3GPP2 X.S0011-003-E

Version: 1.0

Version Date: November 2009

3rd Generation Partnership Project 2
"3GPP2"

cdma2000 Wireless IP Network Standard:

Data Mobility and Resource Management

This page is left blank intentionally.

cdma2000 Wireless IP Network Standard: Chapter 3

CONTENTS

LIST OF FIGURES

LIST OF TABLES

GENERAL DESCRIPTION

This chapter describes the mechanisms at the PDSN resulting from handoff of an MS from one BS/PCF to another BS/PCF, and which may result in changing the serving PDSN for the MS. This chapter describes an optional fast handoff capability, which is a low latency, low data loss handoff mechanism between PDSNs. Fast handoff mechanism delays re-negotiation of PPP until the MS becomes dormant at the Target PDSN. This chapter also describes resource management procedures at the PDSN and the HA that are used following an inter PDSN handoff or under other conditions that require release of resources. Furthermore, a procedure for provisioning the RAN with resource management parameters such as RAN packet data inactivity timers, support for Short Data Burst Indication to the RAN and support for PDSN-PCF flow control are specified in this chapter.

This page is left blank intentionally.

1 Glossary and Definitions

See [Chapter 1].

2 References

See [Chapter 1].

3 Mobility Management

3.1 Mobility Within Radio Access Network

Mobility in the wireless IP network architecture is achieved via handoffs. When a handoff is between PCFs with connectivity to the same PDSN so that the Serving PDSN remains the same before, during, and after handoff, it is called Intra PDSN handoff. When PCFs are connected to different PDSNs, the handoff is termed Inter PDSN handoff.

3.2 Intra PDSN Handoff

The link layer mobility management function is used to manage the change of the A10 connection point of attachment while maintaining the PPP session and IP address(es). The A10 connection point of attachment is the PDSN. When an MS moves from one PCF to another PCF, new A10 connections between the Target PCF and the Serving PDSN are established as necessary.

PCF to PCF handoff may occur while an MS is in the active or dormant state. The purpose of dormant PCF handoff is to maintain the PPP session while an MS is dormant to minimize the use of airlink resources.

The PCF to PCF handoff involves:

- PDSN selection.
- New A10 connection setup.
- Previous A10 connection tear down.

The Target PCF triggers a new A10 connection setup. If the PDSN selected is the same Serving PDSN for the MS, then the PDSN triggers a release of the previous A10 session.

During a PCF to PCF handoff, the selection of the same PDSN is given priority in order to maintain the existing PPP session between the PDSN and the MS. If a different PDSN is selected and the MS still desires packet data service, then a PDSN to PDSN handoff may be performed (see Section 3.3). The PDSN supports a low latency PCF to PCF handoff by bicasting data to the target and previous PCF while the MS performs an active handoff.

Each PCF is uniquely identified by an Access Network Identifier. At handoff, the new PCF performs PDSN selection and forwards both the Previous Access Network Identification (if available from the RAN), and its own Access network Identification to the selected PDSN. If the PDSN recognizes the MSID, it compares the Previous Access Network Identifier if non-zero, to the Stored Access Network Identifier for the call to determine if it has a stale packet data session for the MS. If so, the PDSN performs PPP renegotiation with the MS. See PPP establishment procedures in [Chapter 2] and [Chapter 4].

Detailed requirements and standard procedures for PCF to PCF handoff are described in [4].

3.3 Inter PDSN Handoff

For Simple IP, there is no mobility beyond a PDSN coverage area, unless fast handoff procedures are supported that facilitate the PPP session to be anchored at the Serving PDSN until the MS becomes dormant.

MIP provides the IP layer mobility management function that maintains persistent IP addresses across PDSNs. For a MIP based MS to maintain a persistent IP address while moving between PDSNs, the MS re-registers with its HA as per [RFC 2002] and [RFC 3775] with extensions as outlined in [Chapter 2].

For PDSN to PDSN handoff, the MS may be in active or dormant state. For an active state MS, fast handoff may be supported between PDSNs. If fast handoff is supported, the Target PDSN initiates establishment of a P-P session with the Serving PDSN according to the procedures described later in Section 4. If the MS was in dormant state, the MS transitions to active state for the purpose of establishing connectivity with the new PDSN.

The PDSN to PDSN link for supporting fast handoff is called the P-P interface. Fast handoff with the P-P interface is used to keep the PPP session anchored when the PDSN to PDSN handoff is performed. This allows the existing PPP session to continue, thereby reducing service interruption time and data loss. The forward traffic received at the Serving PDSN is tunneled through the appropriate P-P connection to the Target PDSN. The Target PDSN then forwards the traffic to the MS over the corresponding A10 connection. The reverse traffic from the MS is tunneled through the P-P interface from the Target PDSN to the Serving PDSN. The Serving PDSN then forwards the traffic to the external network.

If fast handoff is not supported, the PDSN to PDSN handoff for MIP involves:

- Establishment of a new PPP session;
- For a MIP4 MS, detection of a new FA via the Agent Advertisement Message;
- Authentication by RADIUS infrastructure;
- For a MIP4 MS, registration with the HA;
- For a MIP6 MS, performing binding update with the HA.

If fast handoff is supported, the PDSN to PDSN handoff for MIP involves:

- Establishment of a P-P connection for each associated A10 connection at the Target PDSN and the continuation of the current PPP session on the Serving PDSN;
- Establishment of a new PPP session and authentication with the RADIUS infrastructure by the Target PDSN when the MS becomes dormant or the MS renegotiates PPP;
- Release of the associated P-P connections while the new PPP session is being established at the Target PDSN;
- For a MIP4 MS, detection of a new FA via the Agent Advertisement Message;
- For a MIP4 MS, registration with the HA;

- For a MIP6 MS, performing binding update with the HA.

If fast handoff is not supported, the PDSN to PDSN handoff for Simple IP involves:

- Establishment of a new PPP session on the Target PDSN.
- Authentication by the RADIUS infrastructure.

If fast handoff is supported, the PDSN to PDSN handoff for Simple IP involves:

- Establishment of a P-P connection for each associated A10 connection at the Target PDSN, and continuation of the current PPP session on the Serving PDSN;
- Establishment of a new PPP session and authentication with the RADIUS infrastructure by the Target PDSN when the MS becomes dormant or the MS renegotiates PPP;
- Release of the associated P-P session while the new PPP session is being established at the Target PDSN.

4 P-P Interface

The P-P interface and related procedures specified in this document only applies to cdma2000®[1] 1x.

4.1 Architecture

The network reference model is depicted in [Chapter 1]. This section describes the functionality for a fast handoff in the context of an inter PDSN handoff. This section provides P-P interface details. See [4] for fast handoff procedures over the A11 interface.

With the implementation of the P-P Interface, the following additional functions are provided by the PDSNs during fast handoff:

- For every A10 connection at the Target PDSN, there is a corresponding P-P connection.
- The Target PDSN is not the end point of PPP at fast handoff.
- The Target PDSN provides transparent bi-directional transport of the bearer data stream over the A10 and P-P connections.
- The Serving PDSN provides bi-directional transport of the bearer data stream over the P-P connections.
- The Target PDSN forwards accounting related airlink records received over an A10 connection to the Serving PDSN over the corresponding P-P connection.
- The Serving PDSN processes airlink records received over the P-P connection similar to the airlink records received over the A10 connection by creating separate UDRs.
- The Target PDSN becomes the Serving PDSN when the MS becomes dormant or the MS initiated PPP renegotiation, in which case the Target PDSN shall use the main service connection to carry on PPP negotiation. When the MS closes the PPP session at the Serving PDSN, the Serving PDSN shall release the P-P connections, and the Target PDSN shall release the A10/A11 connections.

During a fast handoff, either two A10 connections (see Figure 3), or an A10 and P-P connection (see Figure 2), or two P-P connections (see Figure 4) with the same SR_ID and IMSI may exist momentarily due to the PDSN bicasting.

4.2 The P-P Interface Protocol

This section specifies the protocol and messages to be used for signaling for the P-P connections. The P-P Interface protocol is independent of the physical and link layers of the

---

[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.

transport media over which the P-P connection(s) is/are to be established. The underlying transport media provides UDP/IP based packet oriented connectivity.

There are two components for the P-P Interface:

- Signaling: Control messages shall be used for managing the P-P connection(s) between the Serving and the Target PDSNs.
- Bearer Transport: GRE frames shall be used for the transport of bearer data frames between Serving and Target PDSNs.

The Target PDSN shall initiate establishment of a P-P connection, whereas either the Serving PDSN or the Target PDSN may initiate termination of the connection. Termination of a P-P connection shall follow the procedures for A10 connections as specified in [4] in conjunction with the procedures detailed in this chapter. Once a P-P connection has been established, the bearer portion of the P-P connection shall use GRE framing [RFC 2784][RFC 2890] for the transport of bearer data frames. There shall be one P-P connection between the Serving PDSN and the Target PDSN for each A10 connection between the Target PDSN and Target RAN. The GRE payloads in the P-P connection and A10 connection shall be identical for the same connection.

4.2.1 Signaling

The following messages shall be used for P-P Interface call control and signaling:

- P-P Registration-Request.
- P-P Registration-Reply.
- P-P Registration-Update.
- P-P Registration-Acknowledge.
- P-P Session Update.
- P-P Session Acknowledge.

These messages use the same format as A10 connection messages specified in [4], including use of the same UDP port number ’699’. The entire signaling message shall be sent within a single UDP datagram. The source IP address of the P-P Registration-Request, P-P Session-Acknowledge and P-P Registration-Acknowledge messages is set to the Target P-P Address and the destination IP address is set to the Serving P-P Address. The source IP address of the P-P Registration Update, P-P Session-Update and P-P Registration-Reply messages is set to the Serving P-P Address and the destination IP address is set to the Target P-P Address.

The initiator of the P-P connection (Target PDSN) shall pick an available source UDP port, and send a P-P Registration-Request message to the desired destination (Serving PDSN) at UDP port ‘699’. The recipient (Serving PDSN) shall send a P-P Registration-Reply message to the initiator’s (Target PDSN) UDP port that initiated the P-P Registration-Request message. The following indicates the setting of the fields within a P-P Registration signaling message:

Care-of address = Target P-P Address (Only included in P-P Registration-Request message, P-P Registration Acknowledge message and P-P Session Update Acknowledge message).

- Home Address = 0.0.0.0 (in all messages).
- HA Address = Serving P-P Address (in all messages except P-P Registration-Acknowledge and P-P Session Update Acknowledge messages).

- MN-HA Authentication Extension = This element marks the end of the authenticated data in P-P Registration Request and P-P Registration Reply messages.
- Registration Update Authentication Extension = This element marks the end of the authenticated data in P-P Registration Update, P-P Session Update and P-P Session Update Acknowledge messages.

The procedures to support fast handoff over the A10/A11 interface are defined in [4].

4.2.2 Bearer Transport

The P-P bearer frames shall use the same payload format as used on the A10 interface, specified in [4]. The procedures for selection and use of the GRE key are as outlined in [4].

4.3 Fast Handoff procedures overview

The P-P interface shall use the signaling messages defined in section 4.2.1 to manage the P-P connections. The following sections describe the messages and procedures for the P-P interface.

In order to obtain packet data services, the MS performs registration with the packet data network. The service instance(s) is/are assigned and an A10 connection(s) is/are established for each service connection between the Serving RAN and the Serving PDSN on behalf of the MS. For multiple service connection, handling of the bearer data streams over the A10 connections is determined according to [Chapter 4].

During the course of the packet data session, the MS moves into the coverage area of a Target RAN, resulting in an Intra or Inter PDSN handoff. The following two sections specify the Inter PDSN fast handoff for active and dormant service instances separately.

This document assumes that Inter or Intra PDSN handoffs move both active and dormant service connections to the Target RAN. The active and dormant service instances are defined in [4].

4.3.1 Active Service Instances

On detection of a condition that a handoff is required, the Source RAN initiates handoff procedures with the Target RAN (via the MSC).

If the Serving PDSN is reachable from the Target RAN, the fast handoff is performed as specified in [4], and the Serving PDSN shall release:

- Existing A10 connection(s) to the Source RAN.
- P-P connection(s) associated with the MS as a result of a handoff back from the Target PDSN to the Serving PDSN.

If the Serving PDSN is not reachable from the Target RAN, the Target RAN selects a Target PDSN and establishes one A10 connection for each service connection to that PDSN. The A11 Registration-Request message(s) have the 'S' bit set to indicate bicasting of the bearer payloads and contain the Serving P-P Address, the identity of the MS, and an A11 Connection Setup Airlink Record. The Target PDSN shall immediately respond with an A11 Registration-Reply message that contains the serving P-P address as received in the A11 Registration-Request message. For each A10 connection so established, the Target PDSN attempts to establish a P-P connection to the Serving PDSN with the 'S' bit set (to indicate bicasting of the bearer payloads).

The Serving PDSN shall use the SR_ID information in conjunction with the mobile identifier to find the link layer context information associated with the service connection. The Serving PDSN determines whether a P-P connection corresponds to the main service connection by checking the SR_ID received in the associated P-P connection setup message for the IMSI. The Serving PDSN shall apply existing link layer context (e.g., compression, PPP, etc.) when sending packets on the P-P connection.

If the Serving PDSN accepts the P-P Registration-Request message, and the Serving PDSN determines that the P-P connection carries the main service connection, the Serving PDSN shall return a P-P Registration-Reply message with a PPP Link Indicator Extension (see Section 4.6) that indicates that the P-P connection supports the main service connection. The Serving PDSN shall start to bicast bearer data that is appropriately conditioned according to the link layer control to both the Source RAN via the A10 connection and the Target PDSN via the P-P connection (see Figure 2), or to both the previous Target PDSN via the previous P-P connection, and the Target PDSN via the P-P connection (see Figure 4). The Serving PDSN shall bicast until it receives a P-P Registration-Request with the 'S' bit clear. The Target PDSN shall forward bearer data to the Target RAN via the A10 connection.

Upon successful handoff of a service instance to the Target RAN, the Target RAN shall deliver the bearer data from the associated A10 connection to the MS. Also, the Target RAN sends an A11 Registration-Request message with the ‘S’ bit clear and an Active Start Airlink Record to the Target PDSN.

The Target PDSN shall forward the Active Start Airlink Record to the Serving PDSN over the just established P-P connection(s) in a P-P Registration-Request message with the 'S' bit clear. Upon reception of P-P Registration-Request messages with the ‘S’ bit clear, the Serving PDSN shall release the corresponding A10 connections to the Source RAN as identified by the SR_ID, or the P-P connections to the previous Target PDSN.

The Target and Serving P-P addresses, along with the GRE Key form the unique link layer ID for each P-P connection. With the P-P connection(s) in place, bearer data frames pass over these connection(s) in both directions via GRE framing. In the reverse direction, the Serving PDSN shall accept the P-P frames, process and remove the GRE overhead, and then shall process the GRE payload, as necessary. In the forward direction the Serving PDSN shall encapsulate bearer data frames in GRE. The Target PDSN shall process and remove the GRE overhead before passing the bearer data to the associated A10 connection. On the A10 connection, the Target PDSN shall encapsulate the bearer data frames in GRE and shall forward them to the Target RAN. Thus, the Target PDSN shall provide a transparent bi-directional transport for the bearer data frames between the A10 connection and the P-P connection so that there is a point-to-point link layer connection for each service connection between the MS and the Serving PDSN.

The Target PDSN shall maintain the P-P connections by periodically sending P-P Registration-Request messages to the Serving PDSN with ‘S’ bit clear. Each P-P connection shall be maintained as long as the corresponding A10 connection exists at the Target PDSN or until such time as the fast handoff is completed according to Section 4.4.5.

4.3.2 Dormant Service Instances

There are two cases to consider when an MS with dormant service instances moves to an RAN in a different packet zone:

- Case 1: The MS has one or more dormant service instances and no active service instances.
- Case 2: The MS has one or more dormant service instances and one or more active service instances.

Case 1:

Usual dormant handoff procedures apply and there is no fast handoff.

Case 2:

The Target RAN connects active service instances first as detailed in section 4.3.1. When the Target PDSN receives the A11 Registration-Request messages with the A11 connection Setup Airlink Record for the dormant service instances and the 'S' bit set to ‘0’, from the Target RAN, and it determines that there is a fast handoff already in progress for the MS, it shall then establish P-P connections to the Serving PDSN with the ‘S’ bit set to ‘0’ containing the A11 connection Setup Airlink Record for each of the new A10 connections. If the Serving PDSN accepts the P-P Registration-Request message, it shall return a P-P Registration-Reply message to the Target PDSN and shall include the PPP Link Indicator Extension (see Section 4.6) if the P-P connection supports the main service connection. If the Serving PDSN accepts the P-P Registration-Request message, it shall return a P-P Registration-Reply message without the PPP Link Indicator Extension included if the P-P connection supports an auxiliary service connection.

The Serving PDSN shall also release the corresponding A10 connection to the Source RAN as identified by the SR_ID, or the P-P connection to the previous Target PDSN.

If the Target PDSN receives an A11 Registration-Request with the ‘S’ bit cleared and P-P establishment of any service connection has failed, then the Target PDSN shall accept the request. The Target PDSN shall use the PPP establishment procedures as described in [Chapter 4] to establish a new PPP session with the MS.

4.4 Detailed P–P Interface Procedures

4.4.1 P-P Connection Establishment

When a Target PDSN that supports fast handoff receives an A11 Registration-Request from the Target RAN that contains a Serving P-P address, it shall establish a P-P connection to the Serving PDSN. To establish a P-P connection the Target PDSN shall send a P-P Registration-Request message to the Serving PDSN including the A11 Connection Setup Airlink Record (as received from the Target RAN) and start the timer Tregreq (see [4]). If this timer expires, the Target PDSN shall resend the P-P Registration-Request with A11 connection Setup Airlink Record an operator configurable number of times or until an Active Start Airlink Record is received from the Target RAN. In the event any of the P-P connections setup fail, the fast handoff is abandoned and the Target PDSN shall release all P-P connections, if any. The Target PDSN shall negotiate PPP with the MS and shall send its own P-P address to the Target RAN as Serving P-P address (see [4]). Negotiation of PPP at the Target PDSN shall be based on the PPP establishment procedures described in [Chapter 4].

In the P-P Registration-Request message, the Target PDSN shall set the Home Address field to zero, the HA Address field to the Serving P-P address, and the Care-of Address field to the Target P-P address. The Mobile Identifier, SR_ID, and Target PDSN Session Identifier Key shall be included in the Session Specific Extension. The Target PDSN shall assign a Target PDSN Session Identifier Key for the P-P connection. The Target PDSN Session Identifier Key shall be unique within a Target PDSN entity. The ‘S’, ‘T’, and ‘G’ bits shall be set. The Lifetime field shall be set to Tpresetup, whose value is sufficient for the service instance to handoff from the Source RAN to the Target RAN. The IP source and destination addresses in the IP header shall be set to the Target P-P and the Serving P-P address, respectively.

If the P-P Registration-Request message is acceptable, the Serving PDSN shall update the binding record for the MS by creating an association among the IMSI, SR_ID, the Target PDSN Session Identifier Key, Serving PDSN Session Identifier Key (if asymmetric P-P session identifier keys are supported between the Target PDSN and the Serving PDSN), the Target P-P address, and the Serving P-P address. The Serving PDSN shall indicate to the Target PDSN if the newly established P-P connection is the main service connection by including the PPP Link Indicator Extension with a value of 'main service connection' in a P-P Registration-Reply message to the Target PDSN.

The Serving PDSN shall assign a Serving PDSN Session Identifier Key for the P-P connection, if asymmetric P-P session identifier keys are supported between the Target and Serving PDSNs. The Serving PDSN Session Identifier Key is unique within a Serving PDSN entity. The Serving PDSN shall return a P-P Registration-Reply message with an accept indication. In the P-P Registration-Reply message, the Serving PDSN sets the MS Home Address field to zeros. The HA Address fields shall be set to the serving P-P address of the Serving PDSN. The Mobile Identifier, SR_ID and Serving PDSN Session Identifier Key shall be included in the Session Specific Extension. The Lifetime field shall be set to Tpresetup (see [4]), whose value is sufficient for the traffic channel to handoff from the Source RAN to the Target RAN. The IP source address and the IP destination address in the IP header shall be set to Serving P-P address and the Target P-P address, respectively.

On receipt of the P-P Registration-Reply message, the Target PDSN shall create a binding record for the MS by creating an association among the IMSI, SR_ID, the Serving PDSN Session Identifier Key, the Serving P-P Address information, Target PDSN Session Identifier Key, the A10 Interface PDSN Session Identifier Key, the Target PCF Session Identifier Key, and the Target PCF IP address. Bearer data now flows both to the Source RAN via the A10 connection and to the Target PDSN over the newly established P-P connections, or for the case of a continuing fast handoff, to the previous Target PDSN via the previous P-P connection and to the Target PDSN over the newly established P-P connection.

The Target PDSN shall use the SR_ID and the Mobile Identifier to uniquely identify a packet data service connection for a specific MS across RANs and PDSNs.

The GRE keys for the P-P session (i.e., the Target PDSN Session Identifier and Serving PDSN Session Identifier) shall be chosen according to [4].

The Target PDSN shall forward the bearer data to the Target RAN via the pre-setup A10 connection.

On successful handoff of the active service instance(s) to the Target RAN, the Target RAN forwards the Start Airlink Records to the Target PDSN over the pre-setup A11 connection(s), with A10 connection Lifetime set to Trp (see [4]) and 'S' bit cleared . The Target RAN also starts periodically re-registering with the Target PDSN before the expiration of the A10 connection Lifetime.

If the service instance is not handed over to the Target RAN, the pre-setup A11 connection is automatically released on expiry of timer Tpresetup (see [4]) . Upon A11 connection release, the Target PDSN shall release the established P-P connections.

If the P-P connection has been established successfully by the time the Active Start Airlink Record is received from the Target RAN, the Target PDSN shall forward the Active Start Airlink Record over the P-P connection to the Serving PDSN.

On receipt of the A11 Registration-Request message with zero lifetime from the Source RAN, or a P-P Registration-Request message with zero lifetime from the previous Target PDSN (i.e., as in Figure 4), the Serving PDSN shall stop transport of the user data stream to the Source RAN or previous Target PDSN and release the A10 or P-P connection, respectively. Also, following the reception of the Active Stop Airlink Record the Serving PDSN may release the associated A10 connection with the Source RAN, or P-P connection to the previous Target

PDSN. The Target PDSN shall also start periodically re-registering with the Serving PDSN before the expiration of the P-P connection Lifetime. On receipt of P-P Registration-Request message with 'S' bit not set, the Serving PDSN shall stop transport of the bearer data stream to the Source RAN or previous Target PDSN.

4.4.2 P-P Establishment Connection Failure

Depending on the result code, the Target PDSN may attempt to retry setting up of the P-P connection(s). If the P-P connection(s) cannot be established, the Target PDSN shall abandon P-P connection establishment, and shall negotiate PPP with the MS. Negotiation of PPP at the Target PDSN shall be based on the PPP establishment procedures described in [Chapter 4].

At the time an Active Start Airlink Record is received from the Target RAN, if the corresponding P-P connection with the Serving PDSN has not yet been established successfully, the Target PDSN shall fail the fast handoff. It shall initiate release of all P-P connections with the Serving PDSN for this MS, and shall negotiate PPP with the MS. Negotiation of PPP at the Target PDSN shall be based on the PPP establishment procedures described in [Chapter 4].

The P-P Registration-Request message may be retransmitted if no P-P Registration-Reply message is received within a configurable time (TRegreq). Setup of a P-P connection is considered to have failed if no P-P Registration-Reply message is received after a configurable number of P-P Registration-Request message retransmissions.

4.4.3 P-P Connection – Periodic Re-registration

The Target PDSN shall periodically refresh the P-P connection with the Serving PDSN by sending a P-P Registration-Request message before P-P connection registration lifetime (Tpp) expires. The Serving PDSN shall return a P-P Registration-Reply message with an accept indication, including the refreshed Lifetime timer value for the P-P connection. The P-P Registration-Request message may be retransmitted if no P-P Registration-Reply message is received within a configurable time.

If no P-P Registration-Replies are received after a configurable number of P-P Registration-Request message retransmissions for a P-P connection, the Target PDSN shall negotiate a new PPP session with the MS as per the PPP establishment procedures described in [Chapter 4].The Serving PDSN shall close the PPP session if there is no P-P or A10 connection supporting the main service connection.

4.4.4 P-P Interface Release Procedures

This section provides an overview of the P-P interface release procedures. The complete P-P interface release procedures, such as handling of timers, are identical to the A10 connection release procedures found in [4].

The release of P-P connections can be initiated either by the Target PDSN or the Serving PDSN.

4.4.4.1 P-P Connection Release – Target PDSN Initiated

The Target PDSN shall initiate the release of a P-P connection if the corresponding A10 connection has been released, or if the Target PDSN is executing a fast handoff completion as per section 4.4.5. The Target PDSN shall release a P-P connection by sending a P-P Registration-Request message to the Serving PDSN with a lifetime field set to zero. The Target PDSN shall forward any Active Airlink Stop Record received from the Target RAN in the P-P Registration-Request message. The Serving PDSN shall remove the binding information for the P-P connection, and returns a P-P Registration-Reply message with a PPP Link Indicator Extension with the appropriate value. On receipt of the P-P Registration-Reply message, the Target PDSN shall remove binding information for the P-P connection and may initiate PPP negotiation on the main service connection to the MS if the value of the PPP Link Indicator Extension is set to one. The Serving PDSN shall release the associated link context and A10 connection (if one exists).

If the Target PDSN does not receive a P-P Registration-Reply message after sending a configurable number of P-P Registration-Request message retransmissions, the Target PDSN shall remove the binding information for all the P-P connections for the MS.

4.4.4.2 P-P Connection Release – Serving PDSN Initiated

The Serving PDSN shall initiate the release of a P-P connection if:

- the MS returns to an RAN that can reach the Serving PDSN, or
- if the PPP inactivity timer expires and the MS is not Always On, or
- the Serving PDSN closes the PPP session, or
- if the MS renegotiates or closes the PPP session, or
- for administrative reasons.

The Serving PDSN may initiate release of a P-P connection by sending a P-P Registration-Update message to the Target PDSN with a termination indication. When the Serving PDSN releases the P-P connections because the MS closes the PPP session, the Serving PDSN shall indicate to the Target PDSN not to negotiate PPP by including the PPP Link Indicator Extension with a value of 2 (do not negotiate PPP) in a P-P Registration-Reply message to the Target PDSN. When the Serving PDSN releases the P-P connections because the MS renegotiates PPP, the Serving PDSN shall indicate to the Target PDSN to negotiate PPP with a P-P Registration-Update message containing a PPP Link Indicator Extension with a value of 1 (negotiate PPP). In this case the Target PDSN shall reuse the existing A10 connections to renegotiate the PPP link with the MS. If the P-P connection is released by the serving PDSN without an indication to negotiate PPP, the Target PDSN shall release the corresponding A10 connection if one exists. In either case, the Target PDSN shall remove the binding information for the P-P connection, and return a P-P Registration-Acknowledge message. The Target PDSN shall send a P-P Registration-Request message with a lifetime of zero containing any accounting related information received from the Target RAN. On receipt of the P-P Registration-Request message, the Serving PDSN shall respond with a P-P Registration-Reply message and remove binding information for the P-P connection along with any associated link context.

If the Serving PDSN does not receive a P-P Registration-Acknowledge message after transmitting a configurable number of P-P Registration-Update messages, the Serving PDSN shall remove the binding information for all the P-P connections for the MS. It shall also initiate release of the associated link layer context for the MS and A10 connections if one exists.

4.4.5 P-P Fast Handoff Completion

At some point in time, all connected service instances on the Target RAN go dormant. The Target RAN includes an “All Dormant” NVSE in the A11 Registration-Request sent to the Target PDSN when the last service instance goes dormant. This A11 Registration-Request also contains an Active Stop Airlink Record for that last service instance. The Target PDSN shall in turn forward the "All Dormant" NVSE and the Active Stop Airlink Record in the P-P

Registration Request to the Serving PDSN. The Target PDSN shall send an LCP Configure-Request to the MS when it receives a P-P Registration-Reply message containing a PPP Link Indicator Extension with a value of 1 (negotiate PPP).

Simultaneously, the Target PDSN shall initiate release of the P-P connections with the Serving PDSN for the MS.

The Target PDSN becomes the new Serving PDSN after completing a new PPP session negotiation with the MS. The Target PDSN shall update the Target RAN with the new Serving P-P Address (i.e., its own P-P address) in the next A11 Registration-Reply message. The new Serving PDSN shall use the stored A11 Connection Setup Airlink Record from the original A10 connection establishment for accounting purposes.

4.5 Bicasting and Bi-receiving Scenarios

Bicasting is temporary and starts at the Serving PDSN upon reception of an A11 or P-P Registration-Request with the 'S' bit set. Unicast of the payload data resumes at the Serving PDSN upon reception of an A11 or P-P Registration-Request with the 'S' bit clear.

Bi-receiving is temporary and occurs in the following cases:

- The Serving PDSN has A10 connections with both Serving RAN and Target RAN (Figure 1);
- The Serving PDSN has A10 connections with Serving RAN and P-P connections with Target PDSN (Figure 2);
- The Target PDSN has A10 connections with both Serving RAN and Target RAN (Figure 3); or
- The Serving PDSN has P-P connection with two Target PDSNs (Figure 4).

The following scenarios show bicasting and bi-receiving of payload data during fast handoff:

1. Intra PDSN (see Figure 1)
2. Inter PDSN, start of fast handoff (see Figure 2)
3. Intra PDSN, during fast handoff on Target PDSN (see Figure 3)
4. Inter PDSN, during a fast handoff from one Target PDSN to another Target PDSN (see Figure 4).

Cases 1 and 3 are specified in [4].

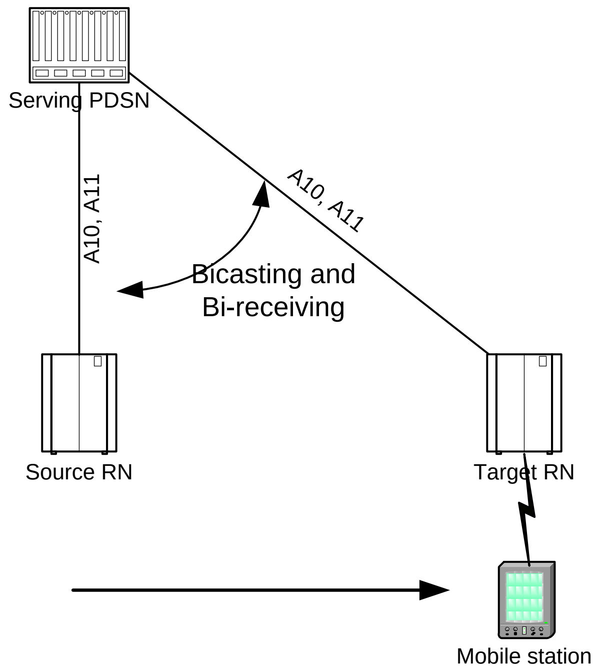

Figure 1 **Intra PDSN Handoff**

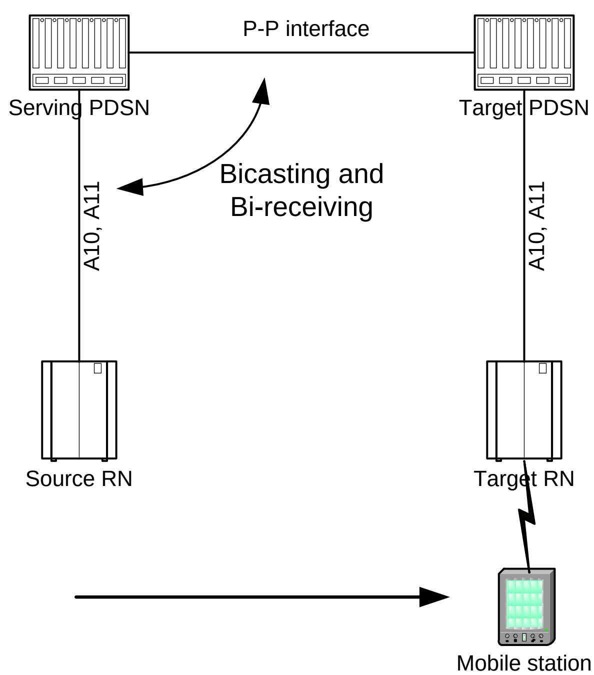

Figure 2 **Inter PDSN, Beginning of Fast Handoff**

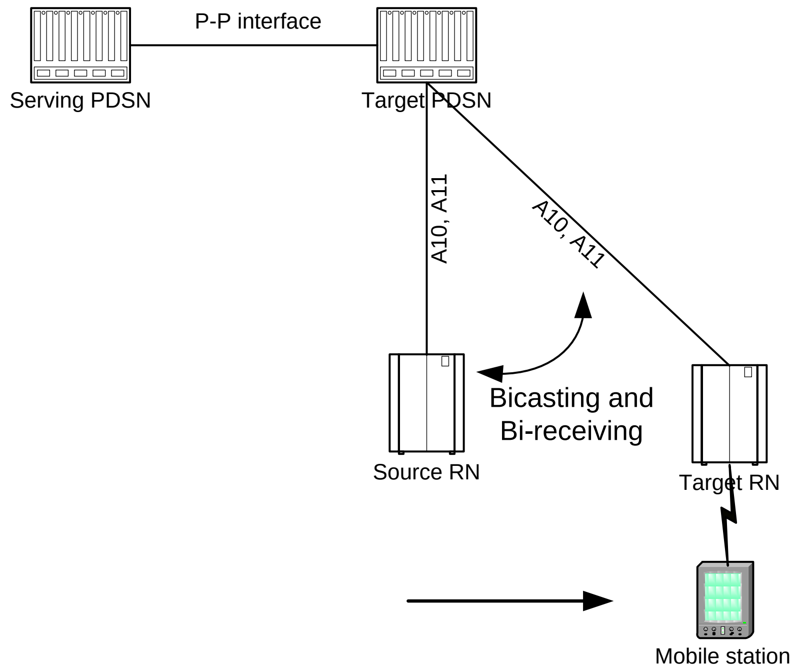

Figure 3 **Intra PDSN, Continuation of Fast Handoff on Target PDSN**

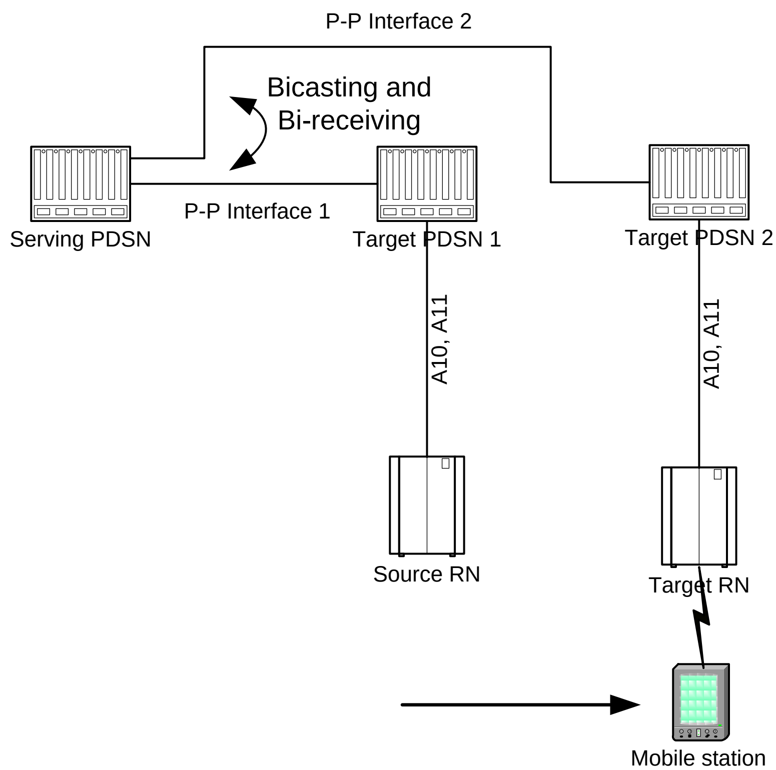

Figure 4 **Inter PDSN Handoff, Continuation of Fast Handoff Between Target PDSNs**

4.6 PPP Link Indicator Extension

The format of a normal P-P vendor specific extension is as follows:

<table>
<tr><td colspan="10"></td><td>1</td><td colspan="9"></td><td>2</td><td colspan="9"></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type</td><td colspan="8">Length</td><td colspan="16">Reserved</td></tr>
<tr><td colspan="32">Vendor/Org-ID</td></tr>
<tr><td colspan="16">Vendor-NVSE-Type</td><td colspan="16">Vendor-NVSE-Value</td></tr>
</table>

Type: 134

Length: 10

Vendor/Org-ID: 5535

Vendor-NVSE-Type: 16

Vendor-NVSE-Value:

0: main service connection
1: negotiate PPP
2: do not negotiate PPP

When the NVSE is present and set to zero, it serves simply to indicate the main service connection. When set to one, it indicates that the PPP session is being renegotiated and the Target PDSN should attempt to negotiate PPP by sending an LCP Configure-Request message to the MS over the main service connection. When set to two, it indicates that the PPP session is closed and the Target PDSN shall not attempt to negotiate the PPP session.

5 Resource Management

Resource management defines the mechanisms to release session related resources at the PDSN and the HA. Resources may be released due to the session being terminated, handoff, the MS becoming unreachable, or for administrative purposes.

The following resources are identified:

- PPP, A10, and P-P sessions.
- MIP bindings.
- Header Compression and Header Removal Contexts.
- Traffic Flow Templates.
- Accounting Usage Data Records.

The PDSN shall support both of the following mechanisms:

- Dynamic Authorization Extensions to RADIUS [RFC 3576].
- Registration Revocation in MIP4 [RFC 3543] with the exceptions as indicated in section 5.2.2.

The HA shall support both of the following mechanism:

- Dynamic Authorization Extensions to RADIUS [RFC 3576].
- Registration Revocation in MIP4 [RFC 3543].

The RADIUS server shall support the following mechanism:

- Dynamic Authorization Extensions to RADIUS [RFC 3576].

While Dynamic Authorization Extensions to RADIUS may be used for both Simple IP and MIP sessions, Registration Revocation in MIP4 is only used for MIPv4 sessions.

The PDSN and the HA shall include in the RADIUS Access-Request message to the Home RADIUS server the 3GPP2 Session Termination Capability (STC) VSA to indicate that they support both Dynamic Authorization Extensions to RADIUS and Registration Revocation in MIP4 using (STC VSA with value 3) (see [Chapter 5]).

Upon receiving a RADIUS Access-Request message containing the STC VSA with value 3, the Home network shall indicate using the STC VSA in the RADIUS Access-Accept message which resource management mechanism shall be used for the packet data session. The STC VSA is interpreted as a bit mask and may take on the following values:

1. Only Dynamic Authorization Extensions to RADIUS is used.
2. Only Registration Revocation in MIP4 is used.
3. Both Dynamic Authorization Extensions to RADIUS and Registration Revocation in MIP4 are used.

5.1 Simple IP

The PDSN shall include a 3GPP2 STC VSA in the RADIUS Access-Request message to the Home RADIUS server. This attribute shall be set to 3 to indicate that Dynamic Authorization Extensions to RADIUS are supported by the PDSN. The PDSN shall also include the NAS-

Identifier attribute containing a Fully Qualified Domain Name (FQDN) for the PDSN in the RADIUS Access-Request message.

If the RADIUS Access-Request message does not include the STC VSA, the Home RADIUS server shall not perform Dynamic Authorization Extensions to RADIUS procedures with the PDSN.

If a RADIUS Access-Request message is received for a user (identified by an NAI and/or IMSI), the Home RADIUS server compares the NAS-Identifier and/or NAS IP address with the stored values (if any). If the received values are different than the stored (non-zero) values, the Home RADIUS server determines that an inter PDSN handoff has occurred, and updates the state information with the received values from the RADIUS Access-Request message. The state information shall include at a minimum the NAS-Identifier, the User-Name (NAI), and may include the NAS IP address, the Framed-IP-Address (MS IP Address), and the Calling-Station ID (IMSI).

The Home RADIUS server shall then send to the previous PDSN a RADIUS Disconnect-Request message as per [RFC 3576] to disconnect the user's PPP session and shall include the DisconnectReason VSA to indicate 'MS mobility detection'. The RADIUS server shall send the Disconnect-Request message to the previous PDSN following successful processing of the RADIUS Access-Request message from the new PDSN and sending of a RADIUS Access-Accept message to the new PDSN.

The RADIUS Disconnect-Request message includes the following attributes:

Table 1 **RADIUS Disconnect-Request Attributes used for 3GPP2 Resource Management**

Attributes	Type	Description
NAS-Identifier	M	Contains the NAS-Identifier of the previous PDSN as was sent in a RADIUS Access-Request message
Correlation ID	O	Uniquely identifies the session to be disconnected.
User-Name	M Note 1	Contains the user's NAI to disconnect
Framed-IP-Address	O	May be included to indicate the MS IP address.
Calling-Station-ID	O	May be included to indicate the IMSI.
DisconnectReason	O	May be included to indicate that the MS has moved to a new PDSN area.
Framed-IPv6-Prefix	O	May be included to indicate the user IPv6 prefix to disconnect.
Framed-Interface-ID	O	May be included to indicate the user IPv6 Interface ID to disconnect.

Note 1: If the PDSN receives a RADIUS Disconnect-Request message containing the User-Name attribute without the correlation ID or Framed-IP-Address, the PDSN shall disconnect all packet data sessions associated with the NAI.

The RADIUS Disconnect-Request message shall be routed through the RADIUS servers using the NAS-Identifier attribute. Upon receiving the RADIUS Disconnect-Request message, the PDSN verifies that the session exists and responds with a Disconnect-Ack message.

If the DisconnectReason VSA is included and indicates 'MS mobility detection', the PDSN shall close the PPP session without initiating an LCP Terminate-Request to the MS and shall release any A10 and P-P sessions.

If the DisconnectReason VSA is not included, and if one or more packet data sessions are active for the MS, the PDSN shall close the PPP session. In this case, the PDSN shall determine if an LCP Terminate-Request should be sent to the MS. For an Always On session, the PDSN shall send an LCP Terminate-Request to the MS. The PDSN should also send an LCP Terminate-Request to a non-Always On session unless it has previously received the 'All Dormant Indicator' NVSE.

If the PDSN releases the resources (PPP, A10 and P-P sessions), it shall subsequently send RADIUS Accounting-Request (stop) message(s). The PDSN shall set the Session Continue attribute to 0 (False) in the RADIUS Accounting-Request (Stop) message before sending it to the RADIUS server.

If the Home RADIUS server receives a RADIUS Accounting-Request (Stop) message with Session Continue VSA set to 'False', the Home RADIUS server shall clear the state information associated with the user and the PDSN that sent the RADIUS Accounting-Request (Stop) with Session Continue VSA set to FALSE. The Home RADIUS server shall not send a RADIUS Disconnect-Request message to that PDSN.

If the PDSN receives a RADIUS Disconnect-Request message and determines that session does not exist or that the request cannot be honored, it shall send a Disconnect-NAK message as per [RFC 3576].

5.2 MIP4

The Home RADIUS server shall use the STC VSA together with the home domain policy and the IPsec policy for the user to determine the session termination mechanism that shall be used for each session. The Home RADIUS server shall not send a RADIUS Disconnect-Request message to the PDSN or the HA if the STC VSA:

- is absent in the RADIUS Access-Request message or,
- indicates support for both mechanisms and the home domain policy allows only Registration Revocation in MIP4 by the HAs.

5.2.1 Dynamic Authorization Extensions to RADIUS

The Home IP network shall use Dynamic Authorization Extensions to RADIUS [RFC 3576] for resource management for MIP sessions when both the HA and the PDSN support both Dynamic Authorization Extensions and Registration Revocation for MIP4, and the home domain policy indicates that Dynamic Authorization Extensions is preferred.

The PDSN shall include in the RADIUS Access-Request message to the Home RADIUS server the 3GPP2 STC VSA with value 3 and the NAS-Identifier attribute containing a Fully Qualified Domain Name (FQDN) for the PDSN and shall be able to process a RADIUS Disconnect-Request message from the RADIUS server. A RADIUS Disconnect-Request message may be received by the PDSN during an active PrePaid packet data session (see [Chapter 6]).

The HA shall send a RADIUS Access-Request message to the home RADIUS server upon receiving the initial RRQ for a user and shall include the STC VSA with value 3, a Correlation ID VSA and the NAS-Identifier attribute containing a Fully Qualified Domain Name (FQDN) of the HA.

If the Home RADIUS server receives a RADIUS Access-Request message from the PDSN for a user (identified by an NAI and/or IMSI) and containing the STC VSA, it compares the NAS-Identifier and/or NAS IP address in the received RADIUS Access-Request message with the stored corresponding values (if any). If the received values are different than the stored (non-zero or null) values, the Home RADIUS server determines that an inter PDSN handoff has occurred, and updates the state information with the received values from the RADIUS Access-Request message. The state information shall include at a minimum the NAS-Identifier, the User-Name (NAI), and may include the NAS IP address, the Framed-IP-Address (MS IP Address), and the Calling-Station ID (IMSI). The Home RADIUS server shall send to the previous PDSN a RADIUS Disconnect-Request message as per [RFC 3576]. The RADIUS Disconnect-Request message should be sent following successful processing of the RADIUS Access-Request message from the new PDSN and sending of a RADIUS Access-Accept message. The RADIUS Disconnect-Request message shall include the attributes as defined in Table 1.

The RADIUS Disconnect-Request message shall be routed through the RADIUS servers using the NAS-Identifier attribute. Upon receiving the RADIUS Disconnect-Request message, the PDSN verifies that the session exists and responds with a Disconnect-Ack message. If the DisconnectReason VSA is included and indicates ‘MS mobility detection’, the PDSN shall close the PPP session without initiating an LCP Terminate-Request to the MS and shall release any corresponding A10 and P-P sessions.

If the DisconnectReason VSA is not included, the PDSN shall perform the following:

- If no more than one packet data session is active for the MS, the PDSN shall close the PPP session and shall clear the MIP binding. In this case, the PDSN shall determine if an LCP Terminate-Request should be sent to the MS. For an Always On session, the PDSN shall send an LCP Terminate-Request to the MS. The PDSN should also send an LCP Terminate-Request to a non-Always On session unless it has previously received the ‘All Dormant Indicator’ NVSE.

- If the packet data session for which the RADIUS Disconnect-Request message is received is a MIP session and more than one packet data session is active for the MS, the PDSN shall remove the binding associated with the packet data session and shall send a unicast Agent Advertisement to the MS Home Address [RFC 2002]. In this Agent Advertisement, the PDSN shall set the B bit and set the sequence number field to zero.

If the PDSN releases the resources (e.g. PPP, A10 and P-P sessions, MIP binding), it shall subsequently send RADIUS Accounting-Request (stop) message(s) to the RADIUS server. The PDSN shall set the Session Continue attribute to 0 (False) in the RADIUS Accounting-Request (Stop) message before sending it to the RADIUS server.

If the Home RADIUS server receives a RADIUS Accounting-Request (Stop) message with Session Continue VSA set to ‘False’, the Home RADIUS server shall clear the state information associated with the user and the PDSN that sent the RADIUS Accounting-Request (Stop) with Session Continue VSA set to FALSE. The Home RADIUS server shall not send a RADIUS Disconnect-Request message to that PDSN.

If the PDSN receives a RADIUS Disconnect-Request message and determines that session does not exist or that the request shall not be honored, it shall send a Disconnect-NAK message as per [RFC 3576]. The Home RADIUS server shall send a RADIUS Disconnect-Request message to the HA if it determines that the session shall be terminated at the HA and the HA previously indicated the support for the Dynamic Authorization Extensions to RADIUS capability.

5.2.2 Registration Revocation in MIP4 at the PDSN

The PDSN shall support Registration Revocation in MIP4 per [RFC 3543]. Upon receiving the initial RRQ from the MS, the PDSN shall send a RADIUS Access-Request message to the Home RADIUS server and shall include the STC VSA and a Correlation ID VSA. The PDSN shall set the STC VSA value to 3. If the RADIUS Access-Accept message includes the STC VSA with value 2 or 3, the PDSN shall use Registration Revocation in MIP4 for the session.

If the RADIUS Access-Accept message includes the STC value with value 1, the PDSN shall not include the Revocation Support Extension in the MIP RRQ message. In this case, the HA shall not include the Revocation Support Extension in the MIP RRP, and both the agents will consider the binding to be not revocable via the Registration Revocation in MIP4 procedures.

A PDSN that is allowed by the Home RADIUS server to participate in registration revocation shall include a Revocation Support Extension in all MIP RRQ messages including MIP Re-registration messages. If the associated MIP RRP also includes a valid Revocation Support Extension, then the PDSN shall follow registration revocation procedures as defined in [RFC 3543], and shall consider the associated registration to be revocable. For a registration that is revocable, the PDSN shall send a Registration Revocation message to the HA when the MIP binding is released.

If the PDSN receives a RADIUS Access-Accept message, which does not contain the STC VSA, the PDSN shall use its local policy to determine if Registration Revocation in MIP4 should be used for the session.

Upon reception of a valid Registration Revocation message for a revocable binding, the PDSN shall clear the associated binding and shall send a Registration Revocation Acknowledgement according to [RFC 3543]. If no other MIP registrations are active on the PPP session associated with the revoked binding then the PDSN shall release the associated PPP, A10 and P-P sessions for the revoked registration, in accordance with [Chapter 2].

If other MIP registrations are active on the PPP session (i.e., multiple MIP sessions), the PDSN may notify the MS of the revoked binding if the I bit is set in the Registration Revocation message received from the HA and the local policy at the PDSN allows notification. If I bit was negotiated by the PDSN and HA for the MIP session and I bit is not set by HA in Registration Revocation message, if the are no other MIP registration active the PDSN shall terminate the PPP, A10 and P-P session for the revoked registration without sending an LCP Terminate Request to the MS

The PDSN shall send a Registration Revocation Acknowledgement according to [RFC 3543]. The PDSN shall send a Registration Revocation Acknowledgement message without processing the request for all Registration Revocation messages when the binding does not exist.

For all Mobile IPv4 sessions, the PDSN shall include MN-NAI extension in all Revocation and Revocation Acknowledge messages after the Revocation message header and before the FA-HA Authentication Extension.

For all Mobile IP sessions that previously negotiated GRE encapsulation and GRE Key using the GRE Key CVSE, the PDSN shall include GRE Key CVSE with the PDSN-assigned key value in all Revocation and Revocation Acknowledge messages. The GRE Key CVSE must be included before the FA-HA Authentication extension (if present).

5.2.2.1 Security of revocation messages

A security Association (SA) shall exist between the PDSN and the HA to protect the MIP Registration Revocation messages. The Registration Revocation message shall be protected using an FA-HA Authentication Extension, if a static/pre-configured FA-HA SA exists, or, using IPsec Security Association, or both. See [Chapter 2] for IPsec SA procedures.

If the PDSN does not have a static FA-HA MIP SA or has not established an IPsec SA with the HA at initial MIP RRQ, then Registration Revocation in MIP4 capability shall not be used, and it shall discard any unprotected Registration Revocation messages that may be received from the HA.

5.2.3 Registration Revocation in MIP4 at the HA

The HA shall support Registration Revocation in MIP4 capability [RFC 3543]. Upon receiving the initial RRQ containing the Revocation Support Extension, the HA shall send a RADIUS Access-Request message to the home RADIUS server and shall include the STC VSA and a Correlation ID VSA. The HA shall set the STC VSA value to 3. If the RADIUS Access-Accept message includes the STC VSA with value 1, the HA shall not use Registration Revocation in MIP4 for the session. If the RADIUS Access-Accept message includes the STC VSA with value 2 or 3, the HA shall use Registration Revocation in MIP4 for the session.

When the HA is allowed by the Home RADIUS server to use Registration Revocation in MIP4 for a session, it shall include a Revocation Support Extension in all MIP RRP for which the associated MIP RRQ contained a valid Revocation Support Extension. A registration for which the HA received a Revocation Support Extension and responded with a subsequent Revocation Support Extension shall be considered revocable by the HA. If the MIP RRQ does not include a Revocation Support Extension, the HA shall not send a Registration Revocation message to that PDSN.

If the HA receives a RADIUS Access-Accept message, which does not contain the STC VSA, the HA shall use its local policy to determine if Registration Revocation in MIP4 should be used for the session.

For a registration that is revocable, the HA shall send a Registration Revocation message to the PDSN in the following circumstances:

- The MIP session is administratively disconnected. In this case, if both the FA and the HA have set the I-bit to 1 in the Revocation Support Extensions, the HA should set the I bit to 1 in the Registration Revocation Message.
- MIP handoff to a different PDSN has been detected, and the Registration Request from the new PDSN has the S bit cleared (i.e. the MS is not requesting for simultaneous binding). In this case, the HA shall set the I bit to 0 in the Registration Revocation message to the previous PDSN.

The format of a Registration Revocation message sent from the HA to the PDSN shall adhere to that of [RFC 3543].

Upon receiving a valid Registration Revocation message, the HA shall send a Registration Revocation Acknowledgement message to the IP source address of the Registration Revocation message and should free up any resources associated with the former binding and discontinue all MIP services for it .

For all Mobile IP sessions, the HA shall include MN-NAI extension in all Revocation and Revocation Acknowledge messages after the Revocation message header and before the FA-HA Authentication Extension.

For all Mobile IP sessions that previously negotiated GRE encapsulation and GRE Key using the GRE Key CVSE, the HA shall include GRE Key CVSE with the HA-assigned key value in all Revocation and Revocation Acknowledge messages. The GRE Key CVSE must be included before the FA-HA Authentication extension (if present).

5.2.3.1 Security of revocation messages

A security Association (SA) shall exist between the PDSN and the HA to protect the MIP Registration Revocation messages. The Registration Revocation message shall be protected using an FA-HA Authentication Extension, if a static/pre-configured FA-HA SA exists, or, using IPsec Security Association, or both. See [Chapter 2] for IPsec SA procedures.

If the HA does not have a static FA-HA MIP SA or an IPsec SA with the PDSN, then Registration Revocation in MIP4 capability shall not be used, and it shall discard any unprotected Registration Revocation messages that may be received from the PDSN.

5.3 MIP6

For MIP6 service; the Home Agent keeps the Binding of the MS's Home Address with the Care-of Address while the MS has roamed into a visited network. The MS gains access to the IPv6 network via a PDSN in the visited network. If the MS goes out of coverage for a long period of time or if the MS turns off power without sending a power down registration [5-9], then the binding cache in the HA will be a hung resource until the lifetime of the BU expires.

The Home IP network shall use Dynamic Authorization Extensions to RADIUS [RFC 3576] for resource management for MIP6 sessions. The HA shall send a RADIUS Access-Request message to the Home RADIUS server upon receiving the initial Binding Update from a user. In this RADIUS Access-Request message, the HA shall include the following attributes/VSAs:

- A Correlation ID VSA.
- The NAS-Identifier attribute containing a Fully Qualified Domain Name (FQDN) of the HA.
- The NAI of the user.
- The HoA from the BU.
- The CoA from the BU.
- The STC VSA with bit-1 set to 1.

The RADIUS Access-Request message is used to authenticate the user, see [Chapter 2]. Upon sending a BA back to the MS with success indication (status code = 0), the HA shall send a RADIUS Accounting-Request (start) message to the Home RADIUS server to indicate the beginning of the MIP6 session. At the end of the MIP6 session, the HA shall send a corresponding RADIUS Accounting-Request (stop) message to the Home RADIUS server.

If the Home RADIUS server does not receive a RADIUS Accounting-Request (Stop) from the HA after having received a RADIUS Accounting-Request (Stop) from the PDSN and there is an active MIP6 binding at the HA, the Home RADIUS server shall send a RADIUS Disconnect-Request Message to the HA.

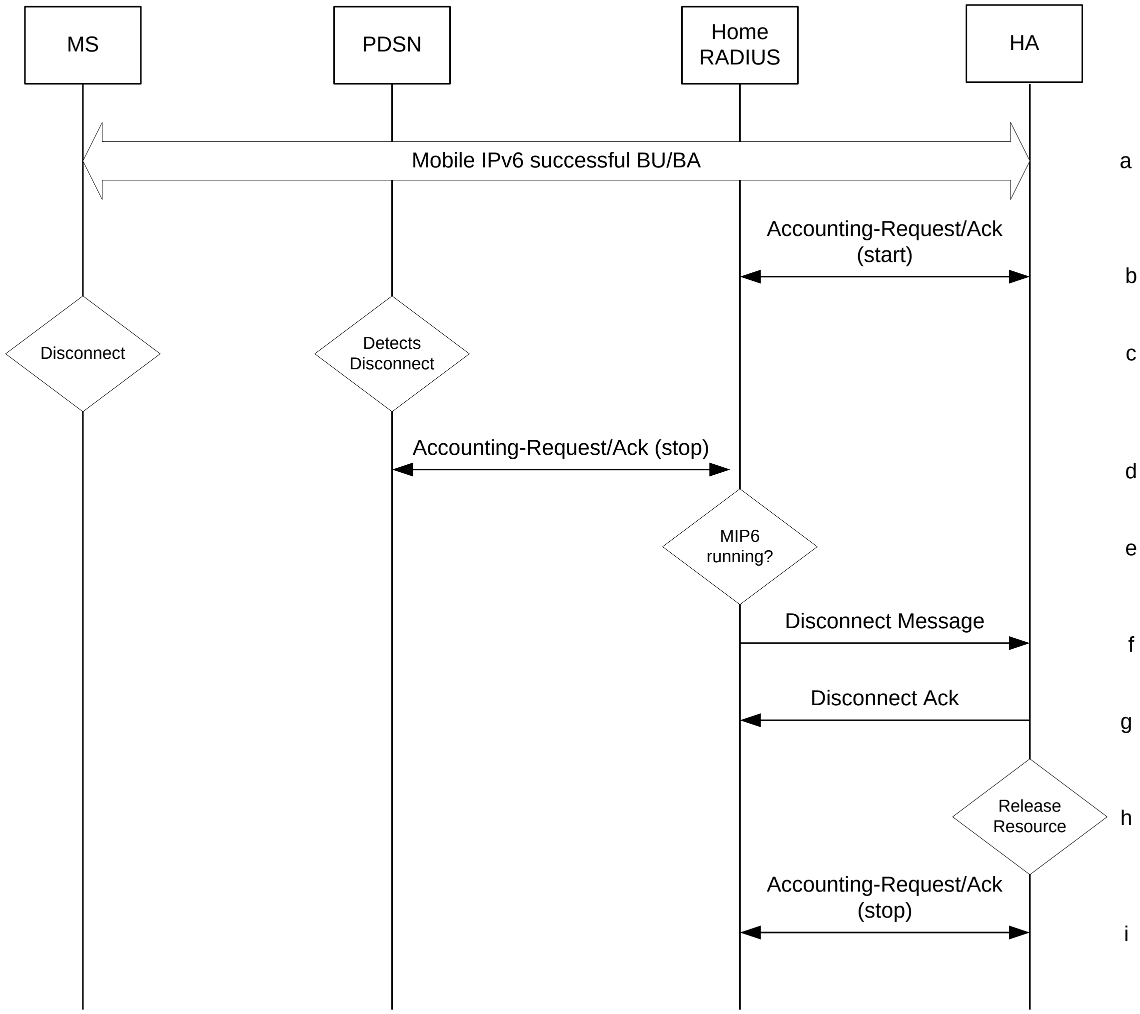

Figure 5 **MIP6 Resource Management**

a. The Mobile Station performs a successful MIP6 Home Registration.

b. Upon sending a Binding Ack with status code =0 (indicating successful MIP6 session creation), the HA sends a RADIUS Accounting-Request (start) message to the Home RADIUS server. The Home RADIUS server sends back a RADIUS Accounting-Response (start).

c. The MS disconnects the packet data session without tearing down the MIP6 session. Alternatively the MS does a power down registration, goes into a long RF fade, runs out of battery or other unexpected event occurs. The PDSN detects disconnect by the mobile. This may be immediate, if the MS did a power down registration or the MS sent an explicit PPP disconnect message. In other scenarios the disconnect detection at the PDSN may be delayed (determined by some timer). This may also happen during inter PDSN dormant Handoff.

d. Upon detection of the packet data (PPP) disconnect the PDSN sends a RADIUS Accounting-Request (Stop) to the Home RADIUS server to indicate the end of the packet data session for the user. The Home RADIUS server sends back a RADIUS Accounting-Response (stop).

e. The Home RADIUS server detects that the MS has a MIP6 binding in an HA for which the Home RADIUS server did not yet receive a RADIUS Accounting-Request (stop) from the HA with the associated CoA. This will trigger the resource release procedure in the Home RADIUS server.

f. The Home RADIUS server sends a RADIUS Disconnect-Request message to the HA including the following attributes:

  - The Correlation ID VSA.
  - The NAS-Identifier attribute containing a Fully Qualified Domain Name (FQDN) of the HA.
  - The NAI of the user.
  - The HoA .
  - The CoA .

g. The HA responds with a RADIUS Disconnect-Request ACK.

h. The HA releases the MIP6 binding (resource).

i. The HA performs a RADIUS Accounting-Stop procedure with the Home RADIUS server in order to complete accounting for the MIP6 session.

The state information in the Home RADIUS server shall include at a minimum the following:

- The Correlation ID (generated by the HA).
- The NAS-Identifier of the HA.
- The NAI of the user.
- The HoA.
- The CoA.

The RADIUS Disconnect-Request message should be sent to the HA following successful processing of the RADIUS Accounting-Request (stop) message from the PDSN. The RADIUS Disconnect-Request message shall include the attributes/VSAs as defined in Table 2.

Table 2 **RADIUS Disconnect-Request Attributes used for MIP6 Resource Management**

Attribute/VSA	Type	Description
NAS-Identifier	M	Contains the NAS-Identifier of the HA.
Correlation ID	M	Uniquely identifies the session to be disconnected.
User-Name	M	Contains the user's NAI to disconnect
MIP6-CoA	M	Included to indicate the Care-of Address of the MS.
DisconnectReason	O	May be included to indicate that the reason for issuing the Disconnect message.
HoA Address (from BU)	M	Included to indicate the Home Address of the MS.

The RADIUS Disconnect-Request message shall be routed through the RADIUS proxy chain using the NAS-Identifier attribute. Upon receiving the RADIUS Disconnect-Request message, the HA shall verify that the MIP6 session exists. If the session exists, the HA responds with a RADIUS Disconnect-Ack message. The HA shall identify the session by using the CoA, the HoA and user's NAI.

If the HA releases the resources (e.g., MIP6 binding), it shall subsequently send a RADIUS Accounting-Request (stop) message to the RADIUS server.

If the HA receives a RADIUS Disconnect-Request message and determines that MIP6 session does not exist, it shall send a RADIUS Disconnect-NAK message as per [RFC 3576].

6 RAN Packet Data Inactivity Timer

In the RAN, the expiration of the RAN PDIT (RAN Packet Data Inactivity Timer) is used to trigger the transition of a packet data service instance from the active state to the dormant state. The RAN PDIT value may be provisioned in the RADIUS server (Visited RADIUS/Home RADIUS), and provided to the RAN via the PDSN, during the user authentication with the RADIUS infrastructure. In this standard, one RAN PDIT value is provisioned for a user and is sent to the RAN over the A10 interface in accordance with [4].

The RAN PDIT value may be stored, on a per user basis, at the Home RADIUS server as part of the user profile, in which case it is sent to the PDSN via the Visited RADIUS server in the RADIUS Access-Accept message. The Visited RADIUS server may override the RAN PDIT value, based on the local policy, prior to forwarding the RADIUS Access-Accept message to the PDSN. If the RADIUS Access-Accept message received from the Home RADIUS does not contain an RAN PDIT VSA , the Visited RADIUS server may include an RAN PDIT VSA with a value, based on the local policy, prior to forwarding the RADIUS Access-Accept message to the PDSN.

If the PDSN supports providing the RAN PDIT to the RAN, the PDSN shall forward the RAN PDIT value to the RAN, in accordance with [4]. In this case the PDSN shall also store the RAN PDIT value in order to support intra PDSN handoffs. If a user initiates multiple packet data sessions, the PDSN may receive more than one RAN PDIT VSA from different home domains. In this case, the largest RAN PDIT value received from different home domains is sent from the PDSN to the RAN. This update may happen during an ongoing packet data session when the PDSN receives a new RAN PDIT value that is greater than the one previously sent to the RAN.

The RAN PDIT value is formatted as an optional extension as specified in [4], and is sent to the RAN over the A10 interface and the P-P interface.

7 cdma2000 1x Short Data Burst/HRPD Data Over Signaling Indication

If the PDSN supports a short data indicator and the PCF has indicated support for cdma2000 1x Short Data/HRPD DOS Indication, the PDSN shall use a configured policy and a packet classification mechanism to tag packets that are suitable for cdma2000 1x SDB/HRPD DOS transmission by the BSC/PCF. When the PDSN tags the packets, it shall include the cdma2000 1x Short Data/HRPD DOS Indicator as an attribute in the GRE header carrying a 3GPP2 packet as specified in [4][17][18]. Detailed specification of Short Data Burst Indication is available in [4].

8 A10 Flow Control

If the PDSN supports GRE packet flow control for an A10 connection and the RAN requests flow control for the connection, the PDSN shall stop sending GRE packets to the RAN on the A10 connection. When the Flow Control Indicator field is set to ‘1’ (XOFF) in the GRE attribute sent by the PCF for an A10 connection, the PDSN may use the Duration Indicator field to determine how to process the packets received for the mobile that map to the A10 connection with transmission off. If the Duration Indicator field is set to ‘0’ (Temporary), then the PDSN may buffer the packets mapped to the connection. If the Duration Indicator field is set to ‘1’ (Indefinite), then the PDSN may discard packets mapped to the connection.

If the PDSN buffers IP packets mapped to a flow for which GRE flow control is turned on and for which a Maximum Buffer Time has been specified by the MS, the PDSN shall not deliver to the RAN packets for which the Maximum Buffer Time is exceeded.

The PDSN shall resume the sending of the GRE packets over the A10 connection when GRE flow control is turned off by the RAN. The PDSN shall transmit any buffered packets first followed by the new packets when the transmission for the A10 connection is restarted.

If the PDSN does not support GRE flow control for an A10 connection, the GRE flow control defaults to off. Detailed specification of PDSN-PCF flow control is available in [4]

9 Radio Access Network Requirements

9.1 General

The PDSN interfaces to the RAN only through the A10/A11 interface and there are no RAN dependent signaling messages transmitted to the PDSN. However, there are some general requirements placed on the RAN:

- Each RAN is connected to at least one PDSN.
- The RAN relays PPP octets between the MS and PDSN.
- For octet oriented service options, the RAN passes octets between the MS and PDSN without any framing conversion.
- The RAN establishes an A10 connection for packet data service instance/link flow as specified in [17][18]. If multiple service connections/link flows are established for a MS, all A10 connections are directed to the same PDSN for that MS.
- The RAN terminates all the A10 connections for the MS if the MS terminates the packet data session with a power down indication.
- The RAN terminates the A10 connection upon request from the PDSN.
- The RAN may buffer user data from the PDSN when radio resources are not in place or insufficient to support the flow of data.

Note: No changes to the IP version used in the RAN are required in order to support IPv6 MSs, i.e., the IP version used in the RAN (including the A10 interface), shall be independent of the IP version of the packets carried in the PPP Sessions.

9.2 A10/A11 Interface Requirements

The PDSN and RAN shall support the A10/A11 interface defined as A10 and A11 interfaces in [4].

In order to support fast handoff, the PDSN and the RAN shall support the A10 and A11 interfaces defined in [4].

For octet oriented service options, the PDSN shall use sequential numbering in the GRE packet header of packets on the A10 interface, to ensure sequential delivery of packets over the A10 interface because:

- The PDSN may send one PPP frame over multiple GRE packets.
- The MS negotiates a header or payload compression algorithm that requires PPP frames to be delivered in sequence.

The PDSN shall contain octets from only one PPP frame in each GRE packet.

9.3 A10 General Handoff Capabilities

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

- The RAN has the capability to determine when an MS enters its coverage area.
- The RAN shall be capable to determine with which PDSN an MS currently has a PPP session, if a PPP session already exists.
- During a packet data session, an MS can move outside the coverage area of one RAN into the coverage area of another RAN. If the previous and the new RAN have connectivity to the same PDSN, the PDSN completes establishment of the A10 session with the new RAN in such a way that the MS maintains the same PPP session. Subsequently, the release of the A10 session will be performed with the previous RAN as described in [4]. If the previous and the new RAN do not have connectivity to the same PDSN, the new RAN establishes a new A10 session to a new PDSN.

Specific handoff procedures for the A10 are not called out in this standard but can be found in [4].