

1 3GPP2 P.R0001
2 Version 1.0.0
3 Version Date: July 14, 2000
4



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

5 **Wireless IP**
6 **Architecture Based on IETF Protocols**

7

8

9

10

11

12

13

14

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.

15

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

1 PURPOSE..... 6

1.1 INTRODUCTION 6

1.2 SYSTEM DESIGN OBJECTIVES 6

2 GLOSSARY AND DEFINITIONS..... 7

2.1 ACRONYMS 7

2.2 DEFINITIONS..... 8

3 REFERENCES..... 10

3.1 MOBILE IP..... 10

3.2 PPP..... 10

3.3 DIFFERENTIATED SERVICES 10

3.4 RADIUS 11

3.5 IP SECURITY 11

3.6 TIA..... 11

3.7 TCP/IP 11

3.8 ITU-T..... 12

4 PACKET DATA SERVICE DESCRIPTIONS 12

4.1 ACCESS LAYER 13

4.2 DATA LINK LAYER..... 13

4.2.1 PPP 13

4.3 NETWORK LAYER 13

4.3.1 ADDRESS MANAGEMENT..... 14

4.3.2 QoS..... 14

4.3.3 IP MULTICAST..... 14

4.4 SECURITY..... 14

4.4.1 RADIO ACCESS SECURITY..... 15

4.4.2 IP NETWORK SECURITY..... 15

4.4.3 USER END-TO-END SECURITY..... 15

4.5 LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE (LAES) 15

4.6 EMERGENCY SERVICES..... 15

5 FUNCTIONAL MODEL..... 16

5.1 HOME AGENT (HA) 16

5.2 PACKET DATA SERVING NODE (PDSN) 16

5.3 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA) 17

5.4 PACKET CONTROL FUNCTION (PCF)..... 17

1	5.5	RADIO RESOURCES CONTROL (RRC)	18
2	5.6	MOBILE STATION	18
3	6	<u>GENERAL ARCHITECTURE</u>	19
4	6.1	OVERVIEW	19
5	6.2	PROTOCOL REFERENCE MODEL	21
6	6.3	SERVICE PROVIDER BOUNDARIES	22
7	6.4	LOGICAL INTERFACES	23
8	6.4.1	R-P INTERFACE	25
9	7	<u>ACCOUNTING</u>	27
10	8	<u>AAA PROTOCOL CONSIDERATIONS</u>	28
11	8.1	AAA PROTOCOL REQUIREMENTS	28
12	8.2	AAA PROTOCOL INTERWORKING	28
13	9	<u>SUPPORT OF DIFFERENTIATED SERVICES</u>	30
14	9.1	VERSION 1 QoS	30
15	9.1.1	MOBILE STATION TO RN	30
16	9.1.2	RN TO PDSN	30
17	9.1.3	PDSN TO IP NETWORK	30
18	9.1.4	PDSN TO RN	30
19	9.1.5	RN TO MOBILE STATION	30
20	9.2	VERSION 2 QoS	31
21	9.2.1	MOBILE STATION TO RN	31
22	9.2.2	DATA LINK LAYER	31
23	9.2.3	NETWORK LAYER	31
24	10	<u>REQUIREMENTS</u>	32
25	10.1	PDSN FUNCTIONS	32
26	10.1.1	CORE PDSN FUNCTIONS	32
27	10.1.2	INCREMENTAL PDSN FUNCTIONS FOR SIMPLE IP SERVICE	32
28	10.1.3	INCREMENTAL PDSN FUNCTIONS FOR MOBILE IP VERSION 1	32
29	10.1.4	INCREMENTAL PDSN FUNCTIONS FOR MOBILE IP VERSION 2	33
30	10.2	HA FUNCTIONS	33
31	10.2.1	HA FUNCTIONS FOR VERSION 1	33
32	10.2.2	INCREMENTAL HA FUNCTIONS FOR VERSION 2	34
33	10.3	AAA SERVER FUNCTIONS	34
34	10.3.1	SIMPLE IP	34
35	10.3.2	MOBILE IP VERSION 1	34
36	10.3.3	MOBILE IP VERSION 2	34

1 **10.4 MOBILE STATION FUNCTIONS 34**
2 10.4.1 CORE MOBILE STATION FUNCTIONS..... 34
3 10.4.2 INCREMENTAL MOBILE STATION FUNCTIONS FOR SIMPLE IP 35
4 10.4.3 INCREMENTAL MOBILE STATION FUNCTIONS FOR MOBILE IP VERSION 1 35
5 10.4.4 INCREMENTAL MOBILE STATION FUNCTIONS FOR MOBILE IP VERSION 2 35
6 **10.5 ACCOUNTING FUNCTIONS 35**

7 **ANNEX: FLOWS 36**

8 **A-1 SIMPLE IP SERVICE INITIATION AND TERMINATION WITH AAA ACCOUNTING..... 36**
9 **A-2: MOBILE IP SERVICE INITIATION 38**
10 **A-3 HANDOFFS BETWEEN RN WITHIN THE SAME PDSN 40**
11 **A-4 HARD HANDOFF BETWEEN PDSNS FOR MOBILE IP 42**
12 **A-5 SIMPLE IP SERVICE TERMINATED BY THE NETWORK..... 44**
13 **A-6 MOBILE IP SERVICE TERMINATED BY THE MOBILE STATION..... 45**
14 **A-7 MOBILE IP SERVICE TERMINATED BY THE NETWORK..... 48**
15 **A-8 DORMANT HANDOFF MAINTAINING SAME PDSN 50**
16
17
18

1		
2	Figure 1: Functional Model.....	16
3	Figure 2: IMT-2000 Architecture Model for Mobile IP	20
4	Figure 3: IMT-2000 Architecture Model for Simple IP.....	21
5	Figure 4: Protocol Reference Model for Simple IP.....	21
6	Figure 5: Protocol Reference Model for Mobile IP Control and IKE.....	22
7	Figure 6: Protocol Reference Model for Mobile IP User Data.....	22
8	Figure 7: Logical Interfaces for Home Agent in the Home Access Provider Network.....	23
9	Figure 8: Logical Interfaces Reference Model for Home Agent Dynamically Assigned in the	
10	Visited Access Provider Network (Version 2 Scenario)	24
11	Figure 9: Logical Interfaces Reference Model for Private Network Access with Mobile IP.....	24
12	Figure 10: Logical Interfaces Reference Model for Simple IP.....	25
13	Figure 11: Accounting Architecture.....	27
14	Figure 12: AAA Protocol Interworking Architecture.....	29
15	Figure 13: A-1 Simple IP Service Initiation with AAA Accounting	37
16	Figure 14: Mobile IP Service Initiation.....	39
17	Figure 15: Handoffs between RN within the Same PDSN	41
18	Figure 16: Hard Handoff between PDSNs for Mobile IP	43
19	Figure 17: Simple IP Service Terminated by the Network	45
20	Figure 18: Mobile IP Service Terminated by the Mobile Station	47
21	Figure 19: Mobile IP Service Terminated by the Network.....	49
22	Figure 20: Dormant Handoff Maintaining Same PDSN.....	51
23		

1 Purpose

1.1 Introduction

This is an informative document that describes the packet data system architecture for a third generation wireless system based on IMT-2000. The general capabilities for this system match those outlined in the ITU IMT-2000 requirements document Q.1701. As a general philosophy behind the design of this architecture, IETF protocols are employed whenever possible to minimize the number of new protocols required and to maximize the utilization of well accepted standards and hence the speed to market.

This document describes an architecture with two general services, local and public data network access and Private data network access, as well as two access methods, Simple IP and Mobile IP. Several advanced features such as security associations and dynamic address assignment, as well as accounting, are accomplished using IETF protocols.

The document begins by describing the services offered. It then describes a functional model and the general functions for each component. Finally, a physical model with the appropriate mappings and detailed requirements is provided. An annex attached provides general message flows.

The standardization of packet data service is anticipated to occur as a phased project. While this document primarily describes features that are required for Version 1, several requirements which are targeted for Version 2 are also described. These features are not deemed reasonable to standardize in the immediate term, but are intended to be future requirements. This document will be revised at a later date to more fully describe subsequent versions.

1.2 System Design Objectives

1. Support a wide range of addressing configurations
 - Support dynamic and static home address configurations
 - Support multiple simultaneous IP addresses
 - Allow for dynamic assignment of the Home Agent in the service provider network as a form of route optimization, as well as in the home IP network as a form of load balancing
2. Provide seamless roaming
 - Provide seamless service while requiring a formal customer-service relationship with one IMT-2000 service provider and only one data network provider (which may be the same provider)
 - Allow IP mobility for visitors whose home network may be an IMT-2000 network, ISP, or private network
 - Provide for secure compulsory tunneling services to home IP networks to avoid overhead on the air interface
3. Provide robust authentication and authorization services
 - Provide separation of access resource authentication and authorization services from those used for IP data resource services
 - Provide complete AAA support services (e.g., broker services, key distribution, registration optimization, address leasing, etc.)
4. Provide QoS support
 - Support differentiated services
5. Provide accounting services
 - Generate accounting data including information on QoS
 - Support reliable distribution and management of accounting information
 - Support accounting mechanisms to enable roaming

1 2 Glossary and Definitions

2 2.1 Acronyms

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

1 **2.2 Definitions**

2

3 Access Provider Network:

4

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

5 Broker AAA:

6

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

10 Broker AAA Network:

11

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

12 Home AAA:

13

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

14 Home Access Provider Network:

15

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

17 Home IP Network:

18

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,
 publicly accessible ISP network or an IMT-2000 network.

21

22 Local Network

23

24 An IP network that is directly connected to the PDSN (nominally, the serving IMT-2000
 service provider network).

25 Packet data service:

26

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

28 Packet data service option:

29

30 A service option provides a means between MS and RN to establish and maintain
 cdma2000 traffic channels for packet data service.

31 Packet data session:

32

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
 maintained.

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

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 remains.
6 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 R-P session:

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

15 Service Provider Network:

16 An IMT-2000 network operated by either the home access provider or the visited access
17 provider.

18 Visited Access Provider Network:

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

21 Visited AAA:

22 The AAA server that resides in the Visited Access Provider Network.

3 References

3.1 *Mobile IP*

Perkins, IPv4 Mobility, RFC 2002, May 1995.

Perkins, IP Encapsulation within IP, RFC 2003, October 1996.

Perkins, Minimal Encapsulation within IP, RFC 2004, October 1996.

Solomon, Applicability Statement for IP Mobility support, RFC 2005, October 1995.

Cong, Hamnlen, Perkins, The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006, October 1995.

Montenegro, Reverse Tunneling for Mobile IP, RFC 2344, May 1998.

Calhoun, Perkins, Mobile IP Foreign Agent Challenge/Response Extension, RFC xxxx, June 2000.

Calhoun, Perkins, Mobile NAI Extension RFC 2794 March 2000.

3.2 *PPP*

Simpson, The Point to Point Protocol (PPP), RFC 1661, July 1994.

Simpson, Mobile-IPv4 Configuration Option for PPP IPCP, RFC 2290, February 1998.

Simpson, PPP in HDLC-like Framing, RFC 1662, July 1994.

Friend, Schneider, PPP LZS-DCP Compression Protocol (LZS-DCP), RFC 1967, August 1996.

Rand, The PPP Compression Control Protocol (CCP), RFC 1962, June 1996.

Friend, Simpson, PPP Stac LZS Compression Protocol, RFC 1974, August 1996.

Woods, PPP Deflate Protocol, RFC 1979, August 1996.

Simpson, PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, August 1996.

McGregor, The PPP Internet Protocol Control Protocol (IPCP), RFC 1332, May 1992.

Pall, Microsoft Point-To-Point Compression (MPPC) Protocol, RFC 2118, March 1997.

Zorn, PPP LCP Internationalization Configuration Option, RFC 2484, January 1999.

3.3 *Differentiated Services*

Nichols, Blake, Baker, Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474, December 1998.

Blake, Black, Carlson, Davies, Wang, Weiss, An Architecture for Differentiated Services, RFC 2475, December 1998.

Heinanen, Baker, Weiss, Wroclawski, Assured Forwarding PHB Group, RFC 2597, June 1999.

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

2 **3.4 RADIUS**

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

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

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

10 **3.5 IP Security**

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

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

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

16
17 Harkins, Carrel, The Internet Key Exchange (IKE), RFC 2409, November 1998.

18 19 **3.6 3GPP2 and TIA**

20 P.S0001-A, Wireless IP Network Standard, July 2000.

21
22 A.S0001, Inter-operability Specification (IOS) for CDMA 2000 Access Network Interfaces,
23 December, 1999.

24
25 TIA/EIA/IS-707-A-1.12: cdma2000 High Speed Packet Data Service Option 33, December 1999.

26
27 C.S0001-A: Introduction to cdma2000 Standards for Spread Spectrum Systems, June 2000.

28
29 C.S0002-A: Physical Layer Standard for cdma2000 Spread Spectrum Systems, June 2000.

30
31 C.S0003-A: Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems,
32 June 2000.

33
34 C.S0004-A: Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum
35 Systems, June 2000.

36
37 C.S0005-A: Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems,
38 June 2000.

39
40 Mobile Identification Number (MIN) [TIA/EIA-41-E]

41
42 TIA/EIA/TSB-29-A, International Implementation of Cellular Radiotelephone Systems Compliant
43 with ANSI/EIA/TIA 553; September 1992

44 **3.7 TCP/IP**

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

46
47 Postel, User Datagram Protocol, RFC 768, August 1980

48
49 Internet Protocol, RFC 791, September 1981

50

1 Postel, Internet Control Message Protocol, RFC 792, September 1981

2

3 Transmission Control Protocol, RFC 793, September 1981

4

5 Braden, Requirements for Internet Hosts – Communication Layers, RFC 1122, October 1989

6 **3.8 ITU-T**

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

9

10 **4 Packet Data Service Descriptions**

11 This section provides a definition of the packet data service as viewed by a mobile user. Two
12 general services are provided to a mobile user by this architecture:

13

- 14 • Local and Public Network Access
- 15 • Private Network Access

16

17 Access to a local network is quite often identical to accessing the public Internet, however, this is
18 not a requirement (i.e., a service provider network may offer services on its own private IP
19 network).

20

21 These two services can be provided by either of the following two access methods:

22

- 23 • Simple IP: This refers to the access method in which the user is assigned a dynamic IP
24 address from a service access provider. The user may maintain its IP address within
25 some network dependent geographical area. When the user moves outside this
26 geographical area, the user will not be able to maintain the IP address.
- 27
- 28 • Mobile IP: This refers to the access method based on RFC 2002. The user may use
29 either a static or dynamic IP address belonging to its home IP network. The user will be
30 able to maintain its IP address even when it moves throughout the IMT-2000 network or
31 other networks.

32

33 Voluntary tunneling for both Mobile IP and Simple IP is outside the scope of this document. So,
34 although a mobile station may choose to employ a collocated Care of Address (COA), from the
35 IMT-2000 network point of view this is the same as Simple IP, and not addressed in this
36 document.

37

38 The roaming subscriber will be able to access these services from multiple IMT-2000 service
39 providers while maintaining a business relationship with only one IMT-2000 service provider. In
40 order for the network to deliver packets to the mobile station, the mobile station must establish
41 packet data session with the IMT-2000 network.

42

43 The requirements for the packet data reference model are organized as follows:

44

- 45 • Access Layer
- 46 • Data Link Layer
- 47 • Network Layer
- 48 • Security

1 **4.1 Access Layer**

2 The mobile station supports the appropriate radio access technology and signaling standards for
 3 the provider network to which it attaches. The access network will authenticate and authorize the
 4 mobile station for access service, establish a connection to the IMT-2000 network, and then
 5 initialize a data link layer. After the data link layer is established, network layer protocols and
 6 procedures are executed to establish the packet data session.

7
 8 The radio access signaling standards will support a single packet data service option for all IP
 9 services both Simple IP and Mobile IP . Therefore, an access signaling request to the radio
 10 network for a connection from the mobile station to the network will not indicate Simple IP or
 11 Mobile IP service, and differentiation of IP data services will occur at PPP or higher layers

12 **4.2 Data Link Layer**

13 The IMT-2000 network will support two types of data link layers

- 14
- 15 • PPP for Version 1 and 2
- 16 • Simple data link-layer protocol for Version 2

17 **4.2.1 PPP**

18 The PPP protocol will be in compliance with RFC 1661, and supports LCP, IPCP, PAP, and,
 19 CHAP. For Simple IP, CHAP is optional. For Mobile IP, CHAP should not be used.

20
 21 Van Jacobson TCP/IP header (RFC 1144) compression will be supported by the network and
 22 mobile station. The PPP compression control protocol (RFC 1962) is used to negotiate a PPP
 23 payload compression algorithm, will be supported by the network, and optionally by the mobile
 24 station.

25
 26
 27 A mobile station will only have one PPP link established at any given time in Version 1.

28
 29 For Mobile IP service, the mobile will not reset the higher layers when the mobile re-establishes
 30 PPP and successfully registers with the same IP address as a result of moving to a new serving
 31 area in the IMT-2000 network.

32 33 **4.3 Network Layer**

34 Two types of network access methods are defined:

- 35
- 36 • Mobile IP:
 - 37 • Local and Public Network Access: The Home Agent resides in the IMT-2000 service
 - 38 provider network, and authentication and authorization information is held and processed
 - 39 by either the IMT-2000 service provider network or a private network.
 - 40 • Private network access service: The Home Agent resides in a private network, and
 - 41 authentication and authorization information is held and processed in the private network.
 - 42 The private network will usually reside behind a firewall, and may possess a non-globally
 - 43 unique address space.
- 44 • Simple IP:
 - 45 • Local and Public Network Access: The IP address is dynamically assigned from the
 - 46 serving network, and Internet access is performed directly.
 - 47 • Private network access service: Identical to Local and Public Network Access with the
 - 48 addition of VPN software on the mobile station. Note: This service using Simple IP is
 - 49 outside the scope of this document.

1 Service selection occurs during PPP initialization or immediately thereafter during Mobile IP
 2 registration. A mobile station may request Simple IP service, and later request Mobile IP service
 3 by sending an Agent solicitation. The network will then provide both Mobile IP and Simple IP
 4 service to the mobile station.

5
 6 For Mobile IP, the IMT-2000 service provider network uses the NAI in the Mobile IP RRQ to
 7 determine the home IP network that contains AAA servers which authenticate and authorize
 8 service. The address of the Home Agent is determined by MIP RRQ, or, in the case of dynamic
 9 Home Agent assignment, by an AAA server. Mobile IP access will support a static Home Agent in
 10 Version 1, and additionally, a dynamically assigned Home Agent in Version 2. With dynamic
 11 Home Agent assignment, either the home IP network or visited access provider network may
 12 assign the Home Agent. The user may connect to multiple target networks at the same time. In
 13 this case, the user would have multiple IP addresses, one per target network. Access to a private
 14 network is via a security association with IPsec between the PDSN and Home Agent.

15
 16 For Mobile IP service, after PPP initialization, the IMT-2000 network will send Agent
 17 Advertisements to the mobile station. To initiate Mobile IP access, the mobile station will then
 18 perform Mobile IP registration. If no Mobile IP Registration is sent by the mobile to the IMT-2000
 19 network, and the network does not require CHAP for Simple IP service, then the IMT-2000
 20 network provides the user with Simple IP service.

21 For Simple IP, the network uses the NAI in CHAP, or optionally constructs an NAI from the IMSI,
 22 using E.212 codes to algorithmically determine NAI realm of the home network. The IMT-2000
 23 service provider may then use the NAI to access AAA servers in the network associated with the
 24 NAI, and may use the NAI for accounting purposes.

25 **4.3.1 Address Management**

26 A mobile may run multiple IP addresses over a PPP link, however, only one Simple IP address is
 27 supported on the link.

28 Mobile IP service will support statically and dynamically assigned home addresses. A mobile may
 29 indicate a request for a dynamic home address assignment in the Mobile IP RRQ, or a mobile
 30 may indicate a static address. Home addresses may be public or private (non-globally unique).
 31 The Home Agent and Foreign Agent must have publicly visible addresses.

32 For Simple IP service, the service provider network provides a dynamic public address, or a
 33 dynamic private address belonging to the access network.

34 **4.3.2 QoS**

35 QoS coordinated between the airlink and IP entities in the IMT-2000 network will not be provided
 36 in Version 1. IP entities in the IMT-2000 network should be able to provide Quality of Service
 37 based on Differentiated Services.

38 **4.3.3 IP Multicast**

39 In Version 1 the access network will not provide IP multicast services using a shared radio access
 40 channel. IP multicast service may be obtained via the use of IGMP.

41 **4.4 Security**

42 From the perspective of the mobile station, security is provided at three levels in this architecture:

- 43 • Radio access
- 44 • IP network
- 45 • User end to end security

1 **4.4.1 Radio Access Security**

2 Access Network security should support authentication of the mobile station to avoid security
3 breaches. In order to avoid casual eavesdropping, air interface encryption should be supported.

4 **4.4.2 IP Network Security**

5 For both Simple IP and Mobile IP access mechanisms, IP network authentication of the mobile
6 station is via a static security association between the mobile station and the home IP network.
7 For Mobile IP, the service provider network shall use the Foreign Agent Challenge to authenticate
8 and authorize the mobile station. For Simple IP the service provider network may use CHAP or
9 PAP to authenticate and authorize the mobile station; if the mobile station does not support CHAP
10 or PAP, there is no IP network authentication.

11 For the case of a mobile station whose home IP network is external to the service provider
12 network, the mobile station and home IP network will use a security association not known by the
13 service provider network to authenticate and authorize the mobile station. In some cases an AAA
14 broker will be used to process and/or forward security information between the service provider
15 network and the home IP network. Both proxy and non-proxy AAA servers may be supported.
16 AAA information between AAA servers may be encrypted. Depending on type of AAA server
17 involved, the AAA information may be further protected with signatures and additional encryption
18 via public key mechanisms within messages to protect the information from AAA brokers which
19 may not be totally trusted by either home IP networks or service provider networks.

20 IP security is able to provide integrity and encryption for Mobile IP registration packets as well as
21 user data packets. The service provider network only provides IP security for user data packets if
22 authorized by the home IP network. By default, the service provider network provides protection of
23 the Mobile IP registration packets, unless instructed by the home network to not do so.

24 Service provider networks may support statically configured keys, dynamic key distribution, or
25 certificates for security between the HA and FA. Security associations between Home and
26 Foreign Agent may exist within Mobile IP via the Mobile IP Foreign-Home Authentication
27 Extension, or may be provided via IPsec AH or ESP protocols. IKE and certificates may be
28 supported. Use of certificates requires a public key infrastructure. The home AAA server may be
29 able to distribute Foreign-Home Authentication Extension keys or a pre-shared key for IKE. The
30 ability to distribute a pre-shared key for IKE is an alternative to the Home and Foreign Agent
31 supporting certificates. Version 1 AAA servers will support hop by hop encryption, but not end to
32 end encryption of AAA attributes and data.

33 Other types of IP security keys may be distributed in Version 2 by AAA servers. These include the
34 Mobile IP MN-FA and MN-HA keys and SPI.

35 **4.4.3 User End-to-End Security**

36 The user may add additional security measures that are outside the scope of this document.

37 **4.5 Lawfully Authorized Electronic Surveillance (LAES)**

38 The packet data architecture shall support LAES for all packet services for both access methods,
39 Simple IP and Mobile IP. The PDSN will provide the access point to the user data stream. A
40 duplicate stream of packets will be sent to an authorized collection point. The packets will be
41 duplicated before any network level encryption is applied. The method of duplication and content
42 of the duplicated packets (user information or header only information) is yet to be determined.

43 **4.6 Emergency Services**

44 No special requirements for Emergency Services support for packet data have been identified for
45 Version 1.

5 Functional Model

The following overview provides definitions of functions needed to support packet data services. The mapping of these functions to physical network nodes is not described here. The relationship among them is shown in Figure 1.

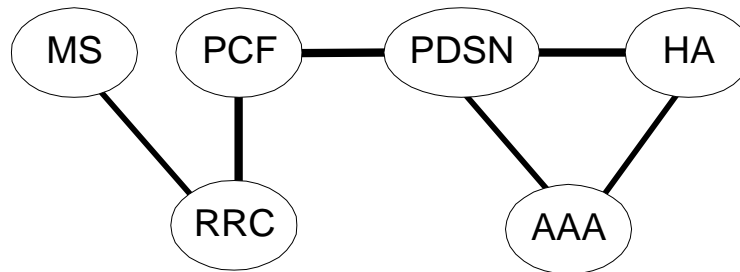


Figure 1: Functional Model

5.1 Home Agent (HA)

- Authenticate Mobile IP registrations from the mobile station
- Redirect packets to the Foreign Agent, and optionally receive and route reverse tunneled packets from the Foreign Agent
- Optionally, establish, maintain, and terminate secure communications to the PDSN (as Mobile IP Foreign Agent) using IKE procedures or the Mobile IP Foreign-Home Authentication Extension. These security associations may be configured statically or dynamically.
- Receive provisioning information from the AAA for users
- Optionally, assigns a dynamic home address

5.2 Packet Data Serving Node (PDSN)

- Establish, maintain, and terminate PPP session to the mobile station
- Assign/provide IP address for Simple IP. The dynamic address may be chosen by the PDSN or AAA.
- Support Foreign Agent functionality
- Initiate authentication, authorization, and accounting to the AAA for the mobile station packet data session.
- For Simple IP, map the mobile station IP address with a unique layer 2 connection used to communicate with the PCF. For Mobile IP, map the mobile station IP and HA addresses with a unique link layer identifier used to communicate with the PCF.
- In Version 2 for Mobile IP, optionally, interact with a previous PDSN to support handoffs between PDSNs that does not involve the home IP network
- Optionally, establish, maintain, and terminate secure communications to the Home Agent using IKE procedures or the Mobile IP Foreign-Home Authentication Extension. These security associations may be configured statically or dynamically.

- 1 • Receive user profile parameters from the AAA for mobile station. The user profile may
- 2 contain differentiated services and security.
- 3 • Record usage data, receive accounting information from the PCF, correlate to generate
- 4 the accounting information, and relay the correlated information to the AAA
- 5 • Route packets to IP networks or directly to the HA in the case of reverse tunneling
- 6 • Interact with the PCF to establish maintain and terminate the layer 2 connection between
- 7 PCF and PDSN.
- 8 • Interact with the serving PCF and the target PCF to maintain PPP session to the mobile
- 9 station as part of the hard handoff or dormant handoff.
- 10 • Monitor the source addresses of packets received from mobile stations. When packets
- 11 are received which have source addresses not assigned or registered to the mobile
- 12 station, the PDSN shall discard the packets and restart PPP to the mobile station.
- 13 • Mark and process packets as necessary according to the QoS profile
- 14 • Optionally send Agent Advertisement(s) if the PCF indicates the mobile station has
- 15 undergone a dormant handoff.

16 **5.3 Authentication, Authorization, and Accounting (AAA)**

- 17 • AAA in service provider network
 - 18 • Pass authentication requests from the PDSN to the home IP network, and
 - 19 authorization responses from the home IP network to the PDSN
 - 20 • Store accounting for the mobile station from the PDSN, and optionally forward to a
 - 21 broker or home IP network.
 - 22 • Provide a user profile and QoS information to the PDSN as received from the home
 - 23 IP network
 - 24 • Optionally, assign dynamic IP address for Simple IP services
 - 25 • Version 2: For Mobile IP, optionally, interact with a previous PDSN to support
 - 26 handoffs between PDSNs that does not involve home IP network
 - 27 • Version 2: For Mobile IP, dynamically identify a HA and assign a user to that HA
- 28 • AAA in a home IP network
 - 29 • Authenticate and authorize the mobile station based on requests from the local AAA.
 - 30 These involve either CHAP for Simple IP or the Foreign Agent Challenge from Mobile
 - 31 IP.
 - 32 • Optionally provide keying information to the HA and local AAA. This keying
 - 33 information may be used for the
 - 34 • Pre-shared key for IKE or the Mobile IP Foreign-Home Authentication Extension
 - 35
 - 36 • Provide a user profile and QoS information to the PDSN
 - 37 • Version 2: For Mobile IP, dynamically identify a HA and assign a user on that HA
- 38 • AAA in a broker network
 - 39 • Forward requests and responses between service provider network and the home IP
 - 40 network which do not have direct bilateral associations. Three modes of broker
 - 41 operation are possible:
 - 42 • Non-transparent: The broker AAA examines requests and responses, and
 - 43 creates new requests and responses. This would most likely occur if the broker
 - 44 AAA network assumes financial responsibility to the serving network.
 - 45 • Transparent: The broker AAA relays requests and responses and does not create
 - 46 new requests and responses.
 - 47 • Redirection: The broker AAA refers the service provider to another AAA
 - 48 • Optionally, verify certificates when passed in AAA requests between home and
 - 49 serving networks

50 **5.4 Packet Control Function (PCF)**

- 51 • Establish maintain and terminate layer 2 connection to the PDSN

- 1 • Interact with PDSN to support dormant handoff
- 2 • Maintain knowledge of radio resource status (e.g. active, dormant)
- 3 • Buffer packets arriving from the PDSN, when radio resources are not in place or are
- 4 insufficient to support the flow from the PDSN
- 5 • Communicate with the RRC to request and manage radio resources in order to relay
- 6 packets to and from the mobile station
- 7 • Relay packets to and from the PDSN
- 8 • As part of the hard handoff to another RRC, forward serving PCF information to the target
- 9 PCF to re-establish the packet data session to the PDSN
- 10 • Map mobile station ID and connection reference to a unique layer 2 connection identifier
- 11 used to communicate with the PDSN
- 12 • Collect and send airlink related accounting information to the PDSN

13 **5.5 Radio Resources Control (RRC)**

- 14 • Optionally support authentication and authorization of the mobile station for radio access
- 15 • Optionally support air interface encryption to the mobile station
- 16 • Establish, maintain, and terminate radio resources for the exchange of packets between
- 17 the mobile station and the PCF
- 18 • Maintain knowledge of radio resource status (e.g., active, dormant)
- 19 • Broadcast packet zone ID in the system overhead message

20 **5.6 Mobile Station**

- 21 • Establish, maintain, and terminate a data link protocol to the PDSN
- 22 • Optionally support air interface encryption to the RRC
- 23 • Optionally support Mobile IP and Simple IP
- 24 • Request appropriate radio resources from the network for the exchange of packets
- 25 • Maintain knowledge of radio resources (e.g., active, dormant) for packet session
- 26 • Buffer packets from the mobile applications when radio resources are not in place or are
- 27 insufficient to support the flow to the network
- 28 • If while dormant, detect a change in the packet zone ID, system ID, or network ID, send
- 29 an Origination message to the RRC to initiate dormant handoff.
- 30 • Version 2: For Mobile IP, optionally support handoffs between PDSNs that does not
- 31 involve the home IP network
- 32 • In Version 2 For Mobile IP, accept a HA dynamically assigned by the AAA in the service
- 33 provider network or home IP network.
- 34 • For Simple IP, accept an IP address dynamically assigned by the PDSN or the AAA in the
- 35 service provider network
- 36 • For Mobile IP, use a static home address, or accept a dynamically assigned home
- 37 address

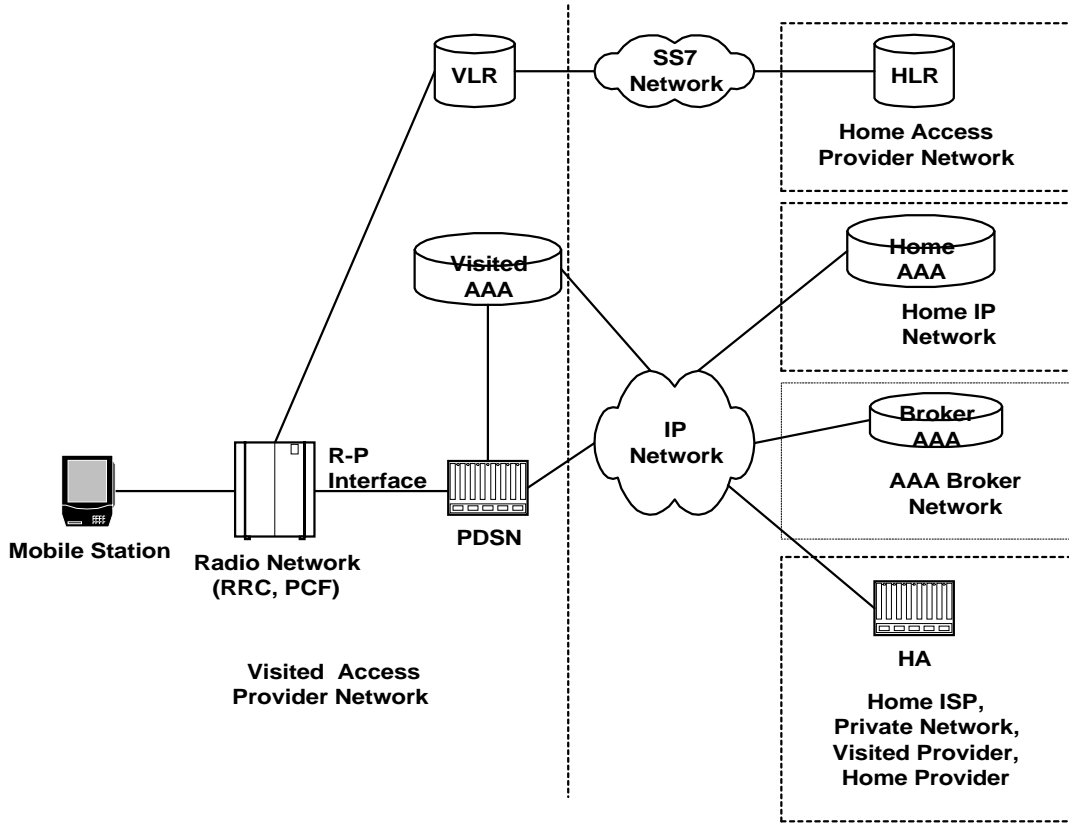
1 **6 General Architecture**

2 **6.1 Overview**

3 The functions of the IMT-2000 entities defined in the functional model may now be used to
4 generate architecture models. The mobile station gains access to a service provider network
5 using the air interface to connect to the Radio Network (RN). A mobile station may access only
6 one service provider network at a time. The service provider network may be the user's home
7 access provider or, in roaming cases, the visited access provider network is used. Access
8 mobility management is achieved using existing air interface procedures that include interactions
9 with Visited Location Registers (VLR) and Home Location Registers (HLR). Information about
10 access service parameters are maintained in the access service profile stored in the HLR and
11 cached in the VLR while the mobile station is registered in the service provider access network.
12 There is an open interface defined between the Radio Network and the PDSN known as the R-P
13 interface. The PDSN interacts with the local or visited AAA server and with other servers using IP
14 protocols within the IP Network. A Protocol Reference Model shows the control and user data
15 protocol relationships among the mobile station, RN, PDSN, end host, and, in the case of mobile
16 IP, the HA. The servers contacted by the PDSN or local AAA server may reside in other IP
17 domains and be operated by other IMT-2000 operators, ISPs, or Private Networks. Other parts of
18 this section describe service provider boundaries and logical interfaces among different boundary
19 configurations.

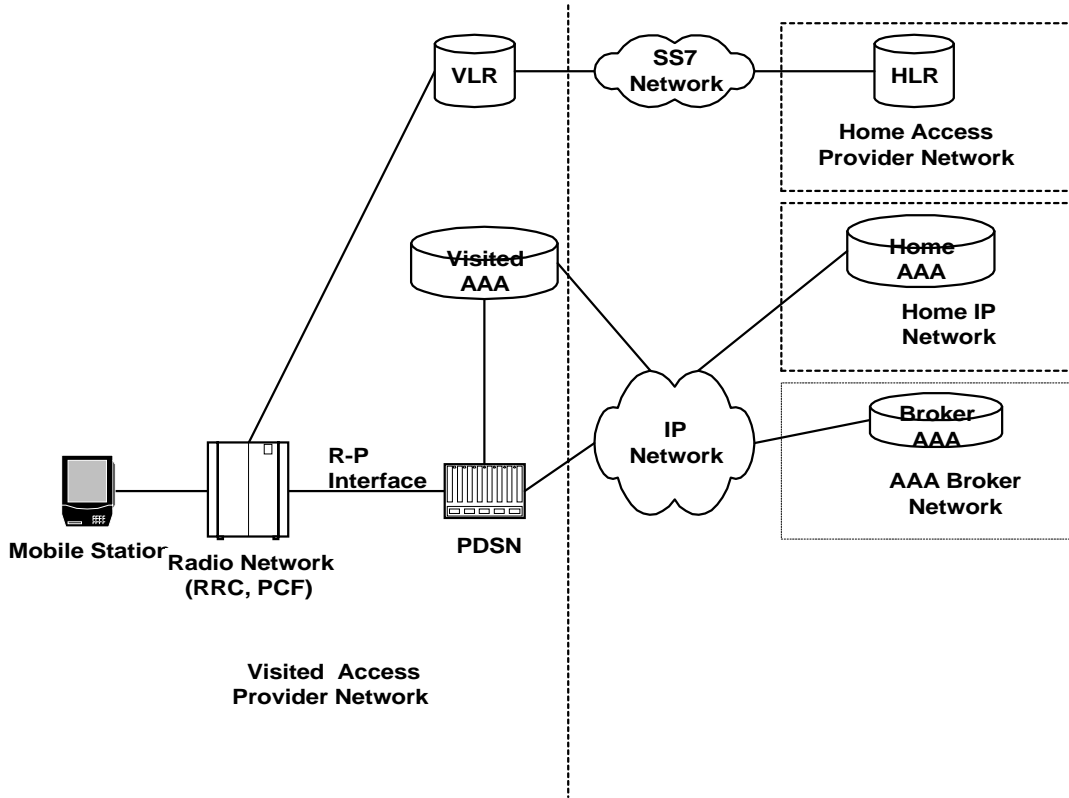
20
21 Figure 2 shows an IMT-2000 network architecture for Mobile IP. Figure 3 shows an IMT-2000
22 network architecture for Simple IP. For Simple IP, the Home Agent is not required, but interaction
23 with a AAA server in the home network IP network is shown as might be used in the roaming
24 case.

25
26 The PDSN in these architectures does not exactly map to the PDSN defined in the ITU document
27 Q.1711. In this architecture, the IP mobility management between PDSNs, and the interfaces to
28 other IP network elements in the architecture, are based on IETF protocols. The PCF functionality
29 focuses on aspects of the air link unique to wireless data. Functions that are defined in the PCF
30 and RRC must remain on one side of the R-P interface while functions defined in the PDSN, HA,
31 and AAA must remain on the other side of the R-P interface.



1
2
3

Figure 2: IMT-2000 Architecture Model for Mobile IP



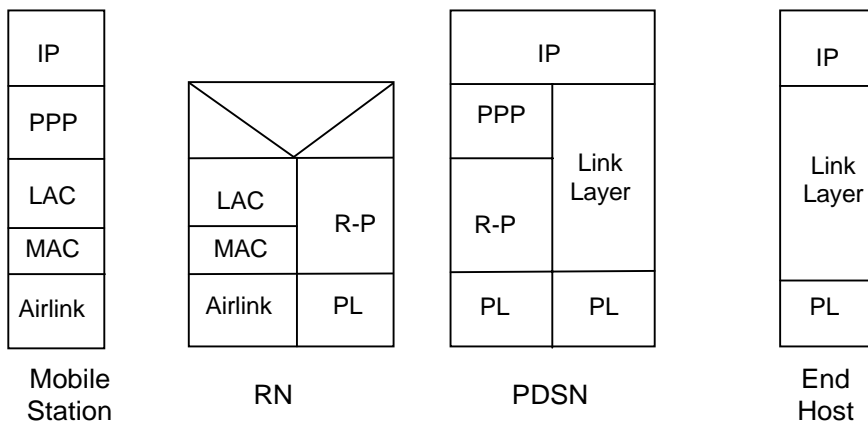
1
2
3

Figure 3: IMT-2000 Architecture Model for Simple IP

4 **6.2 Protocol Reference Model**

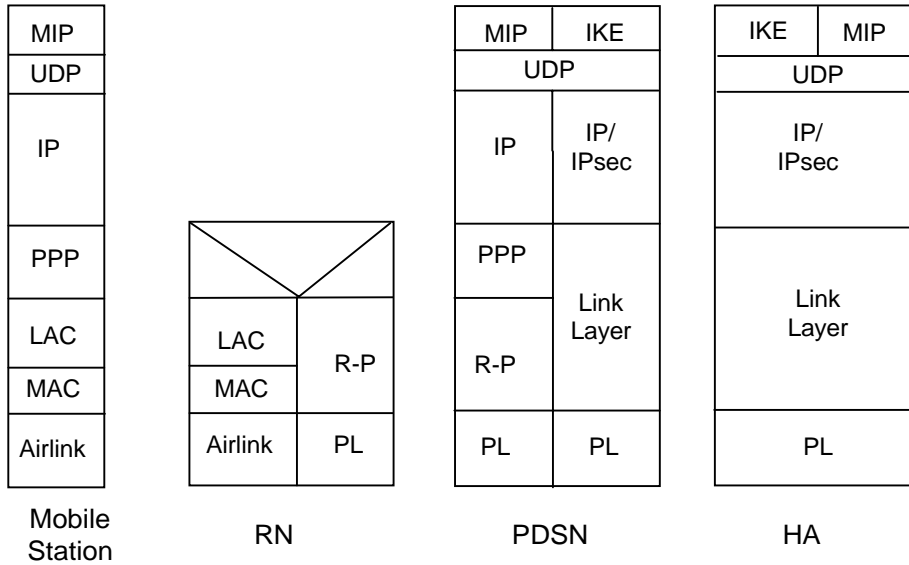
5
6
7

A protocol reference model for Simple IP and Mobile IP control is depicted in Figures 4 and 5, respectively. A protocol reference model for Mobile IP user data is depicted in Figure 6.



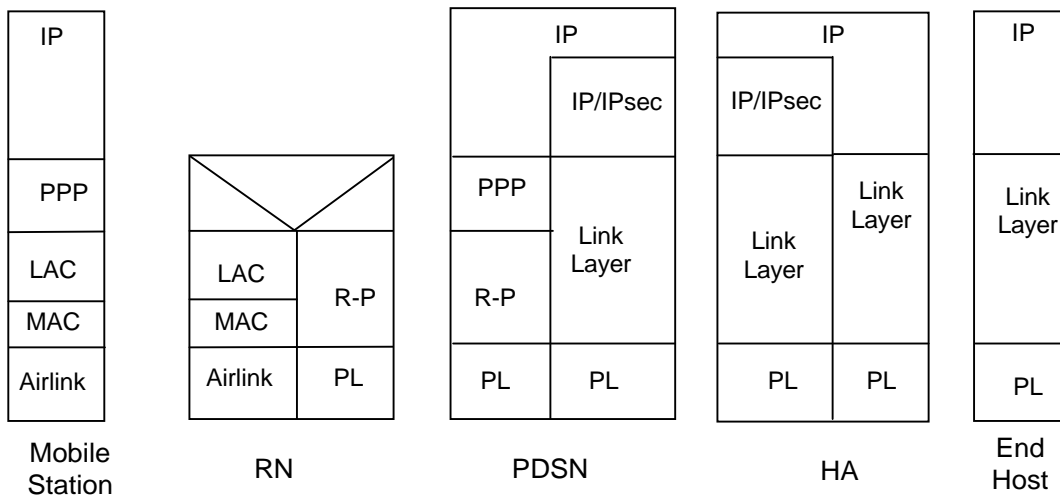
8
9

Figure 4: Protocol Reference Model for Simple IP



1
2
3
4
5

Figure 5: Protocol Reference Model for Mobile IP Control and IKE



6
7
8
9

Figure 6: Protocol Reference Model for Mobile IP User Data

6.3 Service Provider Boundaries

The mobile station retains one business relationship with a service provider network for access service. The mobile station ID (e.g., IMSI) identifies the mobile station to that network. The mobile station may associate with one or more home IP networks such as private networks or home ISPs for data service. These networks identify the mobile user by an NAI. Broker networks may be involved in the support of AAA messaging and functions between the AAA server residing in the

10
11
12
13
14
15

1 service provider network and the AAA server residing in the home IP network. The broker
 2 networks identify the mobile user via the NAI.

3
 4 For the non-roaming case the Visited AAA, VLR, and HLR belong to the home access provider
 5 network. The HA and home AAA may be part of a different home IP network, or may belong to the
 6 home access provider network.

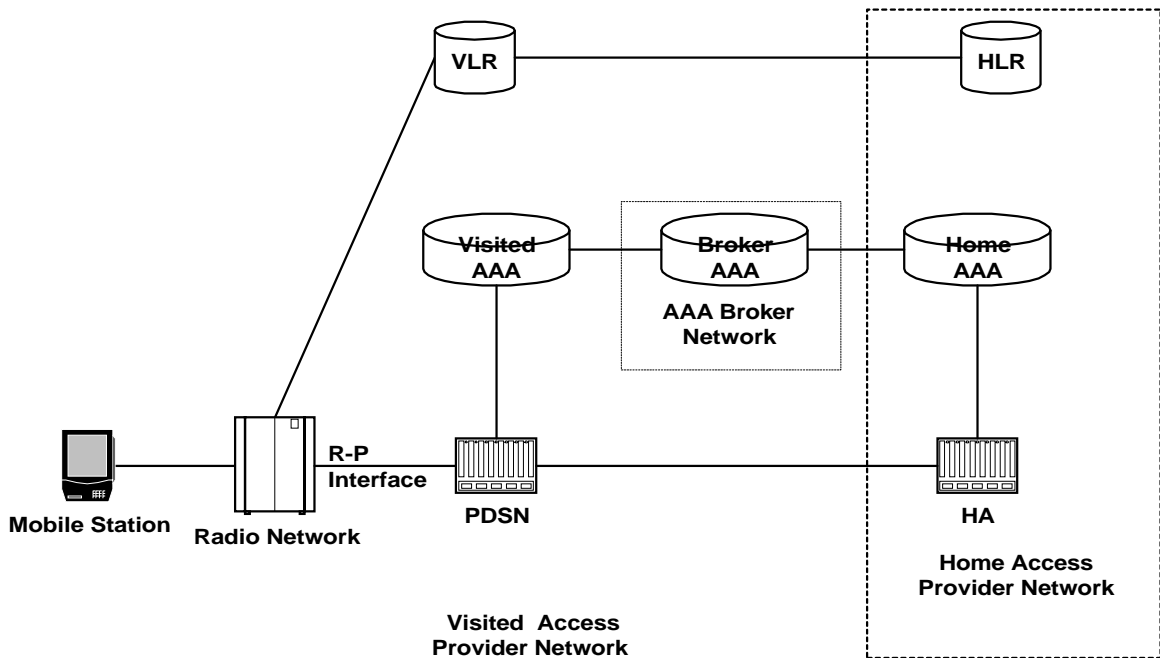
7
 8 For the roaming case, the associations of the entities with the home and visited network are as
 9 follows:

- 10
- 11 • The PDSN will reside in the service provider network.
- 12 • The PDSN will be associated with an AAA server in a service provider network.
- 13 • The Home Agent may reside in either a service provider network or external network.
- 14 • The Home Agent will have an associated AAA server in the network in which it resides.
- 15 • The mobile station will have a business relationship with its home IPnetwork
- 16 • The HLR will reside in the mobile station's home service provider network.
- 17 • The VLR will reside in the visited access service provider network.

18
 19 As stated above, for Simple IP Service, the HA will not be required.

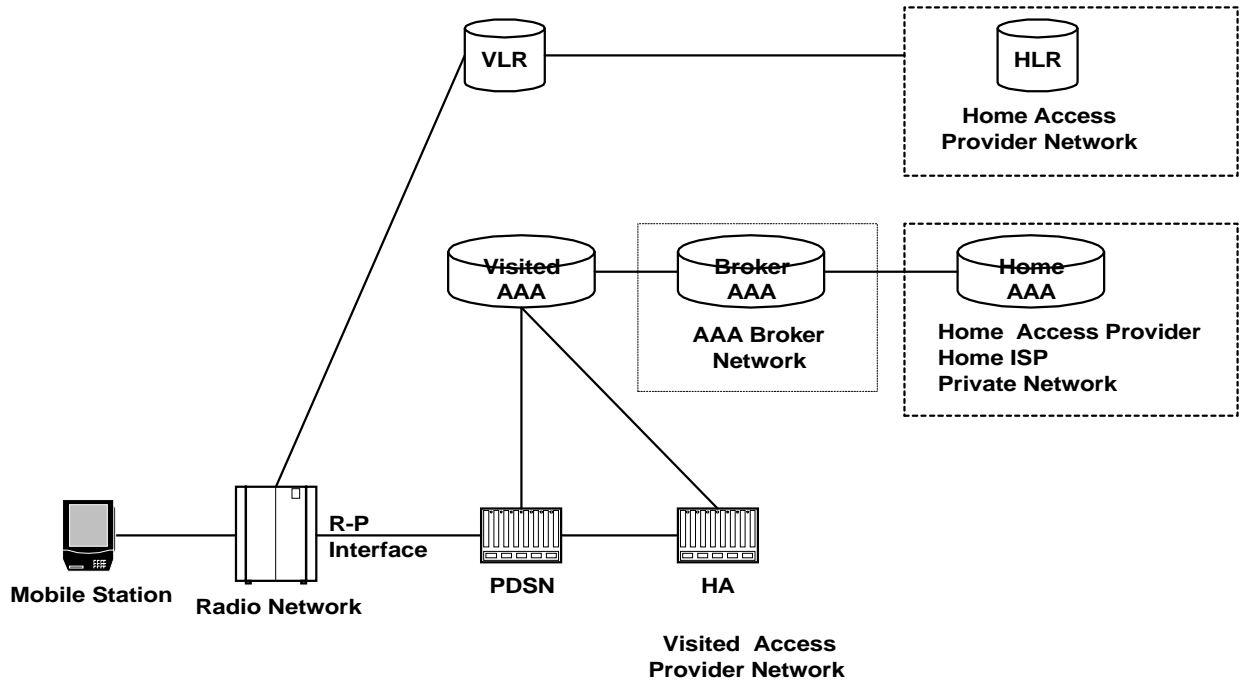
20 **6.4 Logical Interfaces**

21 Figures 7 and 8 show logical network reference models for Mobile IP with peer to peer interfaces
 22 when the Home Agent is in the home and visited access service provider networks, respectively.
 23 (Figure 8 case applies for Version 2). Figure 9 shows the case when the Home Agent is in a
 24 private network, and the PDSN tunnels through a firewall to the Home Agent using IPsec. Note:
 25 Service Level Agreements and configurations of firewalls are outside the scope of this document.
 26 Figure 10 shows the logical network reference model for Simple IP.



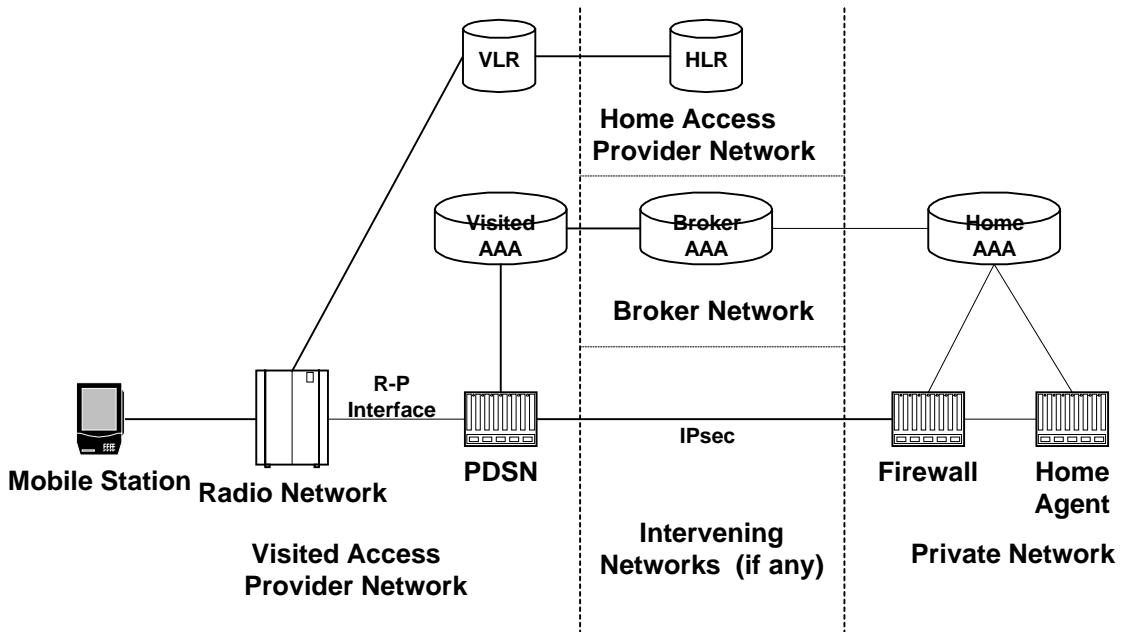
28
 29
 30 **Figure 7: Logical Interfaces for Home Agent in the Home Access Provider Network**

1



2
3
4
5
6
7

Figure 8: Logical Interfaces Reference Model for Home Agent Dynamically Assigned in the Visited Access Provider Network (Version 2 Scenario)



8
9
10
11

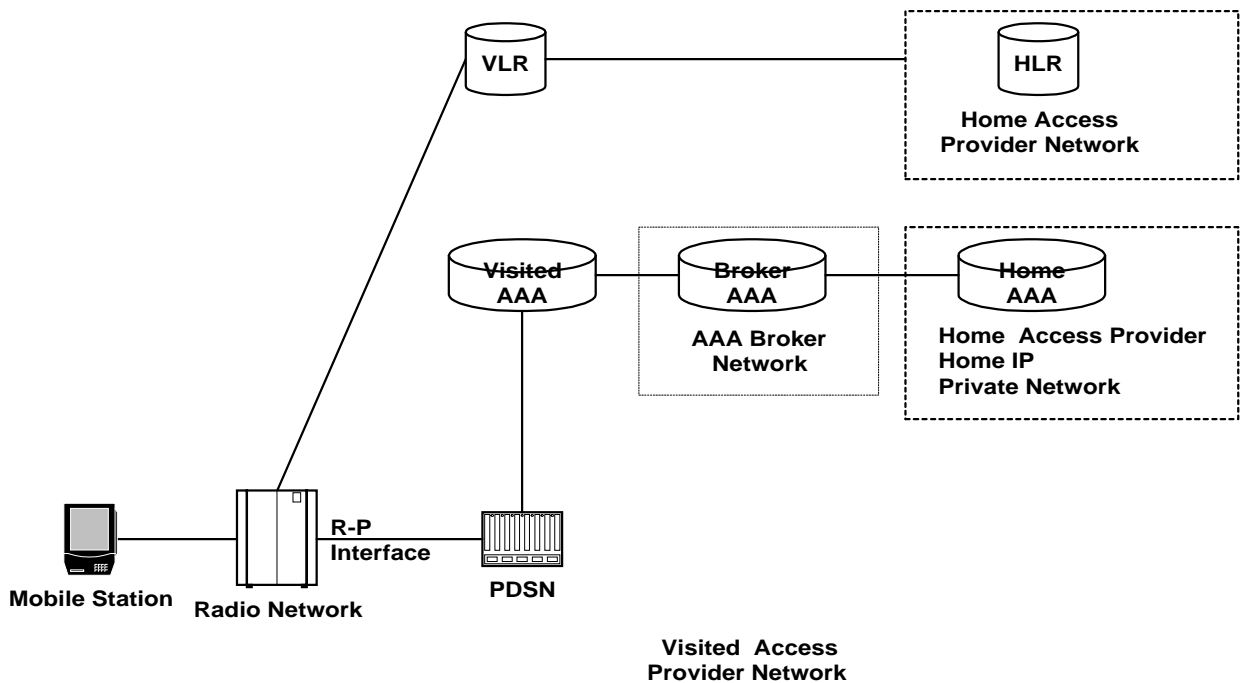
Figure 9: Logical Interfaces Reference Model for Private Network Access with Mobile IP

1 The peer to peer interfaces between network home and visited IMT-2000 (intra-family) entities is
 2 as follows:

- 3
- 4 • HA and PDSN: Mobile IP
- 5 • AAA server to AAA server: AAA Protocol (peer to peer)
- 6 • HLR and VLR: ANSI-41 Protocol
- 7
- 8

9 Intra-service provider interfaces are:

- 10
- 11 • PDSN and AAA: AAA Protocol (client server)
- 12 • HA and AAA: AAA Protocol (client server)
- 13 • RN and PDSN: RN-PDSN (R-P) Interface
- 14



15
 16
 17 **Figure 10: Logical Interfaces Reference Model for Simple IP**
 18

19 **6.4.1 R-P Interface**

20 The interface between the Radio Network (RN) and PDSN is a standard interface called the R-P
 21 interface. This is the point at which radio dependent network elements attach to packet data
 22 network elements.

23 The following is a list of requirements for the operation of this interface:

- 24
- 25 ■ The RN uses a unique layer 2 connection ID ID for each R-P session. The
- 26 ■ Information necessary for establishing an R-P session to the PDSN is exchanged across this
- 27 interface.
- 28 ■ The mobile station's status (e.g. dormant, active) is not communicated across the R-P
- 29 interface.
- 30 ■ The R-P session is maintained even when the mobile station is dormant.

- 1 ▪ The R-P interface shall be able to efficiently transport the widely ranging data rates expected
- 2 for 3G packet data service. It should minimize any additional latency.
- 3 ▪ Congestion control and security mechanisms in the R-P interface are optional.
- 4 ▪ ATM, frame relay, and IP networks are suitable layer-2 subnetworks for this interface.
- 5 ▪ Airlink related accounting information is communicated over this interface.
- 6 ▪ The RN shall establish an R-P session when a packet data session is initiated by the mobile
- 7 station. The RN or PDSN may tear down a R-P session.
- 8 ▪ The R-P interface shall be capable of transporting PPP frames, and may be able to identify
- 9 the QoS of each PPP frame in the direction from the PDSN to the RN.
- 10
- 11

7 Accounting

The flow of accounting information is shown in Figure 11.

The PCF sends airlink usage information to the PDSN. The PDSN will combine information received from the PCF with other IP data specific accounting information and send to the local AAA. The interface between the PDSN and the local AAA may support a reliable AAA protocol. The local AAA may optionally send accounting information to the appropriate home or broker network, optionally using the reliable AAA protocol. This exchange must allow for home network to re-request/re-poll any previously sent accounting information. The home or broker networks may then send the accounting information to appropriate downstream billing servers.

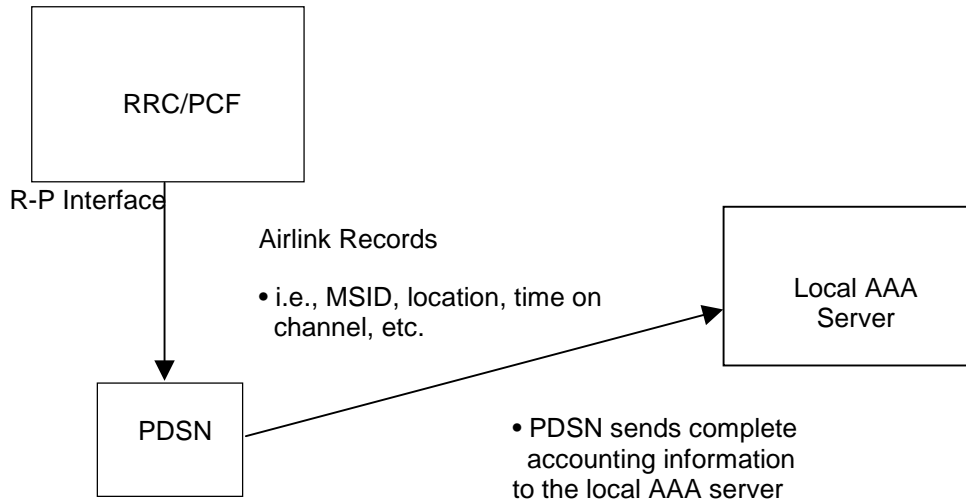


Figure 11: Accounting Architecture

Accounting information needs to be exchanged between the visited AAA servers and home AAA servers using standard encoding/decoding rules (e.g., Accounting Data Interchange Format (ADIF)).

Accounting information will include support for both Simple and Mobile IP. The accounting parameters may include, but are not limited to, NAI, mobile station ID, Session IDs, source and destination addresses, home and foreign AAA server addresses, QoS parameters, PDSN address, octet counts, time stamps in GMT for start and stop of a session(s), and location parameters.

8 AAA Protocol Considerations

8.1 AAA Protocol Requirements

AAA to AAA communications may be protected using IP Security ESP when the data crosses public facilities. The method of establishment of the security association between two AAA servers is outside the scope of this document.

It is desirable that the AAA to AAA protocol supports a reliable transport mechanism. This transport mechanism should be able indicate to an AAA application that a message was delivered to the next peer AAA application or that a time out occurred. Retransmission is then controlled by the reliable AAA transport mechanism, and not by lower layer protocols such as TCP. Even if the AAA message is to be forwarded, or the message's options or semantics do not conform with the AAA protocol, the transport mechanism should acknowledge that the peer received the AAA message. However, if the message fails to pass authentication, it should not be acknowledged. Acknowledgements should be allowed to be piggybacked in AAA messages. The reliable transport mechanism features should have the capability to detect silent failures of the AAA peer or path to the AAA peer, to manage failure on a proactive basis.

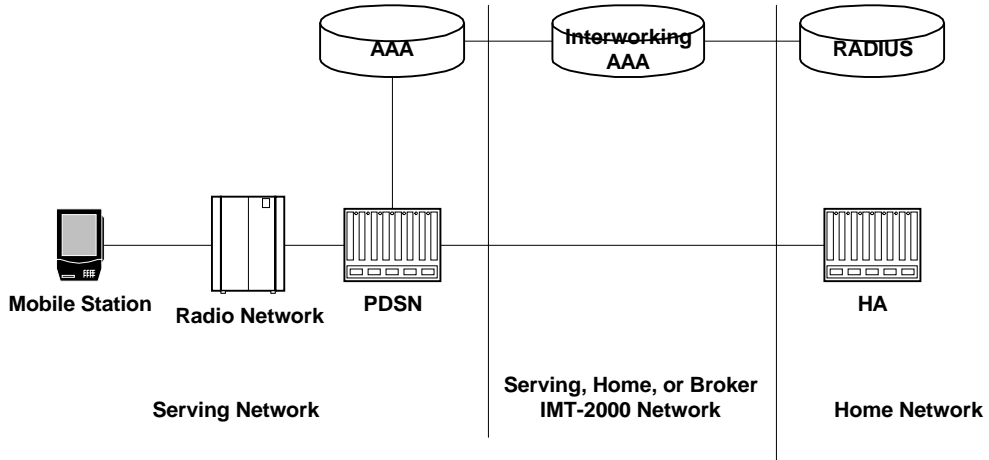
In addition, the AAA to AAA protocols should be capable of transporting a digital certificate in an AAA message, in order to minimize the number of round trips associated with AAA transactions. Note: This applies to AAA applications and not mobile stations. There should be support for both proxy and non-proxy brokers, where non-proxy brokers imply the broker terminates an entire request and initiates a new request. AAA brokers should have the capability to modify certain parts of AAA messages whereby to operate in non-proxy or proxy environments. It is desirable to provide message integrity and identity authentication on a per hop (AAA node) basis. Support for replay protection and optional non-repudiation capabilities for all authorization and accounting messages should be provided. The AAA protocol must provide the capability for accounting messages to be matched with prior authorization messages.

The use of standby or redundant AAA servers (if any) to be used when an AAA server or client fails is outside the scope of this architecture

8.2 AAA Protocol Interworking

It is possible that there will be more than one type of AAA server deployed in IMT-2000 networks. Whereas RADIUS has been deployed in many ISPs and private networks, the IETF is defining new AAA protocols on an on-going basis. An interworking server may be deployed to inter work different AAA protocols.

The interworking AAA server should able to proxy between a new type of AAA protocol and an older one (e.g., RADIUS). Possible configurations of the AAA interworking architecture are shown in Figure 11. This scenario shows an architecture in which an older AAA protocol based server authenticates the mobile station.



1
2
3
4

Figure 12: AAA Protocol Interworking Architecture

9 Support of Differentiated Services

9.1 Version 1 QoS

The QoS will be based on differentiated service policies from the AAA profile and parameters from the HLR. The AAA profile will store the IP level processing policy for the differentiated services service, and the HLR will store information regarding air link characteristics. The PDSN indicates the differentiated services class on the R-P session to the RN for each PPP frame.

In Version 1 each IP address assigned to the mobile station will share the same air link QoS level. For a given mobile station there can be multiple differentiated services QoS from the PDSN into the IP network.

The QoS functionality will have the following requirements supported on the indicated interfaces:

9.1.1 Mobile Station to RN

If the mobile station's applications are differentiated services aware, the mobile station's applications may mark the data traffic in accordance with IETF standards.

9.1.2 RN to PDSN

The RN will forward all user data for a mobile station to the PDSN over the R-P session.

9.1.3 PDSN to IP Network

- A service provider network must not exceed bandwidth for any differentiated services class per prevailing Service Level Agreements between the service provider and supporting ISP.
- The PDSN determines the differentiated services class of a packet by one or more of the following methods:
 - If the mobile station marks its traffic to the PDSN with a differentiated services class indicator, the PDSN may optionally accept and use this classification. The PDSN may overwrite this marking with another differentiated service class based on the AAA profile.
 - In the case that the mobile station does not mark its data traffic to the PDSN with a differentiated service class, the PDSN may optionally classify and prioritize the data traffic originated by the mobile station based on the AAA profile.
 - The differentiated services profile from the HAAA only provides an indication of the IMT-2000 service category, and does convey the actual parameters of the differentiated services service.
 - The PDSN will process data traffic received from the mobile station in accordance with differentiated services requirements as well as policy from the AAA servers. This may include traffic scheduling and traffic conditioning.

9.1.4 PDSN to RN

- The PDSN will process data traffic received from the IP network in accordance with differentiated services requirements as well as policy from the AAA servers. This may include traffic scheduling, traffic conditioning, queuing policies, and assignment of differentiated services classes to the traffic.
- The PDSN will transmit each data packet to the RN and may explicitly indicate the differentiated services code-point of the data packet to the RN over the R-P session (e.g., in the outer IP header of a tunneled packet).

9.1.5 RN to Mobile Station

- The RN may choose to forward the frames to the mobile station based on differentiated service class markings on the R-P link, while maintaining packet order within a given differentiated services class.

- 1 • The RN will not reorder PPP frames if the mobile station negotiates compression algorithms
2 that prohibit reordering.

3 **9.2 Version 2 QoS**

4 In addition to support for multiple IP addresses for a single mobile station, there is a recognized
5 need to provide multiple QoS levels over multiple air link connections for a single IP address. The
6 following requirements are under study for Version 2.

7 **9.2.1 Mobile Station to RN**

8 The mobile station's applications may have an association between differentiated services class
9 and air link connection (e.g., transparent and non-transparent connection) to the RN and may
10 transmit in accordance with that association. The mobile station may optionally support a priority
11 order on the air interface to the RN, based on differentiated services classes.

12 **9.2.2 Data Link Layer**

- 13 • Support a simple data link protocol in addition to PPP.
14 • Optional support for multilink PPP between mobile station and PDSN.
15

16 **9.2.3 Network Layer**

17 Support of end to end QoS in accordance with IETF standards when it is defined.

1 **10 Requirements**

2 **10.1 PDSN Functions**

3 **10.1.1 Core PDSN Functions**

4 A core set of requirements are defined in which the PDSN will:

- 5 • Reside in the service provider network and be allocated by the service provider network
- 6 where the mobile terminal initiates a packet data service.
- 7 • Support a unique R-P session to the PCF for each mobile station. The PDSN interacts
- 8 with a new PCF to facilitate a handoff from a previous PCF, if the previous PCF is
- 9 reachable by the PDSN.
- 10 • Establish, maintain, and terminate the PPP link protocol.
- 11 • Have a publicly visible IP address.
- 12 • Be associated with a local AAA server in the service provider network.
- 13 • Record usage data, receive accounting information from the PCF, correlate to generate
- 14 the accounting information, and relay the correlated information to the local AAA server.
- 15 • Support LAES by providing an access point to authorized collection agencies.
- 16 • Support the capability to run Van Jacobson TCP/IP header compression. The header
- 17 compression is enabled or disabled via IPCP.
- 18 • Support PPP compression control protocol. This protocol is used for negotiating a PPP
- 19 payload compression algorithm.
- 20 • Support differentiated service class information to be applied to all packets, or to packets
- 21 on a per packet basis.
- 22 • Identify the differentiated services level of PPP frames to the RAN via the R-P session.
- 23 • Optionally, support a AAA reliable protocol to the local AAA Server.

24 **10.1.2 Incremental PDSN Functions for Simple IP Service**

25 In addition to the core functions listed above, for Simple IP service, the PDSN will:

- 26
- 27 • Maintain an association between the IP address and the R-P session ID. The association
- 28 is maintained even when the mobile station is dormant.
- 29 • If the mobile station requests Simple IP and does not run CHAP or PAP, the PDSN may
- 30 provide the mobile station with Simple IP. The NAI used in the accounting messages is
- 31 constructed from the IMSI, using E.212 codes to determine the NAI realm of the home
- 32 network.
- 33 • If the mobile station requests Simple IP and does run CHAP, then the PDSN relays NAI
- 34 and CHAP Challenge Response to the local AAA server for authentication. If the
- 35 authentication is successful, the PDSN provides the mobile station with Simple IP and
- 36 sends accounting messages to the local AAA server.
- 37 • Optionally, support address assignment. Address assignment may also be supported via
- 38 the local AAA server.
- 39 • Monitor the source addresses of packets received from mobile stations. When packets
- 40 are received which have source addresses not assigned or registered to the mobile
- 41 station, the PDSN shall discard the packets and restart PPP to the mobile station.

42 **10.1.3 Incremental PDSN Functions for Mobile IP Version 1**

43 This section lists Version 1 requirements. Version 1 supports NAI, FAC, dynamic home address
 44 assignment, dynamic preshared key distribution for IKE between HA and PDSN, Mobile IP
 45 Foreign-Home Authentication Extension, and differentiated services.

46

- 1 • Support a Foreign Agent with reverse tunneling capability (per RFC 2344). The decision
- 2 to use reverse tunnel remains with the mobile station.
- 3 • Support private potentially overlapping addresses for mobile stations.
- 4 • During IPCP, accept a static home address in IP Address Configuration Option (RFC
- 5 1332) from the mobile station.
- 6 • Maintain an association between home address, HA address, and R-P session ID. The
- 7 association is maintained even when the mobile station is dormant.
- 8 • Maintains an association between the IP address, HA address, and the R-P session. The
- 9 R-P session association is maintained even when the mobile station is dormant.
- 10 • During IPCP, if the IP Address Configuration Option does not indicate zero address, upon
- 11 PPP establishment, the PDSN immediately begins to send Agent Advertisements to the
- 12 MS. The PDSN stops sending Agent Advertisements after receiving a MIP RRQ from the
- 13 MS, or when a preset number of Agent Advertisements has been sent.
- 14 • Verifies the FA Challenge Response in an RRQ corresponds to a recent advertisement.
- 15 • At handoff, determine whether Agent Advertisements should be sent based on the packet
- 16 zone ID, system ID, and network ID. Send Agent Advertisement(s) to a mobile station if it
- 17 has moved from a previous PCF that is not reachable by the PDSN
- 18 • Support dynamic home address assignment.
- 19 • Optionally, support AAA AVP extension with differentiated services QoS information.
- 20 • Send accounting messages to the local AAA server upon successful Mobile IP
- 21 registration.
- 22 • Establish a security association to an HA using IKE, if so instructed by the home AAA,
- 23 using certificates, distributed pre-shared key or static pre-shared key.
- 24 • Send security status to the home AAA that indicates to the Home AAA server whether the
- 25 PDSN would be able to use distributed key for IKE, assuming the Home AAA server is
- 26 able to provide one.
- 27 • Support statically configured Mobile IP Foreign-Home Authentication Extension with the
- 28 Home Agent.
- 29 • Verify that the mobile station complies with the reverse tunneling specification provided by
- 30 the home AAA server, and if it does not, send a failed RRP to the mobile station.

31 **10.1.4 Incremental PDSN Functions for Mobile IP Version 2**

32 This section lists Version 2 requirements.

- 34 • Support handoffs between PDSNs that do not involve the home IP network
- 35 • Support dynamic Home Agent assignment by both the home IP network and the service
- 36 provider network

37 **10.2 HA Functions**

38 **10.2.1 HA Functions for Version 1**

39 For Mobile IP service, the Home Agent will support the following requirements:

- 40 • Have a public routable address.
- 41 • Be associated with one or more AAA server(s) in the home IP network.
- 42 • Act as a AAA Client for a new session to request with the following information from the
- 43 associated AAA server;
 - 44 • Dynamic pre-shared key (secret) for IKE that the AAA server previously
 - 45 distributed to the PDSN. The Home Agent must provide the address of the
 - 46 PDSN and its own address as an index to the key.
- 47 • Establish a security association to an FA using pre-shared key for IKE or, optionally,
- 48 certificates with IKE.
- 49 • Support a static Foreign-Home Authentication Extension with the PDSN.
- 50 • Assign a dynamic home address for the mobile station as requested by the mobile
- 51 station. Only one address may be assigned per NAI on a given Home Agent.

1 **10.2.2 Incremental HA Functions for Version 2**

2 For Mobile IP service Version 2, the HA will additionally meet the following requirements:

- 3 • Support dynamic Home Agent assignment by both the home IP network and the service
- 4 provider network.
- 5 • Optionally support a reliable AAA protocol to associated AAA servers.

6 **10.3 AAA Server Functions**

7 **10.3.1 Simple IP**

8 For Simple IP service, the AAA server supports CHAP/PAP, and optionally, address assignment.

9 **10.3.2 Mobile IP Version 1**

- 10 • The visited AAA will be able to forward an AAA request from the PDSN to the home or to a
- 11 broker AAA network based the domain portion of the mobile station's NAI.
- 12 • The home AAA server will be able to determine the user from the NAI, authenticate the
- 13 request, and send authorization and profile information back to the service provider network.
- 14 • The home AAA server will support a statically assigned HA, as indicated by the mobile station.
- 15 • If the mobile station requests dynamic Home Agent assignment, the request will be rejected.
- 16 • A home AAA server will optionally be able to instruct the PDSN to use, or not use, IPsec on
- 17 the registration messages and/or the tunneled data.
- 18 • The home AAA server will be able to optionally distribute a pre-shared secret for IKE.
- 19 • The home AAA server will be able to optionally distribute differentiated service QoS
- 20 information.

21 **10.3.3 Mobile IP Version 2**

22 This section represents additional functions beyond Version 1.

23
24 The home AAA server will support a statically or dynamically assigned Home Agent, as requested
25 by the mobile station. If the mobile station requests dynamic Home Agent assignment, the AAA
26 server in the service provider network will indicate to the AAA server in the home IP network
27 whether it supports dynamic Home Agent assignment. If the service provider network AAA server
28 indicates it can assign the Home Agent, the home AAA server may choose to allow the visited
29 AAA server to perform the Home Agent assignment. Otherwise the home AAA assigns the Home
30 Agent.

31
32 Optionally, the visited AAA server interacts with a previous PDSN to support handoffs between
33 PDSNs in order to not involve the home AAA server.

34 **10.4 Mobile Station Functions**

35 **10.4.1 Core Mobile Station Functions**

36 A core set of functions are defined for the mobile station:

- 37 • Manage radio resources with the RRC for the exchange of packets.
- 38 • Use a single packet data service option for both Mobile IP and Simple IP.
- 39 • Establish, maintain, and terminate PPP to the PDSN.
- 40 • If while dormant, the packet zone ID, system ID, or network ID changes, communicate with
- 41 the RRC to initiate dormant handoff
- 42 • Support the capability to run Van Jacobson TCP/IP header compression. The header
- 43 compression is enabled or disabled via IPCP.
- 44 • Optionally support the capability to run PPP compression control protocol. This protocol is
- 45 used for negotiating a PPP payload compression algorithm.

1 **10.4.2 Incremental Mobile Station Functions for Simple IP**

2 In addition to the core mobile station functions, incremental MS functions are defined for Simple
3 IP:

- 4 • Support the capability to run CHAP and/or PAP.
- 5 • Have the ability to disable/enable CHAP or PAP.
- 6 • Obtain a dynamic IP address via IPCP.

7 **10.4.3 Incremental Mobile Station Functions for Mobile IP Version 1**

8 In addition to the core mobile station functions, incremental mobile station functions are defined
9 for Mobile IP Version 1:

- 10 • Should disable CHAP and PAP.
- 11 • Optionally send Agent Solicitation immediately after PPP is established.
- 12 • Include the NAI and FA Challenge Response in the MIP RRQ.
- 13 • If the mobile station wants to use its static home address, during the IPCP phase of PPP
14 establishment, the mobile station uses IP Address Configuration Option (RFC1332) to
15 indicate this address to the PDSN.
- 16 • If the mobile station wants a dynamic home address, during the IPCP phase of PPP
17 establishment, the mobile station must not send any IPCP address configuration options. The
18 Home Address field of the MIP RRQ is set to zero. The mobile station obtains a dynamic
19 home address in the MIP RRP.

20 **10.4.4 Incremental Mobile Station Functions for Mobile IP Version 2**

21 In addition to the incremental mobile station functions for Mobile IP Version 1, incremental mobile
22 station functions are defined for Mobile IP Version 2:

- 23 • As an alternative to PPP, establish, maintain, and terminate a simple data link-layer protocol.
- 24 • Optionally, include the Previous Foreign Agent Extension.
- 25 • Optionally, request a dynamic Home Agent by setting the Home Agent field of the Mobile IP
26 RRQ to zero, and accept a MN-HA authentication key and SPI.

27 **10.5 Accounting Functions**

28 In the service provider network:

- 29 • Receive all visitor accounting information (start, interim, and stop records) from the
30 PDSN.
- 31 • Redirect visitor accounting information to the appropriate home AAA server.
- 32 • Allow for possible re-request/re-poll from the Home AAA server for previously distributed
33 accounting information.
- 34 • Log all accounting information exchanges for audit and reconciliation purposes.
- 35 • Audit accounting Start, Interim, and Stop messages from PDSNs.

36
37 In the home IP or broker network:

- 38 • Receive accounting information (start, interim, and stop records) from the service provider
39 network AAA servers.
- 40 • Redirect accounting information to downstream billing systems using appropriate
41 interfaces.
- 42 • Allow for possible re-request/re-poll from downstream billing applications.
- 43 • Log accounting information exchanges for audit and reconciliation purposes.
- 44 • Audit accounting Start, Interim, and Stop messages from foreign AAA servers.

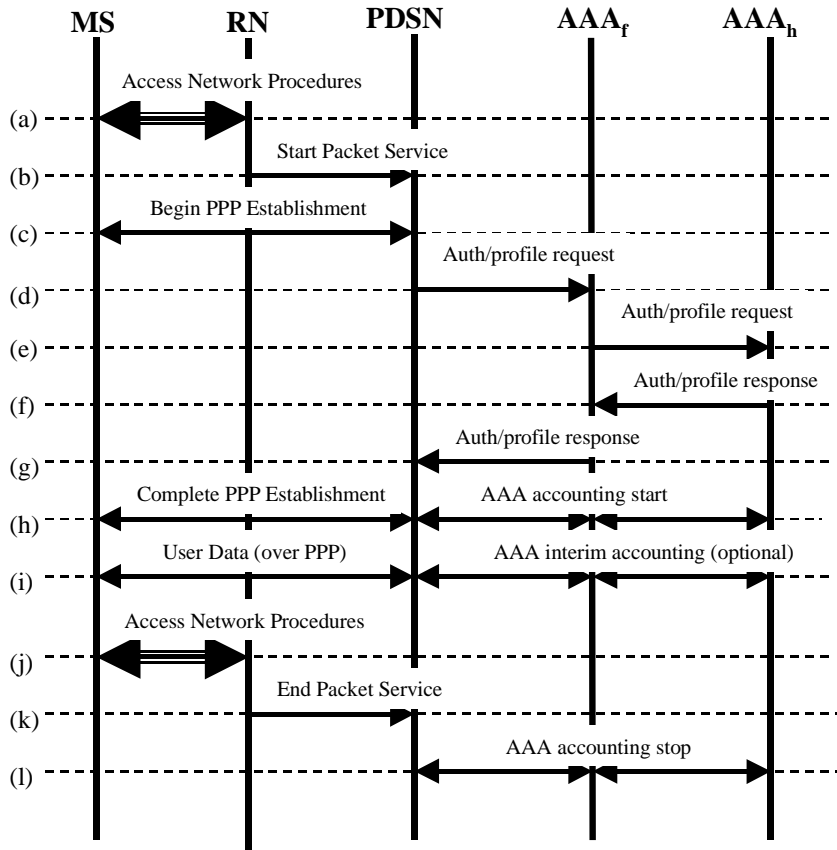
45

1 **Annex: Flows**

2
3 **A-1 Simple IP Service Initiation and Termination with AAA Accounting**

4
5 Figure 13 shows the flow for these messages.

- 6 a) The mobile station acquires the access network, and registers using access network specific
- 7 procedures.
- 8 b) The mobile station initiates packet data session. The RN sends an indication to the PDSN to
- 9 setup a new packet data session.
- 10 c) The PDSN establishes a PPP session with the mobile station.
- 11 d) If authentication (such as CHAP or PAP) is used in PPP, an authentication request is sent to
- 12 the local AAA server. This request may optionally contain a request for user service profile in
- 13 addition to authentication.
- 14 e) The local AAA server proxies the request to the home AAA server.
- 15 f) The home AAA server responds.
- 16 g) The response is sent back to the PDSN via the local AAA server.
- 17 h) PPP has been established. At this point, an AAA accounting start message is forwarded to
- 18 the local AAA server and proxies to the home AAA server.
- 19 i) The data flow is active using a PPP session between the mobile station and the PDSN.
- 20 During data exchange, interim accounting messages may be sent to the local AAA server and
- 21 proxies to the home AAA server.
- 22 j) The mobile station de-registers with the access network and signals to terminate packet data
- 23 session using access network specific procedures.
- 24 k) The RN indicates the end of packet data session to the PDSN.
- 25 l) The PDSN generates an accounting stop message to the local AAA server which is proxied to
- 26 the home AAA server.
- 27



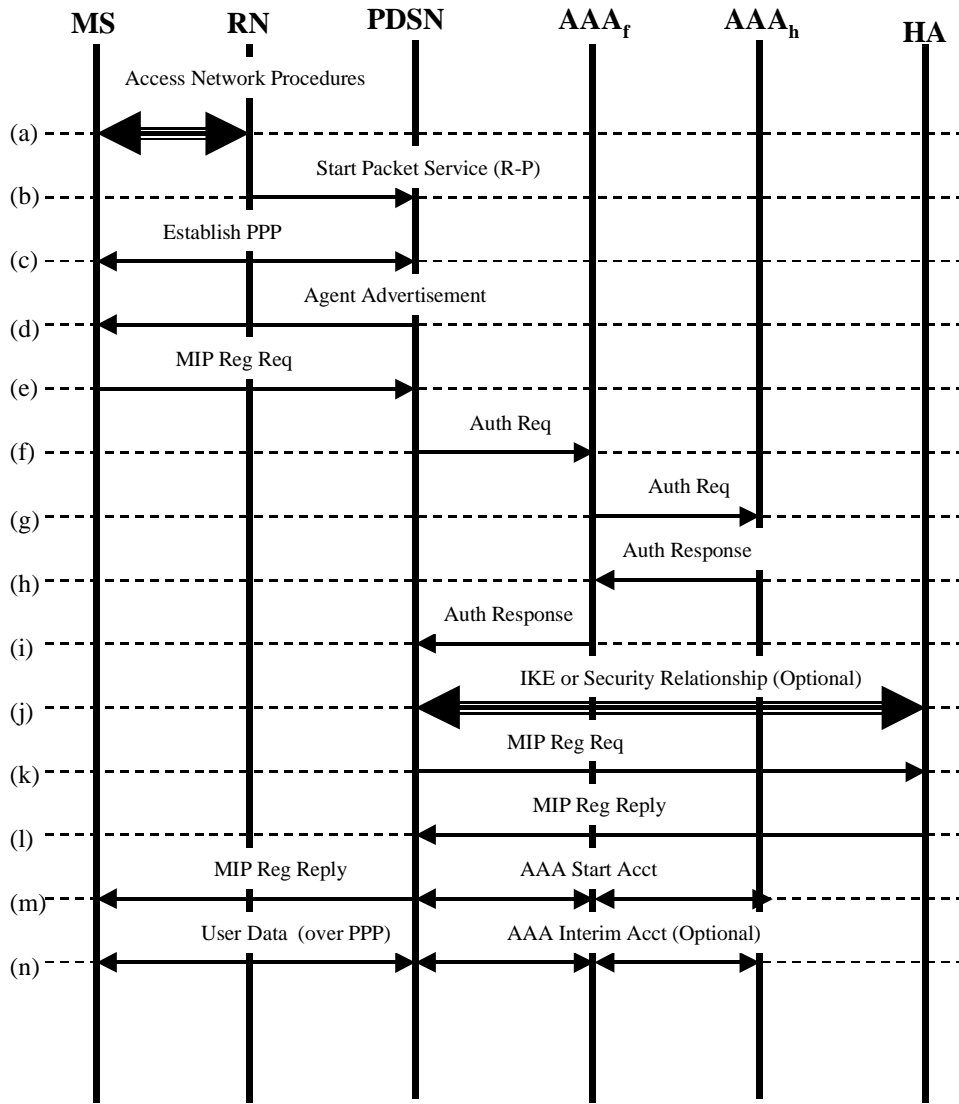
1
2

Figure 13: A-1 Simple IP Service Initiation with AAA Accounting

1 **A-2: Mobile IP Service Initiation**

2
3 Figure 14 shows the flow for these messages.

- 4
- 5 a) The mobile station acquires the access network, and registers using access network specific
 - 6 procedures.
 - 7 b) The mobile station initiates packet data session. The RN sends an indication to the PDSN to
 - 8 setup a new packet data session.
 - 9 c) The PDSN establishes a PPP session with the mobile station.
 - 10 d) After PPP initialization, the PDSN sends Agent Advertisements to the mobile station. The
 - 11 mobile station may send an agent solicitation message to the PDSN (FA) following PPP
 - 12 initialization.
 - 13 e) The mobile station generates a Mobile IP registration request containing the NAI and FAC
 - 14 response.
 - 15 f) Using the AAA protocol, the PDSN sends an authentication request to the AAA_f.
 - 16 g) The AAA_f server uses the NAI to forward the message to the proper AAA_h server, possibly via
 - 17 brokers (not shown).
 - 18 h) The AAA_h responds with an authorization response that may be delivered using security
 - 19 between foreign (visited) and home networks.
 - 20 i) The AAA_f forwards the response to the PDSN.
 - 21 j) The PDSN may optionally create an IP security association with the HA using IKE, if one does
 - 22 not already exist. This may involve either an IKE pre-shared key delivered by the AAA
 - 23 Authorization response or via certificate exchange within IKE. If the Home-Foreign
 - 24 authentication extension key and SPI returned by the AAA, , then the PDSN does not create
 - 25 an IP security association with the HA using IKE.
 - 26 k) The PDSN sends the Mobile IP RRQ to the Home Agent.
 - 27 l) The home agent responds with a Mobile IP RRP.
 - 28 m) The PDSN sends the RRP to the mobile station after recording the reply in the visitor entry
 - 29 list. The PDSN sends an accounting start to the AAA_f (which may forward the message to the
 - 30 AAA_h via optional brokers not shown).
 - 31 n) User data flows over the PPP link to the PDSN. The PDSN optionally sends an interim
 - 32 accounting message to the AAA_f (which may forward the message to the AAA_h via optional
 - 33 brokers not shown).



1
2

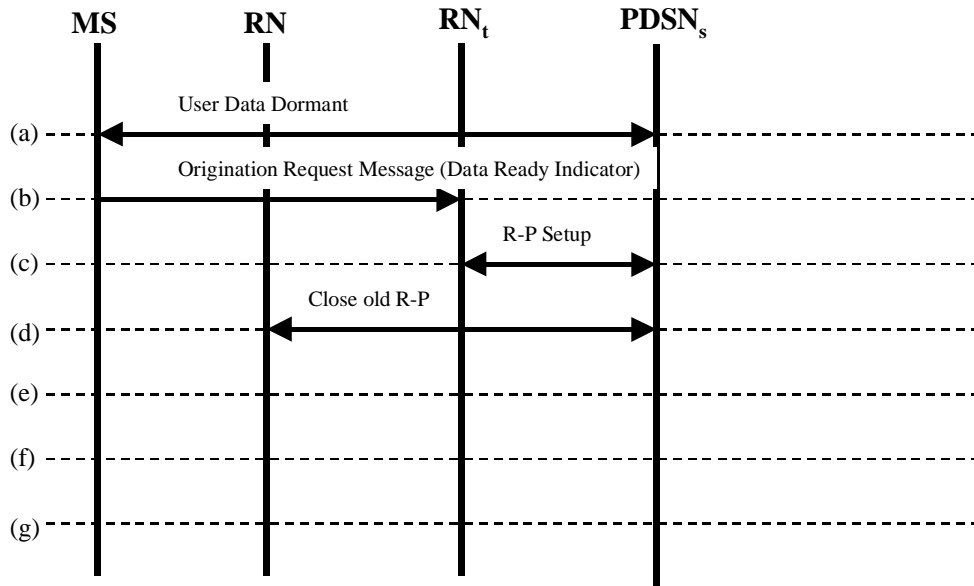
Figure 14: Mobile IP Service Initiation

1 **A-3 Handoffs between RN within the Same PDSN**

2 *Note: This flow is informational and intended to imply the general functioning of the system.*
3 *Specific message sequences will be determined by the R-P interface specification.*

4
5 Figure 15 shows the flow for these messages.

- 6
7 a) The data flow is active using a PPP session between the mobile station and the PDSN.
8 b) At some point the radio system decides a hard handoff is required – the RN must change.
9 The serving RN (RN_s) sends a request to the target Radio Network (RN_t). This information is
10 relayed through the VLR using existing handoff procedures.
11 c) The target RN decides to allow the handoff and sends a response back to the serving RN
12 through existing procedures in the VLR.
13 d) The serving RN notifies the mobile station to perform the hard handoff to the target RN.
14 e) The traffic channel is transferred to the target RN.
15 f) The target RN notifies the PDSN to establish a packet service. The IMSI or other mobile
16 identifier is sent to the PDSN by the target RN. Using the IMSI or other mobile identifier, the
17 PDSN realizes that the existing R-P link is being transferred to the target RN.
18 g) After the handoff is complete, the PDSN closes the R-P session for the mobile station. A AAA
19 stop record followed by a AAA start record may be sent to the AAA server.
20



1
2
3
4
5

Figure 15: Handoffs between RN within the Same PDSN

1

2

3 A-4 Hard Handoff between PDSNs for Mobile IP

4 *Note: This flow is informational and intended to imply the general functioning of the system.*

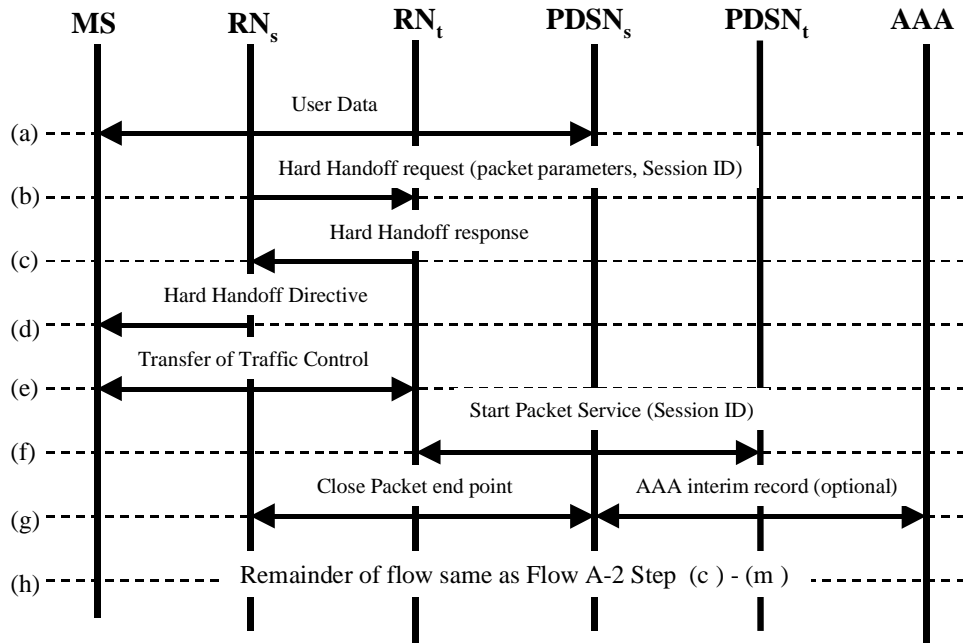
5 *Specific message sequences will be determined by the R-P interface specification.*

6

7 Figure 16 shows the flow for these messages.

8

- 9 a) The data flow is active using a PPP session between the mobile station and the current
10 serving PDSN (PDSN_s).
- 11 b) At some point the radio system decides a hard handoff is required – the RRC must change.
12 The serving Radio Network (RN_s) sends a request to the target Radio Network (RN_t). Packet
13 parameters (including the session_id) are passed to RN_t to expedite the packet data handoff.
14 This information is relayed between RNs using existing handoff procedures.
- 15 c) RN_t decides to allow the handoff and sends a response back to the serving RN through
16 existing procedures in the VLR.
- 17 d) RN_s notifies the mobile station to perform the hard handoff to RN_t.
- 18 e) The traffic channel is transferred to RN_t.
- 19 f) The RN_t notifies the PDSN_t to establish a packet service. The session ID is sent to the
20 PDSN_t. Using the session ID, the PDSN_t realizes that this is a new R-P link (no existing link).
- 21 g) After the handoff is complete, RN_s notifies the PDSN_s that the tunnel end point for the mobile
22 station at this RN is closed. An AAA Interim Accounting record may optionally be sent to the
23 AAA server.
- 24 h) The remainder of the flow (including PPP establishment and Mobile IP registration) is the
25 same as the A-2 steps (c)-(m).

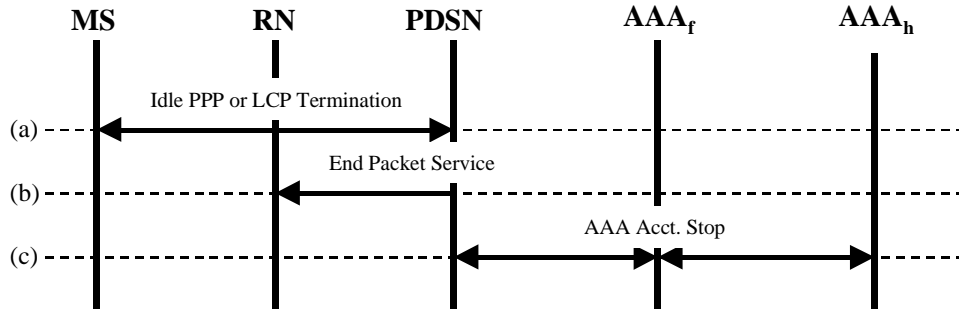


1
2 **Figure 16: Hard Handoff between PDSNs for Mobile IP**

1 **A-5 Simple IP Service Terminated by the Network**

2
3 Figure 17 shows the flow for these messages.

- 4
5 a) The PPP timeout expires in the PDSN after an extended period of inactivity. The PDSN may
6 send an LCP Terminate to the mobile station. The PDSN may also receive LCP Terminate
7 from the mobile station. Either of these actions cause the end of the data session at the
8 PDSN and mobile station.
9 b) The PDSN indicates the end of packet data session to the RN.
10 c) The PDSN generates an accounting stop message to the local AAA server which is proxied to
11 the home AAA server.
12
13



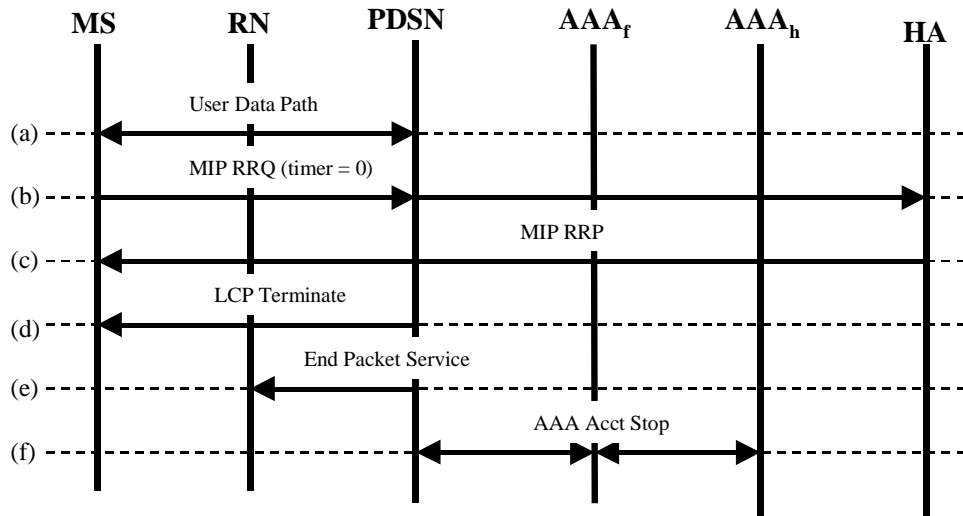
1
2
3

Figure 17: Simple IP Service Terminated by the Network

1 **A-6 Mobile IP Service Terminated by the Mobile Station**

2
3 Figure 18 shows the flow for these messages.

- 4
5 a) The user data flows over the established PPP session.
6 b) The mobile station initiates Mobile IP de-registration (Mobile IP Registration Request (RRQ)
7 with zero value for the registration lifetime). The PDSN relays the RRQ on to the Home
8 Agent.
9 c) The Home Agent returns a response to the PDSN indicating that the Mobile IP service is
10 terminated. The response is sent on to the mobile station.
11 d) The PDSN sends a LCP Terminate message to the mobile station if no other packet data
12 sessions to that mobile station are active. The mobile station may also send a LCP
13 Terminate to the PDSN based on the response from the Home Agent.
14 e) The PDSN indicates an end to the packet data session to the RN.
15 f) The PDSN generates an accounting stop message to the AAA_F server which is proxied to the
16 AAA_H server.
17



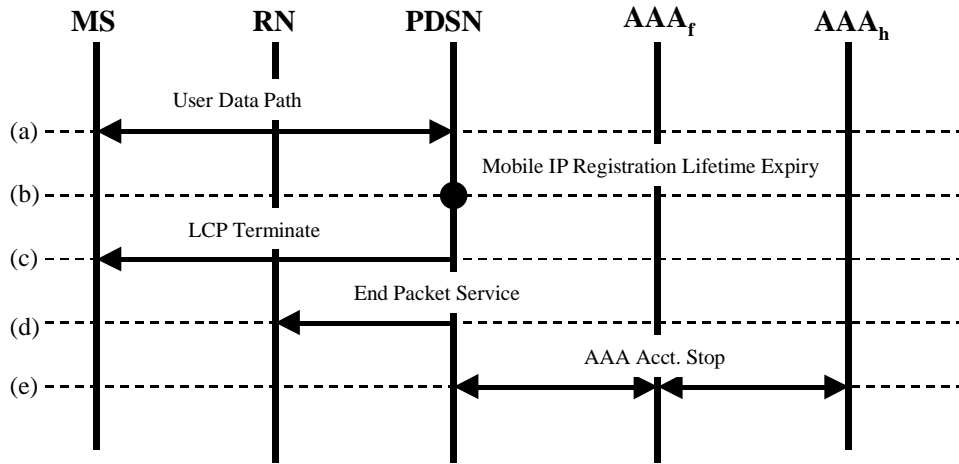
1
2
3

Figure 18: Mobile IP Service Terminated by the Mobile Station

1 **A-7 Mobile IP Service Terminated by the Network**

2
3 Figure 19 shows the flow for these messages.

- 4
5 a) The user data flows over the established PPP session.
6 b) The Mobile IP registration lifetime expires. This may be the case when the mobile station has
7 been turned off, dormant, or moved out of the coverage area of the network.
8 c) The PDSN sends a LCP Terminate message to the mobile station if no other packet data
9 sessions to that mobile station are active..
10 d) The PDSN indicates an end to the packet data session to the RN.
11 e) The PDSN generates an accounting stop message to the AAA_F which is proxied to the AAA_H.
12



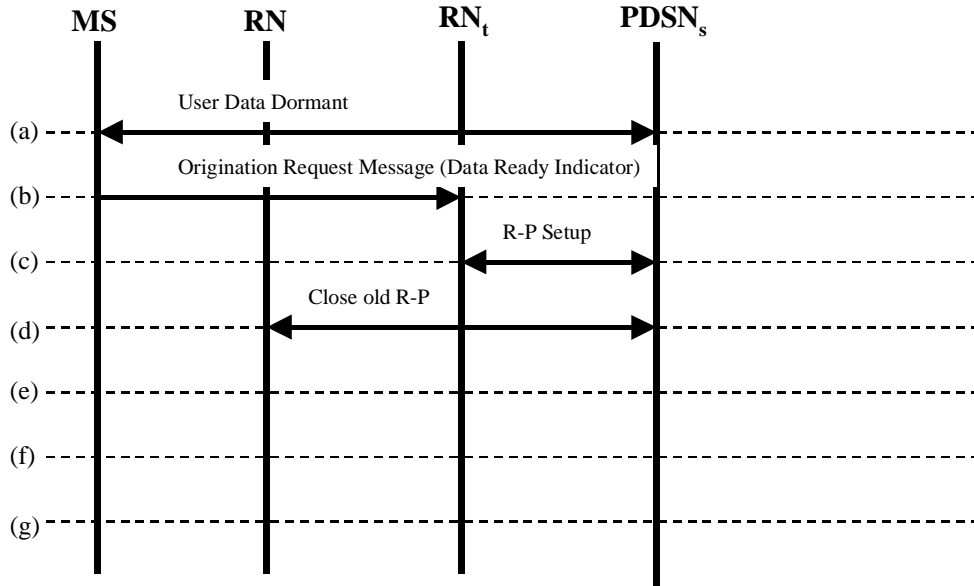
1
2

Figure 19: Mobile IP Service Terminated by the Network

1 **A-8 Dormant Handoff Maintaining Same PDSN**

2
3 Figure A-20 shows the flow for these messages.

- 4
5 a) The user data path between the mobile station and the Radio Network is dormant.
6 b) The mobile station moves into an area that indicates a change in Packet Zone ID. The mobile
7 station sends an Origination Request message to the target RN indicating whether data is
8 ready to be sent.
9 c) The target RN selects and attempts to connect to the serving PDSN.
10 d) The serving PDSN sends a message to the previous RN indicating that the connection has
11 moved.



1
2
3

Figure 20: Dormant Handoff Maintaining Same PDSN