

1
2
3
4
5

3GPP2 P.S0001-A
Version 1.0
Version Date: July 14, 2000



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

6
7

Wireless IP Network 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 **1 INTRODUCTION..... 5**

6 **2 GLOSSARY AND DEFINITIONS 6**

7 2.1 ACRONYMS 6

8 2.2 DEFINITIONS..... 8

9 **3 REFERENCES.....10**

10 3.1 MOBILE IP.....10

11 3.2 PPP.....10

12 3.3 DIFFERENTIATED SERVICES10

13 3.4 RADIUS11

14 3.5 IP SECURITY.....11

15 3.6 IETF OTHER.....11

16 3.7 TIA11

17 3.8 ITU-T.....12

18 **4 PROTOCOL REFERENCE MODEL13**

19 4.1 SIMPLE IP13

20 4.2 MOBILE IP.....13

21 4.3 RADIUS14

22 4.4 NETWORK REFERENCE MODELS15

23 **5 SIMPLE IP OPERATION18**

24 5.1 COMMON SERVICE SPECIFICATION.....18

25 5.1.1 *PPP Session*18

26 5.2 PDSN REQUIREMENTS18

27 5.2.1 *PPP Session*18

28 5.2.1.1 Establishment18

29 5.2.1.2 Termination18

30 5.2.1.3 Authentication.....19

31 5.2.1.4 Addressing with IPCP19

32 5.2.1.5 Compression19

33 5.2.1.6 PPP Octet synchronous Framing19

34 5.2.1.7 Simultaneous Simple IP and Mobile IP Service19

35 5.2.2 *RADIUS Support*19

36 5.2.2.1 NAI Construction in the Absence of CHAP.....20

37 5.2.3 *Ingress Address Filtering*22

38 5.3 RADIUS SERVER REQUIREMENTS22

39 5.4 MOBILE STATION REQUIREMENTS.....23

40 5.4.1 *PPP Session*23

41 5.4.1.1 Establishment.....23

42 5.4.1.2 Termination23

43 5.4.1.3 Authentication.....23

44 5.4.1.4 Addressing with IPCP23

45 5.4.1.5 Compression23

46 5.4.1.6 PPP Framing.....24

47 **6 MOBILE IP OPERATION.....25**

48 6.1 COMMON SERVICE SPECIFICATION.....25

49 6.1.1 *PPP Session*25

50 6.1.2 *Mobile IP*25

1	6.2	PDSN REQUIREMENTS	25
2	6.2.1	<i>PPP Session</i>	25
3	6.2.1.1	Establishment	25
4	6.2.1.2	Termination	25
5	6.2.1.3	Addressing with IPCP	26
6	6.2.1.4	Authentication	26
7	6.2.1.5	Compression	26
8	6.2.1.6	PPP Octet Synchronous Framing.....	26
9	6.2.2	<i>MIP Registration</i>	26
10	6.2.2.1	Agent Advertisements	26
11	6.2.2.2	Addressing and Mobile IP	27
12	6.2.2.3	MIP Extensions	27
13	6.2.2.4	Private Network Support	27
14	6.2.2.5	Reverse Tunneling	27
15	6.2.3	<i>RADIUS Support</i>	28
16	6.2.4	<i>IP Security Support</i>	28
17	6.2.5	<i>Ingress Address Filtering</i>	30
18	6.3	HOME AGENT REQUIREMENTS.....	30
19	6.3.1	<i>Multiple Registrations</i>	30
20	6.3.2	<i>IP Security Support</i>	30
21	6.3.3	<i>Dynamic Home Address Assignment</i>	31
22	6.3.4	<i>Authentication</i>	31
23	6.4	RADIUS SERVER REQUIREMENTS	31
24	6.5	MOBILE STATION REQUIREMENTS.....	31
25	6.5.1	<i>PPP Session</i>	31
26	6.5.1.1	Establishment	32
27	6.5.1.2	Termination	32
28	6.5.1.3	Authentication with CHAP	32
29	6.5.1.4	Addressing with IPCP	32
30	6.5.1.5	Compression	32
31	6.5.1.6	PPP Framing	32
32	6.5.2	<i>MIP Registration</i>	32
33	6.5.2.1	Agent Discovery.....	32
34	6.5.2.2	Registration Messages.....	32
35	6.5.2.3	MIP Extensions	33
36	6.5.2.4	Private Network Support	33
37	7	MOBILITY MANAGEMENT	34
38	7.1	MOBILITY WITHIN RADIO NETWORK.....	34
39	7.2	PCF TO PCF HANDOFF	34
40	7.3	PDSN TO PDSN HANDOFF.....	34
41	8	QUALITY OF SERVICE (QOS)	36
42	8.1	DIFFERENTIATED SERVICES SPECIFICATION	36
43	8.2	PDSN REQUIREMENTS FOR DIFFERENTIATED SERVICES.....	36
44	8.2.1	<i>Service Specification</i>	36
45	8.2.2	<i>3GPP2 Differentiated Service Class Option</i>	37
46	8.3	RN REQUIREMENTS FOR DIFFERENTIATED SERVICE	37
47	8.4	MOBILE STATION REQUIREMENTS FOR DIFFERENTIATED SERVICE	37
48	9	ACCOUNTING	38
49	9.1	GENERAL.....	38
50	9.2	AIRLINK RECORDS	38
51	9.2.1	<i>R-P Session Setup Airlink Record</i>	39
52	9.2.2	<i>Active Start Airlink Record</i>	39
53	9.2.3	<i>Active Stop Airlink Record</i>	40
54	9.2.4	<i>SDB Airlink Record</i>	40

1	9.3	PDSN USAGE DATA RECORD (UDR)	40
2	9.4	ACCOUNTING FORMATS.....	42
3	9.5	PDSN PROCEDURES.....	46
4	9.5.1	<i>R-P Session Setup Airlink Record Arrives</i>	46
5	9.5.2	<i>Packet Data Service Establishment</i>	47
6	9.5.3	<i>Packet Data Service Termination</i>	47
7	9.5.4	<i>User Data Through PDSN</i>	47
8	9.5.5	<i>Active Start Airlink Record Arrives</i>	47
9	9.5.6	<i>Active Stop Airlink Record Arrives</i>	48
10	9.5.7	<i>SDB Airlink Record Arrives</i>	48
11	9.5.8	<i>Interim Record Trigger</i>	48
12	9.5.9	<i>Stop Record Trigger</i>	48
13	9.5.10	<i>Time of Day Timer Expires</i>	48
14	10	R-P INTERFACE	50
15	11	RADIO NETWORK REQUIREMENTS.....	51
16	11.1	R-P GENERAL HANDOFF REQUIREMENTS.....	51
17	12	AIR INTERFACE	52
18		ANNEX A: IKE/ISAKMP PAYLOADS	53
19		ANNEX B: CERTIFICATES	56
20		ANNEX C: RADIUS ATTRIBUTES ANNEX:.....	58

21

Figures

22

23			
24	Figure 1:	Protocol Reference Model for Simple IP	13
25	Figure 2:	Protocol Reference Model for Mobile IP Control and IKE.....	14
26	Figure 3:	Protocol Reference Model for Mobile IP User Data.....	14
27	Figure 4:	RADIUS Protocol Reference Model	15
28	Figure 5:	Reference Model for Access with Mobile IP	16
29	Figure 6:	Reference Model for Access with Simple IP.....	17
30	Figure 7:	The MSID Formats	22
31	Figure 8:	Accounting Architecture.....	38
32	Figure 9:	3GPP2 RADIUS Attribute Format	58

33

Tables

34

35			
36	Table 1:	R-P Session Setup Airlink Fields.....	39
37	Table 2:	Active Start Airlink Fields.....	40
38	Table 3:	Active Stop Airlink Fields.....	40
39	Table 4:	SDB Airlink Fields.....	40
40	Table 5:	Complete UDR	42
41	Table 6:	Accounting Parameter Attribute RADIUS Definitions	45

42

43

1 **1 Introduction**

2 This specification defines requirements for support of wireless packet data networking capability
3 on a third generation wireless system based on cdma2000. This specification is based on
4 P.R0001: Wireless IP Network Architecture based on IETF protocols.

5

6 This specification 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 and
10 hence the speed to market. References to the required IETF protocols are provided in Section 3
11 of this specification.

12

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

23

1 2 Glossary and Definitions

2 2.1 Acronyms

3		
4	AAA	Authentication, Authorization, and Accounting
5	ACCM	Asynchronous Control Character Map
6	AH	Authentication Header
7	CA	Certificate Authority
8	CCP	Compression Control Protocol
9	CHAP	Challenge Handshake Authentication Protocol
10	COA	Care-of-Address
11	CRL	Certificate Revocation List
12	DSA	Digital Signature Algorithm
13	DOI	Domain of Interpretation
14	ESP	Encapsulating Security Payload
15	FA	Foreign Agent
16	FAC	Foreign Agent Challenge
17	HA	Home Agent
18	HLR	Home Location Register
19	IANA	Internet Assigned Numbering Authority
20	IETF	Internet Engineering Task Force
21	IKE	Internet Key Exchange
22	IMSI	International Mobile Station Identity
23	IMT-2000	International Mobile Telecommunications - 2000
24	IP	Internet Protocol
25	IPCP	IP Control Protocol
26	IPsec	IP Security
27	IRM	International roaming MIN
28	ISAKMP	Internet Security Association and Key Management Protocol
29	ISP	Internet Service Provider
30	LAC	Link Access Control
31	LCP	Link Control Protocol
32	MAC	Medium Access Control
33	MIN	Mobile Identification Number
34	MIP	Mobile IP
35	MS	Mobile Station
36	MSID	Mobile Station ID
37	NAI	Network Access Identifier
38	PAP	Password Authentication Protocol
39	PCF	Packet Control Function
40	PDSN	Packet Data Serving Node
41	PL	Physical Layer
42	PPP	Point-to-Point Protocol
43	PSI	PCF Session ID
44	QoS	Quality of Service
45	RADIUS	Remote Authentication Dial In User Service
46	RN	Radio Network
47	RRP	Mobile IP Registration Reply
48	RRQ	Mobile IP Registration Request
49	RSA	Rivest-Shamir-Adleman public key algorithm
50	SA	Security Association
51	SHA	Secure Hash Algorithm
52	SPI	Security Parameter Index

- 1 SS7 Signaling System 7
- 2 TCP Transmission Control Protocol
- 3 UDR Usage Data Record
- 4 UDP User Datagram Protocol
- 5 VLR Visitor Location Register
- 6

1 **2.2 Definitions**

2

3 Access Provider Network:

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

5 Broker RADIUS:

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

11 Broker RADIUS Network:

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

13 Home RADIUS:

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

15 Home Access Provider Network:

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

18 Home IP Network:

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

22 IMT-2000 network:

23 An IMT-2000 home/visited network is characterized by its ability to provide IMT-2000
 24 capabilities to its users as identified in the IMT-2000 capability sets (ITU-Q.1701).
 25

26 Packet data service:

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

29 Packet data service option:

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

32 Packet data session:

33 Describes an instance of continuous use of packet data service by the user. A packet
 34 data session begins when the user invokes packet data service. A packet data session
 35 ends when the user or the network terminates packet data service. During a particular
 36 packet data session, the user may change locations but the same IP address is
 37 maintained.
 38

39 For Simple IP service, moving from the coverage area of one PDSN to another PDSN
 40 constitutes a change in packet data session because a new IP address is assigned by
 41 the new PDSN. For Simple IP service, a packet data session and a PPP session are
 42 concurrent. For Mobile IP service, a packet data session can span several PDSNs as
 43 long as the user continuously maintains mobility bindings at the Home Agent and there is
 44 no lapse in Mobile IP registrations/re-registrations (i.e., the IP address is persistent). For
 45 Mobile IP service, the Packet Data session can exist through several changes of the
 46 PPP session.

1 PPP Session:

2 A PPP session describes the time during which a particular PPP connection instance is
3 maintained in the open state in both the mobile station and PDSN. The PPP session is
4 maintained during periods when the mobile station is dormant. If a user hands off from
5 one RN to another RN but is still connected to the same PDSN, the PPP session
6 remains. If a user changes PDSN, a new PPP session is created at the new PDSN.

7 Private Network:

8 A *Home IP Network* that resides behind a firewall and that may use private IP addresses.

9 Radio Network:

10 The RN is equivalent to the BS as defined in the Network Reference Model
11 (TIA/EIA/TSB100), and corresponds to the collection of radio access equipment that
12 includes the functional entities Radio Resource Control (RRC) and Packet Control
13 Function (PCF) as described in P.R0001. At times the terms PCF and RN are used
14 interchangeably in this document when describing handoffs across the R-P interface.
15

16 R-P Interface:

17 The interface between the Radio Network (specifically the PCF) and the PDSN. This
18 interface is also referred to as the A_{quarter} interface and the A10/A11 interface in A.S0001.

19 R-P session:

20 The R-P session is a logical connection established over the R-P interface for a
21 particular PPP session. If a user changes RNs during packet data service, the R-P
22 session is between the previous RN and PDSN is released and a new R-P session is
23 established between the new RN and the same or new PDSN.

24 Service Provider Network:

25 An IMT-2000 network operated by either the home service provider or the visited service
26 provider. The home service provider maintains the customer business relationship with
27 the user. The visited service provider provides IMT-2000 access services through the
28 establishment of a service agreement with a home service provider.

29 Visited Access Provider Network:

30 The IMT-2000 cellular network providing service to the user when he is roaming outside
31 his home access provider network.

32 Visited RADIUS:

33 The RADIUS server that resides in the Visited Access Provider Network.

34

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 SMIv2, 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 2794]. March 2000.

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, RFC 1662, July 1994.
26
27
28
29 Rand, The PPP Compression Control Protocol (CCP), RFC 1962, 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 1996.
36
37 McGregor, The PPP Internet Protocol Control Protocol (IPCP), RFC 1332, May 1992.
38
39 Pall , Microsoft Point-To-Point Compression (MPPC) Protocol, RFC 2118, March 1997.
40
41 Zorn, PPP LCP Internationalization Configuration Option, RFC 2484, January 1999.

42 **3.3 Differentiated Services**

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

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

3 **3.4 RADIUS**

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

5
6 Rigney, Rubens, Simpson, Willens, Remote Authentication Dial In User Service (RADIUS), RFC
7 2138, August 1997.

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

11 **3.5 IP Security**

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

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

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

17 **3.6 IETF Other**

18 Postel, User Datagram Protocol, RFC 768, August 1980

19
20 Internet Protocol, RFC 791, Sept. 1981

21
22 Postel, Internet Control Message Protocol, RFC 792, September 1981

23
24 Transmission Control Protocol, RFC 793, September 1981

25
26 Braden, Requirements for Internet Hosts - Communication Layers, RFC 1122, October 1989

27
28 Address Allocation for Private Internets, RFC 1918, February, 1996

29
30 Jacobson, Compressing TCP/IP Headers for Low Speed Serial Links, RFC 1144, February 1990.

31 **3.7 3GPP2 and TIA**

32 P.R0001, Wireless IP Network Architecture based on IETF Protocols, July 2000.

33
34 A.S0001, Inter-operability Specification (IOS) for CDMA 2000 Access Network Interfaces,
35 December, 1999.

36
37 TIA/EIA/IS-707-A-1.12: cdma2000 High Speed Packet Data Service Option 33, December 1999.

38
39 C.S0001-A: Introduction to cdma2000 Standards for Spread Spectrum Systems, June 2000.

40
41 C.S0002-A: Physical Layer Standard for cdma2000 Spread Spectrum Systems, June 2000.

42
43 C.S0003-A: Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems,
44 June 2000.

45
46 C.S0004-A: Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum
47 Systems, June 2000.

48

1 C.S0005-A: Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems,
2 June 2000.

3

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

5

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

8 **3.8** *ITU-T*

9 ITU-T Recommendation E.212, The International Identification Plan for Mobile Terminals and
10 Mobile Users

11

12

4 Protocol Reference Model

This section will specify the protocol architecture between the entities of the Wireless IP Network architecture. Refer to P.R0001 for a general description of the Wireless IP Network architecture, its components and message flows.

The mobile station may either be a single MTO type device or may consist of a MT2 and a TE2 device. For a MTO type mobile station, the protocols involving the mobile station terminate within the single MTO device as shown in the Figures below. In the case of a MT2 TE2 type mobile station, the protocol termination within the mobile station are as shown in Figures 1 and 2 of IS- 707-A- 2.12.

Although Mobile IP and Simple IP services are represented in different protocol reference models, the network is able to provide both Simple IP and Mobile IP service simultaneously to a mobile station using the same PPP session.

4.1 Simple IP

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

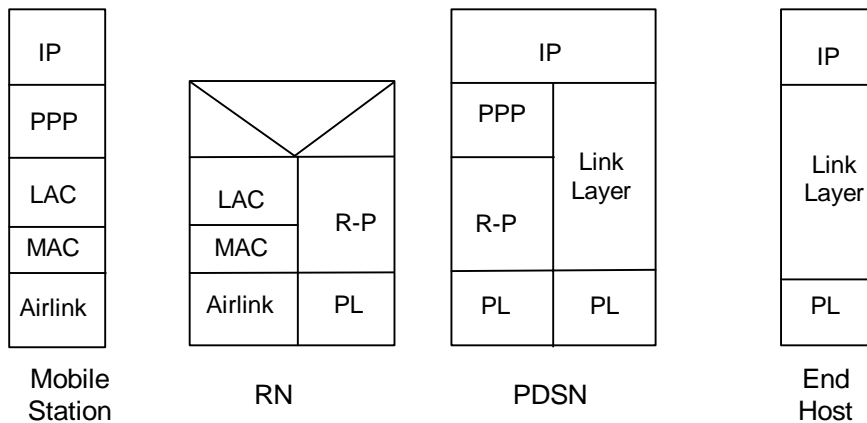
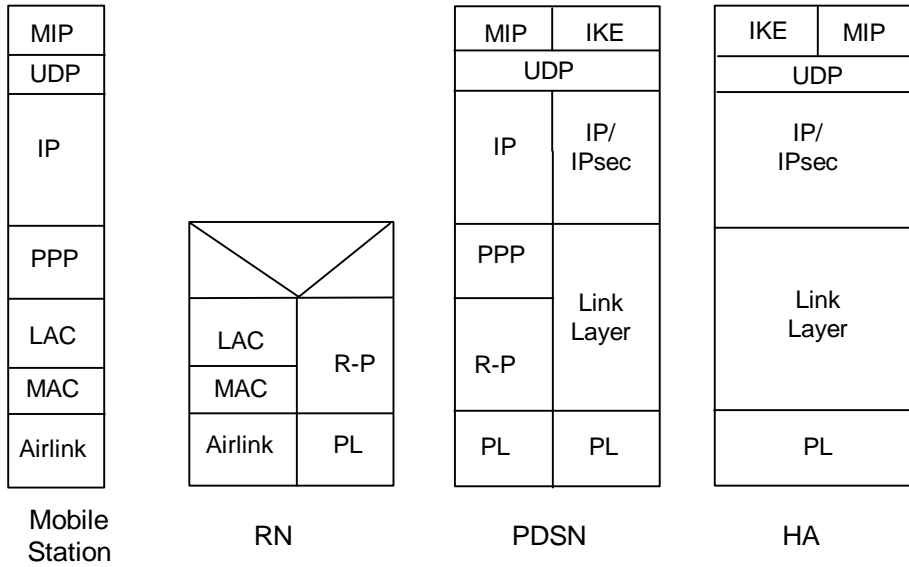


Figure 1: Protocol Reference Model for Simple IP

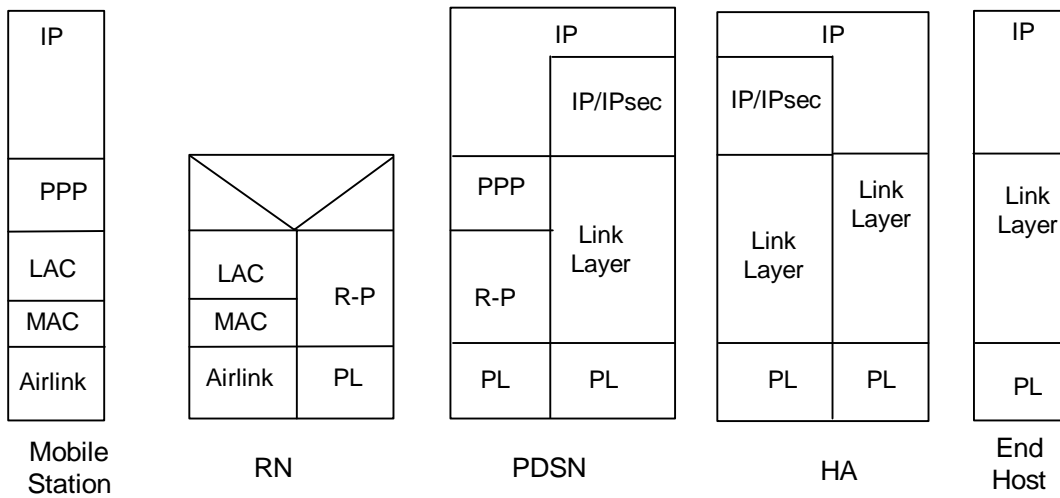
4.2 Mobile IP

Figures 2 and 3 show the protocol reference model for Mobile IP control and data, respectively. IPsec in Figures 2 and 3 will be necessary in some situations and not in other situations, as detailed in Section 6.2.4.



1
2
3
4
5

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



6
7
8

Figure 3: Protocol Reference Model for Mobile IP User Data

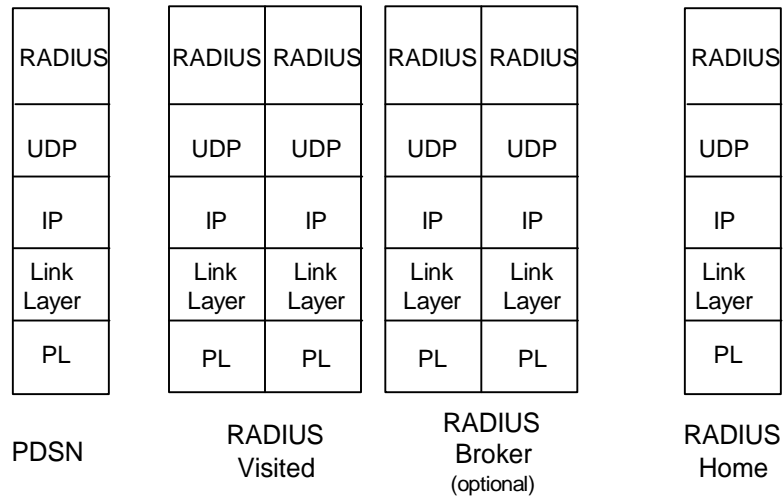
9 **4.3 RADIUS**

10 Figure 4 shows the protocol reference model for RADIUS server to wireless data entity. In the
 11 protocol reference model of Figure 4, the RADIUS servers in the visited access provider and
 12 home IP network communicate via RADIUS proxy servers and one or more RADIUS brokers.

13

14 Note: The broker is optional.

15



1
2
3
4

Figure 4: RADIUS Protocol Reference Model

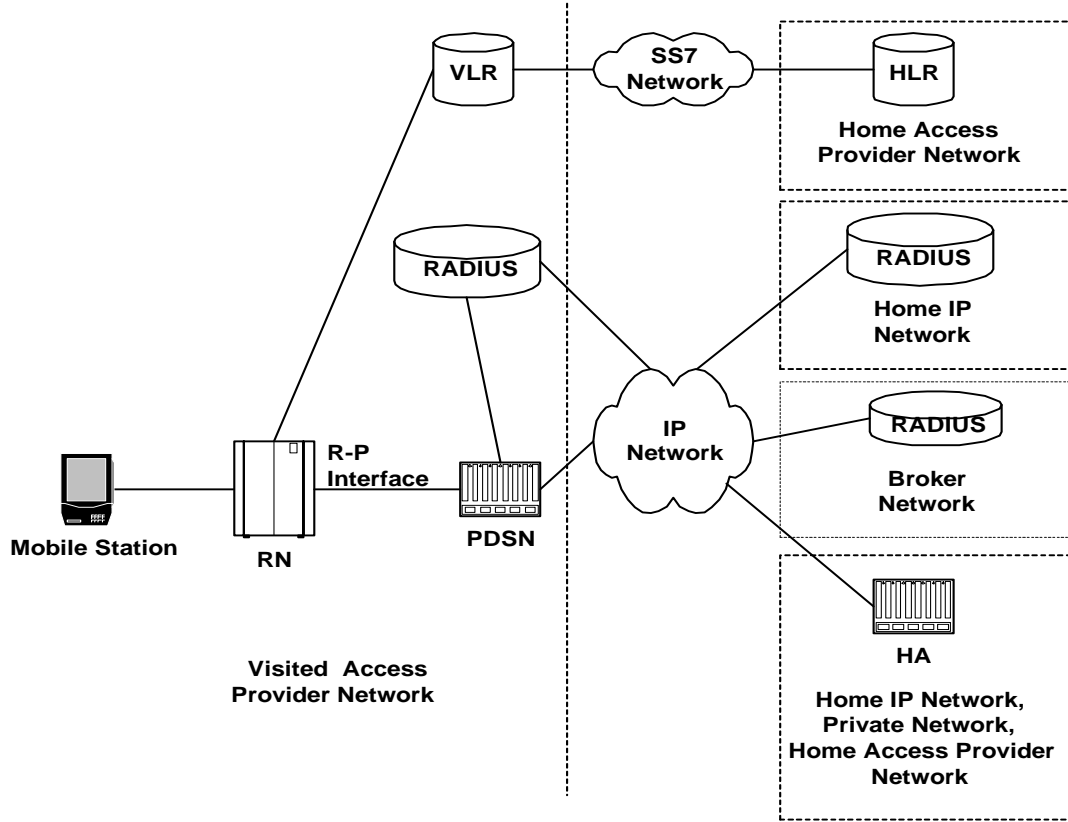
5 **4.4 Network Reference Models**

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

10
11 For the Simple IP Service, the HA will not be required, as shown in Figure 6.

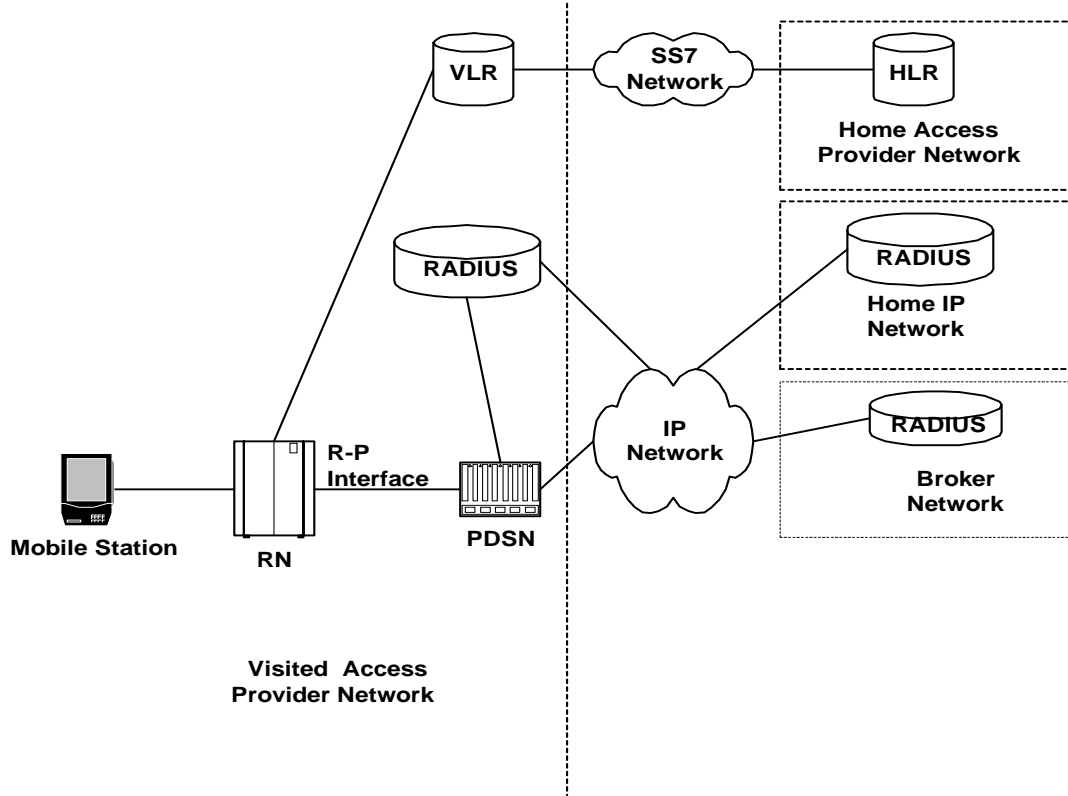
12
13 Note: The IP Network entity in Figures 5 and 6 represent IP Networks that may reside in the
14 public Internet as well as private IP networks within access provider networks and home IP
15 networks.

16



1
2
3
4

Figure 5: Reference Model for Access with Mobile IP



- 1
- 2
- 3
- 4
- 5

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 specification, 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 by a service provider network. The user
5 retains its IP address as long as it is served by a radio network which has connectivity to the
6 address assigning PDSN. There is no IP address mobility beyond this PDSN. Secure access to a
7 home network via Simple IP is beyond the scope of this specification.

8 **5.1 Common Service Specification**

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

11 **5.1.1 PPP Session**

12 PPP shall be the data link protocol between the mobile station and the PDSN. PPP is
13 established prior to any IP datagrams being exchanged between the mobile station and the
14 PDSN.

15
16 PPP shall be supported as defined in the following standards with any limitations or extensions
17 described in this specification:

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

21
22 PPP encryption shall not be negotiated by either the mobile station or PDSN. Only one PPP
23 session shall be supported between the mobile station and the PDSN.

24 **5.2 PDSN Requirements**

25 The PDSN shall support Simple IP operation.

26 **5.2.1 PPP Session**

27 **5.2.1.1 Establishment**

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

32
33 PPP shall support transparency in accordance with section 4.2 of RFC 1662. The PDSN shall
34 attempt to negotiate a control character mapping, with the minimum number of escaped
35 characters by proposing an ACCM of 0x00000000.

36 **5.2.1.2 Termination**

37 The PDSN shall clear the PPP state if there is no established underlying R-P session for the
38 mobile station. The PDSN shall clear the RP-session whenever the PPP session is closed. If
39 the PDSN receives IP packets for a mobile station for which there is no established PPP session
40 for the mobile station, the PDSN shall discard the packet and send an ICMP destination
41 unreachable packet to the source.

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

1
2 The PDSN shall clear the R-P session whenever the PPP Session is closed by the mobile
3 station.

4 **5.2.1.3 Authentication**

5 The PDSN shall support the authentication mechanisms CHAP and PAP. The PDSN shall also
6 support a configuration option to allow a MS to receive Simple IP service without CHAP or PAP.
7 The PDSN shall always propose CHAP as a PPP option in an initial LCP Configure-Request
8 during the PPP establishment.

9
10 If the MS does not support or does not want to use CHAP, but prefers to use PAP, it will send an
11 LCP Configure Nak proposing PAP. The PDSN will accept PAP by sending an LCP Configure-
12 Request with PAP.

13
14 If the MS does not support either CHAP or PAP, it will send an LCP Configure Reject. If the
15 PDSN is configured to allow the MS to receive Simple IP service without CHAP or PAP, the
16 PDSN will adhere to the guidelines in 5.2.2.1.

17 **5.2.1.4 Addressing with IPCP**

18 The PDSN shall assign the mobile station a dynamic IP address for Simple IP service during the
19 IPCP phase of PPP. The IP address may be a private address as per RFC 1918.

20
21 If the MS did not authenticate itself using CHAP or PAP, and the PDSN is not configured to allow
22 the MS to receive Simple IP service without CHAP or PAP, the PDSN shall end the PPP session
23 if the MS sends an IPCP Configure-Request containing the IP Address Configuration Option with
24 value 0.0.0.0.

25 **5.2.1.5 Compression**

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

28
29 The PDSN shall support the following types of PPP compression:

- 30
- 31 • Stac-LZS (RFC 1974);
 - 32 • Microsoft Point-To-Point Compression Protocol (RFC 2118) compression.
 - 33 • Deflate (RFC 2394)

34
35 The PDSN may support other PPP payload compression algorithms.

36 **5.2.1.6 PPP Octet synchronous Framing**

37 The PDSN shall frame PPP packets sent on the PPP link layer using the octet synchronous
38 framing protocol defined in RFC 1662, except that there shall be no inter-frame time fill (see
39 4.4.1 of RFC 1662). That is, no flag octets shall be sent between a flag octet that ends one PPP
40 frame and the flag octet that begins the subsequent PPP frame.

41 **5.2.1.7 Simultaneous Simple IP and Mobile IP Service**

42 This specification allows simultaneous Mobile IP and Simple IP service to the mobile station. If
43 the user desires Simple IP service after previously requesting Mobile IP service, the mobile
44 station must re-negotiate PPP.

45 **5.2.2 RADIUS Support**

46 The PDSN shall act as a RADIUS client in accordance with RFC 2138 and shall communicate
47 user CHAP or PAP authentication information to the local RADIUS server in a RADIUS Access-

1 Request. On receipt of the CHAP or PAP response from the mobile station, the PDSN shall
 2 create an Access-Request containing at a minimum:

- 3
 4 User-Name (1)¹ = NAI
 5 User-password(2) = password (if PAP)
 6 CHAP-Password (3) = CHAP ID and CHAP-response (if CHAP)
 7 NAS-IP-Address (4) = IP address of PDSN
 8 CHAP-Challenge (60)= challenge value issued by PDSN (if CHAP)
 9 Correlation ID (defined in Annex C) = An ID that correlates all accounting sessions
 10 authorized for this NAI by this access request

11
 12 Correlation ID is in addition to those fields specified by RFC 2138.

13
 14 The local RADIUS server will send a RADIUS Access-Accept message to the PDSN. The
 15 RADIUS Access Accept message may contain the Differentiated Service Class Option attribute.
 16 This attribute is defined in Annex C.

17
 18 The PDSN shall act as a RADIUS accounting client in accordance with RFC 2139 and shall
 19 communicate user accounting information to the local RADIUS server in RADIUS Accounting-
 20 Requests. The Accounting-Request shall contain the Accounting Session ID attribute (44)
 21 generated by the PDSN.

22
 23 The security of communications between PDSN and RADIUS server optionally be protected with
 24 IP security. The establishment of the security association is outside the scope of this
 25 specification.

26 **5.2.2.1 NAI Construction in the Absence of CHAP**

27 In the event that the mobile station does not negotiate CHAP, no mobile station NAI is received
 28 by the PDSN. In this case, the PDSN shall not perform additional authentication of the user.
 29 Accounting records however, still must be generated and these records are keyed on the user
 30 NAI. For this reason, the PDSN shall be capable of constructing a properly formed NAI (RFC
 31 2486) based on the MSID of the mobile station. The NAI shall be constructed in the form
 32 <MSID>@<realm>, where <MSID> is the MSID of the mobile station, and <realm> is the
 33 Internet realm of the home network that owns the mobile station MSID.

34
 35 The mobile station shall use one of the following MSID formats (see figure 7):

- 36
 37 • International Mobile Station Identity (IMSI) [E.212]
 38 • Mobile Identification Number (MIN) [TIA/EIA-41-E]
 39 • International Roaming MIN (IRM) [TIA TSB-29]

40
 41 The IMSI is a string of decimal digits, up to a maximum of 15 digits, that identifies a unique MS
 42 internationally. The IMSI consists of three fields: Mobile Country Code (first 3 digits), Mobile
 43 Network Code (next 2 or 3 digits), and Mobile Subscriber Identification Number (maximum of 10
 44 digits). If the MS uses IMSI, the PDSN may determine the realm based on the Mobile Country
 45 Code and Mobile Network Code of the IMSI.

46
 47 The MIN is a string of 10 digits that identifies a unique MS in TIA/EIA-41. The first digit of MIN
 48 cannot be 0 or 1. The MIN consists of three fields: Area Code (first 3 digits), Office Code (next 3
 49 digits), and Subscriber Number (last 4 digits). If the MS uses MIN, the PDSN may determine the
 50 realm base on the Area Code and Office Code of the MIN.

51

¹ The numbers in this list correspond to the RADIUS attribute types defined in RFC 2138 and RFC 2139.

1 The IRM is a string of 10 digits that identifies a unique MS internationally. The first digit of IRM
2 must be 0 or 1. This is used to distinguish IRM from MIN. The IRM consists of three fields:
3 Mobile Country Code (first 3 digits), Mobile Network Code (4th digit), and Subscriber Number
4 (last 6 digits). The Mobile Network Code must be 0 or 1. If the MS uses IRM, the PDSN may
5 determine the realm based on the Mobile Country Code and Mobile Network Code of the IRM.
6

7 The PDSN shall write the constructed NAI into accounting records and the realm value may
8 optionally be used by the visited RADIUS server to forward these records to the correct home
9 RADIUS server for proper summary and settlement². The constructed NAI shall not be used for
10 authentication. The PDSN shall send RADIUS accounting messages to the local RADIUS server
11 using the constructed NAI in the absence of CHAP if configured by the operator.
12

13 If the PDSN is unable to construct an NAI for an MS, then the PDSN may deny service to the
14 MS.
15

² 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.

1

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)

2
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 the
7 mobile station. If the address is not associated with the PPP Session to the mobile station, and
8 is not a MIP RRQ or Agent Solicitation, then the PDSN shall discard the packet, and send an
9 LCP Configure-Request to restart the PPP session³.

10 **5.3 RADIUS Server Requirements**

11 RADIUS Server shall follow the guidelines specified in RFC 2138 and RFC 2139.

12
13 The local RADIUS server shall also support, and the broker RADIUS server should, support the
14 Interim Accounting Record in Annex D and accounting attributes listed in Section 9.4.

15
16 The local RADIUS server shall also support, and the broker and home RADIUS servers should,
17 support the Differentiated Services Class attribute in Annex C.

18
19 If the mobile station uses CHAP or PAP, the RADIUS server will receive a RADIUS Access-
20 Request from the PDSN with CHAP or PAP authentication information, and shall forward the
21 RADIUS Access-Request to the home network or a peer (e.g., a broker) if it does not have the
22 authority to accept/deny the request. This is in accordance with RFC 2138. In that case, the
23 RADIUS server will later receive a RADIUS Access-Accept message from the home or broker
24 network. The RADIUS server shall then send the RADIUS Access-Accept to the PDSN.

25
26 The RADIUS server will receive a RADIUS Accounting Start from the PDSN. The RADIUS
27 server later receives a RADIUS Accounting Stop from the PDSN in accordance with RFC 2139.
28 The RADIUS server may also receive Interim Accounting records between the Accounting Start
29 and Stop messages as necessary in accordance with Annex C. If the RADIUS server is in the
30 visited network, the visited RADIUS server shall forward the RADIUS accounting messages to
31 the home or broker network.

32

³ The reason to restart PPP is because the user could have started a Simple IP session during a previous dormant handoff to another PDSN and returned; in this case the current PDSN would not know the mobile station had invoked Simple IP and received another IP address. Thus, restarting PPP will force the Simple IP session to get a topologically correct address.

1 The security of communications between RADIUS servers may optionally be protected with IP
2 security. The establishment of the security association is outside the scope of this specification.
3 Also see RFC 2138 for additional RADIUS security requirements.

4 **5.4 Mobile Station Requirements**

5 The mobile station may optionally support Simple IP. When the mobile station wants to use
6 Simple IP, the mobile station shall use packet data service option 33 as specified in TIA/EIA/IS-
7 707-A-1.12.

8 **5.4.1 PPP Session**

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

10 **5.4.1.1 Establishment**

11 The mobile station shall exchange LCP messages as described in RFC 1661

12
13 PPP shall support control escaping in accordance with 4.2 of RFC 1662. The PPP Link Layer
14 shall support negotiation of Asynchronous Control Character Mapping as defined in RFC 1662.
15 The mobile station should negotiate a control character mapping. If the mobile station negotiates
16 control character mapping, it should attempt the minimum number of escapes by negotiating an
17 ACCM of 00000000.

18 **5.4.1.2 Termination**

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

22
23 If the mobile station becomes aware that the RN has terminated packet data service, the mobile
24 station may consider its PPP session closed at that point.

25 **5.4.1.3 Authentication**

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

30
31 The mobile station may support PAP authentication for Simple IP. If the mobile station uses
32 PAP, it shall respond to an LCP Configure-Request for CHAP with an LCP Configure-Nak
33 proposing PAP.

34
35 For both CHAP and PAP the MS shall send an NAI of the form user@realm.

36 **5.4.1.4 Addressing with IPCP**

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

40 **5.4.1.5 Compression**

41 The mobile station shall support Van Jacobson TCP/IP header compression (RFC 1144). The
42 TCP/IP header compression shall be configured through IPCP. The mobile station may support
43 PPP Compression Control Protocol (RFC 1962). If the mobile station wishes PPP payload
44 compression, the mobile station should use PPP Compression Control Protocol to negotiate a
45 PPP payload compression algorithm, and the mobile station shall support one of the following
46 compression algorithms:

- 1 • Stac-LZS (RFC 1974);
2 • Microsoft Point-To-Point Compression Protocol (RFC 2118).
3 • Deflate (RFC2394)

4

5 The mobile station may support additional PPP payload compression algorithms.

6 **5.4.1.6 PPP Framing**

7 The mobile station shall use the octet-synchronous framing protocol defined in RFC 1662,
8 except there shall be no inter-frame time fill, i.e., no flag octets shall be sent between a flag octet
9 that ends one PPP frame and the flag octet that begins the subsequent PPP frame.⁴

10

⁴ 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 specification, Mobile IP refers to a service based on a set of RFCs (including RFC 2002), in
4 which the user is provided IP routing service to a public IP network and/or secure IP routing
5 service to predefined private IP networks. The MS is able to use either a non-zero static IP
6 address or a dynamically assigned IP address belonging to its home IP network HA. The MS
7 shall have a non-zero static Home Agent address assigned regardless of whether the mobile
8 station has a static or dynamic Home Address. The user is able to maintain a persistent IP
9 address even when handing off between radio networks connected to separate PDSNs.

10 **6.1 Common Service Specification**

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

13 **6.1.1 PPP Session**

14
15 See Section 5.1.1.

16
17 For Mobile IP, neither CHAP nor PAP should be performed. If CHAP or PAP is performed,
18 longer initial setup time and re-establishment time will occur as the result of an additional
19 RADIUS traversal.

20
21 Note that the MN-AAA Challenge Extension procedures [FAC] shall be performed regardless of
22 whether or not CHAP is performed.

23 **6.1.2 Mobile IP**

24 Mobile IP operation shall be supported as defined in the following standards with any limitations
25 or extensions described in this specification:

- 26
- 27 • RFC 2002-2006;
 - 28 • Reverse Tunneling (RFC 2344);
 - 29 • Foreign Agent Challenge/Response (RFC XXXX);
 - 30 • NAI Extension (RFC 2794)

31 **6.2 PDSN Requirements**

32 The PDSN shall support Mobile IP operation.

33 **6.2.1 PPP Session**

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

35 **6.2.1.1 Establishment**

36 See Section 5.2.1.1.

37 **6.2.1.2 Termination**

38 The PDSN shall clear the PPP state if there is no established underlying R-P session for the
39 mobile station. The PDSN shall clear the RP-session whenever the PPP session is closed. If the
40 PDSN receives IP packets for a mobile station for which there is no established PPP session for
41 the mobile station, the PDSN shall discard the packet and send an ICMP destination
42 unreachable packet to the source. If the PDSN receives a failure code other than 133 or 136 in
43 the RRP, and there are no other active IP addresses on the PPP link, the PDSN should clear the
44 PPP session after delivering the RRP to the mobile station. If the PDSN generates a failure

1 code other than 69, and there are no other active IP addresses on the PPP link, the PDSN
2 should deliver the RRP and clear the PPP sessions.

3
4 For Mobile IP service, the PPP inactivity timer shall be set to a value larger than the FA's
5 maximum allowable values for Mobile IP registration lifetime.

6 **6.2.1.3 Addressing with IPCP**

7 For Mobile IP dynamic home address assignment, prior to the initial MIP registration:

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

11
12 For Mobile IP static home address assignment OR if the mobile station has already been
13 assigned a MIP address and the same MIP session is being continued:

- 14 ▪ If the mobile station uses the IP-Address Configuration Option in the IPCP Configure-
15 Request to indicate its home address, the PDSN shall accept any non-zero value. The
16 address contained in the RRQ shall supersede the (non-zero) address in IPCP.

17
18 The PDSN shall not support RFC 2290. If the mobile station uses the Mobile IPv4 Configuration
19 Option (RFC 2290), the PDSN shall reply with an IPCP Configure-Reject.

20 **6.2.1.4 Authentication**

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

26 **6.2.1.5 Compression**

27 See Section 5.2.1.5.

28 **6.2.1.6 PPP Octet Synchronous Framing**

29 See Section 5.2.1.6.

30 **6.2.2 MIP Registration**

31 **6.2.2.1 Agent Advertisements**

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

40
41 The Mobile IP Registration Lifetime field in the Agent Advertisement shall be smaller than the
42 PPP inactivity timer.

43
44 Upon receiving a handoff indication including SID/NID/PZID of the previous PCF and
45 SID/NID/PZID of the current PCF, if the PDSN already supports a Mobile IP service for the
46 mobile station, the PDSN shall use this information to determine whether or not Mobile IP re-
47 registration is required for the mobile station. If re-registration is required, then the PDSN shall
48 re-negotiate PPP and send Agent Advertisements.

1
2 In order to minimize Agent Advertisements sent over the air, the PDSN shall not send unsolicited
3 Agent Advertisements to a mobile station periodically to refresh the FA advertisement lifetime.
4 The mobile station may send Agent Solicitations when the FA advertisement lifetime expires.
5 The Advertisement Lifetime is a configurable value and the recommended value should be set to
6 9000 seconds (the maximum ICMP router advertisement lifetime).

7 **6.2.2.2 Addressing and Mobile IP**

8 The PDSN shall support both static and dynamic home address assignments. For dynamic
9 home address assignment, the PDSN shall accept Mobile IP RRQs with a 0.0.0.0 source address
10 from the mobile station. For dynamic home address assignment, the PDSN will acquire the
11 home address from the Mobile IP RRP. In order to provide public network access and to
12 provide private network access across the Internet, the PDSN must use a publicly routable and
13 visible care-of-address.

14 **6.2.2.3 MIP Extensions**

15 The PDSN shall include MN-FA Challenge Extension [FAC] in the Agent Advertisement. Since
16 Advertisements are rarely sent (to save air resources) the PDSN shall include in the RRP the
17 next challenge that the mobile should use in its next re-registration with this PDSN. This only
18 applies to re-registrations. The PDSN may re-authenticate the FAC with the home RADIUS
19 server. The frequency of this re-authentication and re-authorization is configurable by the
20 operator. The challenge shall be changed on a serving access provider configurable basis.

21 The PDSN shall not remove the MN-FA Challenge Extension and MN-AAA Authentication
22 Extension from the RRQ.

23 If the PDSN receives an RRQ that does not contain an MN-HA Authentication Extension, it shall
24 send an RRP to the mobile station with an error code of 70 to indicate the RRQ was poorly
25 formed.

26 **6.2.2.4 Private Network Support**

27 The PDSN shall support private home addresses. If the mobile station desires a private home
28 address then the mobile station will negotiate reverse tunneling (RFC 2344). If the mobile
29 station desires a private home address but does not negotiate reverse tunneling, the PDSN shall
30 send a failed RRP with error code 75. The PDSN shall form a logical association that contains
31 the R-P session ID, the mobile station's home address, and the Home Agent address. When the
32 PDSN receives a packet for a registered mobile station from the Home Agent, the PDSN shall
33 map the mobile station's Home Agent address and the home address to one association, and
34 shall transmit the packet on the R-P connection indicated by the R-P Session ID of the
35 association.

36
37 If two Home Agents assign a single mobile station the same address, the PDSN shall send a
38 failed RRP with an Administratively-Prohibited error code (65) to the mobile station. The first
39 assigned address is not affected.

40 **6.2.2.5 Reverse Tunneling**

41 The PDSN shall reject a Mobile IP registration with an error code of 75 if a private home address
42 as defined in RFC 1918 is present in either the RRQ or RRP, and the RRQ did not indicate
43 reverse tunneling.

44
45 If the home RADIUS server sends a Reverse Tunnel Specification attribute in the RADIUS
46 Access-Accept, and the mobile station did not indicate reverse tunneling in the RRQ, the PDSN
47 shall reject the registration with an error code of 75. If the mobile station negotiates reverse
48 tunneling, then the PDSN shall reverse tunnel both direct delivered and encapsulated packets.

1 This applies to unicast, multicast, and broadcast IP destination addresses, even if the direct
 2 delivery mode is used.

3

4 The PDSN must support both direct delivered and encapsulated packets.

5 **6.2.3 RADIUS Support**

6 The PDSN shall act as a RADIUS client in accordance with RFC2138 and shall communicate
 7 user FAC authentication information to the local RADIUS server in a RADIUS Access-Request.
 8 On receipt of the MIP RRQ from the mobile station, the PDSN shall create an Access Request
 9 containing at a minimum the following:

10

- 11 User-Name (1) = MN-NAI field in the MN-NAI Extension
- 12 CHAP-Password (3) = High-order byte of the Challenge Field in the MN-FA Challenge
 13 Extension, followed by the Authenticator field from the MN-AAA Extension
- 14 CHAP-Challenge (60) = MD5 (Preceding MIP RRQ, Type, Length, SPI), followed by the
 15 least-order 237 bytes of the Challenge Field in the MN-FA Challenge Extension.
 16 The MD5 checksum is computed over the MIP RRQ data preceding the MN-AAA
 17 Extension and the Type, Length, SPI fields of the MN-AAA Extension.
- 18 NAS-IP-Address (4) = IP address of the PDSN COA contained in RRQ
- 19 Home Agent Address (as defined in Annex C)= HA address contained in the RRQ
- 20 Correlation ID (as defined in Annex C) = An ID that correlates all accounting sessions
 21 authorized for this NAI by this access request
- 22 Security Status (as defined in Annex C) = security state that may currently exist between
 23 the PDSN and HA

24

25

26

27 If the authentication succeeds, the local RADIUS server will send a RADIUS Access-Accept
 28 message to the PDSN. The RADIUS Access-Accept message may contain the 3GPP2 RADIUS
 29 attributes list in Annex C. If the authentication fails, the local RADIUS server will send a RADIUS
 30 Access-Reject to the PDSN.

31

32 The PDSN shall act as a RADIUS accounting client in accordance with RFC 2139 and shall
 33 communicate user accounting information to the local RADIUS server in RADIUS Accounting-
 34 Requests. The PDSN shall determine at completion of the IPCP phase that an Accounting-
 35 Request Start message shall be sent to the server following a successful Mobile IP registration
 36 Reply received from the HA. The Accounting-Request Start shall contain the Accounting Session
 37 ID and Correlation ID attribute generated by the PDSN.

38

39 The security of communications between PDSN and RADIUS server may optionally be protected
 40 with IP security. The establishment of security is outside the scope of this specification.

41

42 **6.2.4 IP Security Support**

43 There may be a statically configured shared secret for computing the Mobile IP HA/FA
 44 authentication extension in Mobile IP registration messages. If such a shared secret exists, the
 45 PDSN and HA shall use it.

46

47 Additional security associations between the PDSN and HA may also be supported for the
 48 protection of Mobile IP control messages and user data. This specification supports the following
 49 options:

50

51

52

53

- IKE and public certificates
- Dynamic pre-shared IKE secret distributed by the home RADIUS server
- Statically configured IKE pre-shared secret

1 The PDSN shall support IPsec and IKE, including a shared secret for IKE that may be statically
2 or dynamically provisioned. The implementation of IPsec implies support for IPsec AH as a
3 minimum requirement. The PDSN shall support the capability to accept a shared key from the
4 home RADIUS server, and the PDSN may support X.509 based certificates. The Home RADIUS
5 server optionally supports the *3GPP2 RADIUS* attributes and the PDSN shall support the *3GPP2*
6 *RADIUS* attributes.

7
8 The security association shall be determined as follows:

9
10 Upon receiving a MIP RRQ from a mobile station, the PDSN sends an Access-Request message
11 as outlined in Section 6.2.3. That Access-Request shall contain the *Security Status* attribute that
12 has one of possible values:

- 13
- 14 1. IPsec Security Association (SA) already established with the HA
- 15 2. IPsec SA not established and a certificate exists for the HA
- 16 3. IPsec SA not established but the PDSN has a root certificate for the HA
- 17 4. IPsec SA not established, no certificate exists for the HA, but a configured pre-shared
18 IKE secret exists
- 19 5. IPsec SA not established, no certificate exists for the HA, and no configured pre-shared
20 IKE secret exists

21
22 By including the appropriate *3GPP2 Security Level* attributes in the Access-Accept message, the
23 home RADIUS server is able to authorize the PDSN on a per user basis to use IPsec on the
24 registration messages and/or the tunneled data, or not use IPsec at all. If IPsec services are
25 authorized, and the *Security Status* attribute in the Access-Request from the PDSN indicates no
26 security association currently exists, the home RADIUS server may distribute a pre-shared secret
27 for IKE to the PDSN using the *Pre-Shared Secret* attribute in the Access-Accept. If the PDSN
28 has indicated a Security Status of 5, and the Home RADIUS server does not return a pre-shared
29 key, and if the user is authorized to use IPsec, then the PDSN shall reject the RRQ with
30 administratively prohibited code of 65.

31
32 If the Home RADIUS server has indicated that an IP security association shall be used between
33 the PDSN and HA, the PDSN shall provide IPsec services as indicated in the *3GPP2 security*
34 *level* attribute. If no security association currently exists, the PDSN shall attempt to establish the
35 security association using the HA X.509 certificates. If no HA X.509 certificate exists, but the root
36 certificate exists, the PDSN shall attempt to establish the security association using X.509
37 certificates as received in Phase 1 IKE. If the necessary certificates do not exist, the PDSN shall
38 attempt to use the dynamically distributed shared secret for IKE received in the Access-Accept
39 message. If no shared secret was sent, the PDSN shall attempt to use a statically configured
40 IKE pre-shared secret if one exists.

41
42 If the PDSN does not receive the *3GPP2 security level* attribute from the home RADIUS server,
43 and an IPsec security association to the HA already exists, the PDSN shall continue to use the
44 same security association. If no security association exists, then the PDSN shall follow local
45 security policy.

46
47 If reverse tunneling is supported by the Home Agent as indicated by the RADIUS server in the
48 *3GPP2 Reverse Tunnel Specification* attribute, IPsec security is authorized for tunneled data,
49 and the mobile requests reverse tunneling, then the PDSN will provide security on the reverse
50 tunnel.

51
52 The PDSN shall not delete existing IPsec security associations to a HA if the home RADIUS
53 server does not authorize security for the mobile, because other mobiles may be using the same
54 IPsec security association.

55

1 When the PDSN determines that an IPsec security association to protect control messages has
 2 already been established to the Home Agent, the PDSN shall ensure the IPsec security
 3 association is maintained throughout the Mobile IP registration lifetime by periodically refreshing
 4 the security association. The PDSN shall not forward a MIP RRQ to the HA unless an IPsec
 5 security association exists first, if the home network authorizes IPsec services. The PDSN shall
 6 send a failed MIP RRP to the mobile station if the RADIUS Access-Reject is received or if it is
 7 unable to establish an IPsec security association to the HA and IPsec security is authorized by
 8 the home RADIUS server.

9
 10 The home RADIUS server will hide shared secrets using a method based on the RSA Message
 11 Digest Algorithm MD5 [RSA] as described in Section 5.2 of RFC 2138 [RADIUS]. This shared
 12 secret is associated with the next hop RADIUS server.

13
 14 The PDSN shall comply with the specifications in [IKE], and the Annexes A and B in this
 15 specification.

16
 17 In the case of a carrier owned HA, the PDSN must have an security association with an IMT-
 18 2000 HA in order for a registration request to be successfully processed. The security association
 19 may formally be via IPsec (e.g., ESP or AH) or via Mobile IP HA-FA authentication extension⁵.

20 **6.2.5 Ingress Address Filtering**

21 The PDSN shall perform filtering on the source address for packets originating from the mobile
 22 station to ensure that the mobile station is using address(es) assigned by the Home Agent and
 23 for which the registration lifetime has not expired. If a mobile station uses an address not
 24 assigned by the Home Agent, and is not a MIP RRQ or Agent Solicitation, then the PDSN shall
 25 discard the packet, and send an LCP Configure-Request to restart the PPP session⁶.

26 **6.3 Home Agent Requirements**

27 The Home Agent must support basic MIP [RFC 2002-2006], reverse tunneling [RFC 2344] and
 28 Mobile IP NAI extension [RFC 2794]. In order to provide public network access and to provide
 29 private network access across the public network, the HA must use a globally routable and
 30 visible care-of-address.

31 **6.3.1 Multiple Registrations**

32 The Home Agent shall support:

- 33 • Multiple registrations for the same NAI using different static addresses
- 34 • Multiple registrations for different NAIs using static or dynamic address assignments

35 **6.3.2 IP Security Support**

36 The HA shall determine which type (if any) security associations are required with a PDSN. The
 37 HA shall use the same security policy as specified in the home RADIUS server and returned to
 38 the PDSN in the 3GPP2 Security Level attribute.

⁵ This requirement is to prevent users from using collocated COA from high speed interfaces or other interfaces external to an access service provider. Such access circumvents accounting and could result in malicious overloading of the carrier owned HA that adversely affects from wireless data service of users accessing via air interfaces which are subject to charging.

⁶ The reason to restart PPP is because the user could have started a Simple IP session during a previous dormant handoff to another PDSN and returned; in this case the current PDSN would not know the mobile station had invoked Simple IP and received another IP address. Thus, restarting PPP will force the Simple IP session to get a topologically correct address.

1 Security associations are required for MIP control and payload tunnels. Also, IKE requires that
 2 all mobile stations on a given PDSN belonging to the same HA receive the same security
 3 between the PDSN and HA for either registration messages or tunneled data.
 4

5 The Home Agent may request a pre-shared key from the home RADIUS server in an Access-
 6 Request by using a concatenation of the PDSN's care-of-address and home agent address
 7 placed in the *user name* attribute. The security of the Home Agent and RADIUS server is outside
 8 the scope of this specification.

9 **6.3.3 Dynamic Home Address Assignment**

10 The mobile station may send the home agent a MIP RRQ with a 0.0.0.0 home address. If the
 11 Home Agent successfully authenticates the MIP RRQ, the Home Agent shall assign a home
 12 address to the mobile station. The assigned address shall be inserted in the home address field
 13 of the MIP RRP. The Home Agent shall release the home address when the registration expires.

14 **6.3.4 Authentication**

15 Based on the policy of the home network, the HA may optionally process the MN-AAA. If the HA
 16 policy dictates that the HA must process the MN-AAA authentication extension, then the HA shall
 17 authenticate the registration by sending a RADIUS Access-Request to the Home RADIUS server
 18 with the following:
 19

- 20 User-Name (1) = MN-NAI field in the MN-NAI Extension
- 21 CHAP-Password (3) = High-order byte of the Challenge Field in the MN-FA Challenge
 22 Extension, followed by the Authenticator field from the MN-AAA Extension
- 23 CHAP-Challenge (60) = MD5 (Preceding MIP RRQ, Type, Length, SPI), followed by the
 24 least-order 237 bytes of the Challenge Field in the MN-FA Challenge Extension.
 25 The MD5 checksum is computed over the MIP RRQ data preceding the MN-AAA
 26 Extension and the Type, Length, SPI fields of the MN-AAA Extension.
 27

28 **6.4 RADIUS Server Requirements**

29 See Section 5.3.

30
 31 The local RADIUS server shall also support, and the broker and home RADIUS server should
 32 support, the following attributes in Annex C:
 33

- 34 • Security Status Attribute
- 35 • Security Level Attribute
- 36 • Reverse Tunnel Specification
- 37 • Differentiated Services Class Attribute
- 38 • Pre-shared Secret Attribute
- 39 • Correlation ID Attribute
- 40 • Home Agent Attribute

41 **6.5 Mobile Station Requirements**

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

44 **6.5.1 PPP Session**

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

1 **6.5.1.1 Establishment**

2 Same as Section 5.4.1.1.

3 **6.5.1.2 Termination**

4 Same as Section 5.4.1.2.

5 **6.5.1.3 Authentication with CHAP**

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

12

13 If CHAP is performed, performance degradation will occur as the result of an unnecessary
14 RADIUS traversal.

15

16 Note that the FAC shall be performed regardless of whether or not CHAP is performed.

17 **6.5.1.4 Addressing with IPCP**

18 If the mobile station uses a static home address, the mobile station shall use the IP-Address
19 Configuration Option (RFC 1332) to indicate the home address, or omit this option. Since the
20 PDSN will not support RFC 2290, if the mobile station uses Mobile IPv4 Configuration Option,
21 the PDSN will reply with an IPCP Configure-Reject.

22

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

27 **6.5.1.5 Compression**

28 Same as Section 5.4.1.5.

29 **6.5.1.6 PPP Framing**

30 Same as Section 5.4.1.6.

31 **6.5.2 MIP Registration**

32 **6.5.2.1 Agent Discovery**

33 Immediately after PPP is established, the mobile station may send Agent Solicitations. In this
34 case, the mobile station should use the same procedure as described in Section 2.4 of RFC
35 2002. If the mobile station does not have a home address, the mobile station shall use zero in
36 the Source IP Address field of the IP packet that contains the Agent Solicitation. The Agent
37 Advertisement received in response to the Agent Solicitation will contain the Foreign Agent
38 Challenge.

39 **6.5.2.2 Registration Messages**

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

41

42 If the mobile station uses a static home address, the mobile station shall insert the address into
43 the home address field of the Mobile IP RRQ.

44

1 If the mobile station wants a dynamic home address, the mobile station shall use zero in the
2 Home Address field of the Mobile IP RRQ, and the mobile station shall use zero in the Source IP
3 Address field of the IP packet that contains the Mobile IP RRQ. In this case the NAI is used to
4 identify the mobile station. The mobile station shall obtain a home address in the Mobile IP
5 RRP. On subsequent re-registrations while retaining the same home address, the mobile station
6 shall insert the assigned address into the home address field of the Mobile IP RRQ.

7
8 If the mobile station desires reverse tunneling, the mobile station shall set the T-bit in the Mobile
9 IP RRQ.

10
11 If the mobile station and PDSN negotiate in IPCP to use Van Jacobson header compression,
12 then the mobile station shall not set the 'V' bit in the RRQ.

13 **6.5.2.3 MIP Extensions**

14 The mobile station shall include the MN-FA Challenge Extension [FAC], MN-AAA Extension
15 [FAC], and MN-NAI Extension [RFC 2794]. The mobile station shall use a static HA address and
16 shall include the MN-HA Authentication Extension in the RRQ because the mobile station shares
17 a security association with the HA. The mobile station's processing of the MN-HA Authentication
18 Extension is specified in [FAC]. Because advertisements are rarely sent to save air resources,
19 the mobile station should use the challenge value contained in the most recent RRP in the case
20 of re-registrations as described in [FAC].

21
22 The mobile station shall compute the MN-AAA Extension, according to [FAC], based on the
23 shared secret the mobile station has with the home RADIUS server. The mobile station shall
24 compute the MN-HA Authentication Extension, according to [RFC 2002], based on the shared
25 secret the mobile station has with the HA. The mobile station may use the same shared secret
26 or different shared secrets in the computation of the MN-AAA Extension and MN-HA
27 Authentication Extension. This will be coordinated between the mobile station and its home
28 network.

29 **6.5.2.4 Private Network Support**

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

32

1 **7 Mobility Management**

2 **7.1 Mobility within Radio Network**

3 In this specification 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 specification 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 session
8 point of attachment while maintaining PPP session and IP address(es). The R-P session point of
9 attachment is the PCF. When a mobile station moves from one PCF to another PCF, a new R-P
10 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 PPP session while a mobile station is dormant while
14 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 a
24 different PDSN is selected, the old R-P session will expire, unless the mobile station returns to
25 the previous PDSN before the R-P session expires. During PCF to PCF handoff, the selection of
26 the same PDSN should be given priority in order to maintain the PPP session to the mobile
27 station. If a different PDSN is selected and the mobile station still desires packet data service,
28 then a new PPP session must be established.

29

30 Each PCF will be uniquely identified by the combination of the System ID (SID), Network ID
31 (NID), and Packet Zone ID (PZID). At handoff the new PCF will perform PDSN selection and will
32 forward the previous PCF's SID/NID/PZID and the current SID/NID/PZID to the selected PDSN.
33 The PDSN will use this information to determine whether or not Mobile IP re-registration is
34 required for the mobile station. If re-registration is required, the PDSN will re-negotiate PPP and
35 will then send Agent Advertisements.

36 **7.3 PDSN to PDSN Handoff**

37

38 Mobile IP provides the IP layer mobility management function that maintains persistent IP
39 addresses across PDSNs. There is no similar IP layer mobility management function support
40 between PDSNs for Simple IP service. For Mobile IP mobile stations, in order to maintain
41 persistent IP addresses, the mobile station will effect a PDSN to PDSN handoff by registering
42 with its Home Agent as per RFC 2002 with extensions as outlined in Section 6 above.

43

44 A PDSN to PDSN handoff requires the mobile station be active or to transition to the active
45 state. The PDSN to PDSN handoff for Mobile IP involves:

46

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

1
2

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 3GPP2
 4 Differentiated Service Class Options indicated in the user's RADIUS profile. The 3GPP2
 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 services
 8 as defined in:

- 9
- 10 • Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- 11 (RFC 2474);
- 12 • An Architecture for Differentiated Services (RFC 2475);
- 13 • An Expedited Forwarding PHB (RFC 2598);
- 14 • 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 may
 18 optionally accept the marking or may remark the packet based on the user profile's 3GPP2
 19 Differentiated Service Class Options from the home RADIUS server. When the mobile station
 20 has not marked the packets, the PDSN may optionally mark packets from the mobile station to
 21 specific differentiated service classes based on the user profile's 3GPP2 Differentiated Service
 22 Class Options. The user profile may indicate no differentiated services are authorized for the
 23 user, and if so, the PDSN will mark the user's packets as configured by the service provider
 24 network.

25

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

31

32 The PDSN shall send packets received from the IP network for a mobile station onto the R-P
 33 session for the mobile station in accordance with differentiated class behavior of the packet and
 34 the user profile's 3GPP2 Differentiated Service Class Options. The PPP frames that carry the
 35 user packets are encapsulated in GRE packets, which in turn are carried over IP. PPP frame
 36 boundaries may or may not be aligned with GRE packets.

37

38 The PDSN shall use sequential numbering in the GRE packet header, to insure sequential
 39 delivery of packets over the R-P interface, if at least one of the following events occur:

- 40
- 41 • The PDSN is configured to send GRE packets that contain incomplete PPP frames or
- 42 multiple PPP frames.
- 43 • The mobile station negotiates a PPP payload compression algorithm that requires PPP
- 44 frames to be delivered in sequence.
- 45 • The mobile station negotiates Van Jacobson TCP/IP header compression in which the
- 46 Connection ID may be compressed.
- 47

1 If the PDSN uses sequential numbering in the GRE packet header, the PDSN shall indicate one
2 and only one differentiated service class for all IP packets of the R-P session based on the user
3 profile's 3GPP2 Differentiated Service Class Options from the home RADIUS server.
4 The 3GPP2 provider must insure that it does not exceed its service level agreements (SLA) with
5 its supporting ISPs; however, the procedures to insure that SLAs are satisfied are beyond the
6 scope of this specification.

7
8 For packets received from the RN, the PDSN shall not process the differentiated services class
9 field associated with the R-P interface.

10 **8.2.2 3GPP2 Differentiated Service Class Option**

11 As indicated above, the 3GPP2 Differentiated Service Class Options specify groupings of
12 differentiated services classes. For some 3GPP2 Differentiated Service Class Options, not all
13 differentiated service classes may be supported. This option is contained in a user profile
14 parameter in the home RADIUS server, and is returned to the PDSN in the RADIUS Access
15 Accept message. The format of the RADIUS attribute is given in Annex C. The actual
16 parameters associated with these classes, such as classification rules and policing parameters
17 are configured into the PDSN by the visited access provider, and are not sent in the RADIUS
18 profile parameter. The method by which carriers agree to the same PDSN configuration
19 definitions for each class, as well as the method to inform private network owners and ISPs of
20 these class definitions, is outside the scope of this specification.

21 **8.3 RN Requirements for Differentiated Service**

22 The RN may use the Differentiated Service indication from the R-P interface generated by the
23 PDSN to deliver packets to the mobile station. The RN shall not reorder packets of the same
24 differentiated service class.

25
26 The RN does not perform general differentiated services processing functions such as policing,
27 nor does it examine the actual PPP frame itself to perform additional differentiated services
28 information beyond those supported by the PDSN.

29 **8.4 Mobile Station Requirements for Differentiated Service**

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

32

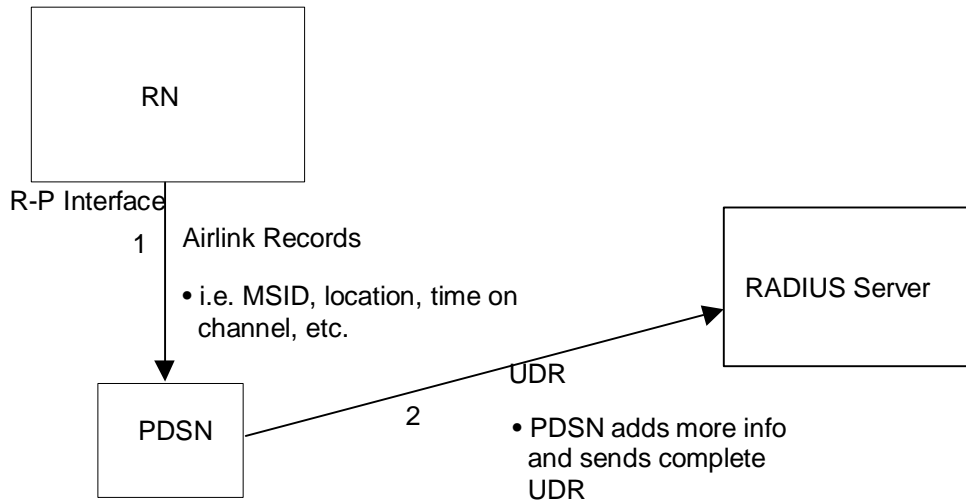
1 **9 Accounting**

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 Usage
 6 Data Record (UDR). After merging, the PDSN will send the UDR to a local RADIUS Server.
 7 The PDSN will maintain the UDR information until the PDSN receives positive acknowledgment
 8 from the RADIUS server that the RADIUS server has correctly received the UDR.
 9 The PDSN will formulate one UDR per IP address per mobile station.

10
 11 The RADIUS server will maintain the UDR until the record is removed by the operator billing
 12 system. The method by which this is done is beyond the scope of this specification as is the
 13 summary, reconciliation, and billing process used by the carriers.

14
 15 The RN sends radio specific parameters in messages called airlink records across the R-P
 16 interface. Once the PDSN combines these with IP network specific parameters, the UDR is sent
 17 to the RADIUS server as a RADIUS Accounting-Request message. This is outlined as below in
 18 Figure 8, and detailed in the subsequent sections.
 19



20
 21
 22
 23 **Figure 8: Accounting Architecture**

24
 25 Table 5 in Section 9.4 contains a complete listing of UDR attributes. Tables 1-4 contains fields
 26 in various air link records generated by the RN. Note that a lower case letter implies a field in an
 27 air link record whereas a capital letter implies an attribute in a UDR.

28 **9.2 Airlink Records**

- 29 The RN generates one of four types of airlink records over the R-P interface:
- 30 ▪ A Connection Setup when the RN establishes an R-P session.
 - 31 ▪ An Active Start record when the MS has started to use traffic channel(s).
 - 32 ▪ An Active Stop record when the MS has stopped using traffic channel(s).
 - 33 ▪ A Short Data Burst (SDB) record when a forward or reverse short data burst is exchanged
 34 with the MS.

The R-P session ID is the PSI used at A10 establishment (session specific extension) and in the GRE key used on the A10 connection.

All the airlink records would include a sequence number initialized to zero at R-P session setup. The sequence number is unique for a single identification triplet (RP session ID, PCF ID, and MSID). Upon receiving the connection setup airlink record, the PDSN updates the UDR with the airlink record information and stores the sequence number. The PCF shall increment the sequence number modulo 256 in the subsequent airlink record transmitted over the corresponding R-P session. The PDSN will then compare the received sequence number with the previously stored sequence number (N). If the received sequence number is in the range from (N+1) modulo 256 to (N+127) modulo 256, inclusive, the PDSN shall act accordingly based on the information contained in the airlink record, and shall update its stored sequence number. If the received sequence number is in the range from (N-128) modulo 256 to (N-1) modulo 256, inclusive, the PDSN shall ignore the message. The same procedure continues for all the subsequent airlink records, until the closing of the R-P session.

Note that in the event of retransmission, the PCF shall retransmit with the same sequence number, and the PDSN shall not update the UDR if the same sequence number corresponding to a single identification triplet is received. There should be only one outstanding unacknowledged airlink record at any given time.

9.2.1 R-P Session Setup Airlink Record

Table 1 contains fields present in R-P Session Setup airlink records.

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = 1 (Connection Setup)	4	integer
y2	R-P Session ID	4	integer
y3	Sequence Number	4	integer
a1	MSID	15	string
d3	Serving PCF	4	ip-addr
d4	BS / MSC ID	12	string

Table 1: R-P Session Setup Airlink Fields

Each R-P session and each airlink record is indexed via the R-P session ID.

9.2.2 Active Start Airlink Record

Table 2 contains fields present in Active Start airlink records.

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = 2 (Active Start)	4	integer
y2	R-P Session ID	4	integer
y3	Sequence Number	4	integer
e1	User Zone	4	integer
f1	Forward Mux Option	4	integer
f2	Reverse Mux Option	4	integer
f3	Forward Fundamental Rate	4	integer
f4	Reverse Fundamental Rate	4	integer
f5	Service Option	4	integer
f6	Forward Traffic Type(Primary, Secondary)	4	integer
f7	Reverse Traffic Type(Primary, Secondary)	4	integer

f8	Fundamental Frame Size (5/20 ms)	4	integer
f9	Forward Fundamental RC	4	integer
f10	Reverse Fundamental RC	4	integer
i4	Airlink Quality of Service (QoS)	4	integer

Table 2: Active Start Airlink Fields

If the e1 and/or i4 parameters in Table 2 change during the active session, the RN shall send an Active Stop airlink record, and an Active Start airlink record with the new parameters.

f1 to f10 are fields from service configuration record.

9.2.3 Active Stop Airlink Record

Table 3 contains fields present in Active Stop airlink records.

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = 3 (Active Stop)	4	integer
y2	R-P Session ID	4	integer
y3	Sequence Number	4	integer
g8	Active Connection Time in Seconds	4	integer

Table 3: Active Stop Airlink Fields

9.2.4 SDB Airlink Record

Table 4 contains fields present in SDB airlink records.

Item	Parameter	Max Payload Length	Format
y1	Airlink Record Type = 4 (SDB)	4	integer
y2	R-P Session ID	4	integer
y3	Sequence Number	4	integer
y4	Mobile Originated/Mobile Terminated Indicator	4	integer
g10	SDB Octet Count	4	integer

Table 4: SDB Airlink Fields

9.3 PDSN Usage Data Record (UDR)

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 Correlation ID is a unique accounting ID created by the PDSN that allows multiple related R-P sessions to be matched.

Table 5 contains the complete UDR and the description of each field.

Item	Parameter	Description
A. Mobile Identifiers		
A1	MSID	Mobile Station ID (e.g. IMSI, MIN, IRM)
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 created by the PDSN that allows stop and start records to be matched in a log file.

C2	Correlation ID	An ID that correlates all accounting sessions authorized for this NAI by this access request
D. Infrastructure Identifiers		
D1	MIP Home Agent (HA)	The IP address of the HA
D2	PDSN/FA Address	IP address or other identifier.
D3	Serving PCF	The IP address of the serving PCF
D4	BS / MSC ID	SID+ NID+ BSC ID
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 and Secondary
F7	Reverse Traffic Type(Primary, Secondary)	Primary and Secondary
F8	Fundamental Frame Size	The fundamental channel has the choice of 5 or 20 ms size. The 5ms frame sized comes from the DCCH (dedicated signaling channel) concept and allows fast response for short signaling messages (short frame can be decoded quickly).
F9	Forward Fundamental RC	
F10	Reverse Fundamental RC	
F11	IP Technology	Identifies Simple IP, Mobile IP, or another technology.
F12	Compulsory Tunnel Indicator	Indicator of invocation of compulsory tunnel 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	Bad PPP frame count	total # PPP frames from the mobile station dropped by PDSN due to uncorrectable errors.
G4	Event Time	Indicates start of accounting session or stop of accounting session if part of a RADIUS start message or stop message, respectively. It is also used in a RADIUS interim message to indicate the time of the event which triggered the interim message.
G8	Active Time	The total active connection time on traffic channel in seconds.
G9	Number of Active Transitions	The total number of non-active to Active transitions by the user.
G10	SDB Octet Count (Terminating)	The total number of octets sent to the user via Short Data Bursts.
G11	SDB Octet Count (Originating)	The total number of octets sent by the user via Short Data Bursts.
G12	Number of SDBs (Terminating)	The total number of Short Data Burst transactions.
G13	Number of SDBs (Originating)	The total number of Short Data Burst transactions.
G14	Number of PPP_bytes received	The count of all bytes received in the reverse direction by the PPP layer in the PDSN.
H. Special Billing Instructions		
H1	Alternate Billing Identifier	An IP address or other identifier of alternate entity for which data session usage may be billed.
I. Quality of Service		

11	IP Quality of Service (QoS)	The home RADIUS server authorizes the mobile to mark packets (only) with these Differentiated Services code points.
12	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 5: 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 6 lists each accounting parameter and its associated RADIUS attribute.

7

8 Note: Attributes of type "26" defined in RFC 2138 and RFC 2139 are vendor specific, and are
9 used to transport 3GPP2 specific parameters. The default Vendor ID value in Vendor Specific
10 attributes shall be 5535 defined in IANA in order for cdma2000 packet data service to support
11 global roaming.

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	8	string	Acct_Session_Id	
C2	Correlation ID	26/44	8	string	Correlation_Id	
D. Infrastructure Identifiers						
D1	MIP Home Agent (HA)	26/7	4	ip-addr	3GPP2_HA_IP_Addr	
D2	PDSN/FA Address	4	4	ip-addr	NAS Address	
D3	Serving PCF	26/9	4	ip-addr	3GPP2_PCF_IP_Addr	
D4	BS / MSC ID	26/10	12	string	3GPP2_BS / MSC Addr	A number formed from the concatenation of SID+ NID+ BSC ID where each item is encoded using four hexadecimal upper case ASCII characters.
E. Zone Identifiers						
E1	User Zone	26/11	4	integer	3GPP2_User_ID	
F. Session Status						
F1	Forward Mux Option	26/12	4	integer	3GPP2_FMUX	
F2	Reverse Mux Option	26/13	4	integer	3GPP2_RMUX	
F3	Forward Fundamental Rate	26/14	4	integer	3GPP2_FRATE	
F4	Reverse Fundamental Rate	26/15	4	integer	3GPP2_RRATE	
F5	Service Option	26/16	4	integer	3GPP2_SO	
F6	Forward Traffic Type	26/17	4	integer	3GPP2_FTYPE	
F7	Reverse Traffic Type(Primary, Secondary)	26/18	4	integer	3GPP2_RTYPE	
F8	Fundamental Frame Size	26/19	4	integer	3GPP2_FSIZE	
F9	Forward Fundamental RC	26/20	4	integer	3GPP2_FRC	
F10	Reverse Fundamental RC	26/21	4	integer	3GPP2_RRC	
F11	IP Technology	26/22	4	integer	3GPP2_IP_Tech	1=Simple IP, 2=Mobile IP
F12	Compulsory Tunnel Indicator	26/23	4	integer	3GPP2_Comp_Flag	0=no tunnel 1=non-secure tunnel 2=secure tunnel

F13	Release Indicator	26/24	4	integer	3GPP2_Reason_Ind	Reasons for stop record: 0=unknown 1=PPP/Service timeout 2=Handoff 3=PPP protocol failure 4=PPP abnormal release 5=PPP termination 6=Mobile IP registration failure
-----	-------------------	-------	---	---------	------------------	--

1 **G. Session Activity**

G1	Data Octet Count (Terminating)	43	4	integer	Acct_Output_Octets	This includes the PPP bytes between flags before escaping.
G2	Data Octet Count (Originating)	42	4	integer	Acct_Input_Octets	This includes the PPP bytes between flags after escaping.
G3	Bad PPP Frame Count	26/25	4	integer	3GPP2_Ba_Frame_Count	
G4	Event Time	55	4	time	3GPP2Event timestamp	In a start or stop message indicates the start or end of the accounting session respectively. In an interim message indicates the time of the event which triggered the interim message
G8	Active Time	46	4	integer	Acct_Session_Time	
G9	Number of Active Transitions	26/30	4	integer	3GPP2_Num_Active	
G10	SDB Octet Count (Terminating)	26/31	4	integer	3GPP2_SDB_Input_Octets	
G11	SDB Octet Count (Originating)	26/32	4	integer	3GPP2_SDB_Output_Octets	
G12	Number of SDBs (Terminating)	26/33	4	integer	3GPP2_NumSDB_Input	
G13	Number of SDBs (Originating)	26/34	4	integer	3GPP2_NumSDB_Output	
G14	Number of PPP bytes received	26/43	4	integer	3GPP2_Num_PPP_Received_Total	The count of all bytes received in the reverse direction by the PPP layer in the PDSN.

2 **H. Special Billing Instructions**

H1	Alternate Billing Identifier	26/35	4	integer	3GPP2_Alt_Billing	
----	------------------------------	-------	---	---------	-------------------	--

3
4

1	I. Quality of Service					
	I1	IP Quality of Service (QOS)	26/36	4	integer	3GPP2_IP_QOS 0=Best Effort 10=AF11 12=AF12 14=AF13 18=AF21 20=AF22 22=AF23 26=AF31 28=AF32 30=AF33 34=AF41 36=AF42 38=AF43 46=EF
	I2	Interconnection IP Network Provider ID	26/37	4	ip-addr	3GPP2_Interconnect_IP
	I3	Interconnecting IP Network Service Quality of Service	26/38	4	integer	3GPP2_Interconnect_QOS currently undefined
	I4	Airlink Quality of Service (QOS)	26/39	4	integer	3GPP2_Air_QOS 16 levels of priority
2	Y. Airlink Record Specific Parameters					
	Y1	Airlink Record Type	26/40	4	integer	3GPP2_Airlink_Record_Type 1=Connection Setup 2=Active Start 3=Active Stop 4=SDB Record
	Y2	R-P Session ID	26/41	4	integer	3GPP2_R-P_Session_ID
	Y3	Airlink Sequence Number	26/42	4	Integer	3GPP2_Airlink_Sequence_Number
	Y4	Mobile Originated / Mobile Terminated Indicator	26/45	4	Integer	3GPP2_Mobile_Terminated_Originated_Indicator 0=Mobile Originated 1=Mobile Terminated
3	Z. Container					
	Z1	Container	26/6	Variable	string	3GPP2_Container See Annex C
4						
5						
6						

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

14
15 A UDR is associated with an NAI, IP address pairs within a PPP session. A UDR stores the
16 accounting information for an NAI, IP pair for the duration of the packet data
17 service in a single PDSN. RADIUS accounting messages are generated from the information in
18 the UDR. The correlation ID is used to match different accounting records (accounting session
19 IDs) across R-P sessions on a single PDSN. One correlation ID is maintained for the life of a
20 UDR. The Accounting session ID is used to match a single RADIUS Start and Stop pair. The R-P
21 session ID corresponds to an R-P connection. A new R-P connection due to intra-PDSN handoff
22 between PCFs would result in a new RP session ID. The MSID is used to select the proper UDR
23 after an intra-PDSN handoff. One R-P session ID may be associated with multiple simultaneous
24 NAI, IP pairs in the PDSN.

25
26 Airlink records are only associated with an R-P session. The PDSN matches the R-P session ID
27 in the airlink record to the R-P session ID in the appropriate UDR(s). If more than one UDR
28 matches, the actions are applied to all UDRs.

29
30 Some events cause certain UDR fields to change in the middle of a session. When this
31 happens, one of two approaches must be taken: (1) a container attribute as specified in Annex C
32 is created and the changed fields embedded in that container attribute. This allows the UDR to
33 continue to accumulate accounting information after an event without transmitting a RADIUS
34 message. Alternatively (2), the PDSN may send a RADIUS-Stop record to capture accounting
35 data before the event, followed by a RADIUS-Start record with the new fields values. In fact, a
36 PDSN may send a RADIUS-Stop and RADIUS-Start anytime during a single session as long as
37 no accounting data is lost. In these cases, the PDSN shall send the same Correlation Session ID
38 in both the RADIUS-Stop and RADIUS-Start records.

39
40 The subsequent sections specify the actions to take for each event.

41 **9.5.1 R-P Session Setup Airlink Record Arrives**

42 When the PDSN receives a Connection Setup Airlink record as a result of a handoff, then the
43 PDSN shall:

- 44
- 45 ▪ Use the previous MSID to find the correct UDR.
- 46 ▪ Either, create a new Container attribute in the UDR with Container-Reason ← Handoff,
47 Event-timestamp ← current time and attributes D2, D3, D4, G1, G2, G3, G8-14.
 - 48 ▪ Use information received from the RN to fill the following fields: D2, D3, D4.
 - 49 ▪ Zero fields G1, G2, G3, G8-14.
- 50 ▪ Or, send a RADIUS Accounting-Request Stop record based on the current UDR.
 - 51 ▪ Use information received from the RN to fill the following fields: D2, D3, D4.
 - 52 ▪ Zero fields G1, G2, G3, G8-14.

- 1 ▪ Send a RADIUS Accounting-Request Start record containing a new Accounting Session
2 ID and same Correlation ID.

3

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

6

- 7 ▪ A1, D3, and D4.

8

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

10 **9.5.2 Packet Data Service Establishment**

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

13

- 14 ▪ Fill the following fields: B1, B2, C1, C2, D1, D2, F11, F12, H1, I1, I2, and I3.
15 ▪ Zero fields G1, G2, G3, G8-14.
16 ▪ Send a RADIUS Accounting-Request Start record based on the current UDR.

17 **9.5.3 Packet Data Service Termination**

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

19

- 20 ▪ Send a RADIUS Accounting-Request Stop record based on the current UDR.
21 ▪ Delete the UDR after receiving acknowledgment from the RADIUS server that it has
22 successfully received the UDR.

23 **9.5.4 User Data Through PDSN**

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

25

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

27

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

29

- 30 ▪ Increment G2 by the number of octets of data.
31 ▪ Increment G14 by the number of octets received at the PPP layer

32 **9.5.5 Active Start Airlink Record Arrives**

33 When the PDSN receives an Active Start airlink record from the RN, the PDSN performs the
34 following.

35

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

37

- 38 • Set UDR fields according to airlink record: E1 ← e1, F1-F10 ← f1-f10, I4 ← i4

39

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

41

- 42 ▪ Either, create a new Container attribute in the UDR with Container-Reason ← Parameter
43 change, Event-timestamp ← current time and attributes E1, G1, G2, G3, G8-G14, I4.
44 ▪ Set UDR fields according to airlink record. E1 ← e1, I4 ← i4 and zero fields G1, G2, G3,
45 G8-14.
46 • Or, send a RADIUS Accounting-Request Stop record based on the current UDR.
47 • Set UDR fields according to airlink record. E1 ← e1, I4 ← i4 and zero fields G1, G2, G3,
48 G8-14.
49 • Send a RADIUS Accounting-Request Start record based on UDR containing a new
50 Accounting Session ID and same Correlation ID.

1
2 Finally, the PDSN shall increment G9 by one.

3 **9.5.6 Active Stop Airlink Record Arrives**

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

- 5
6
 - Increment G8 by the value of g8.

7 **9.5.7 SDB Airlink Record Arrives**

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

9
10 If the mobile originated / mobile terminated indicator is equal to one (mobile terminated SDB),
11 the PDSN shall:

- 12
13
 - Increment G10 by the value of g10.
 - Increment G12 by one.

14
15
16 If the mobile originated / mobile terminated indicator is equal to zero (mobile originated SDB),
17 the PDSN shall:

- 18
19
 - Increment G11 by the value of g10.
 - Increment G13 by one.

21 **9.5.8 Interim Record Trigger**

22 When the Interim Record Trigger initiates, the PDSN shall send a RADIUS Accounting-Request
23 Interim record based on current UDR. The Interim Record Trigger is an operator configurable
24 time interval since the last RADIUS accounting record was sent for a UDR.

25 **9.5.9 Stop Record Trigger**

26 Additional conditions may trigger a RADIUS Accounting Request Stop records to be sent by the
27 PDSN such as:

- 28
29
 - When the size of the RADIUS accounting record to be sent for the UDR exceeds an operator
30 configurable threshold.
 - Any time during a session as an implementation dictates.

31
32
33 When the Stop Record Trigger initiates, the PDSN shall send a RADIUS Accounting-Request
34 Stop record based on current UDR and fields G1, G2, G3, G8-14 are zeroed. Immediately
35 afterwards, the PDSN shall send a RADIUS Accounting-Request Start record based on current
36 UDR containing a new Accounting Session ID and same Correlation ID.

37 **9.5.10 Time of Day Timer Expires**

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

41
42 When an accounting time of day timer expires, the PDSN shall:

- 43
44
 - Either, create a new Container attribute in the UDR with Container-Reason ← Tariff
45 Boundary, Event-timestamp ← current time and attributes G1, G2, G3, G8-G14.
 - Zero fields G1, G2, G3, G8-14.
 - Or, send a RADIUS Accounting-Request Stop record based on the current UDR.
 - Zero fields G1, G2, G3, G8-14.

- 1
 - 2
 - 3
- Send a RADIUS Accounting-Request Start record based on current UDR containing a new Accounting Session ID and same Correlation ID.

1 **10 R-P Interface**

2 The PDSN and RN will support the R-P interface defined as A10 and A11 interfaces of A.S0001.

3

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 PDSN.
- 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 terminate the R-P session if the MS terminates a packet data session or the MS indicates that is no longer reachable.
- 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.
- The RN will pass octets between the mobile station and PDSN without any framing conversion.

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 will have the capability to determine when an MS enters its coverage area.
- The RN will 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 will release and re-establish 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 the same PPP 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 will immediately establish a new R-P session to a new PDSN.

Specific handoff procedures for the R-P are not called out in this specification but can be found in A.S0001.

1 **12 Air Interface**

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

3

- 4 • C.S0001-A Introduction to cdma2000 Standards for Spread Spectrum Systems
- 5 • C.S0002-A Physical Layer Standard for cdma2000 Spread Spectrum Systems
- 6 • C.S0003-A Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum
- 7 Systems
- 8 • C.S0004-A Signaling Link Access Control (LAC) Standard for cdma2000 Spread
- 9 Spectrum Systems
- 10 • C.S0005-A Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum
- 11 Systems

12

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

2 Interoperability between HA and PDSN/FA implementations is a major goal of this specification.
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 nor
8 does it apply to mobile stations using collocated COA for Mobile IP.

9 10 **ISAKMP Fixed Header**

11
12 The PDSN in this specification shall use a Major and Minor Version of 0. The HA shall
13 minimally accept Major and Minor Version of 0. This specification does not make use of
14 the Fixed Header Authentication (A) bit. Subsequent revisions of this specification 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 Phase 1
19 ISAKMP, a Quick Mode for all Phase 2 exchanges, or an Informational exchange to pass
20 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 Security
25 Payload will specify a situation of SIT_IDENTITY_ONLY. Phase 2 ISAKMP Security
26 Payloads will specify situations of SIT_IDENTITY_ONLY for all cases where privacy or
27 only authentication applies (as outlined in the PDSN and HA "IP Security" sections of the
28 Specification).

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 shall
34 propose ISAKMP to the HA for the Phase 1 ISAKMP SA. Service provider owned HAs
35 will support IPsec ESP (using 3DES) for the ISAKMP SA. Non service provider owned
36 HA security policies are outside the scope of this specification, but may reasonably be
37 expected to support 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 be
41 required. The PDSN and HA shall propose either IPsec AH for message authentication,
42 or IPsec ESP for message privacy. The PDSN may choose to use both ESP and AH.

43
44 Mobile IP registration control packets and IP in IP tunneled packets may be protected by
45 IPsec AH or ESP (or both). Security policies to be used between PDSN and HA in this
46 specification will be dictated by the home network not the access provider network. The
47 PDSN shall propose two proposals, IPsec ESP and AH. Service provider owned HAs
48 shall propose only one Proposal, and the PDSN shall accept this proposal.

49
50 The Home RADIUS may deliver a User Profile to the Foreign RADIUS and PDSN that
51 indicates whether security should be supported for IP in IP packets. If the Home
52 RADIUS indicates a request for no security on the IP in IP tunneled packets, the PDSN
53 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

The SPI shall be four octets.

Transform Payload:

The PDSN shall minimally support the ESP_3DES transform for IPsec ESP, and both the HMAC-MD5 and HMAC-SHA transforms for IPsec AH. Service provider 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 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 that 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 Specification.

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

1 **Delete Payload**

2

3

4

5

6

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 service provider 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 service provider network may have a unique certificate which will be
4 configured into the PDSN and HA. The method of configuration of certificates is outside the
5 scope of this specification.

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

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

14 **Certificates for PDSNs and HAs**

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

18
19 `cdma2000.service-provider-name`

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

24
25 The PDSN and HA shall use the SHA-1 as a hash function and either the RSA or DSA signing
26 algorithm, as specified in RFC 2459 to verify a certificate. The private network or ISP shall
27 provide the public key and Distinguished Name of the certificate.

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

30
31 `cdma2000. service-provider-name.PDSN.service-provider-identifier`
32 `cdma2000. service-provider-name.HA.service-provider-identifier`

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

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

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

40 **CA Certificates**

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

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

50
51 The method by which service-providers exchange their CA certificates, as well as of providing
52 certificates into PDSNs and HAs, is outside the scope of this specification.

53

1 **Certificate Revocation List (CRL)**

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

6
7 Service-providers shall exchange revoked certificate information (e.g., serial number). The
8 frequency of the exchange is outside the scope of this specification.

9
10 Possession of a certificate does not imply service since the RADIUS and Mobile IP functions still
11 control the user obtaining service, as well as the HA allowing access to the PDSN.

12
13 The CA certificate shall indicate the carrier CA as Issuer of the CRL. The DN of the Issuer shall
14 be of form:

15 cdma2000.service-provider-name

16
17
18 CRLs exchanged between service provider shall use the SHA-1 as a hash function and either
19 the RSA and DSA signing algorithm as specified in RFC 2459.

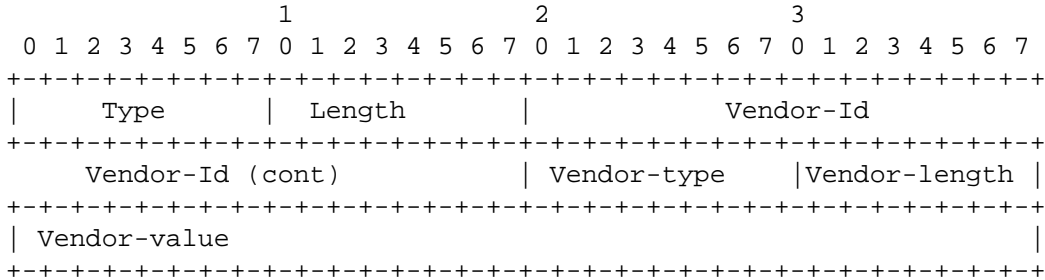
20
21 CRL extensions shall not be supported.

22
23 The method of exchanging CRLs between service providers, or to conveying certificates client
24 private network or partnering ISP, as well providing this information into PDSNs and HAs, is
25 outside the scope of this specification.

26

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

2 This is the general Vendor Specific Format for all 3GPP2 RADIUS attributes. The type and
 3 vendor ID are the same for every attribute. The vendor type, vendor length, and value are
 4 specified below.



Type = cdma specific
 Length >= 9

5
 6 **Figure 9: 3GPP2 RADIUS Attribute Format**

7
 8 **Type:** 26

9
 10 **Length:** greater than 9

11
 12 **3GPP2 Vendor ID:** 5535

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
 22
 - 23 1. IPsec SA already established with the HA
 - 24 2. IPsec SA not established and a certificate exists for the HA
 - 25 3. IPsec SA not established but the PDSN has a root certificate for the HA
 - 26 4. IPsec SA not established, no certificate exists for the HA, but a configured
 27 pre-shared IKE secret exists
 - 28 5. IPsec SA not established, no certificate exists for the HA, and no configured
 29 pre-shared IKE secret exists

30
 31 **Security level:** Indicates the type security the home network authorizes and optionally appears
 32 in the Access-Accept.

33
 34 Vendor-Type = 2
 35 Vendor-Length = 6
 36 Vendor-Value =

- 37
 38
 1. IPsec for registration messages

- 1 2. IPsec for tunnels
- 2 3. IPsec for tunnels and registration messages
- 3 4. No IPsec security

4
5 **Pre-shared secret:** A pre-shared secret for IKE that optionally appears in an Access-Accept.

- 6
- 7 Vendor-Type = 3
- 8 Vendor-Length = 3 or greater
- 9 Vendor-Value = binary value of the pre-shared key

10
11 **Reverse Tunnel Specification:** Indicates the style of reverse tunneling that is required, and optionally appears in an Access-Accept.

- 12
- 13
- 14 Vendor-Type = 4
- 15 Vendor-Length = 6
- 16 Vendor-Value =
- 17
- 18 0 - Reverse tunneling is not required
- 19 1 - Reverse tunneling is required

20
21 **Differentiated Services Class Option Attribute:** The Home RADIUS server authorizes differentiated service via the Differentiated Services Class Options Attribute, and optionally appears in an Access-Accept.

- 22
- 23
- 24
- 25 Vendor-Type = 5
- 26 Vendor-Length = 6
- 27 Vendor-Value 0=Best Effort
- 28 10=AF11
- 29 12=AF12
- 30 14=AF13
- 31 18=AF21
- 32 20=AF22
- 33 22=AF23
- 34 26=AF31
- 35 28=AF32
- 36 30=AF33
- 37 34=AF41
- 38 36=AF42
- 39 38=AF43
- 40 46=EF

41
42 The above values are taken from [RFC 2597, RFC 2598]. There is no intention to convey the actual traffic specification parameters of the differentiated-services service.

43
44
45 **Home Agent Attribute:** The address of the Home Agent.

- 46
- 47 Vendor-Type = 7
- 48 Vendor-Length = 6
- 49 Vendor-Value = 4 octet IP address.

50
51

1 **Annex D**

2 3 Interim RADIUS Accounting

4
5 An Interim Accounting record (with Acct-Status-Type = Interim-Update (3)) shall contain all of the
6 attributes found in an Accounting Stop message with the exception of the Acct-Term-Cause
7 attribute. The values of the attributes in the Interim Accounting record shall be cumulative since
8 the Accounting-Request Start record.
9

10 Since the accounting information is cumulative, the PDSN should ensure that only a single
11 generation of an interim Accounting message for a given user and IP address is present in
12 retransmission queues at any given time.

13
14 The PDSN may add a random delay between Interim Accounting messages for separate
15 sessions. This will ensure that a cycle where all messages are sent at once is prevented.