

1
2 3GPP2 P.S0001
3 Version 1.0
4 Version Date: December 10, 1999
5



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

6 **Wireless IP Network**
7 **Standard**

8

9

10

11

12

13

14

15

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 shoyler@tia.eia.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

16

CONTENTS

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
46
47
48
49
50
51
52

1	INTRODUCTION.....	5
2	GLOSSARY AND DEFINITIONS.....	6
2.1	ACRONYMS.....	6
2.2	DEFINITIONS.....	7
3	REFERENCES.....	9
3.1	MOBILE IP.....	9
3.2	PPP.....	9
3.3	DIFFERENTIATED SERVICES.....	9
3.4	RADIUS.....	10
3.5	IP SECURITY.....	10
3.6	TIA.....	10
3.7	TCP/IP.....	10
4	PROTOCOL REFERENCE MODEL.....	11
4.1	SIMPLE IP.....	11
4.2	MOBILE IP.....	11
4.3	RADIUS.....	12
4.4	NETWORK REFERENCE MODELS.....	13
5	SIMPLE IP OPERATION.....	16
5.1	COMMON SERVICE SPECIFICATION.....	16
5.1.1	<i>PPP Session</i>	16
5.2	PDSN REQUIREMENTS.....	16
5.2.1	<i>PPP Session</i>	16
5.2.1.1	Establishment.....	16
5.2.1.2	Termination.....	16
5.2.1.3	Authentication.....	17
5.2.1.4	Addressing with IPCP.....	17
5.2.1.5	Compression.....	17
5.2.1.6	PPP Octet synchronous Framing.....	17
5.2.2	<i>RADIUS Support</i>	17
5.2.2.1	NAI Construction in the Absence of CHAP.....	18
5.2.3	<i>Ingress Address Filtering</i>	19
5.3	RADIUS SERVER REQUIREMENTS.....	19
5.4	MOBILE STATION REQUIREMENTS.....	19
5.4.1	<i>PPP Session</i>	19
5.4.1.1	Establishment.....	20
5.4.1.2	Termination.....	20
5.4.1.3	Authentication.....	20
5.4.1.4	Addressing with IPCP.....	20
5.4.1.5	Compression.....	20
5.4.1.6	PPP Framing.....	20
6	MOBILE IP OPERATION.....	21
6.1	COMMON SERVICE SPECIFICATION.....	21
6.1.1	<i>PPP Session</i>	21
6.1.2	<i>Mobile IP</i>	21
6.2	PDSN REQUIREMENTS.....	21
6.2.1	<i>PPP Session</i>	21
6.2.1.1	Establishment.....	21

1	6.2.1.2	Termination.....	21
2	6.2.1.3	Addressing with IPCP.....	22
3	6.2.1.4	Authentication with CHAP.....	22
4	6.2.1.5	Compression.....	22
5	6.2.1.6	PPP Octet Synchronous Framing.....	22
6	6.2.2	<i>MIP Registration</i>	22
7	6.2.2.1	Agent Advertisements.....	22
8	6.2.2.2	Addressing and Mobile IP.....	23
9	6.2.2.3	MIP Extensions.....	23
10	6.2.2.4	Private Network Support.....	23
11	6.2.3	<i>RADIUS Support</i>	23
12	6.2.3.1	Local RADIUS Support.....	23
13	6.2.3.2	Home RADIUS Server Support.....	24
14	6.2.4	<i>IP Security Support</i>	24
15	6.2.5	<i>Ingress Address Filtering</i>	25
16	6.3	HOME AGENT REQUIREMENTS.....	25
17	6.3.1	<i>Multiple Registrations</i>	25
18	6.3.2	<i>IP Security Support</i>	25
19	6.3.3	<i>Dynamic Home Address Assignment</i>	25
20	6.4	MOBILE STATION REQUIREMENTS.....	26
21	6.4.1	<i>PPP Session</i>	26
22	6.4.1.1	Establishment.....	26
23	6.4.1.2	Termination.....	26
24	6.4.1.3	Authentication with CHAP.....	26
25	6.4.1.4	Addressing with IPCP.....	26
26	6.4.1.5	Compression.....	26
27	6.4.1.6	PPP Framing.....	26
28	6.4.2	<i>MIP Registration</i>	27
29	6.4.2.1	Agent Discovery.....	27
30	6.4.2.2	Registration Messages.....	27
31	6.4.2.3	MIP Extensions.....	27
32	6.4.2.4	Private Network Support.....	27
33	7	MOBILITY MANAGEMENT	28
34	7.1	MOBILITY WITHIN RADIO NETWORK.....	28
35	7.2	PCF TO PCF HANDOFF.....	28
36	7.3	PDSN TO PDSN HANDOFF.....	28
37	8	QUALITY OF SERVICE (QOS)	29
38	8.1	DIFFERENTIATED SERVICES SPECIFICATION.....	29
39	8.2	PDSN REQUIREMENTS FOR DIFFERENTIATED SERVICES.....	29
40	8.2.1	<i>Service Specification</i>	29
41	8.2.2	<i>IMT-2000 Differentiated Service Class Option</i>	30
42	8.3	RN REQUIREMENTS FOR DIFFERENTIATED SERVICE.....	30
43	8.4	MOBILE STATION REQUIREMENTS FOR DIFFERENTIATED SERVICE.....	30
44	9	ACCOUNTING	31
45	9.1	GENERAL.....	31
46	9.2	AIRLINK RECORDS.....	31
47	9.2.1	<i>Active Start Airlink Record</i>	32
48	9.2.2	<i>Active Stop Airlink Record</i>	33
49	9.2.3	<i>SDB Airlink Record</i>	33
50	9.3	PDSN USAGE DATA RECORD (UDR).....	33
51	9.4	ACCOUNTING FORMATS.....	35
52	9.5	PDSN PROCEDURES.....	38
53	9.5.1	<i>R-P session Establishment</i>	38
54	9.5.2	<i>R-P session Release</i>	38
55	9.5.3	<i>Packet Data Service Establishment</i>	38
56	9.5.4	<i>Packet Data Service Termination</i>	39
57	9.5.5	<i>User Data Through PDSN</i>	39

1	9.5.6	Active Start Airlink Record Arrives	39
2	9.5.7	Active Stop Airlink Record Arrives	39
3	9.5.8	SDB Airlink Record Arrives	39
4	9.5.9	Interim Timer Expires	40
5	9.5.9.1	Time of Day Timer Expires	40
6	10	R-P INTERFACE	41
7	11	RADIO NETWORK REQUIREMENTS	42
8	11.1	R-P GENERAL HANDOFF REQUIREMENTS	42
9	12	AIR INTERFACE	43
10		ANNEX A: IKE/ISAKMP PAYLOADS	44
11		ANNEX B: CERTIFICATES	47
12		ANNEX C: CDMA2000 RADIUS ATTRIBUTES ANNEX:	49

13
14
15

Figures

16	Figure 1: Protocol Reference Model for Simple IP	11
17	Figure 2: Protocol Reference Model for Mobile IP Control and IKE	12
18	Figure 3: Protocol Reference Model for Mobile IP User Data	12
19	Figure 4: RADIUS Protocol Reference Model Using RADIUS	13
20	Figure 5: Reference Model for Access with Mobile IP	14
21	Figure 6: Reference Model for Access with Simple IP	15
22	Figure 7: The MSID Formats	19
23	Figure 8: Accounting Architecture	31
24	Figure 9: cdma2000 RADIUS Attribute Format	49

25
26
27

Tables

29	Table 1: Airlink Record Fields	32
30	Table 2: Airlink Record Fields	32
31	Table 3: Service Configuration Fields	32
32	Table 4: Service Configuration Fields	33
33	Table 5: Active Stop Airlink Fields	33
34	Table 6: SDB Airlink Fields	33
35	Table 7: Complete UDR	35
36	Table 8: Accounting Parameter Attribute RADIUS Definitions	37
37		

1 **1 Introduction**

2 This standard defines requirements for support of wireless packet data networking capability
3 on a third generation wireless system based on cdma2000. This standard is based on PN-
4 4286; Wireless IP Network Architecture based on IETF protocols.

5

6 This standard defines the two methods for accessing Public networks (Internet) and Private
7 networks (Intranets): Simple IP and Mobile IP, and the required Quality of Service and
8 Accounting support. IETF protocols are widely employed whenever possible to minimize the
9 number of new protocols required and to maximize the utilization of well accepted standards
10 and hence the speed to market. References to the required IETF protocols are provided in
11 Section 3 of this standard.

12

13 Following this introduction, the Glossary and Definitions are given in Section 2, and
14 References are provided in Section 3. Section 4 describes the protocol reference models for
15 Simple IP, Mobile IP, RADIUS, and the overall wireless packet data network. Sections 5 and
16 6 describe Simple IP operation and Mobile IP operation, respectively. The common service
17 specification and the requirements placed on the network elements (PDSN, and RADIUS
18 Server) and the mobile station to support each operation is described in the corresponding
19 section. Section 7 describes Mobility Management for PCF-PCF and PDSN-PDSN handoff.
20 Specifications required for Quality of Service and Accounting are described in Sections 8 and
21 9, respectively. Sections 10, 11, and 12 describe the R-P Interface, Radio Network
22 Requirements, and Air Interface, respectively.

1 **2 Glossary and Definitions**

2 **2.1 Acronyms**

3		
4		
5	AH	Authentication Header
6	CHAP	Challenge Handshake Authentication Protocol
7	CRL	Certificate Revocation List
8	DOI	Domain of Interpretation
9	ESP	Encapsulating Security Payload
10	FA	Foreign Agent
11	FAC	Foreign Agent Challenge
12	HA	Home Agent
13	HLR	Home Location Register
14	IKE	Internet Key Exchange
15	IMSI	International Mobile Station Identity
16	IMT-2000	International Mobile Telecommunications - 2000
17	IP	Internet Protocol
18	IPCP	IP Control Protocol
19	IRM	International roaming MIN
20	ISAKMP	Internet Security Association and Key Management Protocol
21	ISP	Internet Service Provider
22	LAC	Link Access Control
23	LCP	Link Control Protocol
24	MSID	Mobile Station Identifier
25	MAC	Medium Access Control
26	MIN	Mobile Identification Number
27	MIP	Mobile IP
28	MS	Mobile Station
29	NAI	Network Access Identifier
30	PAP	Password Authentication Protocol
31	PCF	Packet Control Function
32	PDSN	Packet Data Serving Node
33	PL	Physical Layer
34	PPP	Point-to-Point Protocol
35	QoS	Quality of Service
36	RADIUS	Remote Authentication Dial In User Service
37	RN	Radio Network
38	RRP	Mobile IP Registration Reply
39	RRQ	Mobile IP Registration Request
40	SA	Security Association
41	SPI	Security Parameter Index
42	SS7	Signaling System 7
43	TCP	Transmission Control Protocol
44	UDR	Usage Data Record
45	UDP	User Datagram Protocol
46	VLR	Visitor Location Register

2.2 Definitions

Access Provider Network:

An IMT-2000 cellular network providing access to the mobile user.

Broker RADIUS:

An intermediate RADIUS server that has security relationships with the *Visited RADIUS* and the *Home RADIUS* and is used to securely transfer RADIUS messages between the *Visited Access Provider Network* and the *Home IP Network*. In some situations, there may be more than one broker RADIUS in the path between visited RADIUS and home RADIUS.

Broker RADIUS Network:

A network with an administrative domain that contains the *Broker RADIUS*.

Home RADIUS:

The RADIUS server that resides in the *Home IP Network*.

Home Access Provider Network:

The IMT-2000 cellular network that is the home for the mobile subscriber unit. The user may have a different home network for data services.

Home IP Network:

The home network that provides IP based data services to the user. This network is where the user's NAI is homed. This network may be a private corporate network, publicly accessible ISP network or an IMT-2000 network.

Packet data service:

A general term describing a packet switched data service offered by an IMT-2000 network to a mobile subscriber (user).

Packet data service option:

A service option provides a means between MS and RN to establish and maintain cdma2000 Traffic Channels for packet data service.

Packet data session:

Describes an instance of continuous use of packet data service by the user. A packet data session begins when the user invokes packet data service. A packet data session ends when the user or the network terminates packet data service. During a particular packet data session, the user may change locations but the same IP address is maintained.

Therefore for Simple IP service, moving from the coverage area of one PDSN to another PDSN constitutes a change in packet data session. For Simple IP service, a packet data session and a PPP session occur at the same time. For Mobile IP service, a packet data session can span several PDSNs as long as the user continuously maintains mobility bindings at the Home Agent and there is no lapse in Mobile IP registrations/re-registrations.

PPP Session:

A PPP session describes the time during which a particular PPP connection instance is maintained in the open state in both the mobile station and PDSN. The PPP session is maintained during periods when the mobile station is dormant. If a user hands off from one RN to another RN but is still connected to

1 **the same PDSN, the PPP session remains. If a user changes PDSN, a new PPP**
2 **session is created at the new PDSN.**

3 Private Network:
4 **A *Home IP Network* that resides behind a firewall and that may use private IP**
5 **addresses.**

6 R-P session:
7 **The R-P session is a logical connection established over the R-P interface for a**
8 **particular PPP session. If a user changes RNs during packet data service, the**
9 **R-P session is moved from the old RN to the new RN (still connected to the same**
10 **PDSN). If the user changes PDSNs during packet data service, a new R-P**
11 **session is established and the previous R-P session is released.**

12 Service Provider Network:
13 **An IMT-2000 network operated by either the home service provider or the visited**
14 **service provider. The home service provider maintains the customer business**
15 **relationship with the user. The visited service provider provides IMT-2000**
16 **access services through the establishment of a service agreement with a home**
17 **service provider.**

18 Visited Access Provider Network:
19 **The IMT-2000 cellular network providing service to the user when he is roaming**
20 **outside his home access provider network.**

21 Visited RADIUS:
22 **The RADIUS server that resides in the Visited Access Provider Network.**

1 **3 References**

2 **3.1 *Mobile IP***

- 3 Perkins, IPv4 Mobility, RFC 2002, May 1995.
4
5 Perkins, IP Encapsulation within IP, RFC 2003, October 1996.
6
7 Perkins, Minimal Encapsulation within IP, RFC 2004, October 1996.
8
9 Solomon, Applicability Statement for IP Mobility support, RFC 2005, October 1995.
10
11 Cong, Hamnlen, Perkins, The Definitions of Managed Objects for IP Mobility Support Using
12 SMLv2, RFC 2006, October 1995.
13
14 Montenegro, Reverse Tunneling for Mobile IP, RFC 2344, May 1998.
15
16 Calhoun, Perkins, Mobile IP Foreign Agent Challenge/Response Extension, RFC xxxx,
17 December 1999.
18
19 Calhoun, Perkins, Mobile NAI Extension RFC xxxx December 1999.

20 **3.2 *PPP***

- 21 Simpson, The Point to Point Protocol (PPP), RFC 1661, July 1994.
22
23 Simpson, Mobile-IPv4 Configuration Option for PPP IPCP, RFC 2290, February 1998.
24
25 Simpson, PPP in HDLC-like Framing, RFC1662, July 1994.
26
27 Friend, Schneider, PPP LZS-DCP Compression Protocol (LZS-DCP), RFC1967, August 1996.
28
29 Rand, The PPP Compression Control Protocol (CCP), RFC1962, June 1996.
30
31 Friend, Simpson, PPP Stac LZS Compression Protocol, RFC 1974, August 1996.
32
33 Woods, PPP Deflate Protocol, RFC 1979, August 1996.
34
35 Simpson, PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, August
36 1996.
37
38 McGregor, The PPP Internet Protocol Control Protocol (IPCP), RFC 1332, May 1992.
39
40 Pall , Microsoft Point-To-Point Compression (MPPC) Protocol, RFC 2118, March 1997.
41
42 Zorn, PPP LCP Internationalization Configuration Option, RFC 2484, January 1999.

43 **3.3 *Differentiated Services***

- 44 Nichols, Blake, Baker, Black, Definition of the Differentiated Services Field (DS Field) in the
45 IPv4 and IPv6 Headers, RFC 2474, December 1998.
46
47 Blake, Black, Carlson, Davies, Wang, Weiss, An Architecture for Differentiated Services, RFC
48 2475, December 1998.
49
50 Heinanen, Baker, Weiss, Wroclawski, Assured Forwarding PHB Group, RFC 2597, June
51 1999.
52

1 Jacobson, Nichols, Poduri, An Expedited Forwarding PHB, RFC 2598, June 1999.

2 **3.4 RADIUS**

3 Rigney, RADIUS Accounting, RFC 2139, April 1997.

4
5 Rigney, Rubens, Simpson, Willens, Remote Authentication Dial In User Service (RADIUS),
6 RFC 2138, August 1997.

7
8 Rivest, R., and S. Dusse, "The MD5 Message-Digest Algorithm", RFC 1321, MIT Laboratory
9 for Computer Science, RSA Data Security Inc., April 1992.

10 **3.5 IP Security**

11 Kent, Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.

12
13 Kent, Atkinson, IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

14
15 Kent, Atkinson, IP Authentication Header, RFC 2402, November 1998.

16 **3.6 TIA**

17 TIA TR-45.6, TSB XXX, Wireless IP Network Architecture based on IETF Protocols, January
18 2000.

19
20 3GPP2 TSG-A, 3GPP2 Access Network Interfaces Technical Specification (3G-IOS) Version
21 4.0.0, December 1999.

22
23 TIA TR-45.5, IS-707-A.1.12: cdma2000 High Speed Packet Data Service for Service Option
24 33, Nov. 1999.

25
26 TIA TR-45.5, IS-2000-1: Introduction to cdma2000 Standards for Spread Spectrum Systems,
27 July 1999.

28
29 TIA TR-45.5, IS-2000-2: Physical Layer Standard for cdma2000 Spread Spectrum Systems,
30 July 1999.

31
32 TIA TR-45.5, IS-2000-3: Medium Access Control (MAC) Standard for cdma2000 Spread
33 Spectrum Systems, July 1999.

34
35 TIA TR-45.5, IS-2000-4: Signaling Link Access Control (LAC) Standard for cdma2000 Spread
36 Spectrum Systems, July 1999.

37
38 TIA TR-45.5, IS-2000-5: Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread
39 Spectrum Systems, July 1999.

40
41 ITU-T Recommendation E.212, The International Identification Plan for Mobile Terminals and
42 Mobile Users

43
44 Mobile Identification Number (MIN) [TIA/EIA-41-E]

45
46 TIA/EIA/TSB-29-A, International Implementation of Cellular Radiotelephone Systems
47 Compliant with ANSI/EIA/TIA 553; September 1992

48 **3.7 TCP/IP**

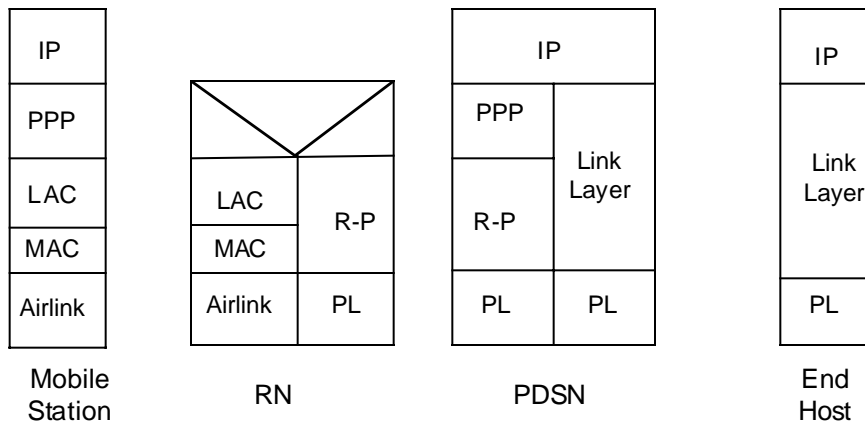
49 Jacobson, Compressing TCP/IP Headers for Low Speed Serial Links, RFC 1144, February
50 1990.

1 **4 Protocol Reference Model**

2 This section will specify the protocol architecture between the entities of the Wireless IP
3 Network architecture. Refer to TSB XXX for a general description of the Wireless IP Network
4 architecture, its components and message flows. Note that although the Mobile IP and
5 Simple IP services are represented in different protocol reference models, the network is able
6 to provide both Simple IP and Mobile IP service simultaneously to a mobile station.

7 **4.1 Simple IP**

8 Figure 1 shows the protocol reference model for Simple IP service.
9
10



11
12
13
14

Figure 1: Protocol Reference Model for Simple IP

15 **4.2 Mobile IP**

16 Figures 2 and 3 show the protocol reference model for Mobile IP control and data,
17 respectively. IPsec in Figures 2 and 3 will be necessary in some situations and not in other
18 situations. For example: IKE and IPsec AH are mandatory for the Mobile IP control when the
19 HA is in the IMT-2000 network. When the HA is in a private network, IKE and IPsec AH for
20 Mobile IP control are optional. Typically, when the HA is in a private network, the private
21 network will require IPsec ESP for the IP in IP tunnel. When the HA is in the home access
22 provider network, the carrier may choose to use IPsec ESP between HA and FA.
23

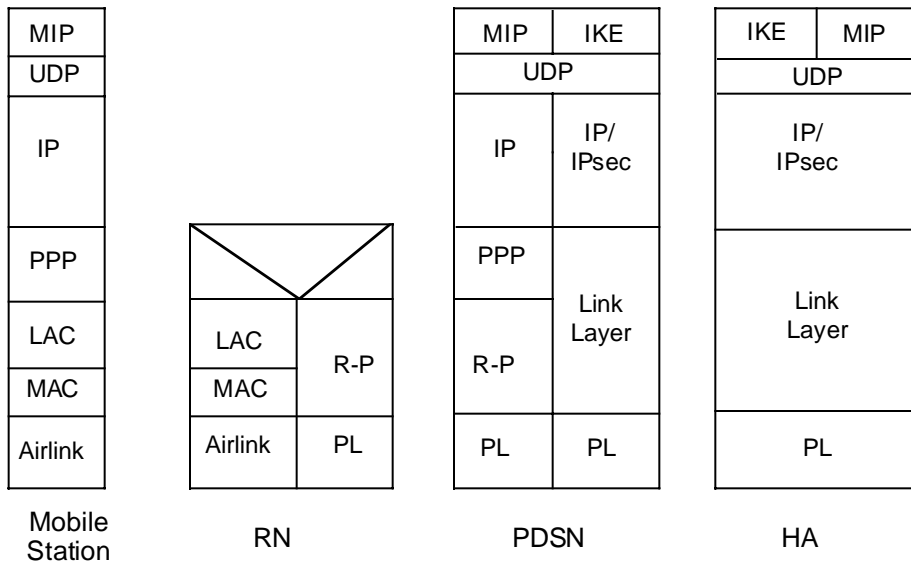


Figure 2: Protocol Reference Model for Mobile IP Control and IKE

1
2
3
4
5

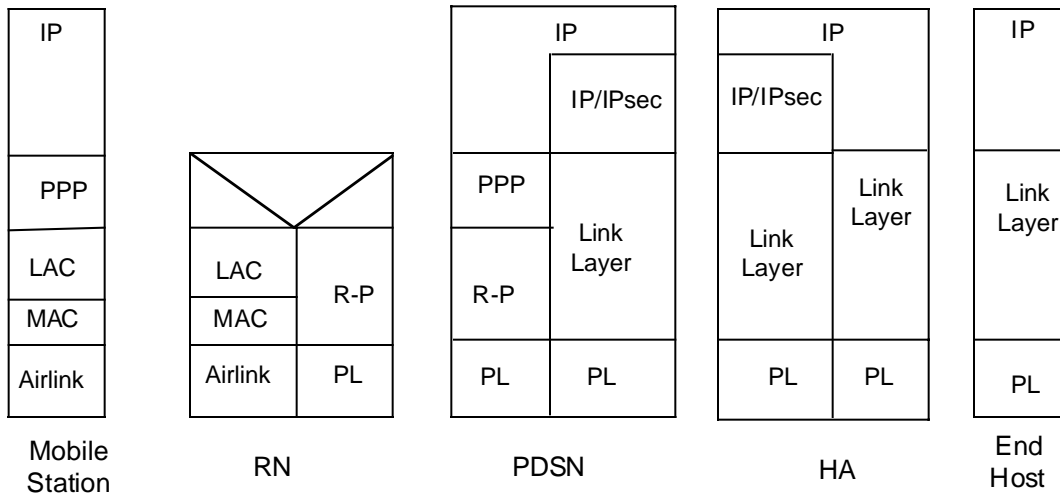


Figure 3: Protocol Reference Model for Mobile IP User Data

6
7
8

4.3 RADIUS

Figure 4 shows the protocol reference model for RADIUS server to wireless data entity. In the protocol reference model of Figure 4, the RADIUS servers in the serving carrier and home network (which may be a private network or carrier network) communicate via RADIUS proxy servers and one or more RADIUS brokers.

Note: The broker is optional.

9
10
11
12
13
14
15
16

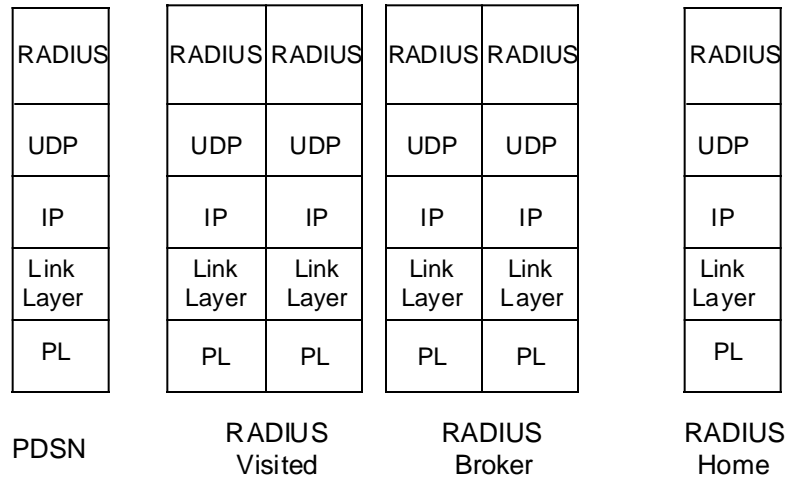


Figure 4: RADIUS Protocol Reference Model Using RADIUS

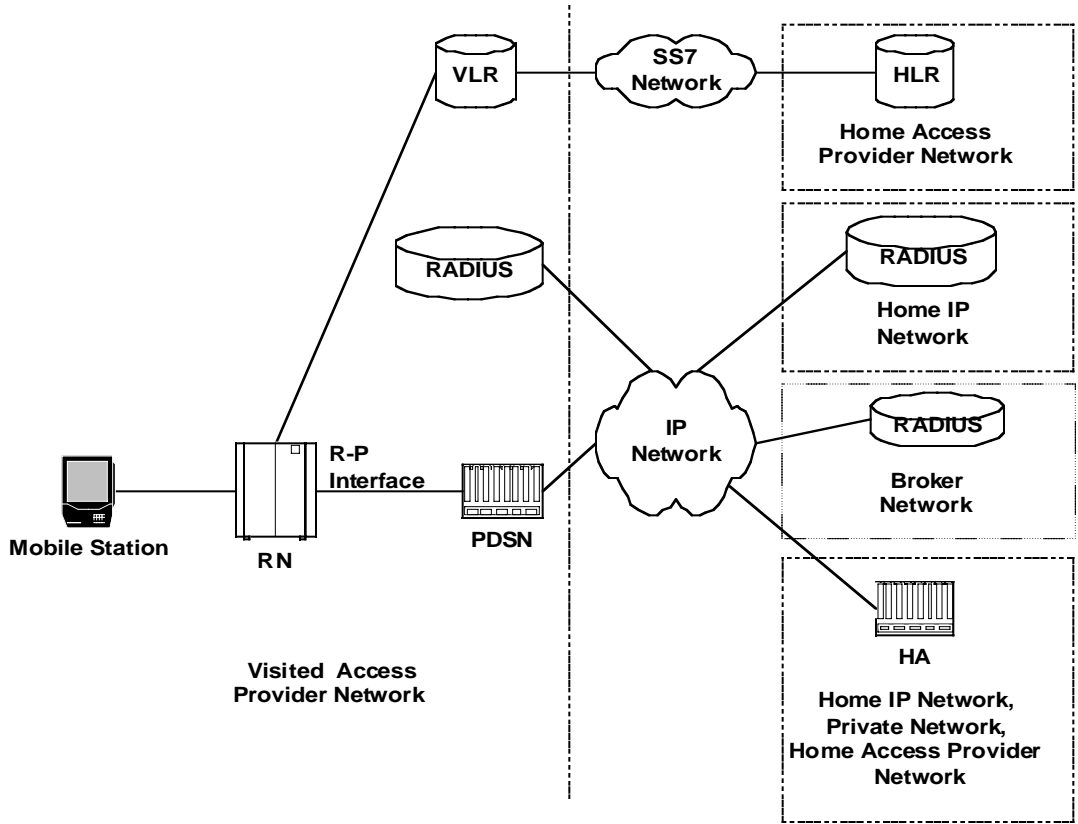
1
2
3
4

4.4 Network Reference Models

Figure 5 shows an IMT-2000 network reference model with IMT-2000 service provider boundaries. For the case of Mobile IP Service to the public Internet in which the mobile station is roaming, the HA will reside in a home access provider network. For private network or home ISP access, the HA will reside in the respective external network.

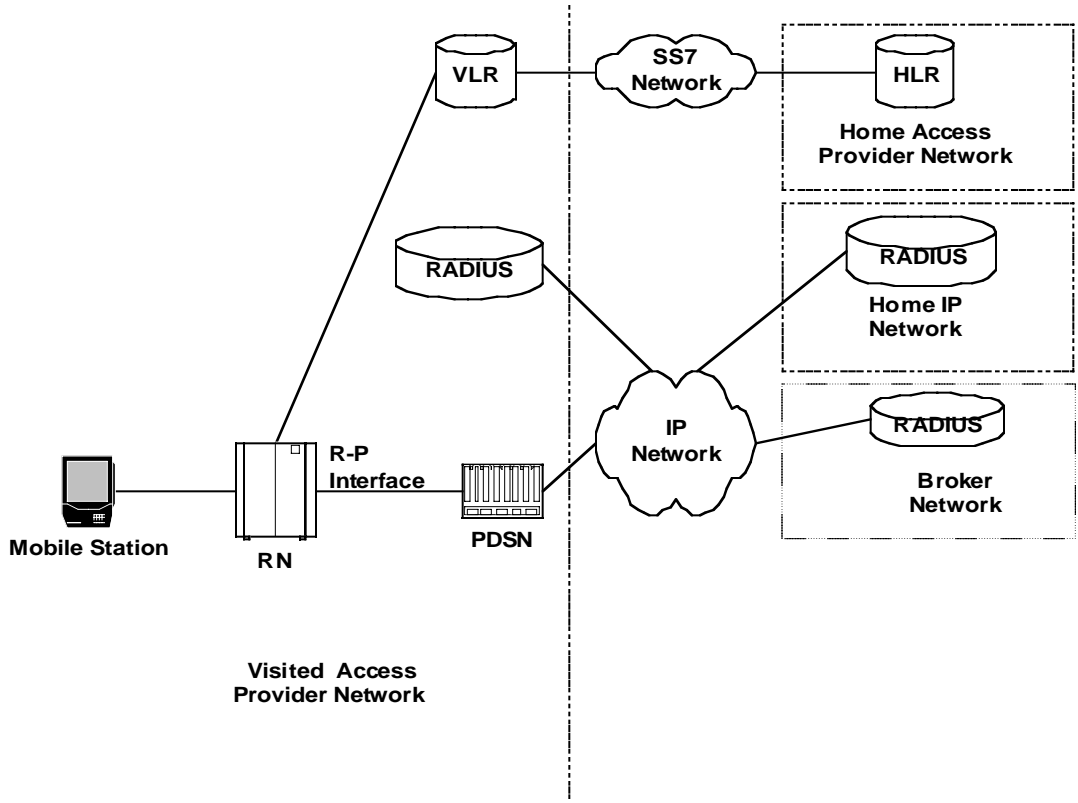
10
11
12

For the Simple IP Service, the HA will not be required, as shown in Figure 6.



1
2
3
4

Figure 5: Reference Model for Access with Mobile IP



1
2
3
4

Figure 6: Reference Model for Access with Simple IP

1 **5 Simple IP Operation**

2 This section describes the requirements and procedures for Simple IP operation. In this
3 standard, Simple IP refers to a service in which the user is assigned a dynamic IP address
4 from the local PDSN and is provided IP routing service to a visited access provider network.
5 The user may maintain its IP address as long as it is served by a radio network which has
6 connectivity to the address assigning PDSN. There is no IP address mobility beyond this
7 PDSN, and secured access to a home network, via Simple IP, is beyond the scope of this
8 standard.

9 **5.1 Common Service Specification**

10 The common requirements for several network elements (e.g., PDSN and mobile station) for
11 Simple IP operation are described here.

12 **5.1.1 PPP Session**

13 PPP shall be the data link protocol between the mobile station and the PDSN for Simple IP
14 operation. PPP must be established before any IP datagrams can be exchanged between
15 mobile station and PDSN.

16
17 PPP shall be supported as defined in the following standards with any limitations or
18 extensions described in this standard.:

- 19 • Point to Point Protocol (RFC 1661);
- 20 • PPP byte oriented HDLC (RFC 1662);
- 21 • IPCP (RFC 1332)

22
23 PPP encryption shall not be negotiated by either the mobile station or PDSN. Only one PPP
24 session shall be supported between the mobile station and the PDSN.

25 **5.2 PDSN Requirements**

26 The PDSN shall support Simple IP operation. The PDSN requirements for Simple IP operation
27 are described here.

28 **5.2.1 PPP Session**

29 **5.2.1.1 Establishment**

30 Immediately after the RN opens an R-P interface connection to a mobile station, the PDSN
31 shall send an LCP Configure-Request for a new PPP session to the mobile station. If the RN
32 establishes an R-P session corresponding to a mobile station for which a PPP session
33 already exists, the PDSN shall not send an LCP Configure-Request to the mobile station.
34

35 PPP shall support control escaping in accordance with 4.2 of RFC 1662. The PPP Link Layer
36 shall support negotiation of async control character mapping as defined in RFC 1662. The
37 PDSN shall negotiate a control character mapping, and shall attempt to negotiate the
38 minimum number of escapes by negotiating an ACM of 00000000.

39 **5.2.1.2 Termination**

40 The PDSN shall clear the PPP state if there is no established underlying R-P session for the
41 mobile station.

42
43 The PDSN shall support a PPP inactivity timer for each PPP session. When the inactivity
44 timer expires, the PDSN shall terminate the PPP session and shall take usual steps such as
45 release of the R-P session to the RN that supports the expired PPP session.

46
47 The PDSN shall clear the R-P session whenever the PPP Session is closed.

1 **5.2.1.3 Authentication**

2 The PDSN shall support authentication via CHAP during PPP establishment. The PDSN shall
3 support a configuration option to require CHAP. The PDSN shall propose CHAP as a PPP
4 option in an LCP Configure-Request. A mobile station may be configured by the network
5 operator to not negotiate CHAP. For such mobile stations, the mobile station may send an
6 LCP Configure Nak proposing PAP. The PDSN may accept PAP by sending an LCP
7 Configure-Request with PAP

8
9 If the PDSN is not configured to require CHAP, and PAP is not negotiated, then the PDSN
10 shall adhere to the guidelines in 5.2.2.1. If the PDSN is configured to require CHAP or PAP
11 and the mobile station sends a Configure Reject, the PDSN shall end the PPP session.

12 **5.2.1.4 Addressing with IPCP**

13 The PDSN shall assign the mobile station a dynamic IP address for Simple IP service during
14 the IPCP phase of PPP.

15 **5.2.1.5 Compression**

16 The PDSN shall support CCP (RFC 1962) for the negotiation of PPP compression. The
17 PDSN shall support Van Jacobson TCP/IP header compression (RFC 1144).

18
19 The PDSN shall support the following types of PPP compression:

- 20
21 • Stac-LZS (RFC 1974);
22 • Microsoft Point-To-Point Compression Protocol (RFC 2118) compression.
23 • Deflate (RFC2394)

24 **5.2.1.6 PPP Octet synchronous Framing**

25 The PDSN shall frame PPP packets sent on the PPP link layer using the octet synchronous
26 framing protocol defined in RFC 1662, except that there shall be no inter-frame time fill (see
27 4.4.1 of RFC 1662). That is, no flag octets shall be sent between a flag octet that ends one
28 PPP frame and the flag octet that begins the subsequent PPP frame.

29 **5.2.2 RADIUS Support**

30 On receipt of the CHAP response from the mobile station, the PDSN shall create an Access-
31 Request containing at a minimum:

- 32
33 User-Name (1) = NAI
34 User-password(2) = password (if PAP)
35 CHAP-Password (3) = CHAP ID and CHAP-response if CHAP
36 NAS-IP-Address (4) = IP address of PDSN
37 CHAP-Challenge (60) if CHAP
38 Accounting Session ID (44) (same as R-P session ID)

39
40 The PDSN shall act as a RADIUS client in accordance with RFC 2138 and shall communicate
41 user CHAP or PAP authentication information to the local RADIUS server in a RADIUS
42 Access-Request. The local RADIUS server will send a RADIUS Access-Accept message to
43 the PDSN. The RADIUS Access Accept message may contain the Differentiated Service
44 Indication attribute. This attribute is defined in Annex C.

45
46 The PDSN shall act as a RADIUS accounting client in accordance with RFC2139 and shall
47 communicate user accounting information to the local RADIUS server in RADIUS Accounting-
48 Requests. The Accounting-Request shall contain the Accounting Session ID attribute (44)
49 generated by the PDSN.

1 The security of communications between PDSN and RADIUS server as well as between
2 RADIUS servers may optionally be protected with IP security. The establishment of the
3 security association is outside the scope of this standard.

4 **5.2.2.1 NAI Construction in the Absence of CHAP**

5 In the event that the mobile station does not negotiate CHAP, no mobile station NAI is
6 received by the PDSN. In this case, the PDSN shall not perform additional authentication of
7 the user. Accounting records however, still must be generated and these records are keyed
8 on the user NAI. For this reason, the PDSN shall be capable of constructing a properly
9 formed NAI (RFC 2486) based on the MSID of the mobile station. The NAI shall be
10 constructed in the form <MSID>@<realm>, where <MSID> is the MSID of the mobile station,
11 and <realm> is the Internet realm of the home network that owns the mobile station MSID.

12
13 The mobile station shall use one of the following MSID formats (see figure 7):

- 14 • International Mobile Station Identity MSID (IMSI) [E.212]
- 15 • Mobile Identification Number (MIN) [TIA/EIA-41-E]
- 16 • International Roaming MIN (IRM) [TIA TSB-29]

17
18
19 The IMSI is a string of decimal digits, up to a maximum of 15 digits, that identifies a unique
20 MS internationally. The IMSI consists of three fields: Mobile Country Code (first 3 digits),
21 Mobile Network Code (next 2 or 3 digits), and Mobile Subscriber Identification Number
22 (maximum of 10 digits). If the MS uses IMSI, the PDSN may determine the realm by using a
23 lookup table that maps the Mobile Country Code and Mobile Network Code of the IMSI to a
24 string representing the realm.

25
26 The MIN is a string of 10 digits that identifies a unique MS in TIA/EIA-41. The first digit of
27 MIN cannot be 0 or 1. The MIN consists of three fields: Area Code (first 3 digits), Office Code
28 (next 3 digits), and Subscriber Number (last 4 digits). If the MS uses MIN, the PDSN may
29 determine the realm by using a lookup table that maps the Area Code and Office Code of the
30 MIN to a string representing the realm.

31
32 The IRM is a string of 10 digits that identifies a unique MS internationally. The first digit of
33 IRM must be 0 or 1. This is used to distinguish IRM from MIN. The IRM consists of three
34 fields: Mobile Country Code (first 3 digits), Mobile Network Code (4th digit), and Subscriber
35 Number (last 6 digits). The Mobile Network Code must be 0 or 1. If the MS uses IRM, the
36 PDSN may determine the realm by using a lookup table that maps the Mobile Country Code
37 and Mobile Network Code of the IRM to a string representing the realm.
38 The PDSN shall write the constructed NAI into accounting records and the realm value will be
39 optionally used by the visited RADIUS server to forward these records to the correct home
40 RADIUS server for proper summary and settlement¹. The constructed NAI shall not be used
41 for authentication. The PDSN shall send RADIUS accounting messages to the local RADIUS
42 server using the constructed NAI in the absence of CHAP if configured to do by the operator.
43 If the mobile station does not support CHAP and the PDSN is not configured to require
44 CHAP, then the PDSN shall construct an NAI based on the mobile station ID as specified in
45 this section.

¹ The home RADIUS server may require an MSID to user conversion table to map the constructed NAI to the user's actual NAI to complete the billing process in cases where the constructed NAI differs from the actual NAI. This conversion list must be provided by the visited access network provider by some means.

1
2

IMSI	Mobile Country Code (3 digits)	Mobile Network Code (2 or 3 digits)	Mobile Subscriber Identification Number (10 digits max)
MIN	Area Code (3 digits)	Office Code (3 digits)	Subscriber Number (4 digits)
IRM	Mobile Country Code (3 digits)	Mobile Network Code (1 digit)	Subscriber Number (6 digits)

3
4

Figure 7: The MSID Formats

5 **5.2.3 Ingress Address Filtering**

6 The PDSN shall check the source IP address of every packet received on the PPP link from
7 the mobile station. If the address is not associated with the PPP Session to the mobile
8 station, and is not a MIP RRQ or Agent Solicitation, then the PDSN shall discard the packet,
9 and send an LCP Configure-Request to restart the PPP session. Once the mobile station
10 invokes Simple IP then ingress filtering must be performed on all packets.

11 **5.3 RADIUS Server Requirements**

12 RADIUS Server shall follow the guidelines specified in RFC 2138, RFC 2139, draft-ietf-radius-
13 radius-v2-01.txt, and draft-ietf-radius-accounting-v2-01.txt.

14

15 If the mobile station uses CHAP, the RADIUS server will receive a RADIUS Access Request
16 from the PDSN with CHAP authentication information, and shall forward the RADIUS Access
17 Request to the home network or a peer (e.g., a broker) if it does not have the authority to
18 accept/deny the request. This is in accordance with RFC 2138 and draft-ietf-radius-
19 radius-v2-01.txt.

20

21 In that case, the RADIUS server will later receive a RADIUS Access Accept message from the
22 home or broker network. The RADIUS server shall then send the RADIUS Access Accept to
23 the PDSN. The RADIUS server will receive a RADIUS Accounting Start from the PDSN. The
24 RADIUS server later receives a RADIUS Accounting Stop from the PDSN in accordance with
25 RFC 2139 and draft-ietf-radius-accounting-v2-01.txt. If the RADIUS server is in the visited
26 network, the visited RADIUS server shall forward the RADIUS accounting messages to the
27 home or broker network.

28

29 The security of communications between RADIUS servers may optionally be protected with IP
30 security. The establishment of the security association is outside the scope of this Standard.
31 Also see RFC 2138 for additional RADIUS security requirements.

32 **5.4 Mobile Station Requirements**

33 The mobile station may optionally support Simple IP. When the mobile station wants to use
34 Simple IP, the mobile station shall use packet data service option 33 as specified in
35 TIA/EIA/IS-707A-1.12.

36 **5.4.1 PPP Session**

37 The mobile station shall use PPP as the data link protocol for Simple IP.

1 **5.4.1.1 Establishment**

2 The mobile station shall exchange LCP messages as described in RFC 1661, and shall
3 support the LCP extensions defined in RFC 2484

4
5 PPP shall support control escaping in accordance with 4.2 of RFC 1662. The PPP Link Layer
6 shall support negotiation of async control character mapping as defined in RFC 1662. The
7 mobile station should negotiate a control character mapping. If the mobile station negotiates
8 control character mapping, it should attempt the minimum number of escapes by negotiating
9 an ACM of 00000000.

10 **5.4.1.2 Termination**

11 When the mobile station wishes to terminate packet data service, the mobile station should
12 send LCP-terminate to the PDSN to gracefully close the PPP session before terminating the
13 packet data service with the RN.

14
15 If the mobile station becomes aware that the RN has terminated packet data service, the
16 mobile station may consider its PPP session closed at that point.

17 **5.4.1.3 Authentication**

18 The mobile station shall support CHAP authentication for Simple IP. However, the network
19 operator may configure a mobile station to not use CHAP. In that case, the mobile station
20 shall be permitted to skip over the CHAP phase by sending a Configure-Reject to the PDSN
21 in response to a Configure-Request that offers the CHAP option.

22
23 The mobile station may support PAP authentication for Simple IP. If the mobile station uses
24 PAP, it shall respond to an LCP Configure-Request for CHAP with an LCP Configure-Nak
25 proposing PAP.

26 **5.4.1.4 Addressing with IPCP**

27 The mobile station shall send an IP address of 0.0.0.0 during the IPCP phase to request a
28 dynamic IP address from the network. The mobile station shall accept the address provided
29 by the PDSN.

30 **5.4.1.5 Compression**

31 The mobile station shall support Van Jacobson TCP/IP header compression (RFC 1144).
32 The TCP/IP header compression shall be configured through IPCP. The mobile station may
33 support PPP Compression Control Protocol (RFC 1962). If the mobile station wishes PPP
34 payload compression, the mobile station should use PPP Compression Control Protocol to
35 negotiate a PPP payload compression algorithm, and the mobile station shall support one of
36 the following compression algorithms:

- 37 • Stac-LZS (RFC 1974);
- 38 • Microsoft Point-To-Point Compression Protocol (RFC 2118).
- 39 • Deflate (RFC2394)

40
41 The mobile station may support additional PPP payload compression algorithms.

42 **5.4.1.6 PPP Framing**

43 The mobile station shall use the octet-synchronous framing protocol defined in RFC 1662,
44 except there shall be no inter-frame time fill, i.e., no flag octets shall be sent between a flag
45 octet that ends one PPP frame and the flag octet that begins the subsequent PPP frame.²

² N.B.: If the mobile station consists of a laptop and a relay-model handset, the laptop may send inter-frame time fill that prevents the mobile from becoming dormant.

1 **6 Mobile IP Operation**

2 This section describes the requirements and procedures for Mobile IP operation. In this
3 standard, Mobile IP refers to a service based on RFC 2002 in which the user is provided IP
4 routing service to a public IP network and/or secure IP routing service to predefined private IP
5 networks. The user may either use a static IP address belonging to its home network HA, or
6 it may be assigned a dynamic address belonging to its home network HA. The user is able to
7 maintain its IP address connectivity even when handing off between radio networks
8 connected to separate PDSNs.

9 **6.1 Common Service Specification**

10 The common requirements for several network elements (e.g., PDSN and mobile station) for
11 Mobile IP operation are described here.

12 **6.1.1 PPP Session**

13 PPP shall be the data link protocol between the mobile station and the PDSN for Mobile IP
14 operation. PPP must be established before any IP datagrams can be exchanged between
15 mobile station and PDSN.

16
17 PPP shall be supported as defined in the following standards with any limitations or
18 extensions described in this standard:

- 19
- 20 • Point to Point Protocol (RFC 1661);
- 21 • PPP byte oriented HDLC (RFC 1662);
- 22 • IPCP (RFC 1332)
- 23

24 PPP encryption shall not be negotiated by either the mobile station or PDSN. Only one PPP
25 session shall be supported between the mobile station and the PDSN.

26
27 For Mobile IP, CHAP should not be performed. If CHAP is performed, performance
28 degradation will occur as the result of an un-needed RADIUS traversal. Note that the FAC
29 shall be performed regardless of whether or not CHAP is performed.

30 **6.1.2 Mobile IP**

31 Mobile IP operation shall be supported as defined in the following standards with any
32 limitations or extensions described in this standard:

- 33
- 34 • RFC 2002-2006;
- 35 • Reverse Tunneling (RFC 2344);
- 36 • Foreign Agent Challenge/Response (RFC XXXX);
- 37 • NAI Extension (RFC XXXX)

38 **6.2 PDSN Requirements**

39 The PDSN shall support Mobile IP operation

40 **6.2.1 PPP Session**

41 . The PDSN shall support multiple Mobile IP home addresses over the single PPP session.

42 **6.2.1.1 Establishment**

43 See Section 5.2.1.1.

44 **6.2.1.2 Termination**

45 The PDSN shall clear the PPP state if there is no established underlying R-P session for the
46 mobile station.

47

1 For Mobile IP service, the PPP inactivity timer shall be set to a value larger than the FA's
2 maximum allowable values for Mobile IP registration lifetime.

3 **6.2.1.3 Addressing with IPCP**

4 For Mobile IP dynamic home address assignment, upon the initial MIP registration:

- 5 ▪ The mobile station will not include an IP-Address Configuration Option in the IPCP
6 Configure Request to the PDSN, and,
- 7 ▪ The PDSN shall not assign an IP address to the mobile station.

8
9 For Mobile IP static home address assignment OR if the mobile station has already been
10 assigned a MIP address and the same MIP session is being continued:

- 11 ▪ If the mobile station uses the IP-Address Configuration Option in the IPCP Configure
12 Request to indicate its home address, the PDSN shall accept any non-zero value.
- 13 ▪ If the mobile station uses the Mobile IPv4 Configuration Option (RFC 2290), the PDSN
14 shall reply with an IPCP Configure-Reject and the mobile station then re-send the IPCP
15 Configure Request with the IP-Address Configuration Option.

16 **6.2.1.4 Authentication with CHAP**

17 The PDSN shall propose CHAP in an LCP Configure-Request. For Mobile IP the mobile
18 station should not use CHAP and should respond with an LCP Configure-Reject requesting
19 no CHAP authentication. The PDSN shall re-send an LCP Configure-Request without the
20 authentication option after receiving the LCP Configure-Reject (CHAP) from mobile stations.
21 Mobile stations will respond with an LCP Configure-Ack as described in RFC 1661.

22 **6.2.1.5 Compression**

23 The PDSN shall support CCP for the negotiation of PPP compression. The PDSN shall
24 support Van Jacobson TCP/IP header compression.

25
26 The PDSN shall support the following types of PPP compression:

- 27
- 28 • Stac-LZS (RFC 1974);
- 29 • Microsoft Point-To-Point Compression Protocol (RFC 2118) compression.

30 **6.2.1.6 PPP Octet Synchronous Framing**

31 See Section 5.2.1.6.

32 **6.2.2 MIP Registration**

33 **6.2.2.1 Agent Advertisements**

34 For the mobile station that uses Mobile IP, the PDSN shall begin transmission of an operator
35 configurable number of Agent Advertisements immediately following establishment of PPP, or
36 upon reception of an Agent Solicitation message from the mobile station. If the mobile
37 station sends a Mobile IP RRQ to the PDSN, the PDSN shall cease sending Agent
38 Advertisements. Once the PDSN sends the configurable number of Advertisements, the
39 PDSN shall not send further Advertisements, unless it receives an Agent Solicitation message
40 from the mobile station. For Simple IP service, the PDSN shall not send any Agent
41 Advertisements to the mobile station following establishment of PPP.

42
43 The Mobile IP Registration Lifetime field in the Agent Advertisement shall be smaller than the
44 PPP inactivity timer.

45
46 The PDSN may send Agent Advertisement(s) if the PCF indicates the mobile station has
47 undergone a dormant handoff.

48
49 In order to minimize Agent Advertisements sent over the air, the PDSN shall not send
50 unsolicited Agent Advertisements to a mobile station periodically to refresh the FA

1 advertisement lifetime. The mobile station may send Agent Solicitations when the FA
2 advertisement lifetime expires. The Advertisement Lifetime field should be set to 9000
3 seconds.

4 **6.2.2.2 Addressing and Mobile IP**

5 The PDSN shall support both static and dynamic home address assignments. For dynamic
6 home address assignment, the PDSN shall accept Mobile IP RRQs with a 0.0.0.0 source
7 address from the mobile station. For dynamic home address assignment, the PDSN will
8 acquire the home address from the Mobile IP RRP. The PDSN shall use a publicly routable
9 and visible care-of-address.

10 **6.2.2.3 MIP Extensions**

11 The PDSN shall include MN-FA Challenge Extension [FAC] in the Agent Advertisement. The
12 challenge shall be changed on a periodic basis.

13 **6.2.2.4 Private Network Support**

14 The PDSN shall support private home addresses. If the mobile station desires a private
15 home address then the mobile station should negotiate reverse tunneling (RFC 2344). The
16 PDSN shall form a logical association that contains the R-P session ID, the mobile station's
17 home address, and the Home Agent address. When the PDSN receives a packet for a
18 registered mobile station from the Home Agent, the PDSN shall map the mobile station's
19 Home Agent address and the home address to one association, and shall transmit the
20 packet on the R-P connection indicated by the link address of the association.

21
22 If two Home Agents assign a mobile station the same address, the PDSN shall send a failed
23 RRP with an Administratively-Prohibited error code (65).

24 **6.2.3 RADIUS Support**

25 **6.2.3.1 Local RADIUS Support**

26 On receipt of the MIP RRQ from the mobile station, the PDSN shall create an Access
27 Request containing the User-Name, CHAP-Password, CHAP-Challenge, NAS-IP-Address
28 Attributes HA address, and Security Status:::

29

30 User-Name Attribute = MN-NAI field in the MN-NAI Extension

31 CHAP-Password Attribute = High-order byte of the Challenge Field in the MN-FA
32 Challenge Extension, followed by the Authenticator field in the MN-RADIUS
33 Extension

34 CHAP-Challenge Attribute = MD5 (Preceding MIP RRQ, Type, Length, SPI), followed
35 by the least-order 237 bytes of the Challenge Field in the MN-FA Challenge
36 Extension. The MD5 checksum is computed over the MIP RRQ data preceding
37 the MN-RADIUS Extension and the Type, Length, SPI fields of the MN-RADIUS
38 Extension.

39 NAS-IP-Address Attribute = IP address of the PDSN COA contained in RRQ
40 HA address contained in the RRQ
41 Security Status

42

43 The PDSN shall act as a RADIUS client in accordance with RFC2138 and shall communicate
44 user FAC authentication information to the local RADIUS server in a RADIUS Access-
45 Request.

46

47 The local RADIUS server will send a RADIUS Access-Accept message to the PDSN. The
48 RADIUS Access-Accept message may contain the cdma2000 RADIUS attributes in Annex C.

49

50 The PDSN shall act as a RADIUS accounting client in accordance with RFC 2139 and shall
51 communicate user accounting information to the local RADIUS server in RADIUS Accounting-

1 Requests. The Accounting-Request shall contain the Accounting Session ID attribute (44)
2 generated by the PDSN.

3
4 The security of communications between PDSN and RADIUS server may optionally be
5 protected with IP security. The establishment of security is outside the scope of this standard.

6 **6.2.3.2 Home RADIUS Server Support**

7 See 6.3.4.

8 **6.2.4 IP Security Support**

9 This Standard allows a number of security options between PDSN (FA) and HA:

- 10 • Dynamic pre-shared IKE secret distributed by the home RADIUS server;
- 11 • Statically configured HA/FA authentication extension shared secret;
- 12 • Statically configured IKE pre-shared secret;
- 13 • IKE and public certificates.

14
15
16 There may be a statically configured HA/FA authentication extension secret for the Mobile IP
17 registration messages. If such a static secret exists, the PDSN and HA shall use it.

18
19 The PDSN shall support IPsec and IKE, and support a statically configured pre-shared secret
20 for IKE. The PDSN may optionally support certificates.

21
22 A home RADIUS server will optionally be able to instruct the PDSN to use IPsec on the
23 registration messages and/or the tunneled data, or not use IPsec at all. The home RADIUS
24 server will optionally distribute a pre-shared secret for IKE. The PDSN shall support the
25 capability to accept a pre-shared key from the home RADIUS server.

26
27 If the home network has indicated that IPsec security associations shall be used between HA
28 and FA, then the PDSN shall establish security associations using certificates, if the PDSN
29 has a certificates with the Home Agent. If certificates with the Home Agent do not exist, then
30 the PDSN shall use a dynamically distributed shared secret for IKE in preference to a
31 statically configured one.

32
33 The PDSN shall determine the security type for HA/PDSN communications as follows:
34 Upon receiving a MIP RRQ from a mobile station, the PDSN sends an Access-Request as
35 outlined in Section 6.x.x.x. That Access-Request should contain *Security Status* attribute
36 that has one of possible values

- 37
- 38 1. IPsec SA already established
- 39 2. IPsec SA not established and a certificate exists for the HA
- 40 3. IPsec SA not established, no certificate exists for the HA, but a configured pre-
41 shared IKE secret exists
- 42 4. IPsec SA not established, no certificate exists for the HA, and no configured pre-
43 shared IKE secret exists
- 44

45 If the PDSN does not send the Security Status attribute then no dynamic pre-shared key for
46 IKE will be returned by the home RADIUS server.

47
48 The Home RADIUS server optionally supports the *cdma2000 RADIUS* attributes and the
49 PDSN shall support the *cdma2000 RADIUS* attributes. The home RADIUS server may
50 authorize the user for IKE services using the *cdma2000 security level* attribute in the Access-
51 Accept. If the Home RADIUS server authorizes IPsec services, and if the *Security Status*
52 attribute in the Access-Request from the PDSN indicates no security association currently
53 exists, and no certificate for the Home Agent exists, then the home RADIUS may also
54 optionally return a pre-shared key for the PDSN using the *Pre-Shared Secret* attribute in the
55 Access-Accept.

1 If the user is authorized for IPsec services, then the PDSN shall provide IPsec services as
2 indicated in the *cdma2000 security level* attribute. If a pre-shared key is provided, then the
3 PDSN shall use the pre-shared key. If reverse tunneling is supported by the Home Agent as
4 indicated by the RADIUS server in the *cdma2000 Reverse Tunnel Specification* attribute, and
5 IPsec security is authorized for tunneled data, and the mobile requests reverse tunneling,
6 then the PDSN will provide security be provided on the reverse tunnel.
7

8 The PDSN shall not delete existing IPsec security associations to a HA if the home RADIUS
9 server does not authorize security for the mobile, because other mobiles may be using the
10 same IPsec security association. However, a home network will incur charges for the mobile if
11 the Home Agent has negotiated encryption for any mobiles.
12

13 When the PDSN determines that an IPsec security association to protect control messages
14 has already been established to the Home Agent, the PDSN shall ensure the IPsec security
15 association is maintained throughout the Mobile IP registration lifetime by periodically
16 refreshing the security association. The PDSN shall not forward a MIP RRQ to the HA unless
17 an IPsec security association exists first, if the home network authorizes IPsec services. The
18 PDSN shall send a failed MIP RRP to the mobile station if the RADIUS Access-Reject is
19 received or if it is unable to establish an IPsec security association to the HA and IPsec
20 security is authorized by the home RADIUS server.
21

22 The home RADIUS server will hide shared secrets using a method based on the RSA
23 Message Digest Algorithm MD5 [RSA] as described in Section 5.2 of RFC2138 [RADIUS].
24 This shared secret is associated with the next hop RADIUS server.
25

26 The PDSN shall comply with the specifications in [IKE], and the Annexes A and B in this
27 Standard.

28 **6.2.5 Ingress Address Filtering**

29 The PDSN is not required to perform ingress filtering, if the mobile station only uses MIP
30 service.

31 **6.3 Home Agent Requirements**

32 The Home Agent must support basic MIP [RFC 2002-2006], reverse tunneling [RFC 2344],
33 NAI [RFC XXXX], and have a public address.

34 **6.3.1 Multiple Registrations**

35 The HA shall support multiple registrations for dynamic address assignment from the same
36 mobile station provided the mobile station uses different NAIs for each address. The HA shall
37 assign unique addresses to the mobile station for each registration.

38 **6.3.2 IP Security Support**

39 The HA shall determine which type (if any) security associations are required with a PDSN.
40

41 Note: Separate security associations are required for MIP control and IP in IP tunnels. Also,
42 IKE requires that all mobile stations on a given HA address receive the same security for
43 either registration messages or tunneled data.

44 The Home Agent may request a pre-shared key from the home RADIUS server in an Access-
45 Request that using a concatenation of the PDSN's care-of-address and home agent address
46 placed in the *user name* attribute. The security of the Home Agent and RADIUS server is
47 outside the scope of this Standard.

48 **6.3.3 Dynamic Home Address Assignment**

49 The mobile station may send the home agent a MIP RRQ with a 0.0.0.0 home address. In
50 this case, if the home agent successfully authenticates the registration based on the shared
51 secret using the mobile station's NAI, the home agent shall assign a home address to the

1 mobile station. The assigned address shall be inserted in the home address field of the MIP
2 RRP. The home agent shall release the home address when the registration expires.

3 **6.4 Mobile Station Requirements**

4 The mobile station may optionally support Mobile IP. If the mobile station wants to use Mobile
5 IP, the mobile station shall use packet data service option 33 as specified in TIA/EIA/IS-
6 707A-1.12.

7 **6.4.1 PPP Session**

8 The mobile station shall use PPP as the data link protocol for Mobile IP. The mobile station
9 may support multiple Mobile IP home addresses over a single PPP session.

10 **6.4.1.1 Establishment**

11 Same as Section 5.4.1.1

12 **6.4.1.2 Termination**

13 Same as Section 5.4.1.2.

14 **6.4.1.3 Authentication with CHAP**

15 The mobile station should not use CHAP for Mobile IP. When the mobile station receives a
16 LCP Configuration-Request requesting CHAP authentication, the mobile station should reply
17 with a LCP Configure-Reject requesting no CHAP authentication. The PDSN will re-send an
18 LCP Configure-Request without the authentication option after receiving the LCP Configure-
19 Reject (CHAP) from mobile stations. Mobile stations shall respond with an LCP Configure-Ack
20 as described in RFC 1661.

21
22 If CHAP is performed, performance degradation will occur as the result of an unnecessary
23 RADIUS traversal. Note that the FAC shall be performed regardless of whether or not CHAP
24 is performed.

25 **6.4.1.4 Addressing with IPCP**

26 If the mobile station uses a static home address, the mobile station shall use the IP-Address
27 Configuration Option (RFC 1332) to indicate the home address, or omit this option. Since the
28 PDSN will not support RFC 2290, if the mobile station uses Mobile IPv4 Configuration Option,
29 the PDSN will reply with IPCP Configure-Reject, and the mobile station then shall use IP-
30 Address Configuration Option.

31
32 If the mobile station requires a dynamic home address assigned through Mobile IP, the
33 mobile station shall not include IP-Address Configuration Option in the IPCP Configure-
34 Request to the PDSN. On subsequent PPP establishments while maintaining a MIP
35 registration, the mobile station shall use IP Address Configuration Option to indicate this
36 address, or omit the option.

37 **6.4.1.5 Compression**

38 Same as Section 5.4.1.5.

39 **6.4.1.6 PPP Framing**

40 Same as Section 5.4.1.6.

1 **6.4.2 MIP Registration**

2 **6.4.2.1 Agent Discovery**

3 Immediately after PPP is established, the mobile station may send Agent Solicitations. In this
4 case, the mobile station should use the same procedure as described in Section 2.4 of RFC
5 2002. If the mobile station does not have a home address, the mobile station shall use zero
6 in the Source IP Address field of the IP packet that contains the Agent Solicitation. The
7 Agent Advertisement received in response to the Agent Solicitation will contain the Foreign
8 Agent Challenge.

9 **6.4.2.2 Registration Messages**

10 Upon receiving Agent Advertisements, the mobile station shall send a Mobile IP RRQ.

11
12 If the mobile station wants a dynamic home address, the mobile station shall use zero in the
13 Home Address field of the Mobile IP RRQ, and the mobile station shall use zero in the Source
14 IP Address field of the IP packet that contains the Mobile IP RRQ. In this case the NAI is
15 used to identify the mobile station. The mobile station shall obtain a home address in the
16 Mobile IP RRP. On subsequent re-registrations while retaining the same home address, the
17 mobile station shall insert the assigned address into the home address field of the Mobile IP
18 RRQ.

19
20 If the mobile station desires reverse tunneling, the mobile station shall set the T-bit in the
21 Mobile IP RRQ.

22 **6.4.2.3 MIP Extensions**

23 The mobile station shall include the MN-FA Challenge Extension [FAC], MN-RADIUS
24 Extension [FAC], MN-NAI Extension [NAI], and MN-HA Authentication Extension [RFC 2002]
25 in the MIP RRQ.

26
27 The mobile station shall compute the MN-RADIUS Extension, according to [FAC], based on
28 the shared secret the mobile station has with the home RADIUS server. The mobile station
29 shall compute the MN-HA Authentication Extension, according to [RFC 2002], based on the
30 shared secret the mobile station has with the HA. The mobile station may use the same
31 shared secret or different shared secrets in the computation of the MN-RADIUS Extension
32 and MN-HA Authentication Extension. This will be coordinated between the mobile station
33 and its home network.

34 **6.4.2.4 Private Network Support**

35 If the mobile station wants private network access through Mobile IP, the mobile station shall
36 use reverse tunneling.

1 **7 Mobility Management**

2 **7.1 Mobility within Radio Network**

3 In this standard the term "handoff" is defined to mean continuity of some state during an
4 interface change from one entity to another. In the absence of any continuity of state
5 whatsoever, this standard will not refer to such interface changes as "handoffs".

6 **7.2 PCF to PCF Handoff**

7 The link layer mobility management function is used to manage the change of the R-P
8 session point of attachment while maintaining existing communications. The R-P session
9 point of attachment is the PCF. When a mobile station moves from one PCF to another PCF,
10 a new R-P session is required to be setup for every packet data session.

11
12 PCF to PCF handoff may happen while a mobile station is active or dormant. The purpose of
13 dormant PCF handoff is to maintain link layer connectivity while a mobile station is dormant
14 while minimizing the use of airlink resources.

15
16 The PCF to PCF handoff involves:

- 17
- 18 • PDSN selection
- 19 • New R-P session setup
- 20 • Previous R-P session tear down
- 21

22 The new PCF triggers a new R-P session setup. If the PDSN selected is the same (current)
23 PDSN for the mobile station, then the PDSN triggers a release of the previous R-P session. If
24 a different PDSN is selected, the old R-P session will expire, unless the mobile station returns
25 to the previous PDSN before the R-P session expires. During PCF to PCF handoff, an effort
26 is made to select the same PDSN, and thereby maintain the link layer connection to the
27 mobile station. If a different PDSN is selected, a PDSN to PDSN handoff occurs only if the
28 mobile station has an existing Mobile IP session before the new PDSN is selected, and
29 performs a successful Mobile IP registration.

30 **7.3 PDSN to PDSN Handoff**

31 During a packet data session, when a mobile station moves from one PDSN to another
32 PDSN, a new PPP session is always established for every packet data session.

33
34 Mobile IP provides IP layer mobility management function that maintains existing
35 communications across PDSNs. There is no similar IP layer mobility management function
36 support between PDSNs for Simple IP service. For Mobile IP mobile stations, in order to
37 maintain IP connectivity, the mobile station will effect a PDSN to PDSN handoff by registering
38 with its Home Agent as per RFC 2002 with extensions as outlined in Section 6 above. For
39 Simple IP mobile stations, there is no PDSN to PDSN handoff, and IP connectivity cannot be
40 maintained. In this case, a new packet data session is established along with the PPP
41 session.

42
43 The PDSN to PDSN handoff for Mobile IP involves:

- 44
- 45 • Establishment of new PPP session
- 46 • Detection of new Foreign Agent via the Agent Advertisement Message
- 47 • Registration with the Home Agent
- 48

49 A PDSN to PDSN handoff requires the mobile station be active or to transition to the active
50 state.

1 **8 Quality of Service (QoS)**

2 This section specifies extensions to the Simple IP and Mobile IP services. This extension
3 includes differentiated services behavior of the mobile station and PDSN, and IMT-2000
4 differentiated service class options indicated in the user's RADIUS profile. The IMT-2000
5 differentiated service class options specify groupings of differentiated services classes.

6 **8.1 Differentiated Services Specification**

7 The mobile station may optionally support, and the PDSN should support, differentiated
8 services as defined in:

- 9 • Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
10 (RFC 2474);
- 11 • An Architecture for Differentiated Services (RFC 2475);
- 12 • An Expedited Forwarding PHB (RFC 2598);
- 13 • Assured Forwarding PHB Group (RFC 2597).

15 **8.2 PDSN Requirements for Differentiated Services**

16 **8.2.1 Service Specification**

17 When a mobile station has marked packets with a differentiated services class, the PDSN
18 may optionally accept the marking or may remark the packet as the user profile's IMT-2000
19 Differentiated Service Class Options from the home RADIUS server indicates. When the
20 mobile station has not marked the packets, the PDSN may optionally mark packets from the
21 mobile station to specific differentiated service classes as the user profile's IMT-2000
22 Differentiated Service Class Options. The PDSN may indicate a differentiated services class
23 for each packet via the R-P interface as described in Section 10

24
25 Note: the user profile may indicate no differentiated services are authorized for the user, and
26 if so, the PDSN will mark the user's packets as configured by the service provider network.

27
28 For Mobile IP service, the Home Agent shall copy the differentiated services class of each
29 packet to the differentiated service field of the tunnel, in accordance with RFC 2002. For
30 Mobile IP service with reverse tunneling enabled, the PDSN shall determine the differentiated
31 services field of each tunneled packet to the Home Agent based on the user profile and
32 other considerations specified in this section.

33
34 The PDSN shall send packets received from the IP network for a mobile station onto the R-P
35 connection for the mobile station in accordance with differentiated class behavior of the
36 packet and the user profile's IMT-2000 Differentiated Service Class Options.

37
38 Differentiated Service Class marking shall be done only when the PDSN sends the complete
39 PPP frame in a single Aquater frame boundary (marking the packet type in the Aquater
40 Packet Type header parameter as PPP). If the PDSN sends incomplete frames, multiple PPP
41 frames or parts of multiple PPP frames (marking the packet type in the Aquater Packet Type
42 header parameter as non-PPP), the differentiated service class marking of the PPP frame
43 shall not be used in the routing header of the Aquater frame.

44
45 If the mobile station negotiates a PPP payload compression algorithm that requires PPP
46 frames to be delivered in sequence, or if the mobile station uses VJ compression in which the
47 Connection ID is compressed, then the PDSN shall indicate to the RN one and only one
48 differentiated services class on the R-P interface for all the mobile station's packets. In this
49 case, the RN will not allow any reordering of PPP frames for that user. When the PDSN
50 assigns a single differentiated services level for all frames destined for the RN based on the
51 user profile's IMT-2000 Differentiated Service Class Options from the Home RADIUS server.

52

1 If the mobile station negotiates a compression algorithm, or no compression algorithm, that
2 does not rely on a sequential delivery of packets, or VJ compression ID is not compressed,
3 then the PDSN shall not use sequential numbering of packets in the routing header of the
4 Aquater interface. The RN may reorder PPP frames received for that user and multiple
5 differentiated service levels may be used for the frames destined for the RN for that user (one
6 service level per PPP frame).

7
8 The IMT-2000 provider must insure that it does not exceed its service level agreements (SLA)
9 with its supporting ISPs; however, the procedures to insure that SLAs are satisfied are
10 beyond the scope of this Standard.

11
12 For packets received from the RN, the PDSN shall not process the differentiated services
13 class field associated with the R-P interface. The RN may transmit packets to the mobile
14 station in accordance with the differentiated services class indicated on the R-P interface.

15 **8.2.2 IMT-2000 Differentiated Service Class Option**

16 As indicated above, the IMT-2000 Differentiated Service Class Options specify groupings of
17 differentiated services classes. For some IMT-2000 Differentiated Service Class Options, not
18 all differentiated service classes may be supported. This option is contained in a user profile
19 parameter in the home RADIUS server, and is returned to the PDSN in the RADIUS
20 Accounting Request message. The format of the RADIUS attribute is given in Annex C. The
21 actual parameters associated with these classes, such as classification rules and policing
22 parameters are configured into the PDSN by the carrier operator, and are not sent in the
23 RADIUS profile parameter. The method by which carriers agree to the same PDSN
24 configuration definitions for each class, as well as the method to inform private network
25 owners and ISPs of these class definitions, is outside the scope of this Standard.

26 **8.3 RN Requirements for Differentiated Service**

27 The RN may use the Differentiated Service indication from the R-P interface generated by the
28 PDSN to deliver packets to the mobile station. When the PDSN assigns a single
29 differentiated services level for all frames destined for the RN, the RN will not allow any
30 reordering of the PPP frames.

31
32 The RN does not perform general differentiated services processing functions such as
33 policing, nor does it examine the actual PPP frame itself to perform additional differentiated
34 services information beyond those supported by the PDSN.

35 **8.4 Mobile Station Requirements for Differentiated Service**

36 The mobile station may support differentiated services or may rely on the network to perform
37 packet marking.

1 **9 Accounting**

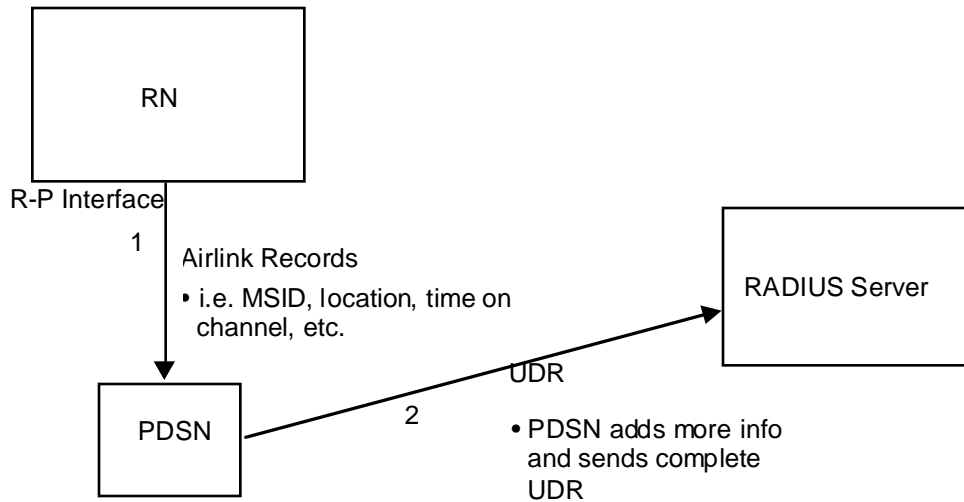
2 **9.1 General**

3 Packet Accounting parameters are divided into radio specific parameters collected by the RN,
4 and IP network specific parameters collected by the PDSN. The PDSN merges the radio
5 specific parameters for a given user session with the IP network specific ones to form a
6 Usage Data Record (UDR). After merging, the PDSN will send the UDR to a local RADIUS
7 Server. The PDSN will maintain the UDR information until the PDSN receives positive
8 acknowledgment from the RADIUS server that the RADIUS server has correctly received the
9 UDR.

10 The PDSN will formulate one UDR per IP address per mobile station per session.

11
12 The RADIUS server will maintain the UDR until the record is removed by the carrier's billing
13 system. The method by which this is done is beyond the scope of this standard as is the
14 summary, reconciliation, and billing process used by the carriers.

15
16 The RN sends radio specific parameters in messages called airlink records across the R-P
17 interface. Once the PDSN combines these with IP network specific parameters, the UDR is
18 sent to the RADIUS server as a RADIUS Accounting-Request message. This is outlined as
19 below in Figure 8, and detailed in the subsequent sections.



21
22
23
24 **Figure 8: Accounting Architecture**
25

26 **9.2 Airlink Records**

27 The RN generates one of three types of airlink records over the R-P interface:

- 28
29
- 30 ▪ An Active Start record when the MS has started to use traffic channel(s) .
 - 31 ▪ An Active Stop record when the MS has stopped using traffic channel(s).
 - 32 ▪ A Short Data Burst (SDB) record when a forward or reverse short data burst is exchanged with MS.
- 33

34 If some parameter(s) of the active session have changed, the RN shall send an Active Stop
35 airlink record, and an Active Start airlink record with the new parameters.

1
2
3

Table 1 is a summary of the fields in airlink records generated by the RN. .

Item	Parameter	Max Payload Length	Format
a. Mobile Identifiers			
a1	MSID	15	string
c. Session Identifiers			
C1	R-P Session ID	4	string
d. Infrastructure Identifiers			
d3	Serving PCF	4	ip-addr
d4	BS / MSC ID	6	octet
e. Zone Identifiers			
e1	User Zone	2	octet
f. Session Status			
f1	ServiceConfiguration Parameters	11	octet
f4	Mobile Originated/Mobile Terminated Indicator	1	octet
g. Session Activity			
g3	Active Connection Time in Seconds	4	integer
g10	SDB Octet Count	4	time
i. Quality of Service			
i4	Airlink Quality of Service (QoS)	4	integer

4
5
6
7
8
9

Table 1: Airlink Record Fields

Table 2 contains information present in the R-P session setup message, and shall not to be duplicated in each airlink record.

Item	Parameter	Max Payload Length	Format
a1	MSID	15	string
d3	Serving PCF	4	ip-addr
d4	BS / MSC ID	6	octet

10
11
12
13
14
15
16
17
18

Table 2: Airlink Record Fields

Each R-P session and each airlink record is indexed via the R-P session ID. The R-P session ID is the R-P tunnel identifier for a particular mobile station and PDSN.

Table 3 contains fields from service configuration record are provided in airlink records. They are recorded in the UDR.

Item	Service Configuration Parameters	Max Payload Length	Format
f1.1	Forward Mux Option	1	octet
f1.2	Reverse Mux Option	1	octet
f1.3	Forward Fundamental Rate	1	octet
f1.4	Reverse Fundamental Rate	1	octet
f1.5	Service Option	2	octet
f1.6	Forward Traffic Type(Primary, Secondary)	1	octet
f1.7	Reverse Traffic Type(Primary, Secondary)	1	octet
f1.8	Fundamental Frame Size (5/20 ms)	1	octet
f1.9	Forward Fundamental RC	1	octet
f1.10	Reverse Fundamental RC	1	octet

19
20

Table 3: Service Configuration Fields

9.2.1 Active Start Airlink Record

Table 4 contains fields present in Active Start airlink records.

21
22

1

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = Active Start	1	octet
c1	R-P Session ID	4	string
e1	User Zone	2	octet
f1	Service Option	2	octet
i4	Airlink Quality of Service (QoS)	4	integer

2

3

Table 4: Service Configuration Fields

9.2.2 Active Stop Airlink Record

4

Table 5 contains fields present in Active Stop airlink records.

5

6

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = Active Stop	1	octet
c1	R-P Session ID	4	string
f6	Release indicator	1	octet
g8	Active Connection Time in Seconds	4	integer

7

8

Table 5: Active Stop Airlink Fields

9.2.3 SDB Airlink Record

9

Table 6 contains fields present in SDB airlink records.

10

11

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = SDB	1	octet
c1	R-P Session ID	4	string
f4	Mobile Originated/Mobile Terminated Indicator	1	octet
g10	SDB Octet Count	4	time

12

13

Table 6: SDB Airlink Fields

9.3 PDSN Usage Data Record (UDR)

14

The Accounting Session ID is a unique accounting ID created by the PDSN that allows start and stop RADIUS records from a single R-P session to be matched. The Multi-Session ID is a unique accounting ID created by the PDSN that allows multiple related R-P sessions to be matched.

15

16

17

18

19

Table 7 contains the complete UDR and the description of each field.

20

21

Item	Parameter	Description
A. Mobile Identifiers		
a1	MSID	
B. User Identifiers		
B1	IP Address	IP address of the mobile station.
B2	Network Access Identifier (NAI)	user@domain construct which identifies the user and home network of the mobile station.
C. Session Identifiers		
C1	Account Session ID	A unique accounting ID ID created by the PDSN that allows stop and start records to be matched in a log file.
C2	Multi-Session ID	A unique accounting ID created by the PDSN that allows multiple related sessions to be matched in a log file.
D. Infrastructure Identifiers		
D1	MIP Home Agent (HA)	IP address or other identifier.

D2	PDSN/FA Address	IP address or other identifier.
D3	Serving PCF	IP address or other identifier.
D4	BS / MSC ID	IP address or other identifier.
D5	R-P Session ID	The R-P session ID is the R-P tunnel identifier for a particular mobile station and PDSN.
E. Zone Identifiers		
E1	User Zone	Tiered Services user zone.
F. Session Status		
F1	Forward Mux Option	
F2	Reverse Mux Option	
F3	Forward Fundamental Rate	
F4	Reverse Fundamental Rate	
F5	Service Option	
F6	Forward Traffic Type	Primary, Secondary
F7	Reverse Traffic Type(Primary, Secondary)	
F8	Fundamental Frame Size	5/20 ms
F9	Forward Fundamental RC	
F10	Reverse Fundamental RC	
F11	IP Technology	Simple IP, Mobile IP, other.
F12	Compulsory Tunnel Indicator	Indicator of invocation and count of compulsory tunnels established on behalf of MS for providing private network and/or ISP access during a single packet data connection.
F13	Release Indicator	Specifies reason for sending a stop record.
G. Session Activity		
G1	Data Octet Count (Terminating)	total # of octets sent to the user.
G2	Data Octet Count (Originating)	total # of octets sent by the user.
G3	Dropped Octet Count	total # of octets dropped by PDSN due to uncorrectable errors.
G4	Session Start Date	Indicates start of session.
G5	Session Start Time	Indicates start of session.
G6	Session Stop Date	Indicates end of session.
G7	Session Stop Time	Indicates end of session.
G8	Active Time	total active connection time on traffic channel in seconds.
G9	Number of Active Transitions	total # of non-active to Active transitions by the user.
G10	SDB Octet Count (Terminating)	total # of octets sent to the user via Short Data Bursts.
G11	SDB Octet Count (Originating)	total # of octets sent by the user via Short Data Bursts.
G12	Number of SDBs (Terminating)	total # of Short Data Burst transactions.
G13	Number of SDBs (Originating)	total # of Short Data Burst transactions.
H. Special Billing Instructions		
H1	Alternate Billing Identifier	IP address or other identifier of alternate entity for which data session usage may be billed.
I. Quality of Service		
I1	IP Quality of Service (QoS)	When guaranteed service is utilized in a packet data session, different rating schemes may be applied for that usage.
I2	Interconnection IP Network Provider ID	Identifies IP network which connects wireless carrier network to destination.

13	Interconnecting IP Network Service Quality of Service	Identifies QoS offered by IP network which connects wireless carrier network to destination.
14	Airlink Quality of Service (QoS)	Identifies airlink QoS

1
2

Table 7: Complete UDR

3 **9.4 Accounting Formats**

4 The RADIUS server will support RADIUS attribute formats as defined in RFC 2138 and RFC
5 2139. RN parameters transmitted across the R-P interface shall follow the RADIUS format.
6 Table 8 lists each accounting parameter and its associated RADIUS attribute.

7
8 Note: Attributes are of type "26" defined in RFC 2138 and RFC 2139 are vendor specific, and
9 are used to transport CDMA radio specific parameters.

1
2
3
4
5
6
7
8

RADIUS Attribute Definitions						
Item	Parameter	Type	Maximum Payload Length	Format	Field	Special Values
A. Mobile Identifiers						
A1	MSID	31	15	string	Calling_ID	
B. User Identifiers						
B1	IP Address	8	4	ip-addr	Framed IP Address	
B2	Network Access Identifier (NAI)	1	64	string	User-Name	
C. Session Identifiers						
C1	Account Session ID	44	4	string	Acct_Session_Id	
C2	Multi-Session ID	50	4	string	Acct_Multi_Session_Id	
D. Infrastructure Identifiers						
D1	MIP Home Agent (HA)	26/7	4	ip-addr	CDG_HA_IP_Addr	
D2	PDSN/FA Address	4	4	ip-addr	NAS Address	
D3	Serving PCF	26/9	4	ip-addr	CDG_PCF_IP_Addr	
D4	BS / MSC ID	26/10	6	octet	CDG_BS / MSC Addr	SID+ NID+ BSC ID
D5	R-P Session ID	?	?	?	?	?
E. Zone Identifiers						
E1	User Zone	26/11	2	octet	CDG_User_ID	
F. Session Status						
F1	Forward Mux Option	26/12	1	octet	CDG_FMUX	
F2	Reverse Mux Option	26/13	1	octet	CDG_RMUX	
F3	Forward Fundamental Rate	26/14	1	octet	CDG_FRATE	
F4	Reverse Fundamental Rate	26/15	2	octet	CDG_RRATE	
F5	Service Option	26/16	1	octet	CDG_SO	
F6	Forward Traffic Type	26/17	1	octet	CDG_FTYPE	
F7	Reverse Traffic Type(Primary, Secondary)	26/18	1	octet	CDG_RTYPE	
F8	Fundamental Frame Size	26/19	1	octet	CDG_FSIZE	
F9	Forward Fundamental RC	26/20	1	octet	CDG_FRC	
F10	Reverse Fundamental RC	26/21	1	octet	CDG_RRC	
F2	IP Technology	26/22	1	octet	CDG_IP_Tech	1=Simple IP, 2=Mobile IP
F3	Compulsory Tunnel Indicator	26/23	1	octet	CDG_Comp_Flag	0=no tunnel, 1=MIP IPSec

F6	Release Indicator	26/24	1	octet	CDG_Reason_Ind	Reasons for stop record: 0=unknown, 1=MS release, 2=PDSN release, 3=PPP/Service timeout 4=Handoff 5=PPP protocol failure 6=Unknown failure 7=Time of day timer 8=RN Failure
----	-------------------	-------	---	-------	----------------	--

1 **G. Session Activity**

G1	Data Octet Count (Terminating)	42	4	integer	Acct_Input_Octets	
G2	Data Octet Count (Originating)	43	4	integer	Acct_Output_Octets	
G3	Dropped Octet Count	26/25	4	integer	CDG_Dropped_Octets	
G4	Connection Start Date	26/26	4	time	CDG_Start_Date	
G5	Connection Start Time	26/27	4	time	CDG_Start_Time	
G6	Connection Stop Date	26/28	4	time	CDG_Stop_Date	
G7	Connection Stop Time	26/29	4	time	CDG_Stop_Time	
G8	Active Time	46	4	integer	Acct_Session_Time	
G9	Number of Active Transitions	26/30	4	integer	CDG_Num_Active	
G10	SDB Octet Count (Terminating)	26/31	4	integer	CDG_SDB_Input_Octets	
G11	SDB Octet Count (Originating)	26/32	4	integer	CDG_SDB_Output_Octets	
G12	Number of SDBs (Terminating)	26/33	4	integer	CDG_NumSDB_Input	
G13	Number of SDBs (Originating)	26/34	4	integer	CDG_NumSDB_Output	

2 **H. Special Billing Instructions**

H1	Alternate Billing Identifier	26/235	4	integer	CDG_Alt_Billing	
----	------------------------------	--------	---	---------	-----------------	--

3 **I. Quality of Service**

I1	IP Quality of Service (QOS)	26/36	4	integer	CDG_IP_QOS	currently undefined
I2	Interconnection IP Network Provider ID	26/237	4	ip-addr	CDG_Interconnect_IP	
I3	Interconnecting IP Network Service Quality of Service	26/38	4	integer	CDG_Interconnect_QOS	currently undefined
I4	Airlink Quality of Service (QOS)	26/339	4	integer	CDG_Air_QOS	16 levels of priority

4
5 **Table 8: Accounting Parameter Attribute RADIUS Definitions**

1 **9.5 PDSN Procedures**

2 There are several kinds of events that cause the PDSN to take some action:

- 3
- 4 1. R-P session establishment.
- 5 2. R-P session release.
- 6 3. Data service establishment on the PDSN. This includes a PPP instance and IP service
- 7 (Simple IP, Mobile IP, etc.).
- 8 4. Data service termination on the PDSN. This includes releasing the PPP instance.
- 9 5. Arrival of forward direction or reverse direction user data.
- 10 6. Reception of Active Start airlink record.
- 11 7. Reception of Active Stop airlink record.
- 12 8. Reception of SDB airlink record.
- 13 9. Interim timer expiry.
- 14 10. Time of day timer expiry.

15
16 A UDR is associated with an R-P session and an IP address within a PPP session.). The
17 Accounting Session ID (C1) corresponds to a single R-P session and an IP address within a
18 PPP session. The Multi-Session ID (field C2) corresponds to an IP address within a PPP
19 session.

20
21 Note that one R-P session ID may be associated with multiple simultaneous IP addresses in
22 the PDSN. In this case, a different UDR is created for each IP address. Each of these UDRs
23 contain different Accounting Session and Multi-Session IDs, but all contain the same R-P
24 session ID. Another possibility is that several R-P sessions are established during the life of
25 an IP address within a PPP session due to RN handoff or other reasons. In that case, a
26 sequence of UDRs is created with different Accounting Session IDs, but the same Multi-
27 Session ID.

28
29 Airlink records are only associated with an R-P session. The PDSN matches the R-P session
30 ID in the airlink record to the R-P session ID in the appropriate UDR(s). If more than one UDR
31 matches, the actions are applied to all UDRs.

32
33 The subsequent sections specify the actions to take for each event.

34 **9.5.1 R-P session Establishment**

35 If the R-P session is established as a result of a handoff, then the PDSN shall:

- 36
- 37 ▪ Use the previous R-P session ID (before handoff) to find the correct UDR.
- 38 ▪ Use information received from the RN to fill the following fields: A1, D4, D5.
- 39 ▪ Send a RADIUS Accounting-Request Start record.
- 40

41 Otherwise, the PDSN shall use information it receives from the RN to fill the following fields of
42 the new UDR(s):

- 43
- 44 ▪ A1, D3, D4, and D5
- 45

46 The PDSN will populate the remaining fields of the UDR at a later point in time.

47 **9.5.2 R-P session Release**

48 If the R-P session is released as the result of a handoff, then the PDSN shall:

- 49
- 50 ▪ Send a RADIUS Accounting-Request stop record based on the current UDR.

51 **9.5.3 Packet Data Service Establishment**

52 After the PDSN establishes packet data service (i.e., Simple IP or Mobile IP service), to the
53 mobile station the PDSN shall:

- 1
2 ▪ Fill the following fields: B1, B2, C1, C2, D1, D2, F11, F12, H1, I1, I2, and I3.
3 ▪ Send a RADIUS Accounting-Request Start record based on the current UDR.

4 **9.5.4 Packet Data Service Termination**

5 After the PDSN terminates data service to the mobile station the PDSN shall:

- 6
7 ▪ Send a RADIUS Accounting-Request Stop record based on the current UDR.
8 ▪ Delete the UDR after receiving acknowledgment from the RADIUS server that it has
9 successfully received the UDR

10 **9.5.5 User Data Through PDSN**

11 For any user data processed by the PDSN in the forward direction, the PDSN shall:

- 12 ▪ Increment G1 by the number of octets of data.

15 For any user data processed by the PDSN in the reverse direction, the PDSN shall:

- 16 ▪ Increment G2 by the number of octets of data.

18 **9.5.6 Active Start Airlink Record Arrives**

19 When the PDSN receives an Active Start airlink record from the RN, the PDSN performs the
20 following.

21 If the UDR is new (some fields are blank), the PDSN shall:

- 22 • Set UDR fields according to airlink record: $E1 \leftarrow e1$, $F1-F10 \leftarrow f1.1-f1.10$, $I4 \leftarrow i4$

26 Otherwise, if airlink record indicates parameters E1, F1, or I4 have changed, the PDSN shall:

- 27 • Send a RADIUS Accounting-Request Stop record based on current UDR.
28 • Set UDR fields according to airlink record. $E1 \leftarrow e1$, $F1-F10 \leftarrow f1.1-f1.10$, $I4 \leftarrow i4$,
29 and zero fields G1-G13
30 • Send a RADIUS Accounting-Request Start record based on UDR.
31 • The PDSN shall increment G9 by one.

33 **9.5.7 Active Stop Airlink Record Arrives**

34 When the PDSN receives an Active Stop airlink record from the RN, the PDSN shall:

- 35 ▪ Increment G8 by the value of g8.

37 **9.5.8 SDB Airlink Record Arrives**

38 When the PDSN receives an SDB airlink record from the RN, the PDSN performs the
39 following.

40 If f4 indicates a mobile terminated SDB, the PDSN shall:

- 41 ▪ Increment G10 by the value of g10.
42 ▪ Increment G12 by one.

46 Otherwise, if f4 indicates a mobile originated SDB, the PDSN shall:

- 47 ▪ Increment G11 by the value of g10.
48 ▪ Increment G13 by one.

1 **9.5.9 Interim Timer Expires**

2 When the accounting interim timer expires, the PDSN shall:

3

- 4 ▪ Send a RADIUS Accounting-Request Interim record based on current UDR(s).

5 **9.5.9.1 Time of Day Timer Expires**

6 The time of day timer(s) shall be a set of operator configurable timers for a certain time of day.
7 These timers may be used, for example, to delineate peak and off-peak billing hour
8 boundaries.

9

10 When an accounting time of day timer expires, the PDSN shall:

11

- 12 ▪ Send a RADIUS Accounting-Request Stop record based on current UDR.
13 ▪ Zero fields G1-13.
14 ▪ Send a RADIUS Accounting-Request Start record based on current UDR.

1 **10 R-P Interface**

2 The PDSN and RN will support the R-P interface defined as A10 and A11 interfaces of 3G-
3 IOS V4.0.0.

11 Radio Network Requirements

The PDSN interfaces to the Radio Network only through the R-P interface and there are no RN dependent signaling messages transmitted to the PDSN. However, there are some general requirements placed on the RN:

- Each RN will be connected to at least one PDSNs.
- The RN will relay PPP frames between the MS and PDSN.
- The RN will establish an R-P session for each MS initiating a packet data session.
- The RN will manage radio resources to exchange user data with mobile stations.
- The RN will buffer user data from the PDSN when radio resources are not in place or insufficient to support the flow of data.

11.1 R-P General Handoff Requirements

These requirements cover the duration of a packet data session and include periods when the RN does not allocate radio resources to the MS (if such a dormant/standby capability is supported by the RN).

- The RN shall have the capability to determine when an MS enters its coverage area.
- The RN shall be able to determine with which PDSN an MS currently has a PPP session, if a PPP session already exists.
- During a packet data session, an MS may move outside the coverage area on an RN into the coverage area of another RN. If the old and new RN have connectivity to the same PDSN, the RNs shall move the R-P session so that it connects the new RN serving the MS and the PDSN in such a way that the MS maintains connectivity to the data network throughout the packet data session.
- During a packet data session, an MS may move outside the coverage area on an RN into the coverage area of another RN. If the old and new RN do not have connectivity to the same PDSN, the new RN shall immediately establish a new R-P session to a new PDSN so that the MS maintains connectivity to the data network throughout the packet data session.
- Specific handoff procedures for the R-P are not called out in this standard but can be found in 3G-IOS V4.0.0.
- The RN will pass octets between the mobile station and PCF without any framing conversion. The PCF will pass octets between the RN and the PDSN without any framing conversion.

1 **12 Air Interface**

2 The mobile station and RN will support the air interface as specified in:

3

4

5

6

7

8

9

10

11

- IS-2000-1 Introduction to cdma2000 Standards for Spread Spectrum Systems
- IS-2000-2 Physical Layer Standard for cdma2000 Spread Spectrum Systems
- IS-2000-3 Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems
- IS-2000-4 Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems
- IS-2000-5 Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems

1 **Annex A: IKE/ISAKMP Payloads**

2 Interoperability between HA and PDSN/FA implementations is a major goal of this Standard.
3 This Annex addresses ISAKMP payloads in which multiple options exist. The following
4 requirements must be met by the PDSN and HA, assuming IP security between the HA and
5 PDSN/FA is required. Payloads in which no options exist do not appear in this Annex.
6

7 Note: If the HA (home network) does not require any security then Annex A does not apply
8 nor does it apply to Mobile IP for collocated COA.
9

10 **ISAKMP Fixed Header**

11
12 The PDSN in this standard shall use a Major and Minor Version of 0. The HA shall
13 minimally accept Major and Minor Version of 0. This Standard does not make use of
14 the Fixed Header Authentication (A) bit. Subsequent revisions of this Standard will
15 allow for other ISAKMP Major and Minor Versions to accommodate advances in
16 ISAKMP and IKE standards.
17

18 The ISAKMP Fixed Header may indicate an Aggressive Mode exchange for the
19 Phase 1 ISAKMP, a Quick Mode for all Phase 2 exchanges, or an Informational
20 exchange to pass notification regarding security life times.
21

22 **Security Association Payload:**

23
24 All Security Association Payloads will use the IPsec DOI. The Phase 1 ISAKMP
25 Security Payload will specify a situation of SIT_IDENTITY_ONLY. Phase 2 ISAKMP
26 Security Payloads will specify situations of SIT_IDENTITY_ONLY for all cases where
27 privacy or only authentication applies (as outlined in the PDSN and HA "IP Security"
28 sections of the Standard).
29

30 **Proposal Payload:**

31
32 Because the mobile station first makes contact with the PDSN, the PDSN shall be the
33 Initiator of the Phase 1 ISAKMP SA. The HA shall be the Responder. The PDSN
34 shall propose IPsec ESP to the HA for the Phase 1 ISAKMP SA. Carrier owned HAs
35 will support IPsec ESP for the ISAKMP SA. Non carrier owned HA security policies
36 are outside the scope of this Standard, but may reasonably be expected to support
37 the same Proposal.
38

39 For Phase 2 Quick Mode exchanges, both the PDSN and HA will be Initiators and
40 Responders because symmetrical, bi-directional security between PDSN and HA will
41 be required. The PDSN and HA shall propose either IPsec AH for message
42 authentication, or IPsec ESP for message privacy.
43

44 Mobile IP registration control packets and IP in IP tunneled packets may be protected
45 by IPsec AH or ESP. Security policies to be used between PDSN and HA in this
46 Standard will be dictated by the home network not the access provider network. The
47 PDSN shall propose two proposals, IPsec ESP and AH, and the HA will chose one.
48 Carrier owned HAs shall propose only one Proposal, and the PDSN shall accept this
49 proposal. Non carrier owned HAs should be expected to propose only one proposal,
50 and the PDSN shall assume IPsec AH if both are proposed by a non carrier owned
51 HA.
52

53 The Home RADIUS may deliver a User Profile to the Foreign RADIUS and PDSN that
54 indicates whether security should be supported for IP in IP packets. If the Home
55 RADIUS indicates a request for no security on the IP in IP tunneled packets, the
56 PDSN shall delete any SAs used to protect the IP in IP user traffic.

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
46
47
48
49
50
51
52
53
54
55
56
57
58

The SPI shall be four octets.

Transform Payload:

The PDSN shall minimally support the ESP_3DESttransform for IPsec ESP, and the both HMAC-MD5 and HMAC-SHA transforms for IPsec AH. Carrier HAs shall likewise support these two transforms. The PDSN may optionally support and propose other transforms. An HA shall select one of the transforms offered by the PDSN. The PDSN should limit the number of transform proposals it makes to the HA.

The PDSN and HA IP security negotiations should complete within three messages for an Aggressive exchange and two messages for the Quick Mode exchange.

Key Exchange Payload

The Key Exchange Payload from the PDSN to the HA shall specify the Phase 1 Revised Mode of Public Encryption mechanism RFC 2408 when a pre-shared key is not available. The PDSN shall use public keys from the peer's Certificate. When a pre-shared key is available, the PDSN shall specify Phase 1 Authenticated With a Pre-Shared Key mode of operation.

The PDSN shall not use the (optional) Key Exchange Payload in a Phase 2 Quick Mode security association establishment.

Identification Payload

For IPsec security of the Mobile IP registration packets, the PDSN shall identify a protocol type of UDP, port 434, and the destination IP address of the HA, respectively. For IPsec security of the Mobile IP registration packets, the HA shall identify a protocol type of UDP, port 434, and the destination IP address of the PDSN, respectively.

The PDSN shall identify a tunnel protocol type that matches the encapsulation type requested by the mobile station's RRQ, and the destination IP address of the HA, respectively. The HA shall identify a protocol type matches the encapsulation type requested by the mobile station's RRQ, and the destination IP address of the PDSN, respectively.

Certificate Payload

The Certificate Payload shall carry X.509 version 3 certificates.

Signature Payload

The PDSN and HA shall not include this payload.

Notification Payload

The Notification Payload carries error messages and reason codes regarding failure for a peer to be able to establish a security association. The PDSN and HA handling of a failed security association establishment is specified in the main body of the Standard.

The PDSN and HA shall use the "SA Lifetime Notify" code as a trigger to refresh the indicated security association.

Delete Payload

1
2
3

The PDSN shall send a delete payload if Mobile IP registration fails (for example a refresh, or if a user authorization fails, or upon request from a carrier administrator).

1 **Annex B: Certificates**

2 PDSNs and HAs shall use X.509 Version 3 certificates in conformance with RFC 2459. Each
3 PDSN and HA in a carrier network shall have a unique certificate which will be configured into
4 the PDSN and HA. The method of configuration is outside the scope of this standard.

5
6 Note: This Annex only applies to FA COA. Security between a collocated COA mobile station
7 and the HA is outside the scope of this standard.

8
9 Each carrier shall be a Certificate Authority for itself and its client private networks and partner
10 ISPs for PDSNs and HAs that may be accessed by PDSNs. All PDSNs and HAs shall be
11 configured with all carrier CA certificates. There should be one CA certificate from each
12 carrier.

13
14 **Certificates for PDSNs and HAs**

15
16 The Distinguished Name contained in the Issuer field is of form:

17
18 `cdma2000.carrier-name`

19
20 The HA or PDSN determines the issuing carrier (i.e., the CA) from the *carrier-name* attribute of
21 the Issuer's Distinguished Name. The HA and PDSN then use the *carrier-name* attribute to
22 locally access the CA's public key.

23
24 The PDSN and HA shall use the SHA-1 as a hash function and either the RSA or DSA
25 signing algorithm, as specified in RFC 2549 to sign a certificate. The private network or ISP
26 shall provide the public key and Distinguished Name of the certificate.

27
28 The Distinguished Name contained in the Subject field is of form:

29
30 `cdma2000.carrier-name.PDSN.carrier-identifier`
31 `cdma2000.carrier-name.HA.carrier-identifier`

32
33 Certificates in the PDSN and HA will not use the Unique-Identifier field.

34
35 Certificate extensions for PDSN and HA certificates shall not be supported.

36
37 The method of providing PDSNs and HAs signed certificates to PDSNs and HAs is outside
38 the scope of this standard.

39
40 **CA Certificates**

41
42 Carrier certificates shall be configured into all PDSNs and HAs. A carrier CA contains the
43 public key that the PDSN or HA shall use to verify the signature of a certificate received in a
44 Phase 1 ISAKMP exchange.

45
46 A CA certificate shall conform to the X.509 V3 certificates in RFC 2459. Since the carrier CA
47 distributes its own certificate, the Authority Key Identifier and Subject Key Identifier
48 extensions shall not be included in the certificate.

49
50 The method by which carriers exchange their CA certificates, as well as of providing
51 certificates into PDSNs and HAs, is outside the scope of this standard.

52
53 **Certificate Revocation List (CRL)**

54

1 CRLs shall be used to store the identities of certificates which have been compromised or are
2 otherwise invalid. CRLs shall conform to X.509 v2 as specified in RFC 2459. A future version
3 of this standard will make use of the Online Certificate Status Protocol.
4

5 Carriers shall exchange revoked certificate information (e.g., serial number). The frequency of
6 the exchange is outside the scope of this standard. Each carrier will then create and sign an
7 "aggregate CRL", and configure this aggregate CRL into the PDSNs. The HAs will only
8 require a CRL that contains revoked carrier certificates; this CRL is expected to be null since
9 carrier CRLs is not expected to be compromised or otherwise invalid.

10

11 Note: Possession of a CRL does not imply service since RADIUS and MIP functions still
12 control the user obtaining service, as well as the HA allowing access to the PDSN.
13

14 CRLs exchanged between carriers to form the aggregate CRL shall conform to X.509 v2 as
15 specified in RFC 2459.
16

17 The CA certificate shall indicate the carrier CA as Issuer of the CRL. The DN of the Issuer
18 shall be of form:
19

20 cdma2000.carrier-name
21

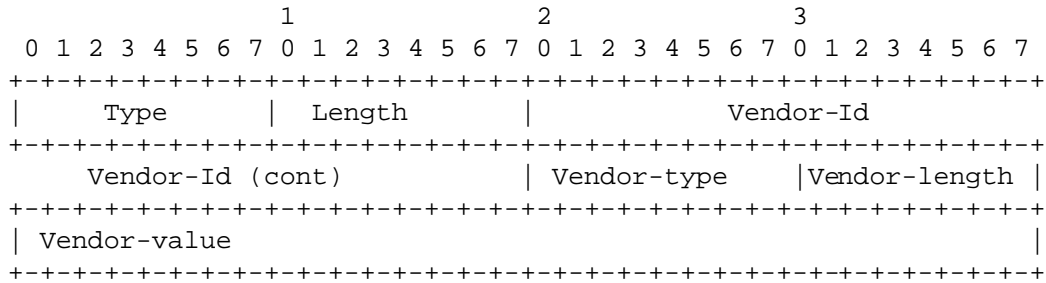
22 CRLs exchanged between carriers, and aggregate CRLs configured into a PDSN or HA shall
23 use the SHA-1 as a hash function and either the RSA and DSA signing algorithm as
24 specified in RFC 2549.
25

26 CRL extensions shall not be supported.
27

28 The method of exchanging CRLs between carriers , or to conveying certificates client private
29 network or partnering ISP, as well providing this information into PDSNs and HAs, is outside
30 the scope of this standard.

1 **Annex C: cdma2000 RADIUS Attributes Annex:**

2 This is the general Vendor Specific Format for all cdma2000 RADIUS attributes. The type,
 3 length and vendor ID are the same for every attribute. The vendor type, vendor length, and
 4 value are specified below.



Type = cdma specific
 Length >= 9

5 **Figure 9: cdma2000 RADIUS Attribute Format**

6
 7
 8 **Type:** 26

9
 10 **Length:** greater than 9

11
 12 **cdma2000 Vendor ID:** 4 octets

13
 14 **Security Status:** Indicates whether a security association exists and whether certificates are
 15 available. This optionally appears in an Access-Request.

16
 17 Vendor Type = 1
 18 Vendor Length = 6
 19 Vendor Value =

- 20
 21 1. IPsec SA already established
 22 2. IPsec SA not established and a certificate exists for the HA
 23 3. IPsec SA not established, no certificate exists for the HA

24
 25 **Security level:** Indicates the type security the home network authorizes and optionally
 26 appears in the Access-Accept.

27
 28 Vendor Type = 2
 29 Vendor Length = 6
 30 Vendor Value =

- 31
 32 1. IPsec for registration messages
 33 2. IPsec for tunnels
 34 3. IPsec for tunnels and registration messages
 35 4. No IPsec security

36
 37 **Pre-shared secret:** A pre-shared secret for IKE which optionally appears in an Access-
 38 Accept

39
 40 Vendor Type = 3

1 Vendor Length = 3 or greater
2 Vendor Value = binary value of the pre-shared key
3
4 **Reverse Tunnel Specification:** Indicates the style of reverse tunneling that is required, and
5 optionally appears in an Access-Accept.
6
7 Vendor Type = 4
8 Vendor Length = 6
9 Vendor Value =
10
11 0 - Reverse tunneling is not required.
12 1 - Reverse tunneling with Direct Delivery style
13 is required. All traffic will be tunneled to the HA.
14 2 - Reverse tunneling with Encapsulated Delivery
15 style is required and Direct Delivery packets should
16 be silently dropped by the FA.
17 3 - Reverse tunneling is required, but Encapsulated
18 Delivery mode may be negotiated. Encapsulated
19 packets will be tunneled to the HA and Direct
20 Delivered packets will be routed directly to the
21 CN.
22 4 - Like (3), but with a private MN address. The FA
23 must use NAT to propagate Direct Delivery packets.
24
25 **Differentiated Services Class Option Attribute:** The Home RADIUS server authorizes
26 differentiated service via the Differentiated Services Class Options Attribute, and optionally
27 appears in an Access-Accept.
28
29 Vendor Type = 5
30 Vendor Length = 6
31 Vendor Value = tbd (The meaning of any specific values is outside the scope of this
32 Standard).
33
34 There is no intention to convey the actual parameters of the differentiated services service
35 required.
36
37 **R-P Link Id:** Contains the R-P Link Id received in the airlink records and must appear in an
38 Accounting-Request.
39
40 Vendor Type = 6
41 Vendor Length = 3 or more
42 Vendor Value = The R-P link ID that is returned on the R-P interface from the PDSN.
43