3GPP2 X.S0011-001-E

Version: 1.0

Version Date: November 2009

cdma2000 Wireless IP Network Standard:

Introduction

This page is left blank intentionally.

cdma2000 Wireless IP Network Standard: Chapter 1

CONTENTS

LIST OF FIGURES

LIST OF TABLES

REVISION HISTORY

Table 1 **Revision History**

Revision	Date	Remarks
Rev. 0	December 2000	Initial Publication
Rev. A	May 2001	Added specification or clarification for the following items: ▪ New mechanism for PDSN/HA pre-shared secret distribution for IKE ▪ Security status is replaced by IKE Pre-shared Secret Request attribute ▪ New counters G15 and G16 for MIP signaling ▪ Clarifications with respect to counters G1 and G2 ▪ A new indicator in RADIUS stop message to indicate session still in progress (to avoid release of the IP address) ▪ Removal of RADIUS accounting fields H1, I2, and I3 ▪ New accounting session to be created when F1, F2 accounting fields vary ▪ Non-zero and zero IP address in IP Configuration option in IPCP is treated as Simple IP by PDSN. MIP is supported with null IP address configuration option (i.e., not included). ▪ The Active Time attribute format changed from standard RADIUS encoding to 3GPP2 specific encoding.
Rev. B	September 2002	This document has been revised to support the following features: ▪ Simultaneous multiple service instances concept introduced. ▪ RTP/UDP/IP Header Reduction Schemes ▪ Differentiated Services QoS Policy ▪ Fast handoff for data call (i.e., tunneled PPP between PDSNs) ▪ Dynamic Home Agent allocation with RADIUS ▪ Optional support for DNS server address auto configuration in MS ▪ Always On support ▪ IP Reachability Service with dynamic DNS update ▪ Simple IPv6 ▪ Remote address based accounting
Rev. C	August 2003	New format: the document is split into 6 chapters identified by YYYYY.xxx-C, where YYYY is the document number and xxx is the chapter number. ▪ Multiple Service Instance support ▪ LLAROHC Header Compression and LLA Header Removal ▪ Enhanced CRTP as an additional compression scheme

		▪ Dynamic flow mapping/treatment ▪ PrePaid Packet Data service (phase 1) ▪ PDSN/HA Resource management ▪ Accounting support for 1xEVDV ▪ Packet Data Inactivity Timer ▪ IKE/IPsec clarifications ▪ IP Reachability enhancements ▪ Enhancements to Always On ▪ Enhancements to Simple IPv6
Rev. B Version 2.0	September 2004	This is an addendum to correct errors and omissions in the Revision B Version 1.0 of this document.
Rev. D	February 2006	▪ IPv6 Mobility ▪ Support for end-to-end QoS (MS-PDSN QoS signaling) ▪ Hot-lining ▪ MS-PDSN Version/Capabilities Indication ▪ Short Data Burst Indication Support ▪ RAN-PDSN Flow control Support ▪ DHCPv4 and DHCPv6 ▪ IP Reachability for MIPv6 ▪ Auxiliary Service Connection SO67 support.
Rev. D Version 2.0	October 2008	This is an addendum to correct errors in the Revision D Version 1.0 of this document.
Rev. E Version 1.0	November 2009	▪ Additional PPP Authentications ▪ NCP Inactivity Timer Support ▪ NEMO Support ▪ Network initiated QoS ▪ IP service authorization ▪ EAP support for Access Authentication

FOREWORD

(This foreword is not part of this Standard.)

This document was prepared by 3GPP2 TSG-X.

This document consists of multi-chapter documents that together describes specifications for cdma2000 Wireless IP Network .

This document is subject to change following formal approval. Should this document be modified, it will be re-released with a change of release date and an identifying change in version number as follows:

X.S0011-00n-X-y

where:

- X an uppercase numerical or alphabetic character [A, B, C, …] that represents the revision level.
- n a numeric string [1, 2, 3, …] that indicates a chapter.
- y a numeric string [1, 2, 3, …] that indicates a point release level.

1 Introduction

This document defines requirements for support of wireless packet data networking capability on a third generation wireless system based on cdma2000® [1]. This document supports the services and architecture in [1].

This document defines the two methods for accessing public networks (Internet) and private networks (intranets): Simple IP and MIP. It describes the required Quality of Service, Security, Mobility Management, and Accounting capabilities needed to support both methods. IETF protocols are widely employed whenever possible to minimize the number of new protocols required and to maximize the utilization of well accepted standards.

This document is organized into a series of related chapters, some of which address capabilities common to both IP access service types: MIP and Simple IP, and others may describe capabilities applicable to a specific IP access service. The chapters included in this series are:

Chapter 1 cdma2000 Wireless IP Network Standard: Introduction.

Chapter 2 cdma2000 Wireless IP Network Standard: Simple IP and MIP Access Services.

Chapter 3 cdma2000 Wireless IP Network Standard: Packet Data Mobility and Resource Management.

Chapter 4 cdma2000 Wireless IP Network Standard: Quality of Service and Header Reduction.

Chapter 5 cdma2000 Wireless IP Network Standard: Accounting Services and 3GPP2 RADIUS VSAs.

Chapter 6 cdma2000 Wireless IP Network Standard: PrePaid Packet Data Service.

In this set of documents we refer to other documents in the set strictly by their chapter numbers as in [Chapter 1].

Chapter 1 This chapter presents an overview of the document content, and contains the complete glossary and definitions applicable to all the chapters. It describes the network and protocol reference models for the wireless IP Network entities: PDSN, HA and RADIUS server.

Chapter 2 This chapter describes the basic IP access services: Simple IPv4/IPv6, MIP6 and MIP4 with Dynamic Home Agent, and Home IP address Assignment. It also addresses the security requirements between the Wireless IP Network nodes: PDSN, HA and RADIUS servers. The chapter includes other capabilities such as Always On, multiple simultaneous MIP4/IPv6 and Simple IPv4/IPv6 packet data session, IP Reachability Service, DHCP support and Hot-Lining.

---

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

Chapter 3 This chapter describes packet data intra-PDSN, inter-PDSN handoff as well as inter-PDSN fast handoff capabilities and the RAN requirements. The chapter includes mechanisms for PDSN and HA resource management and provisioning of dormancy timers in the RAN. This chapter also includes support for RAN-PDSN Flow Control and Short Data Burst indication.

Chapter 4 This chapter describes user Differentiated services capability, multiple service connections, flow mapping and treatment, and MS-PDSN QoS signaling. The chapter also includes a detailed description of Link Layer Assisted Robust Header compression and Header Removal treatment to support Voice over IP Service over an auxiliary service connection. In addition, this chapter adds Auxiliary Service Connection SO67 support that allows for the efficient transport of IP packets from the PDSN to the RAN without HDLC-like framing and PPP encapsulation.

Chapter 5 This chapter describes source IP address and remote IP address based accounting and detailed procedures required for this series of standards. It also includes a description of the 3GPP2 RADIUS VSAs required to support this series of standards.

Chapter 6 This chapter describes the PrePaid Packet Data Service for the Wireless IP Network users and includes the PrePaid service architecture, the detailed procedures and the requirements on the Wireless IP Network elements.

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

2 References

2.1 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Specification. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For non-specific reference, the latest version applies. In the case of a reference to a 3GPP2 document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

2.1.1 IETF

RFC 768	Postel, User Datagram Protocol, August 1980.
RFC 791	Internet Protocol, Sept. 1981.
RFC 792	Postel, Internet Control Message Protocol, September 1981.
RFC 793	Transmission Control Protocol, September 1981.
RFC 1034	Mockapetris, Domain Names - Concepts and Facilities, November 1987.
RFC 1035	Mockapetris, Domain Names - Implementation and Specification, November 1987.
RFC 1122	Braden, Requirements for Internet Hosts - Communication Layers, October 1989.
RFC 1144	Jacobson, Compressing TCP/IP Headers for Low Speed Serial Links, February 1990.
RFC 1321	Rivest, The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science, RSA Data Security Inc., April 1992.
RFC 1332	McGregor, The PPP Internet Protocol Control Protocol (IPCP), May 1992.
RFC 1542	W. Wimer, Clarifications and Extensions for the Bootstrap Protocol, October 1993.
RFC 1661	Simpson, The Point-to-Point Protocol (PPP), July 1994.
RFC 1662	Simpson, PPP in HDLC-like Framing, July 1994.
RFC 1702	S. Hanks, T. Li, D. Farinacci, P. Traina, Generic Routing Encapsulation over IPv4 networks, October 1994.
RFC 1886	Thompson, Huitema, DNS Extensions to Support IP Version 6, December 1995.

RFC 1877	Cobb, PPP Internet Protocol Control Protocol Extensions for Name Server Addresses, December 1995.
RFC 1889	Schulzrinne, Casner, Frederick, Jacobson, RTP: A Transport Protocol for Real-Time Applications, January 1996.
RFC 1918	Rekhter, Moskowitz, Karrenberg, de Groot, Lear, Address Allocation for Private Internets, February 1996.
RFC 1962	Rand, The PPP Compression Control Protocol (CCP), June 1996.
RFC 1974	Friend, Simpson, PPP Stac LZS Compression Protocol, August 1996.
RFC 1979	Woods, PPP Deflate Protocol, August 1996.
RFC 1994	Simpson, PPP Challenge Handshake Authentication Protocol (CHAP), August 1996.
RFC 2002	Perkins, IPv4 Mobility, May 1995.
RFC 2003	Perkins, IP Encapsulation within IP, October 1996.
RFC 2004	Perkins, Minimal Encapsulation within IP, October 1996.
RFC 2005	Solomon, Applicability Statement for IP Mobility support, October 1995.
RFC 2006	Cong, Hamlen, Perkins, The Definitions of Managed Objects for IP Mobility Support Using SMIv2, October 1995.
RFC 2118	Pall, Microsoft Point-To-Point Compression (MPPC) Protocol, March 1997.
RFC 2131	R. Droms, Dynamic Host Configuration Protocol, March 1997.
RFC 2132	S. Alexander, R. Droms, DHCP Options and BOOTP Vendor Extensions, March 1997.
RFC 2136	Vixie, Thomson, Rekhter, Bound, Dynamic Updates in the Domain Name System (DNS UPDATE), April 1997.
RFC 2138	Rigney, Rubens, Simpson, Willens, Remote Authentication Dial In User Service (RADIUS), August 1997.
RFC 2139	Rigney, RADIUS Accounting, April 1997.
RFC 2153	Simpson, PPP Vendor Extensions, May 1997.
RFC 2205	Braden et al. Resource ReSerVation Protocol (RSVP), Version1 Functional Specification, September 1997.
RFC 2210	Wroclawski, J., The Use of RSVP with IETF Integrated Services, September 1997.
RFC 2212	Shenker, S., Partridge, C., Guerin, R., Specification of Guaranteed Quality of Service, September 1997.
RFC 2215	Shenker, S., Wroclawski, J., General Characterization Parameters for Integrated Service Network Elements, September 1997.
RFC 2290	Simpson, Mobile-IPv4 Configuration Option for PPP IPCP, February 1998.
RFC 2327	M. Handley, V. Jacobson, SDP Session Description Protocol, April 1998.
RFC 2373	Hinden, Deering, IP Version 6 Addressing Architecture, July 1998.

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

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

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

RFC 2407 Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.

RFC 2408 Maughan et al, Internet Security Association and Key Management Protocol (ISAKMP), November 1998.

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

RFC 2459 Housley, Housley, Polk, Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

RFC 2460 Deering, Hindin, Internet Protocol, Version 6 (IPv6) Specification, December 1998.

RFC 2461 Narten, Nordmark, Simpson, Neighbor Discovery for IP Version 6 (IPv6), December 1998.

RFC 2462 Thomson and Narten, IPv6 Stateless Address Auto-configuration, December 1998.

RFC 2463 Conta, Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, December 1998.

RFC 2472 Haskin, Allen, IP Version 6 over PPP (IPv6CP), December 1998.

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

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

RFC 2486 Aboba, Beadles, The Network Access Identifier, January 1999.

RFC 2507 Degermark, Nordgren, Pink, IP Header Compression, February 1999.

RFC 2509 Egan, Casner, Bormann, IP Header Compression over PPP, February 1999.

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

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

RFC 2784 Farinacci et al, Generic Routing Encapsulation (GRE), March 2000.

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

RFC 2865 Rigney, Willens, Livingston, Reubens, Merit, Simpson, Daydreamer, Remote Authentication Dial In User Service (RADIUS), June 2000.

RFC 2866 Rigney, RADIUS Accounting, June 2000.

RFC 2868 Zorn et al., RADIUS Attributes for Tunnel Support, June 2000.

RFC 2869 Rigney, Willats, Calhoun, RADIUS Extensions, June 2000.

RFC 2874	Crawford, Huitema, DNS Extensions to Support IPv6 Address Aggregation and Renumbering, July 2000.
RFC 2890	Dommety, Key and Sequence Number Extensions to GRE, September, 2000.
RFC 2983	Black, Differentiated Services and Tunnels, October 2000.
RFC 3006	Davie, Iturralde, Oran, Casner, Wroclawski, Integrated Services in the Presence of Compressible Flows, November 2000.
RFC 3012	Calhoun, Perkins, Mobile IPv4 Challenge/Response Extensions, November 2000.
RFC 3024	Montenegro, Reverse Tunneling for Mobile IP, January 2001.
RFC 3041	Narten, Draves, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, January 2001.
RFC 3046	M, Patrick, DHCP Relay Agent Information Option, January 2001.
RFC 3095	Borman, et al, Robust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed, July 2001.
RFC 3162	Zorn et al., RADIUS and IPv6, August 2001.
RFC 3203	Y. Yohen et al., DHCP Reconfigure Extension, Dec. 2001.
RFC 3241	Borman, ROHC over PPP, January 2002.
RFC 3242	Jonsson, Pelletier, Robust Header Compression (ROHC): A link Layer Assisted Profile for IP/UDP/RTP, April 2002.
RFC 3315	R. Droms et al., Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.
RFC 3319	H. Shulzrinne, Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers, July 2003.
RFC 3361	H. Shulzrinne, Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers, Aug. 2002.
RFC 3363	Bush, Durand, Fink, Gudmundsson, Hain, Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS), August 2002.
RFC 3408	Liu, Le, Zero-byte Support for Bidirectional Reliable Mode (R-mode) in Extended Link-Layer Assisted RObust Header Compression (ROHC) Profile, December 2002.
RFC 3513	Hinden, Deering, Internet Protocol Version 6 (IPv6) Addressing Architecture, April 2003.
RFC 3527	Kinnear et al., Link Selection sub-option for the Relay Agent Information Option for DHCPv4, April 2003.
RFC 3543	Glass, Chandra, Registration Revocation in Mobile IPv4, July 2003.
RFC 3544	Koren, et al, IP Header Compression over PPP, June 2003.
RFC 3545	Koren, et al, Compressing IP/UDP/RTP headers on links with high delay, packet loss and reordering, June 2003.

RFC 3576 Chiba, Dommety, Eklund, Mitton, Aboba, Dynamic Authorization Extensions to Remote Authentication Dial-In User Service (RADIUS), July 2003.

RFC 3579 B. Aboba, et. al., RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), September 2003.

RFC 3587 Hinden, Nordmark, Deering, An IPv6 Aggregatable Global Unicast Address Format, August 2003.

RFC 3646 R. Droms, DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Dec. 2003.

RFC 3736 R. Droms, Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6, April 2004.

RFC 3748 B. Aboba, et. al., Extensible Authentication Protocol (EAP), June 2004.

RFC 3775 D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, June 2004.

RFC 3776 J. Arkko, V. Devarapalli, F. Dupont, Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, June 2004.

RFC 3925 J. Littlefield, Vendor-Identifying Vendor Options for DHCPv4, 2004.

RFC 3963 V. Devarapalli, et. al., Network Mobility (NEMO) Basic Support Protocol, January 2005.

RFC 4187 J. Arkko, et. al., Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), January 2006.

RFC 4280 K, Chowdhury, et al, Dynamic Host Configuration Protocol (DHCP) Options for Broadcast and Multicast Control Servers, November 2005.

RFC 4283 A. Patel, et al, Mobile Node Identifier Option for Mobile IPv6 (MIPv6), November 2005.

RFC 4285 A. Patel, et al, Authentication Protocol for Mobile IPv6, November 2005.

[draft-ietf-mip6-bootstrapping-integrated-dhc] K. Chowdhury, A. Yegin, MIP6-bootstrapping via DHCPv6 for the Integrated Scenario, draft-ietf-mip6-bootstrapping-integrated-dhc.

[Editor's Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor's Note is removed, the inclusion of the above document is for informational purposes only.]

[Draft-ietf-mip6-hiopt] Hee Jin Jang, Alper Yegin, JinHyeock Choi, DHCP Option for Home Information Discovery in MIPv6, Draft-ietf-mip6-hiopt.

[Editor's Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor's Note is removed, the inclusion of the above document is for informational purposes only.]

2.1.2 3GPP2 and TIA

[3] TIA/EIA-553-A, Mobile Station - Base Station Compatibility Standard, November 1999.

[4] A.S0011-17-C v1.0, Interoperability Specification (IOS) for cdma2000 Access Network Interfaces, March 2005.

[5] C.S0001-D, Introduction for cdma2000 Standards for Spread Spectrum Systems, March 2004.

[6] C.S0002-D, Physical Layer Standard for cdma2000 Standards for Spread Spectrum Systems, March 2004.

[7] C.S0003-D, Medium Access Control (MAC) Standard for cdma2000 Standards for Spread Spectrum Systems, March 2004.

[8] C.S0004-D, Signaling Link Access Control (LAC) Standard for cdma2000 Standards for Spread Spectrum Systems, March 2004.

[9] C.S0005-D, Upper Layer (Layer 3) Signaling Standard for cdma2000 Standards for Spread Spectrum Systems, March 2004.

[10] C.S0016-A v2.0, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, December 2001.

[11] C.S0017-A v1.0, Data Service Options for Spread Spectrum Systems , July 2004.

[12] N.S0009, TIA/EIA-41-D Modifications to Support IMSI, January 2002.

[15] C.S0024-A v1.0, cdma2000 High Rate Packet Data Air Interface Standard, April 2004.

[16] C.S0047-0 v1.0, Link-Layer Assisted Service Options for Voice-Over-IP: Header Removal (SO60) and Robust Header Compression (SO61), April 2003.

[17] A.S0008, Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces with Session Control in the Access Network.

[18] A.S0009-0 v1.0, Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces with Session Control in the Packet Control Function.

[19] X.S0054-910-A, Converged Access Network Data Dictionary, August, 2008.

[20] C.S0063-0, cdma2000 High Rate Packet Data Supplemental Services.

[21] X.S0061-0 v1.0, Network PMIP Support, December, 2008.

[22] X.S0057-0 v1.0, E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects, April, 2009.

2.1.3 ITU-T

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

[X.500] ITU-T recommendation X.509, Public-key and Attribute Certificate Frameworks.

2.2 Informative References

2.2.1 3GPP2 and TIA

This section provides references to other documents that may be useful for the reader of this document.

[1] P.R0001, cdma2000 Wireless IP Architecture Based on IETF Protocols, August 2000.

[2] N.S0017-B v1.0, International Implementation of Wireless Telecommunication Systems Compliant with TIA/EIA-41, December 2002.

[13] C.R1001-E, Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards, October. 2005.

[14] S.R0005-B, Network Reference Model for cdma2000 Spread Spectrum Systems, May 2001.

3 Definitions, Symbols and Abbreviations

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

3.1 Definitions

A Resource Record

In the DNS, the A resource record type [RFC 1035] is a record specific to the Internet class that stores a single IPv4 address.

AAAA Resource Record

In the DNS, the AAAA resource record type [RFC 1886] is a record specific to the Internet class that stores a single IPv6 address.

A6 Resource Record

In the DNS, the A6 resource record type [RFC 2874] is a record specific to the Internet class that stores IPv6 address.

A10 Connection

A connection between a PCF and a PDSN that uses a GRE tunnel to transport user data for one or more IP flows for an MS. This is the A10 connection specified in [4].

A10 Interface

The interface between the PCF and PDSN that transports user traffic as specified in [4].

A10 Network

An IP network as defined in [4] connecting the PCFs with the PDSNs.

A11 Interface

The interface between the PCF and PDSN that carries signaling information as specified in [4].

Access Provider Network

A cdma2000 network that provides access to cdma2000 users.

Always On

The Always On Service maintains the subscriber's packet data session in the local network (i.e., for Always On service, the PDSN does not initiate release of the subscriber's packet data session, unless the PDSN determines the user is no longer reachable).

Auxiliary Link Flow

For HRPD, an auxiliary link flow refers to a link flow that is in addition to the main link flow and is initiated on a per need basis, e.g., when a service such as VoIP is invoked.

Auxiliary Service Connection

A logical connection between the MS and the PDSN that is in addition to the main service connection and is established on a per need basis, e.g., when a service such as VoIP is invoked. The data for an auxiliary service connection is usually carried over an auxiliary link flow (HRPD)/auxiliary service instance (cdma2000 1x) and corresponding auxiliary A10 connection.

Auxiliary Service Instance

A cdma2000 1x term, auxiliary service instance refers to an additional service instance (in addition to the main service instance) that is initiated on a per need basis, e.g., when a service such as VoIP is invoked.

Broker RADIUS Server

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

Broker RADIUS Network

A collection of administrative domains that contain Broker RADIUS servers.

Default Treatment

The default treatment is the header and payload compressions that are applied to a packet. The particular compression technique for a given packet is chosen from the set of techniques negotiated during IPCP and CCP.

Fast Handoff

An inter PDSN based low latency handoff between PCFs. Fast handoff between two PDSNs allows a mobile's PPP session to be maintained via a layer two tunnel passing through a Target PDSN to the Serving PDSN. Note: There is also an intra PDSN fast handoff that is described in [4] that is outside the scope of this document.

Handoff

In this document the term "handoff" is defined to mean continuity of IP bindings or PPP link layer state during an interface change from one entity to another. In the absence of any continuity of state whatsoever, this document does not refer to such interface changes as "handoffs".

Home RADIUS

The RADIUS server that resides in the Home IP Network.

HAAA

The AAA server that resides in the Home IP Network.

Home Access Provider Network

A cdma2000 wireless network that is the home for the mobile subscriber.

Home Address

An MS IP address that remains unchanged regardless of the MS's point of attachment to the network.

Home IP Network

The home network that provides IP based data services to the user. This network is where the user's NAI is homed. This network may be a private network, publicly accessible ISP network, or a cdma2000 wireless network.

Hot-Line Application

The Hot-Line Application is the target of redirection of a hot-lined user's packet data service. The Hot-Line Application is responsible for notifying the user of their Hot-Line status, and interacting with the user to resolve the reason for which he/she was put in the Hot-Lined state. The Hot-Line Application interacts with the HAAA instructing it to Hot-Line a user or to turn Hot-Lining off. The specification of the Hot-Line Application is outside the scope of this document.

Hot-Line Device

The Hot-Line Device is the PDSN or the HA that is communicating with the Home RADIUS Server for the purpose of Hot-Lining the user's packet data session.

Hot-Lined User

A Hot-Lined user is a user whose packet data service has been redirected to a Hot-Line Application and/or blocked by the operator.

Intra PDSN Handoff

A handoff that is between PCFs with direct connectivity to the same PDSN.

Inter PDSN Handoff

A handoff that is between PCFs with connectivity to different PDSNs.

IP Flow

A series of packets that share a specific instantiation of IETF protocol layers. For example, an RTP flow may consist of the packets of an RTP/UDP/IP protocol instantiation, all of which share the same source and destination IP addresses and UPD port numbers.

Link Flow

For HRPD, a link flow is an octet or a packet data stream between an MS and the RAN. Associated with each link flow are one or more ReservationLabels. This document defines two categories of link flow, a main link flow and auxiliary link flow. A link flow corresponds to an RLP flow in [15].

Link Local Address

An IPv6 address whose scope is local to a link.

Main A10 Connection

A connection of type SO33 or SO59 between a PCF and a PDSN that uses a GRE tunnel to transport user data and PPP signaling.

Main Link Flow

For HRPD, the link flow that carries ReservationLabel 0xFF. This specification allows exactly one main link flow per MS.

Main Service Connection

Refers to the logical connection established between the MS and the PDSN over which user traffic and PPP signaling is carried. A main service connection is carried over the main link flow (HRPD)/main service instance (cdma2000 1x) and the corresponding main A10 connection. This specification allows exactly one main service connection per MS.

Main Service Instance

For cdma2000 1x, an MS initiated connection between the MS and the RAN of SO 33. This specification allows exactly one main service instance per MS.

MIP

In this document set the when the term MIP appears we are refers to functionality or capabilities that apply to both MIP4 (Mobile IPv4) and MIP6 (Mobile IPv6).

MS-directed Flow ID-to-A10 connection Mapping

A technique where the MS signals the PDSN explicitly the mapping of IP flow(s) to an A10 connection.

Non-specific Traffic Flow Template

A Non-Specific TFT has the NS bit is set to 1. The PDSN gets the mapping of the flows to the A10 connections from the RAN (see RAN-directed FLOW_ID-to-A10 connection mapping) via A11 signaling. For Non-Specific TFT, the PDSN has one TFT for each MS IP address in support of RAN-directed FLOW_ID-to-A10 connection mapping.

Packet Data Service

A general term used for any packet switched data service offered by an access provider network to a user through the user's MS.

Packet Data Service Option

A number specified in [13] that is used to identify a packet switched data service. A packet data service option may be of type 33, 66 [11], 60/61[16], 59 [17], 64 [17,18] or 67[13, 17, 18].

Packet Data Session

Describes continuous use of packet data service by the user. A packet data session begins when the user invokes packet data service. A packet data session ends when the user or the network terminates packet data service. During a particular MIP packet data session, the user may change its point of attachment while maintaining the same home address.

For Simple IP service, changing points of attachments constitutes a change in packet data session because a new IP address is assigned by the new point of attachment. For Simple IP service, a packet data session and a PPP session are concurrent, where as for MIP service, the packet data session can exist through several changes of the PPP session.

Point of Attachment

Point of attachment refers to the node where the MS is connected to access the IP network. In the context of this document, it refers to the PDSN entity.

Pi

Pi is the interface between the PDSN and the public Internet.

P-P Connection

A connection between a Serving and a Target PDSN that uses a GRE tunnel to transport user data for a single service instance during fast handoff.

P-P Interface

The interface between the Target PDSN and the Serving PDSN that is used to support fast handoff.

P-P Session

The set of all P-P connections for a single MS.

PPP Session

A PPP session describes the time during which the Main Service Connection is maintained between the MS and the Serving PDSN. The PPP session is maintained while the MS is dormant. If a user hands off from one RAN to another RAN but is still connected to the same PDSN, the PPP session remains.

PrePaid Packet Data Service

A function that allows a user to pay in advance for the use of packet data service.

PrePaid Server (PPS)

A function that manages prepaid accounts for the users. It maintains the PrePaid accounts on a per user basis or on a per service type basis for a user. It communicates with the PrePaid client for control of the PrePaid packet Data Service.

PrePaid Client (PPC)

A function that resides in the wireless IP network and communicates with the PrePaid Server function (PPS) to control the prepaid user's packet data session. It requests PrePaid account authorization for a user and monitors the user's packet data session to determine when the limits of the authorization are reached.

PrePaid User

A user who paid for the packet data service in advance. The user is charged by either the wireless IP Network Provider or a 3rd Party Packet PrePaid Service Provider.

Private Address

An IP address conforming to [RFC 1918].

Private Network

An IP Network that is isolated from the global Internet. Generally this type of network may reside behind a firewall, proxy-servers or a NAT (-PT) and may use private IPv4 addresses.

QoS BLOB

An object containing a set of QoS Sub BLOBs for one or more Flow IDs. It also specifies the operation to be performed by the RAN upon receipt from the MS of the QoS Sub BLOB for a Flow ID, such as add/update/remove. The QoS BLOB is only used by cdma2000 1x mobiles.

QoS Sub BLOB

An object containing a set of QoS parameter values or QoS Flow Profile IDs for one Flow ID. A QoS Sub BLOB can be Requested (by the mobile) and Granted (by the RAN) and updated (by the PDSN). This object is used in both cdma2000 1x and HRPD systems.

RADIUS

The specific AAA server implementation used in cdma2000 networks for AAA functionality. The RADIUS servers may be located in the Home IP Network, the Broker RADIUS Network, or the Visited Access Provider Network.

Radio Access Network

The RAN is equivalent to the BS and the PCF as defined in the Network Reference Model [14]. In this document, the terms PCF and RAN are used interchangeably when describing handoffs across the A10 interface. The RAN is equivalent to the Radio Access Network (RAN) specified in [4].

RAN-directed FLOW_ID-to-A10 connection Mapping

The mechanism where the PDSN determines the mapping of an IP flow to an A10 connection based on IP flow identifier information received both from the MS via TFT and from the RAN via A11 signaling.

Reservation

Air interface resources set up by the access network to carry one or more IP flows. A reservation is identified by its ReservationLabel. A ReservationLabel is bound to a link flow.

ReservationLabel

A one octet number that, along with the direction of the corresponding IP flow(s), identifies a Reservation. A ReservationLabel is referred to as Flow Id in this document.

Service Connection

A logical connection between an MS and PDSN used to transport user data for the MS. There are two types of service connection: main and auxiliary (see Main service connection and auxiliary service connection.) Each service connection is comprised of two parts: MS to RAN and RAN to PDSN. In cdma2000 1x, the MS to RAN portion is called a service instance (see service instance.) In HRPD, the MS to RAN portion is called a link flow (see link flow.) In both cdma2000 1x and HRPD, the RAN to PDSN portion is called the A10 connection (see A10 connection.) Under some circumstances the IP flow can be carried on a different link flow/service instance from the link flow/service flow normally associated to an A10 connection.

Service Instance

For cdma2000 1x, a connection between an MS and RAN used to transport user data for a packet data service.

Serving PDSN

A PDSN that supports the PPP session to an MS.

Serving A10 Address

The A10 network interface IP address of the Serving PDSN or that of the Target PDSN when fast handoff is used.

Serving P-P Address

The P-P network interface IP address of the Serving PDSN.

Specific Traffic Flow Template

A Specific TFT is used for cdma2000 1x MS only. A specific TFT has the NS bit set to 0. The PDSN determines the mapping of the IP flows to the A10 connections from the TFT itself using the SR_ID. For a Specific TFT, there is one TFT for each MS IP address and A10 connection pair.

SR_ID

Used in cdma2000 1x, a unique number assigned to each service instance.

Target PDSN

A PDSN that co-operates with a Target RAN over the A10 interface, and co-operates with the Serving PDSN over the P-P interface to provide link layer tunneling between the Serving PDSN and the Target RAN in the context of a fast handoff.

Target P-P Address:

The P-P network interface IP address of the Target PDSN.

Traffic Flow Template:

The Traffic Flow Templates (TFT) may include packet filter(s) that identify the IP flow(s) in both the forward and reverse directions as indicated by the MS. The TFTs are used to map forward traffic to the main or the auxiliary A10s and to indicate if a specific flow treatment (e.g. Header Compression technique) should be applied for the forward packet that matches the packet filter. In the reverse direction, the TFT is used for accounting purposes. There are two types of TFTs: specific and non-specific (see Specific Traffic Flow Template and Non-specific Traffic Flow Template).

User Profile:

The User Profile is an abstraction for the collection of all the parameters applied to the user. The User Profile includes the Subscriber QoS profile (which itself includes the Allowed Differentiated Services Marking and Service Option profile).

Visited Access Provider Network:

The visited service provider provides access services through the establishment of a service agreement with a home service provider.

Visited RADIUS:

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

3.1.1 Symbols and Abbreviations

The following are examples of the appearance of abbreviations:

A10	RAN-PDSN Interface
AAA	Authentication, Authorization, and Accounting
ACCM	Asynchronous Control Character Map
AH	Authentication Header
AVP	Attribute Value Pair
BA	Binding Acknowledgement
BU	Binding Update
BCE	Binding Cache Entry
BCMCS	Broadcast and Multicast Service
BS	Base Station
CA	Certificate Authority
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CN	Correspondent Node
CoA	Care-of Address
COA	Change of Authorization
CRL	Certificate Revocation List
CSRC	Contributing Source
CVSE	Critical Vendor/Organization Specific Extension
DAD	Duplicate Address Detection
D-H	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
DSA	Digital Signature Algorithm
DSCP	Differentiated Service Code Point
DOI	Domain Of Interpretation
DQ	Duration Quota
DT	Duration Threshold
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
FA	Foreign Agent
FAC	Foreign Agent Challenge
GRE	Generic Routing Encapsulation
HA	Home Agent
HAAA	Home AAA
HAO	Home Address Option
HDLC	High-level Data Link Control
HG	Header Generator
HL	Home Link
HLR	Home Location Register
HoA	Home Address
HoTi	Home Test Init

HRPD	High Rate Packet Data
HRL	Header Reduction Lower
HRU	Header Reduction Upper
IANA	Internet Assigned Numbers Authority
ID	Identification
IETF	Internet Engineering Task Force
IID	Interface Identifier
IK	Integrity Key
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IMT-2000	International Mobile Telecommunications - 2000
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPCP	Internet Protocol Control Protocol
ICMP	Internet Control Message Protocol
IPv6CP	IPv6 Control Protocol
IPsec	IP Security
IR	Initialization and Refresh Packet [RFC 3095]
IRM	International Roaming MIN
IRS	IP Reachability Service
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
LAC	Link Access Control
LCP	Link Control Protocol
LLA	Link-Layer Assisted
MAC	Medium Access Control/Message Authentication Code
MEID	Mobile Equipment Identifier
MH	Mobility Header
MIN	Mobile Identification Number
MIP	Mobile IP
MIP4	Mobile IPv4
MIP6	Mobile IPv6
MS	Mobile Station
MSID	Mobile Station ID
NAI	Network Access Identifier
NAS	Network Access Server
NAT (-PT)	Network Address Translation – Protocol Translation
NCP	Network Control Protocol
NEMO	Network Mobility
NHP	No-Header Packet (as defined in [RFC 3242])
NID	Network ID
NVSE	Normal Vendor Specific Extension
ORO	Option Request Option
OUI	Vendor's Organizationally Unique Identifier
PAP	Password Authentication Protocol
PCF	Packet Control Function
PDCH	Packet Data CHannel

PDSN	Packet Data Serving Node
PHB	Per Hop Behavior
Pi	PDSN – Internet (Interface)
PL	Physical Layer
P-P	PDSN-PDSN (Interface)
PPAC	PrePaid Accounting Capability
PPAQ	PrePaid Accounting Quota (duration/volume)
PPC	PrePaid Client
PPP	Point-to-Point Protocol
PPS	PrePaid Server
PSI	PCF Session ID
PTS	PrePaid Tariff Switch
PZID	Packet Zone ID
QID	Quota IDentifier
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RC	Radio Configuration
RH	Routing Header
RHP	ROHC Header Packet (as defined in [RFC 3242])
RLP	Radio Link Protocol
RAN-PDIT	Radio Access Network-Packet Data Inactivity Timer
RO	Route Optimization
ROHC	Robust Header Compression
RR	Return Routeability
RRP	MIP Registration Reply
RRQ	MIP Registration Request
RS	Router Solicitation
RSA	Rivest-Shamir-Adleman public key algorithm
RTP	Real-time Transport Protocol
SA	Security Association
SAD	Security Association Database
SDP	Session Description Protocol
SDB	Short Data Burst
SHA	Secure Hash Algorithm
SI	Service instance
SID	System Identification
SIP	Session Initiation Protocol
SO	Service Option
SPD	Security Policy Database
SPI	Security Parameter Index
SR_ID	Service Reference Identifier
SSRC	Synchronization Source
SS7	Signaling System 7
STC	Session Termination Capability
TCP	Transmission Control Protocol
TFT	Traffic Flow Template

TIA	Telecommunication Industry Association
TITSU	Time Interval After Tariff Switch Update
TOS	Type Of Service
TSI	Tariff Switch Interval
TSIG	Transaction Signature
TTL	Time To Live
UDP	User Datagram Protocol
UDR	Usage Data Record
UR	Update Reason
VAAA	Visited AAA
VLR	Visitor Location Register
VoIP	Voice over IP
VQ	Volume Quota
VQO	Volume Quota Overflow
VSA	Vendor Specific Attribute
VSE	Vendor Specific Extension
VT	Volume Threshold
VTO	Volume Threshold Overflow
VUATS	Volume Used After Tariff Switch
VUATSO	Volume Used After Tariff Switch Overflow

4 Protocol Reference Models

This section specifies the protocol architecture between the entities of the Wireless IP Network architecture. Refer to [1] for the description of the Wireless IP Network architecture, its components and message flows. To support fast handoff, an optional interface between PDSN entities is defined in this document. The architecture in [1] for both MIP and Simple IP has been amended to show the new reference point between two adjacent PDSNs.

4.1 Network Reference Models

Figure 1 shows a reference model for Simple IP service with fast handoff.

Figure 2 shows a reference model for MIP service with fast handoff. For Internet access when the MS is in the home network or roaming, the HA resides in a home access provider network. For private network or home ISP access, the HA resides in the respective external network.

The IP Network entity in Figure 1 and represents IP Networks that may reside in the public Internet as well as private IP networks between access provider networks and home IP networks.

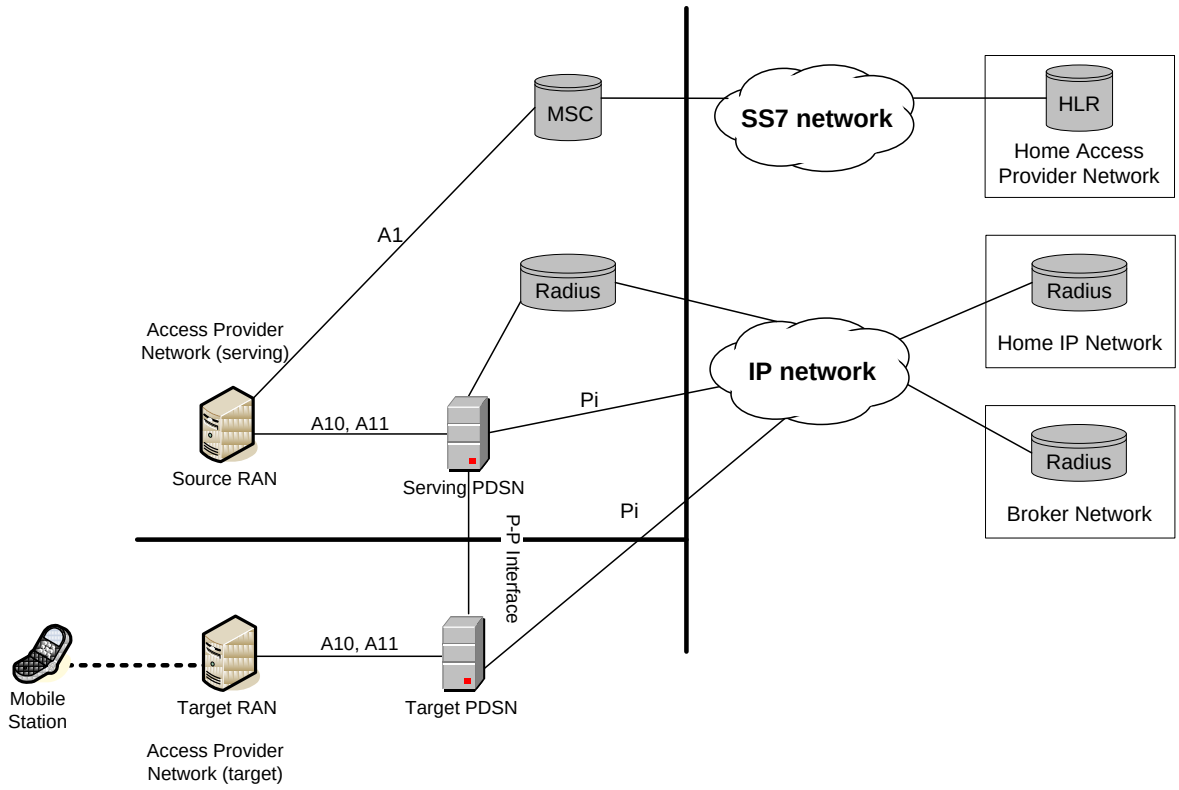

Figure 1 **Reference Model for Simple IP Access with Fast Handoff**

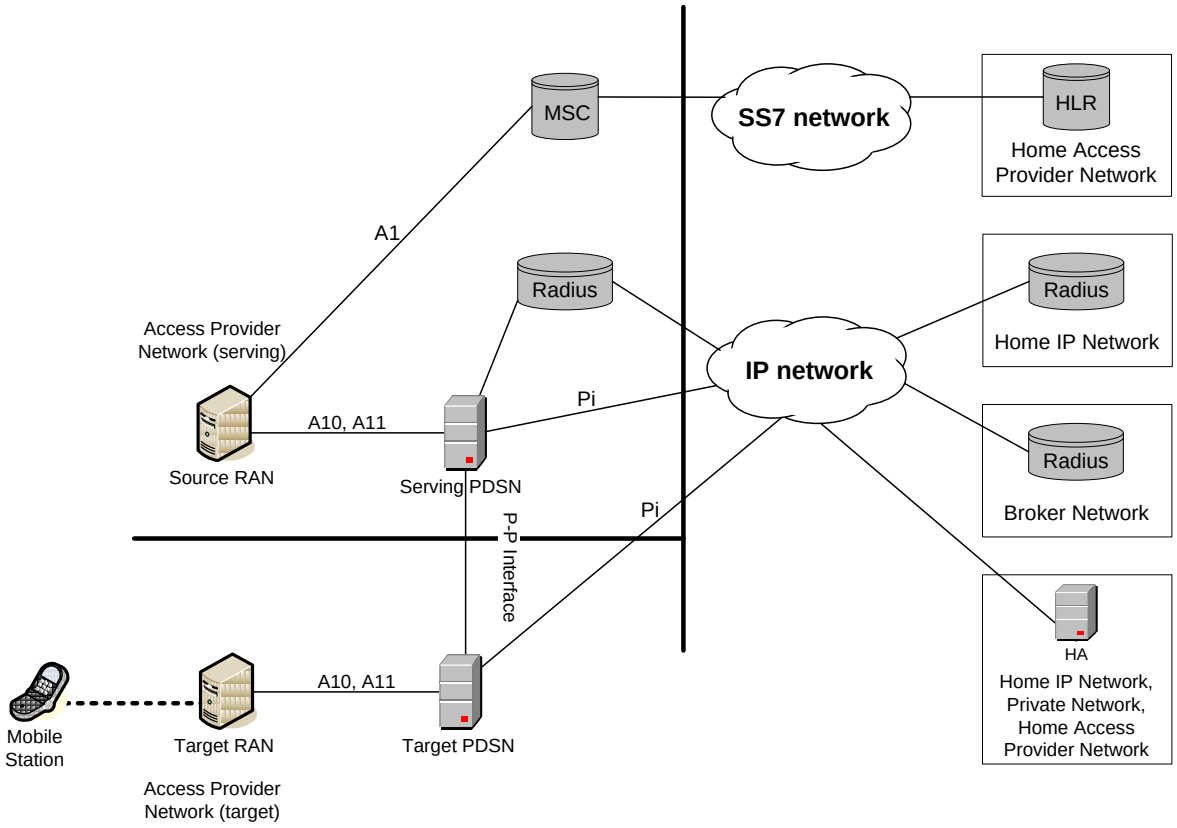

Figure 2 **Reference Model for MIP Access with Fast Handoff**

The MS is implemented as a single MT0 type device or as a MT2 and a TE2 pair. See [11] for details.

Although MIP and Simple IP services are represented in different protocol reference models, the network provides both Simple IP and MIP service simultaneously to an MS using the same PPP session. The network supports IPv4 and IPv6 MSs simultaneously. The network provides Simple IPv4, Simple IPv6, MIP4, and MIP6 service for the same MS over the same PPP session. Support of IPv6 MSs in the network is independent of the IP version used for transport in the RAN.

4.2 Simple IP

Figure 3 shows the protocol reference model for Simple IPv4 or IPv6 service. Figure 4 shows the protocol reference model for Simple IP access during fast handoff.

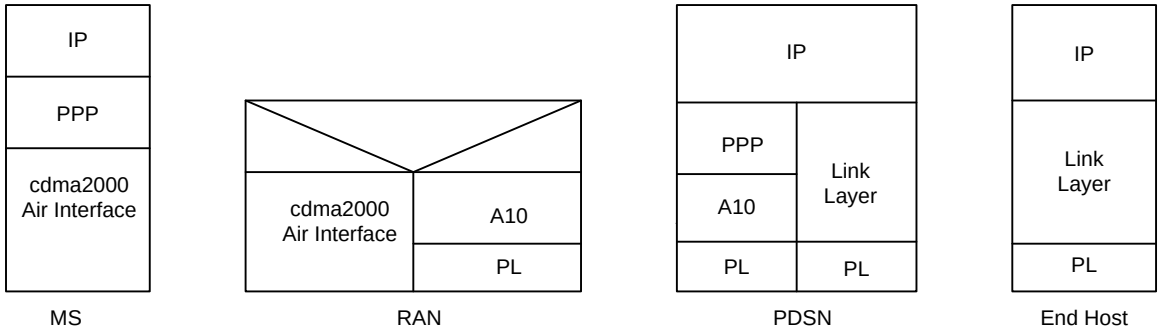

Figure 3 **Protocol Reference Model for Simple IP Access**

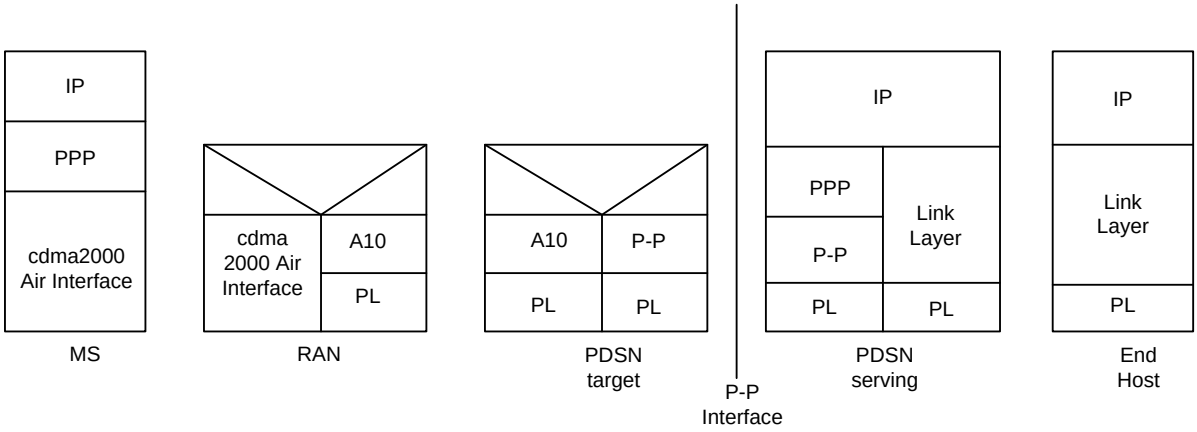

Figure 4 **Protocol Reference Model for Simple IP Access During Fast Handoff**

4.3 MIP4

Figure 5 and Figure 6 show the protocol reference model for MIP4 control and user data, respectively. IPsec is required in some situations, and not in other situations, as detailed in Chapter 2.

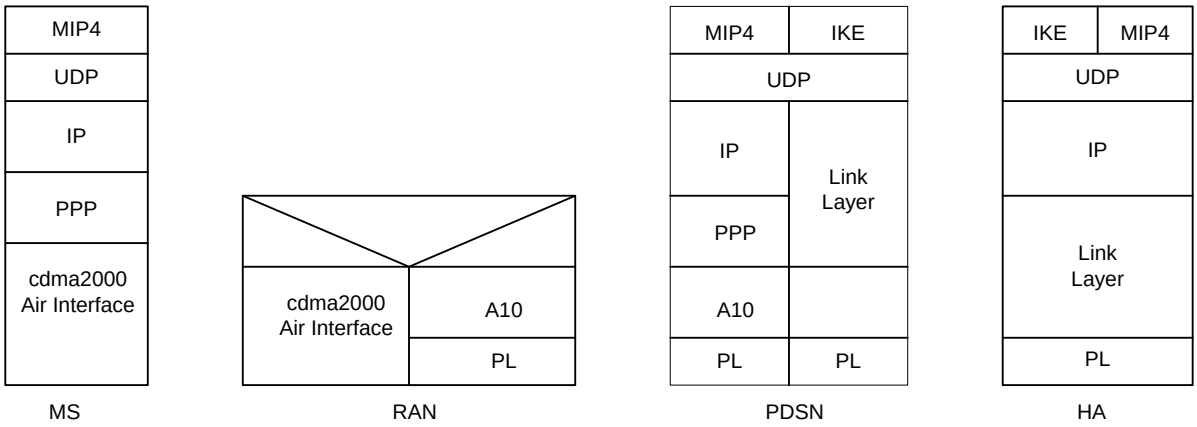

Figure 5 **Protocol Reference Model for MIP4 Control and IKE**

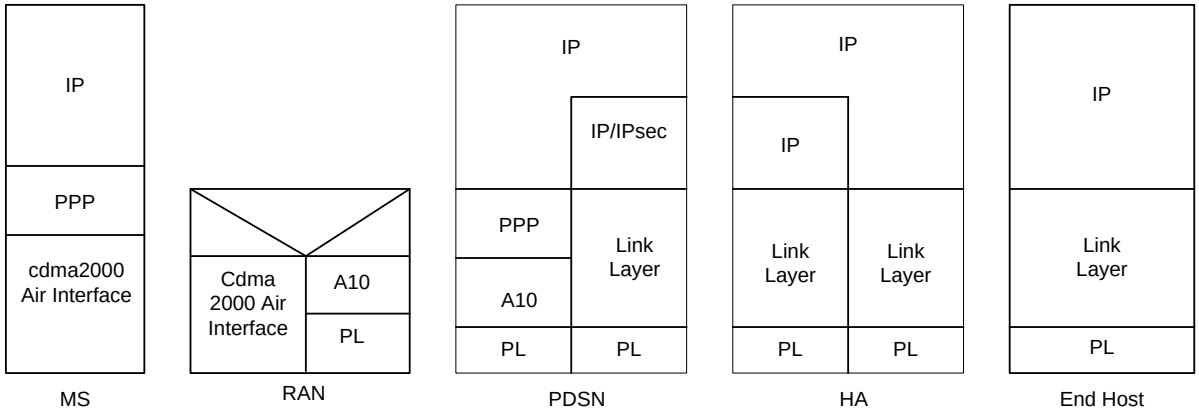

Figure 6 **Protocol Reference Model for MIP4 User Data**

The protocol architecture for MIP4 control and user data during fast handoff is illustrated Figure 7 and Figure 8 , respectively.

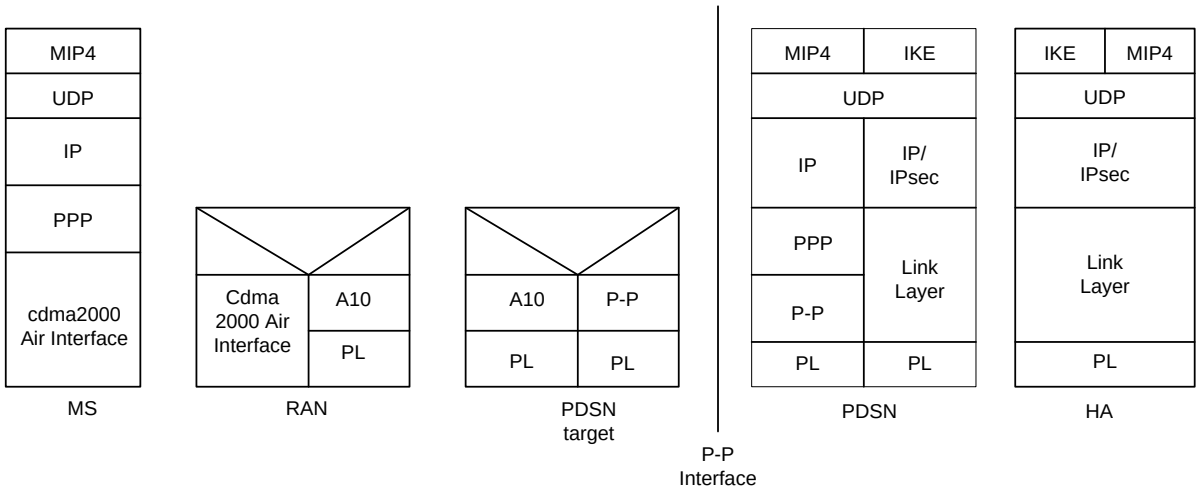

Figure 7 **Protocol Reference Model for MIP4 Control and IKE During Fast Handoff**

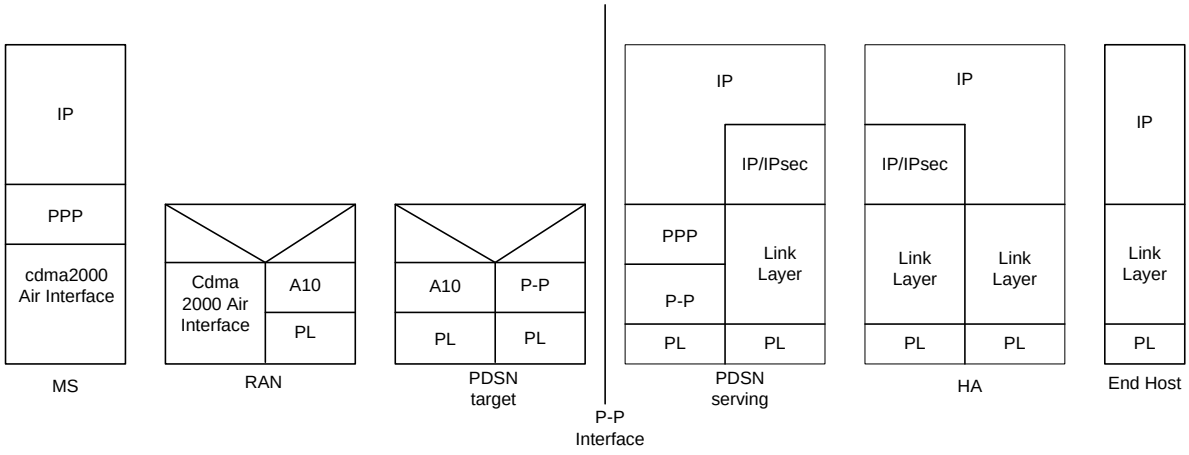

Figure 8 **Protocol Reference Model for MIP4 User Data During Fast Handoff**

The protocol reference models for control and user data during fast handoff are illustrated in Figure 9 and Figure 10, respectively.

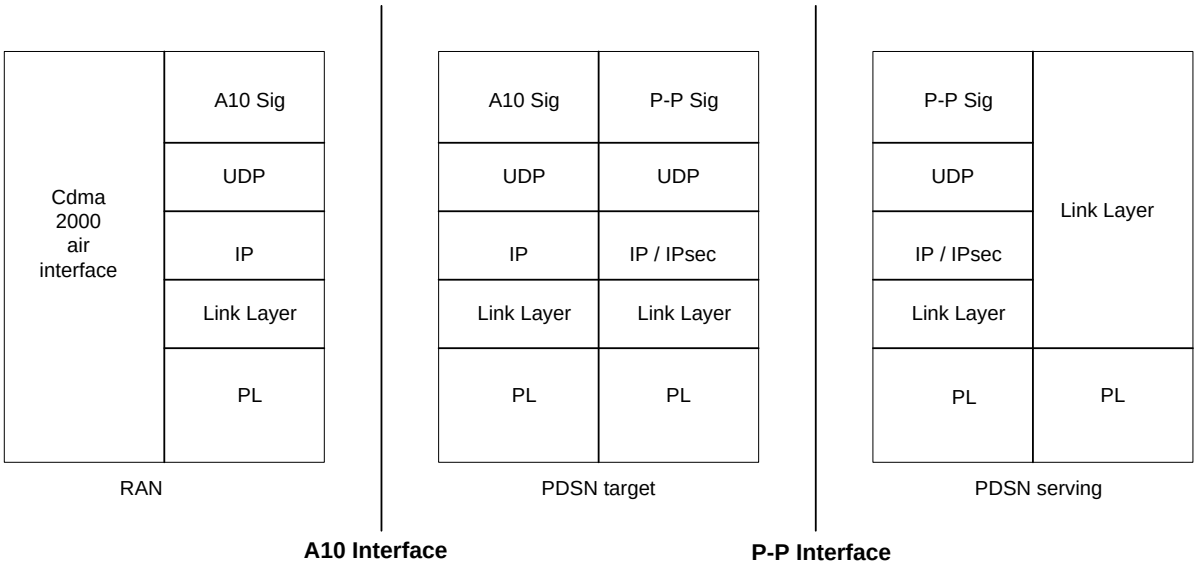

Figure 9 **Protocol Reference Model for Signaling for Fast Handoff**

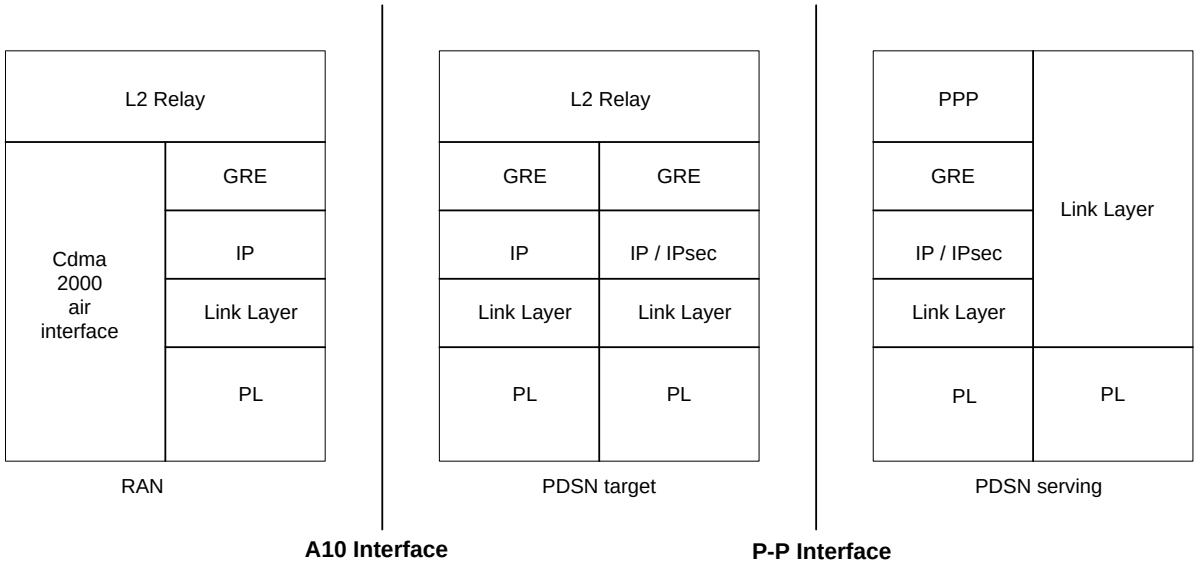

Figure 10 **Protocol Reference Model for User Data for Fast Handoff**

4.4 MIP6

Figure 11 , Figure 12 and Figure 13 show the protocol reference models for MIP6 control data between the MS and the HA, user data in MS-HA bi-directional tunneling mode, and user data in route optimization mode, respectively.

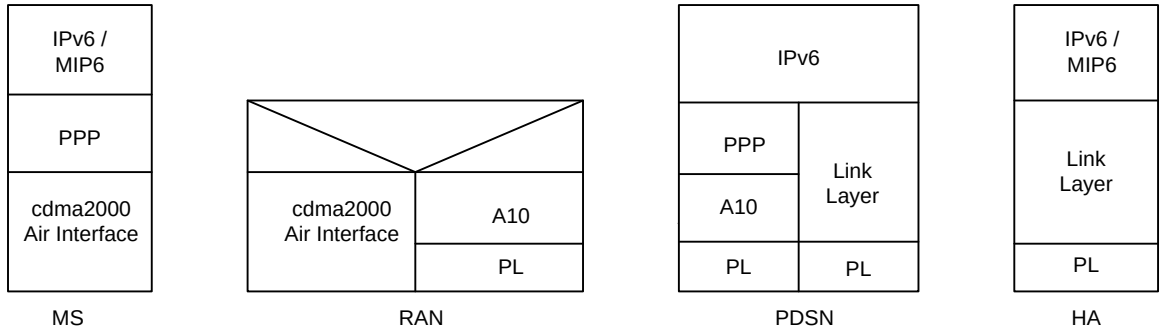

Figure 11 **Protocol Reference Model for MIP6 Control**

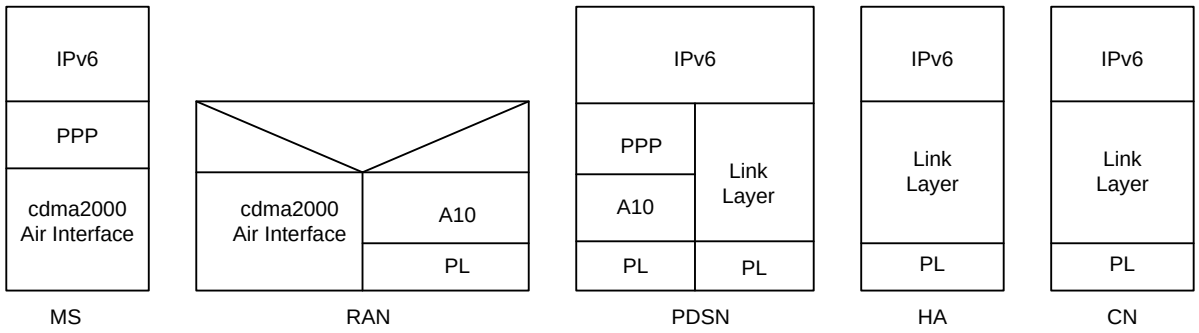

Figure 12 **Protocol Reference Model for MIP6 User Data with Bi-directional Tunneling**

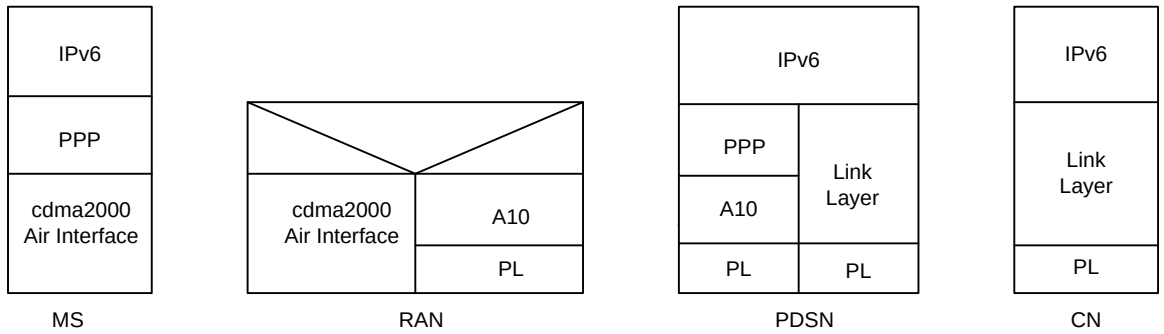

Figure 13 **Protocol Reference Model for MIP6 User Data in RO mode**

The protocol reference models for MIP6 control data between the MS and the HA, user data in MS-HA bi-directional tunneling mode, and user data in route optimization mode during fast handoff are illustrated in Figure 14 and Figure 15 and Figure 16 , respectively.

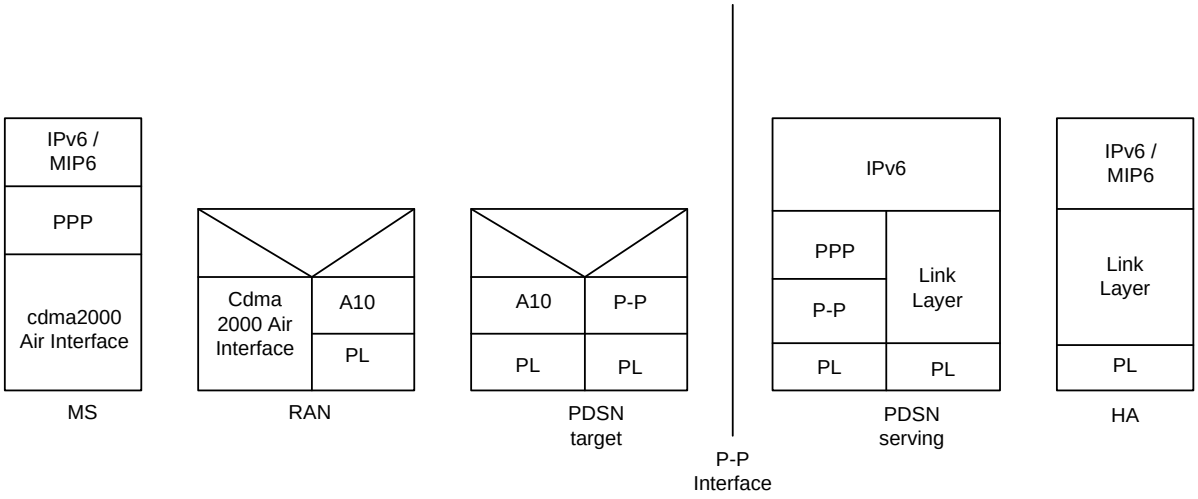

Figure 14 **Protocol Reference Model for MIP6 Control during Fast Handoff**

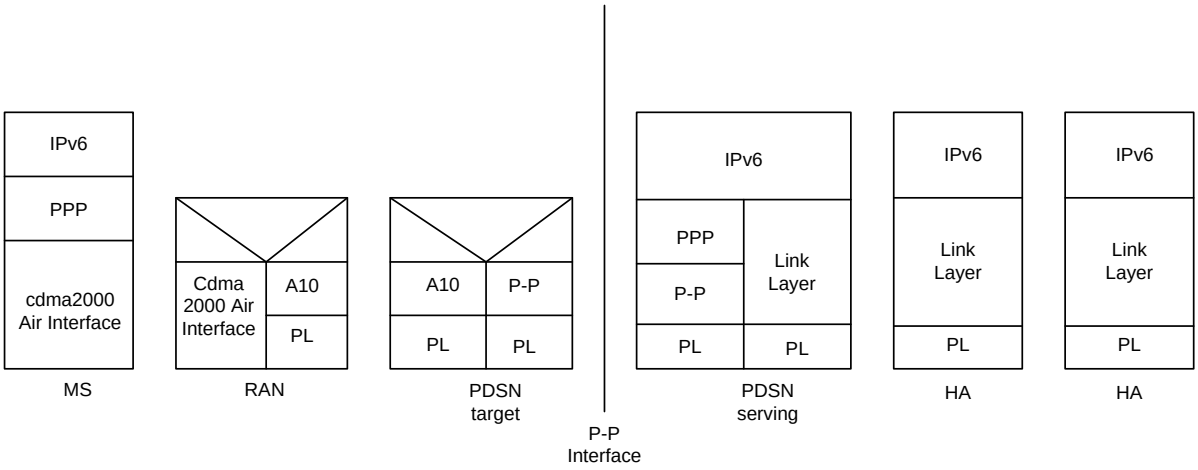

Figure 15 **Protocol Reference Model for MIP6 User Data with Bi-directional Tunneling during Fast Handoff**

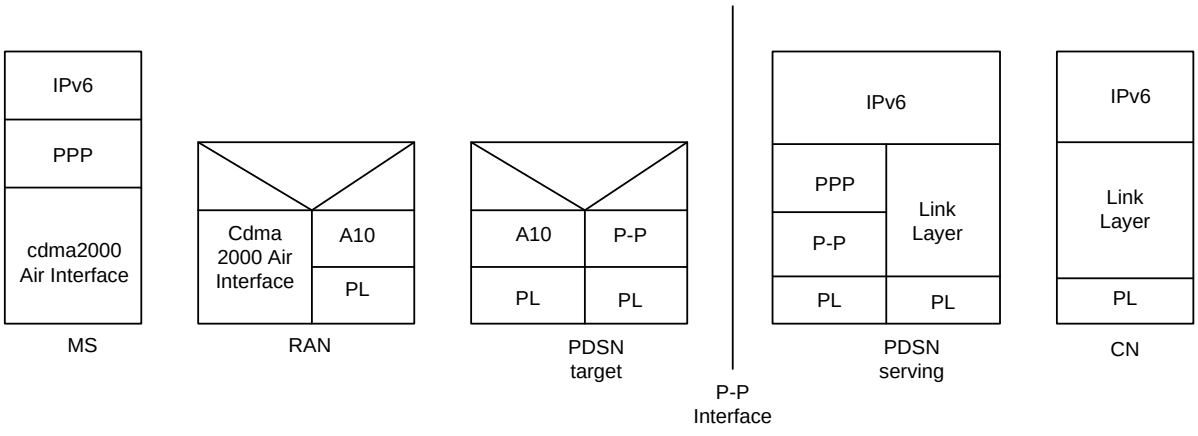

Figure 16 **Protocol Reference Model for MIP6 User Data in RO mode during Fast Handoff**

4.5 RADIUS

Figure 17 shows the protocol reference model for the RADIUS entities in the wireless network (as illustrated in Figure 1 and Figure 2) between the PDSN (RADIUS client) and the Home RADIUS server. In this model, the RADIUS servers in the visited network communicate with the RADIUS servers in the home network via zero or more optional proxy (or Broker) RADIUS servers.

A RADIUS server may run IPv4, IPv6, or both. The method of inter-working between IPv4 and IPv6 RADIUS clients and servers is outside the scope of this document.

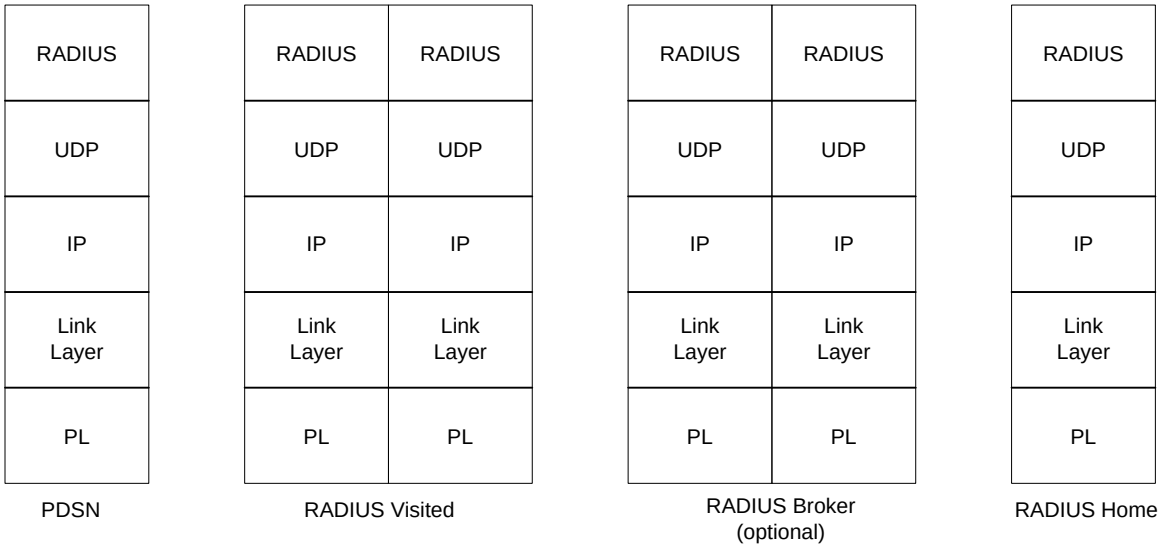

Figure 17 **RADIUS Protocol Reference Model**