends the
11 Modify PDP Context Request it to the MS.
- 12 15. The MS responds with the Modify PDP Context Accept to the SGSN that in turn sends
13 the Update PDP Context Response to the IIF GGSN functionality.
- 14 16. The IIF RADIUS client functionality sends a RADIUS Accounting-Request (Start) to the
15 home AAA server [2]. Standard IETF attributes and mandatory 3GPP2-vendor-specific
16 attributes are included to convey accounting records (section 8.1.3.2).
- 17 17. The home AAA server responds with a RADIUS Accounting-Response (Start).
- 18 18. Bearer traffic traverses through the IIF in both directions, since reverse tunneling from
19 the IIF to HA is enabled in this example. For routing MS-originated packets, the IIF
20 routes packets received from the MS's GTP tunnel (identified by a TEID) to the MS's
21 HA via a Mobile IP reverse tunnel. For routing MS-terminated packets, the IIF routes
22 packets received from the HA-to-FA tunnel to the MS's GTP tunnel. IPsec can be used
23 to protect the Mobile IP tunnels between HA and IIF, and the GTP tunnels between IIF
24 and SGSN.

25 9.2 GPRS Foreign Mode with Simple IP

26 Figure 9 depicts a call flow example for the roaming scenario where a cdma2000 packet data native
27 subscriber operates Simple IP in the GPRS foreign mode. In this example, the MS has shared secrets
28 with the home cdma2000 system for Simple IP authentication (i.e., CHAP). The MS establishes a
29 PPP session, via L2TP, to the home cdma2000 system. During the PPP establishment, the home
30 cdma2000 system assigns an IP address to the MS dynamically. All the MS's data traffic (MS-
31 originated and –terminated) traverses through the IIF and home cdma2000 system. The IIF generates
32 3GPP2 packet data accounting records and sends it to the home cdma2000 system via RADIUS.

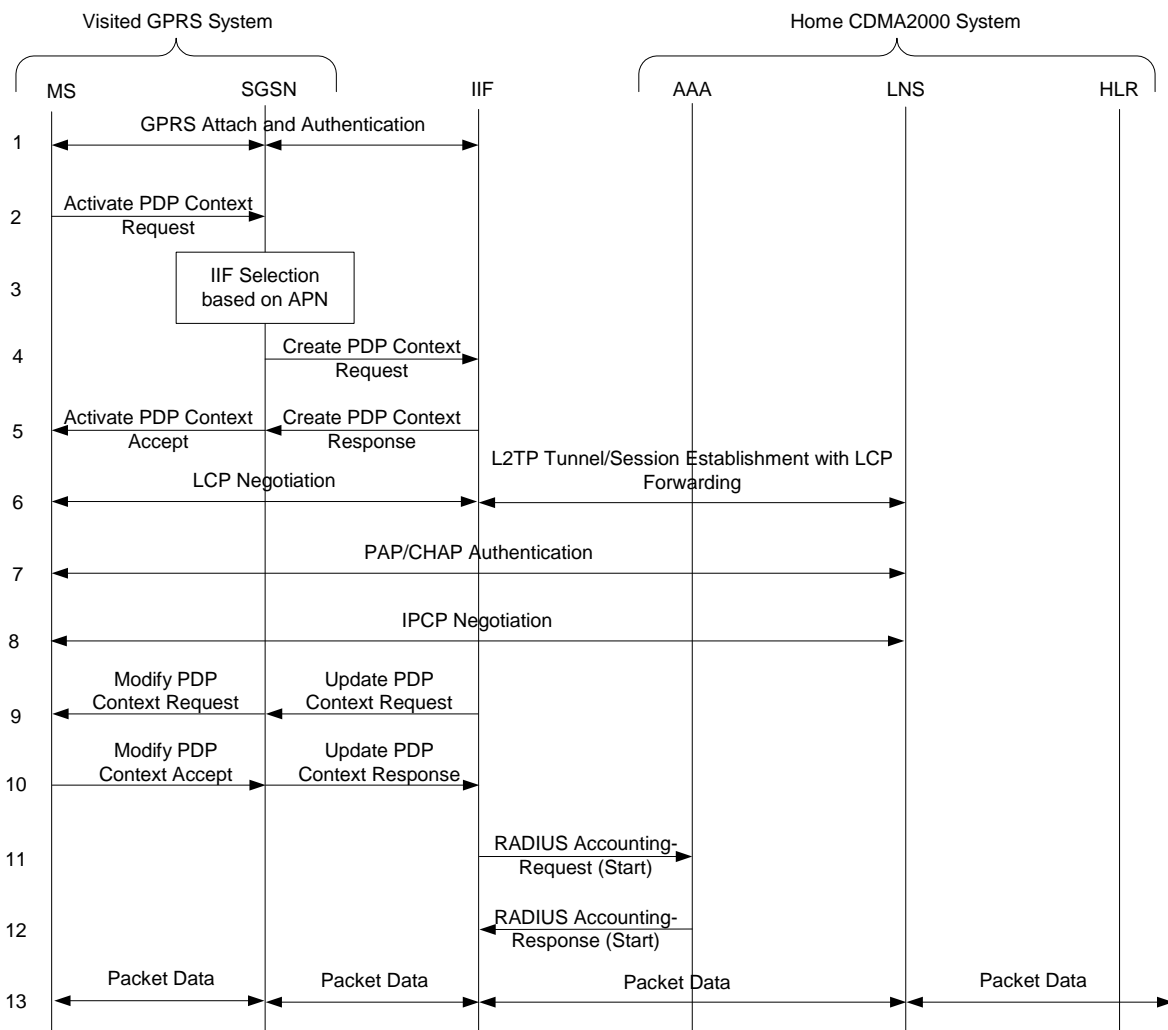


Figure 9 Simple IP operation in the GPRS foreign mode

1. The MS performs GPRS attach with an SGSN. The authentication associated with the GPRS attach is a SIM-based authentication requiring the Ki secret. The IIF supports the GSM HLR functionality and is configured with the Ki secret. The IIF is not required to communicate with the HLR in the home cdma2000 system for the authentication.
2. The MS sends the Activate PDP Context Request to the SGSN. The message includes the APN (Access Point Name). The APN has the format <Network ID>.mnc<MNC>.mcc<MCC>.gprs. The <Network ID> (e.g., cdma2000carrier.com) indicates that the MS wants connectivity to its home cdma2000 system. The <MNC> and <MCC> are derived from the MS's IMSI. The Requested PDP Address is left empty (see section 8.2.4) in the message so that the IIF GGSN functionality will not assign an IP address to the MS. Instead, the address will be assigned by the LNS.
3. The SGSN selects a GGSN based on the APN. The SGSN queries a DNS server (not shown in the figure) and obtains a list of available GGSNs that can be used to support the requested APN. In this case, the APN's Network ID indicates a cdma2000 operator; thus, the DNS server returns with the IIF's IP address.

- 1 4. The SGSN sends the Create PDP Context Request to the selected IIF GGSN functionality
2 to set up a PDP context for the MS. The message includes the APN, but the Requested
3 PDP Address is left empty (see section 8.2.4).
- 4 5. The IIF GGSN functionality sends the Create PDP Context Response to the SGSN that in
5 turn sends the Activate PDP Context Accept to the MS. The PDP Address in both
6 messages is set to 0.0.0.0 to indicate that the PDP address will be assigned later.
- 7 6. After the PDP context is established, the MS and IIF perform PPP LCP negotiation. The
8 IIF acts as a LAC functionality that establishes L2TP tunnels with a LNS. The IIF
9 determines which LNS based on the requested APN². After the L2TP tunnel/session
10 establishment, the IIF LAC functionality forwards LCP message between the LNS and
11 MS. During the LCP negotiation, the LNS and MS negotiate PAP or CHAP as the PPP
12 authentication protocol.
- 13 7. PPP authentication (PAP or CHAP) is performed. The MS's credential is authenticated
14 by the home AAA in the cdma2000 system. The RADIUS interaction between the LNS
15 and home AAA is not shown in the figure.
- 16 8. The LNS and MS perform PPP IPCP negotiation. The IIF LAC functionality relays IPCP
17 messages between the L2TP tunnel and PDP context. During the negotiation, the LNS
18 assigns an IP address to the MS. The IIF monitors for this address and uses it as the
19 MS's PDP address.
- 20 9. The IIF GGSN functionality also needs to notify the SGSN and MS about the updated
21 PDP address. Recall that the PDP address is set to 0.0.0.0 initially. Therefore, the IIF
22 GGSN functionality sends the Update PDP Context Request to the SGSN which in turn
23 sends the Modify PDP Context Request to the MS.
- 24 10. The MS responds with the Modify PDP Context Accept to the SGSN that in turn sends
25 the Update PDP Context Response to the IIF GGSN functionality.
- 26 11. The IIF RADIUS client functionality sends the RADIUS Accounting-Request (Start) to
27 the home AAA server [2]. Standard IETF attributes and mandatory 3GPP2-vendor-
28 specific attributes are included to convey accounting records (section 8.2.3).
- 29 12. The home AAA server responds with the RADIUS Accounting-Response (Start).
- 30 13. Bearer traffic traverses through the IIF in both directions. For routing MS-originated
31 packets, the IIF routes packets received from the MS's GTP tunnel (identified by a TEID)
32 to the MS's L2TP tunnel/session. For routing MS-terminated packets, the IIF routes
33 packets received from the MS's L2TP tunnel/session to the MS's GTP tunnel. IPsec can
34 be used to protect the L2TP tunnel/session between LNS and IIF, and the GTP tunnels
35 between IIF and SGSN.

36 **9.3 cdma2000 Packet Data Foreign Mode with Mobile IPv4**

37 Figure 10 depicts a call flow example for the roaming scenario where a GPRS native subscriber
38 operates Mobile IPv4 [2] in the cdma2000 packet data foreign mode. In this example, the home
39 GPRS system doesn't support HA; thus, the MS has shared secrets with the IIF HA functionality for
40 Mobile IP authentication. The home GPRS system assigns an IP address to the MS dynamically. All
41 MS's data traffic (MS-originated and –terminated) traverses through the IIF and home GPRS system.
42 The IIF receives cdma2000 accounting records from the visited cdma2000 system and may map them
43 to GPRS accounting records and forwards them to the home GPRS system via RADIUS.

² In this example, the IIF is configured with the LNS information (e.g., LNS's IP address) corresponding to an APN.

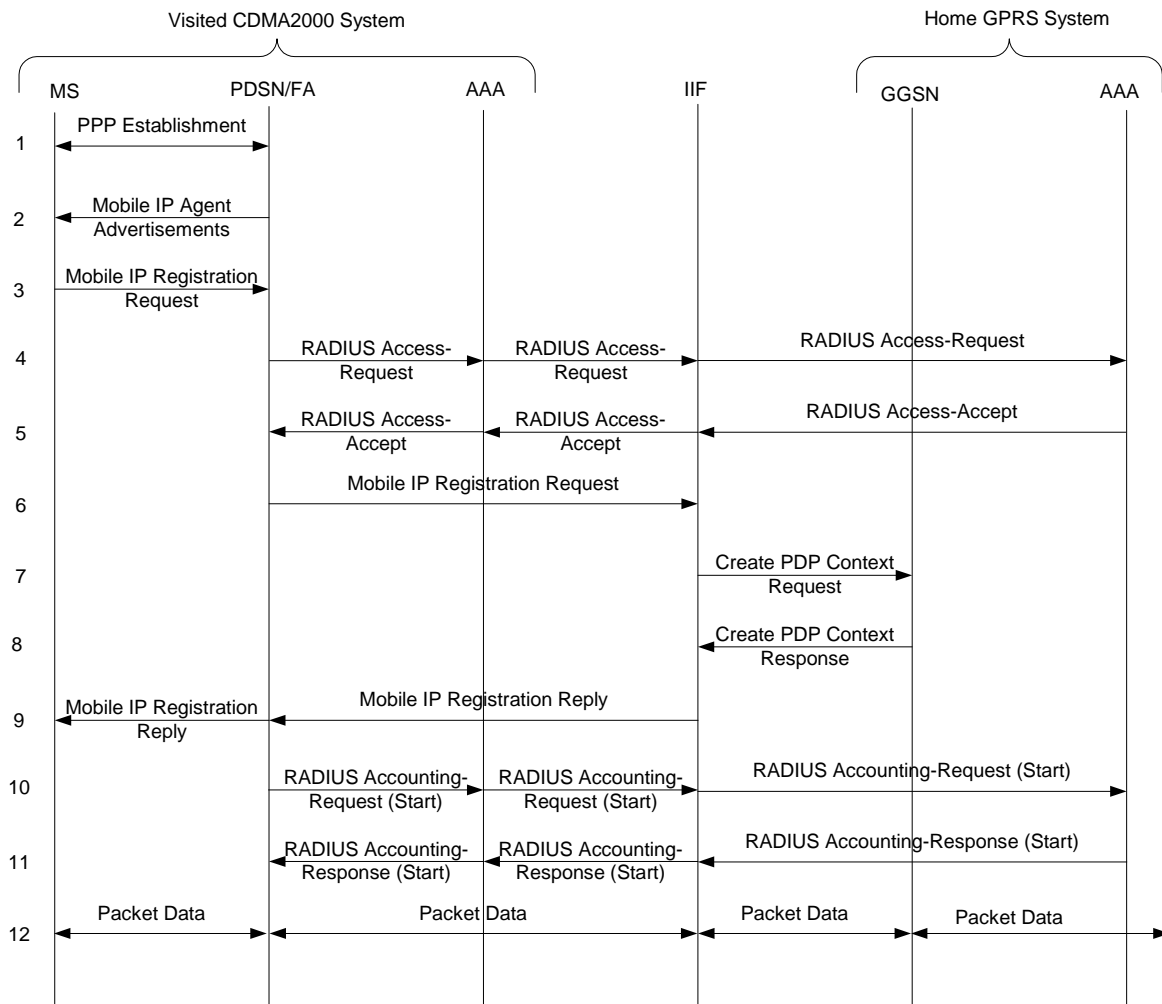
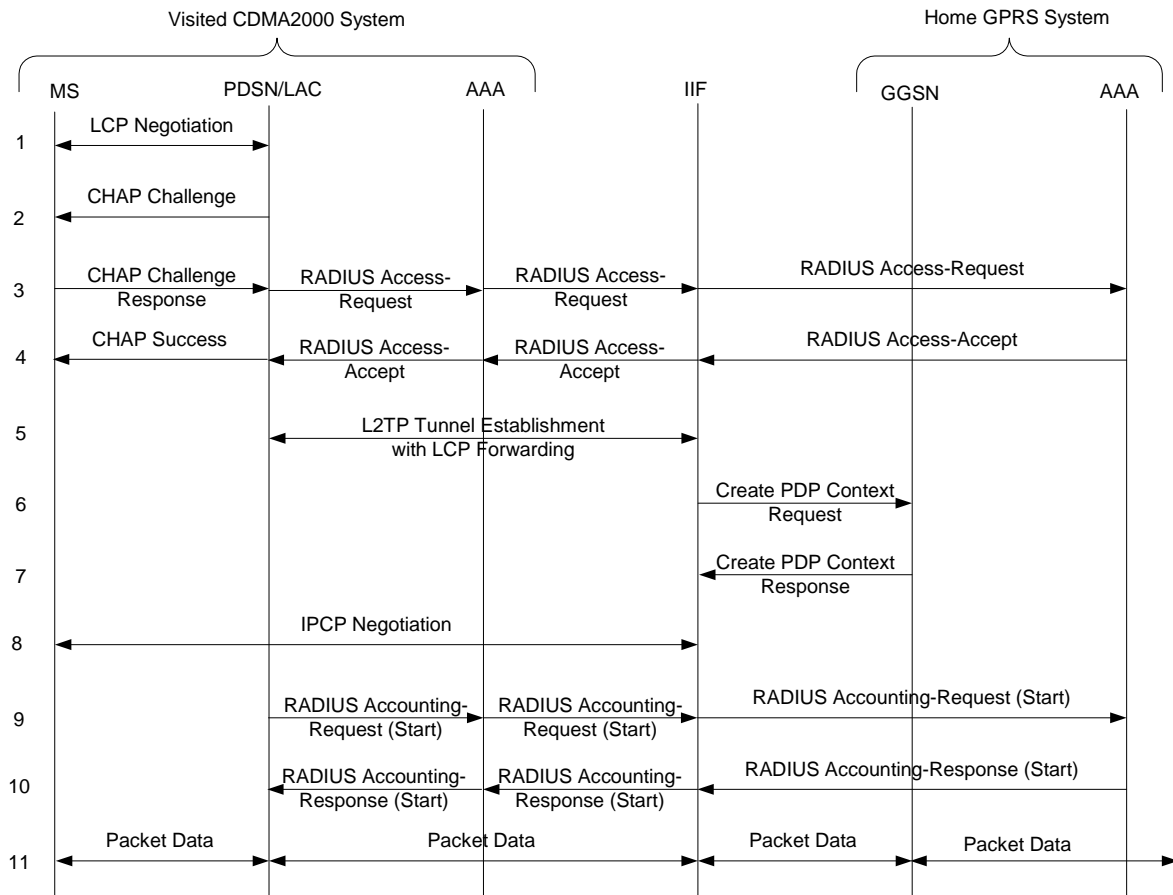


Figure 10 Mobile IPv4 operation in the cdma2000 packet data foreign mode

1. The MS originates SO 33 and establishes a PPP session with the PDSN/FA.
2. The PDSN/FA sends one or more Mobile IP Agent Advertisements to the MS, because the omission of the IP-Address Configuration Option during the PPP IPCP negotiation is the indication that the MS wishes to use Mobile IP. The Agent Advertisement contains the FA Care-of Address and the FA Challenge (FAC).
3. The MS sends the Mobile IP Registration Request to the PDSN/FA. The following information is contained in the Registration Request:
 - MS's NAI [7] has the format <username>@<domain_name>, where the domain_name identifies the MS's home GPRS system.
 - MN-HA authenticator is computed based on the content of the Registration Request and the secret shared between the MS and HA [9]
 - MN-AAA authenticator is computed based on the FAC and the secret shared between the MS and home AAA server [9].
 - HA Address field is set to the permanent HA of the MS.

1 secrets with the home AAA in the GPRS system for CHAP authentication. The home GPRS system
 2 assigns an IP address to the MS dynamically. All MS's data traffic (MS-originated and –terminated)
 3 traverses through the IIF and home GPRS system. The IIF receives cdma2000 accounting records
 4 from the visited cdma2000 system and maps them to GPRS accounting records and forwards them to
 5 the home GPRS system via RADIUS.



6
7 **Figure 11 Simple IP operation in the cdma2000 packet data foreign mode**

- 8
9
10
11
12
13
14
15
16
17
18
19
20
1. The MS originates SO 33 and initiates PPP LCP negotiation with the PDSN/LAC. CHAP is negotiated as the protocol for PPP authentication.
 2. The PDSN/LAC sends a CHAP challenge to the MS.
 3. The MS replies with its NAI and a challenge response computed based on the challenge and the shared secret with its home AAA in the GPRS system. The PDSN/LAC sends a RADIUS Access-Request. Because the domain name of the MS's NAI indicates a GPRS system, the RADIUS Access-Request is routed to the home AAA in the GPRS system via the visited AAA and IIF. The IIF modifies the message in accordance with 8.4.2.1.
 4. If the authentication is successful, the home AAA responds with a RADIUS Access-Accept. The message is routed back to the PDSN/LAC via the IIF and visited AAA. The IIF inserts the Tunnel-Server-Endpoint attribute in the RADIUS Access-Accept. This attribute informs the PDSN/LAC to establish an L2TP tunnel/session with the IIF LNS functionality. In addition, the IIF modifies the RADIUS Access-Accept in accordance

- 1 with 8.4.2.2. The PDSN/LAC sends the CHAP Success to inform the MS about the
2 successful authentication.
- 3 5. The PDSN/LAC establishes an L2TP tunnel/session with the IIF LNS functionality.
4 During the L2TP tunnel/session establishment, the PDSN/LAC forwards the LCP
5 information (exchanged between the MS and PDSN/LAC) to the IIF LNS functionality.
6 The IIF LNS functionality may initiate CHAP challenge (not shown in the figure) to
7 authenticate the MS before IPCP negotiation.
- 8 6. The IIF SGSN functionality establishes GTP tunnels with a GGSN in the home GPRS
9 system and requests an IP address from the GGSN. The IIF derives an APN that has the
10 format <Network ID>.mnc<MNC>.mcc<MCC>.gprs. The <Network ID> is the realm
11 portion of the MS's NAI and is used to indicate which GGSN the MS wants to access for
12 the requested service. The <MNC> and <MCC> are from the MS's IMSI. The MS's
13 NAI and IMSI are available from the RADIUS Access-Request in step 3. The IIF SGSN
14 functionality uses the derived APN as the lookup name to query GPRS DNS server (not
15 shown in the figure) and obtains a list of available GGSNs that can be used to support the
16 requested service. The IIF SGSN functionality sends the Create PDP Context Request to
17 the selected GGSN. The Requested PDP Address in the message is left empty (see
18 section 8.4.3.3) to request a new IP address.
- 19 7. The GGSN responds with the Create PDP Context Response including the new IP
20 address assigned to the MS.
- 21 8. This new IP address is assigned to the MS during the PPP IPCP negotiation between the
22 IIF LNS functionality and MS.
- 23 9. The PDSN sends the RADIUS Accounting-Request (Start) containing cdma2000 packet
24 data accounting information [2]. Because the domain name of the MS's NAI indicates a
25 GPRS system, the RADIUS Accounting-Request (Start) is routed to the home AAA in
26 the GPRS system via the visited AAA and IIF. The IIF may modify the message in
27 accordance with 8.4.2.3.
- 28 10. The home AAA replies with the RADIUS Accounting-Response (Start) that is routed
29 back to the PDSN via IIF and visited AAA.
- 30 11. Bearer traffic traverses through the IIF in both directions. For routing MS-originated
31 packets, the IIF routes packets received from the MS's L2TP tunnel/session to the MS's
32 GTP tunnel (identified by a TEID). For routing MS-terminated packets, the IIF routes
33 packets received from the MS's GTP tunnel to the MS's L2TP tunnel/session. IPsec can
34 be used to protect the L2TP tunnel/session between PDSN/LAC and IIF, and the GTP
35 tunnels between IIF and GGSN.