3GPP2 A.S0017-C v3.0

September 2010

Interoperability Specification (IOS) for cdma2000 Access Network Interfaces — Part 7 (A10 and A11 Interfaces)

(3G-IOS v5.0.2)

Revision History

Date	Revision	Description
February 2005	A.S0017-C v1.0	Initial revision. For features supported, refer to [11], section 1.1.3.
December 2005	A.S0017-C v2.0	Support for Enhanced Frequency Hashing and Band Subclasses and support for cdma2000 Pre-Rev D MEID capable mobiles.
September 2010	A.S0017-C v3.0	A1/A1p support for callback of an emergency call.

Table of Contents

List of Tables

Foreword

This foreword is not part of this standard.

This document was produced by TSG-A of the Third Generation Partnership Project 2. This document was developed in accordance with the procedural guidelines of 3GPP2 and its Organizational Partners, and represents the consensus position of these groups.

1.0 Introduction

1.1 Overview

This document contains the message procedures, bitmaps, information elements, and timers used to define the A11 interface.

1.1.1 Purpose

The purpose of this document is to provide the standard for interfacing one or more PDSNs with one or more PCFs. This document defines the functional capabilities, including services and features, of the specified interfaces. These services and features are the defining characteristics that are the basis for the overall system standard.

1.1.2 Scope

This standard provides the specification for the interface that coincides with the Reference Point "A_{quater}" defined in the 3GPP2 Wireless Network Reference Model shown in [I-1]. The scope of this standard includes the following topics:

- Descriptions of the specified functional capabilities that provide packet data services across the PCF-PDSN interface;
- Descriptions of the division of responsibility of the functions provided between the PCF and the PDSN without prescribing specific implementations.

1.2 References

References are either normative or informative. A normative reference is used to include another document as a mandatory part of a 3GPP2 specification. Documents that provide additional non-essential information are included in the informative references section.

1.2.1 Normative

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based upon this document are encouraged to investigate the possibility of applying the most recent editions published by them.

[1~7] Reserved.

[8] 3GPP2 X.S0011-C v2.0, *Wireless IP Network Standard*, six parts, October 2006.
[9] Reserved.
[10] Reserved.
[11] 3GPP2 A.S0011-C v3.0, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 1 Overview*, September 2010.
[12] Reserved.
[13] 3GPP2 A.S0013-C v3.0, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 3 Features*, September 2010.
[14] Reserved.
[15] Reserved.

[16] 3GPP2 A.S0016-C v3.0, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 6 (A8 and A9 Interfaces)*, September 2010.
[17] Reserved.
[18] IETF, RFC 1305 – Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992.
[19] IETF, *RFC 1321 – MD5 Message Digest Algorithm*, April 1992.
[20] IETF, *RFC 2002 – IP Mobility Support*, October 1996.
[21] IETF, *RFC 2784 – Generic Routing Encapsulation (GRE)*, March 2000.
[22] IETF, *RFC 2865 – Remote Authentication Dial In User Service (RADIUS)*, June 2000.
[23] IETF, *RFC 2866 – RADIUS Accounting*, June 2000.
[24] IETF, *RFC 2890 – Key and Sequence Number Extensions to GRE*, September 2000.
[25] IETF, *RFC 3115 – Mobile IP Vendor/Organization-Specific Extensions*, April 2001.

1.2.2 Informative

[I-1] 3GPP2 S.R0005-B v2.0, *Network Reference Model for cdma2000 Spread Spectrum Systems*, May 2007.

1.3 Terminology

1.3.1 Acronyms

Acronym	Meaning
3GPP2	3rd Generation Partnership Project 2
ASCII	American Standard Code for Information Interchange
ANID	Access Network Identifiers
BCD	Binary Coded Decimal
BS	Base Station
BSID	Base Station ID
CANID	Current Access Network Identifiers
CVSE	Critical Vendor/Organization Specific Extension
DAI	Data Available Indicator
DCCH	Dedicated Control Channel
EIA	Electronic Industries Alliance
ESN	Electronic Serial Number
FCH	Fundamental Channel
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Number Authority
IEI	Information Element Identifier
IETF	Internet Engineering Task Force

Acronym	Meaning
IMSI	International Mobile Subscriber Identifier
IOS	Interoperability Specification
IP	Internet Protocol
LSB	Least Significant Bit
MEI	Mobility Event Indicator
MEID	Mobile Equipment Identifier
MSB	Most Significant Bit
MSID	Mobile Station IDentification
NID	Network Identification
NVSE	Normal Vendor/Organization Specific Extension
P-P	PDSN-PDSN
PANID	Previous Access Network Identifiers
PCF	Packet Control Function
PDSN	Packet Data Serving Node
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RC	Radio Configuration, Radio Class
RN-PDIT	Radio Network Packet Data Inactivity Timer
SDB	Short Data Burst
SID	System Identification
SPI	Security Parameter Index
TIA	Telecommunications Industry Association
TLV	Type Length Value

1.3.2 Definitions

Refer to [11] for additional definitions.

1.4 Message Body, Coding, and Ordering of Elements

For each A11 interface message there are a number of information elements that are individually defined in section 4.2. Each information element in a given message is tagged with a reference in section 4.2, a direction indication (i.e., some elements within a message are bi-directional and others are not), and a mandatory/optional type (M/O) indicator. Information elements that are marked as optional carry an additional indication of being either required (R) or conditional (C) (refer to below). Some information elements are reused in multiple messages.

The DIRECTION indication associated with each message element pertains to the use of that particular message element when used with the particular message (i.e., use of the message element may be different in other messages). The format of the DIRECTION indication is as follows:

Table 1.4-1 Element Flow DIRECTION Indication

PCF -> PDSN	Element flows from the PCF to the PDSN
PDSN -> PCF	Element flows from the PDSN to the PCF

The inclusion of information elements in each message is specified as follows:

M Information elements which are mandatory for the message.

O Information elements which are optional for the message.

R Required in the message whenever the message is sent.

C Conditionally required. The conditions for inclusion of this element are defined in the operation(s) where the message is used (refer to [13]) and in footnotes associated with the table defining the order of information elements in the message.

Information elements which are mandatory for a given message shall be present, and appear in the order shown in the message definitions in this chapter. Mandatory and Optional/Required IEs differ predominantly in error processing, refer to section 1.6.

Information elements which are optional for a given message are included as needed for specific conditions. When included, they shall appear in the order shown in the message definition given in this chapter.

An information element may be mandatory for some messages and optional for other messages.

The bitmap tables in the message subsections of 3.0 are patterned after the format for the information elements of section 4.2 and use the following conventions:

⇒ **Element Name{<# instances>:**

= Name of information element.

Different elements within a message are separated by double lines.

Fields within elements are separated by single lines.

Octets are renumbered at the beginning of every element.

[<values>] = Set of allowed values.

} Element Name The number of instances of an element is 1 by default. If the **Element Name{<# instances … }Element Name** notation is used, the <**# instances**> notation indicates:

n = exactly n occurrences of the element

n+ = n or more occurrences of the element

1..n = 1 to n inclusive occurrences of the element

label {<# instances>:

<octet 1>

<octet m>

} label = Number of instances of the bracketed set of fields where <**# instances**> notation indicates:

n = exactly n occurrences of the field

n+ = n or more occurrences of the field

1..n = 1 to n inclusive occurrences of the field

ssss ssss

… = Variable length field.

ssss ssss

1.5 Forward Compatibility Guidelines

This standard is intended to evolve to accommodate new features and capabilities. To ensure that equipment implemented to one revision level interoperates with equipment implemented to later revision levels, the following guidelines are defined for the processing of messages and for the development of messages in future revisions of this standard.

Unexpected signaling information may be received at an entity due to differing revision levels of signaling protocol at different entities within a network: an entity using a more enhanced version of the protocol may send information to an entity implemented at a lower level of the protocol which is outside the protocol definition supported at that receiving entity.

It may happen that an entity receives unrecognized signaling information, i.e., messages, element types or element values. This can typically be caused by the upgrading of the protocol version used by other entities in the network. In these cases the following message processing guidelines are invoked to ensure predictable network behavior.

The sending entity shall send messages that are correctly formatted for the version of the IOS declared to be implemented by the sending entity. To preserve the interoperability between a PDSN and a PCF that have different IOS versions, the use of two element types for the Vendor/Organization Specific Extension element is required, starting with IOS version 4.1. The two types of Vendor/Organization Specific Extension elements i.e., the Critical Vendor/Organization Specific Extension (CVSE) and the Normal Vendor/Organization Specific Extension (NVSE) are defined in [25] where each CVSE/NVSE has a 16 bit application type associated with it. This standard further defines the 16-bit application type as an 8-bit application type and an 8-bit application sub type. Also, the CVSEs/NVSEs introduced in this standard set the Vendor ID to the Internet Assigned Number Authority (IANA) registered 3GPP2 vendor ID.

If a receiving entity receives a CVSE that contains an unrecognized application type/application sub-type the receiving entity shall reject the message containing this application type/application sub-type with an error code indicating that the message was rejected due to the presence of an unknown CVSE. To support new features over the A11 signaling interface, new application types/application sub-types shall be included in an NVSE element. If the receiving entity receives an NVSE with an unrecognized application type/application sub-type, the receiving entity shall ignore the NVSE and process the rest of the A11 signaling message. Within a CVSE or NVSE element containing recognized application type and subtype, if any application data fields are not recognized, those fields are ignored and the remainder of the element is processed to the extent possible.

1.6 Message Processing Guidelines

The following message processing guidelines apply unless overridden by explicit processing directions in other places within this standard.

In the guidelines in this section, “optional” includes both “optional – conditional” and “optional – required” information elements as indicated in the message tables in section 3.0.

1. If a message is received containing a Message Type value which is not defined for the revision level implemented then the message shall be discarded and ignored. There shall be no change in state or in timers due to receipt of an unknown message.
2. If a message is received without an expected mandatory information element for the revision level implemented then the message shall be discarded and ignored. There shall be no change in state or in timers due to receipt of the message.
3. If a message is received that contains an information element which is defined for the revision level implemented but contains invalid values in some fields, these fields shall be ignored and the remainder of the information element processed to the extent possible. The message and all other information elements shall be processed to the extent possible. Failure handling may be initiated if call processing cannot continue. Also refer to message processing guidelines 9 and 10. This guideline does not apply to the CVSE information element; refer to section 1.5 for more information.
4. If a message is received that contains an Information Element Identifier which is not defined for the revision level implemented then that element shall be discarded and

ignored. The message shall be processed to the extent possible. Failure handling may be initiated if call processing cannot continue.

5. If a known but unexpected optional information element is received, that information element shall be ignored. The message and all other information elements shall be processed.
6. If a message is received without an expected optional information element the message shall be processed to the extent possible. Failure handling may be initiated if call processing cannot continue.
7. If a field within a received information element contains a value which is specified as "reserved" or is otherwise not defined in the revision level implemented, this field shall be ignored and the remainder of the information element processed to the extent possible. In this situation, all other information elements shall be processed to the extent possible.
8. Octets and bits designated as "Reserved" or which are undefined for the revision implemented shall be set to zero by a sending entity and ignored by a receiving entity.
9. If an element is received containing a field that is larger than expected, i.e., is indicated as having more bits/octets than expected, then the expected bits/octets of that field shall be processed to the extent possible and the additional bits/octets shall be ignored.
10. If an element is received containing a field that is smaller than expected, i.e., is indicated as having fewer bits/octets than expected, then the length field or other indicator shall be considered correct and the bits/octets actually present in the element shall be processed to the extent possible. Failure handling may be initiated if call processing cannot continue.

1.7 Message Definition Guidelines

1. New messages shall have a Message Type that has never been previously used.
2. Information Element Identifiers may be reused in future revisions only when:

   - The old use of the element identifier is not used in the new revision, and
   - The new use of the element identifier is used only in new messages which were not defined in previous revisions.

   The old use of the element identifier shall be supported within the context of the old messages in which it was used.
3. Defined valid values of Information Elements may be changed in future revisions. The new version shall define the error handling when previously valid values are received.
4. Octets and bits which are undefined or which are defined as reserved may be used in future revisions.
5. The Mandatory/Optional designation of Information Elements within a message shall not change.
6. Mandatory Information elements shall be sent in the order specified in section 3.0.
7. New optional Information Elements in a message shall be defined after all previously defined optional Information Elements other than the authentication extension information elements (e.g. Mobile-Home Authentication Extension and Registration Update Authentication Extension), which shall always be the last information element in the message.

8. All new Information Elements shall be defined with a length field.
9. New information may be added to the end of an existing Information Element, provided that the Information Element is defined with a length field.

1.8 Application of Mobile IP

The A10/A11 interfaces are modeled after Mobile IP; refer to [20]. However, the two protocols have been developed to meet different sets of requirements. With respect to the model in this specification, the PDSN emulates the Home Agent (HA), and the PCF emulates the Mobile node and the Foreign Agent. Note that this application of Mobile IP is different from the application of Mobile IP as specified in [8], which occurs at a higher layer and is transparent to the IOS.

By basing the A10/A11 interface on [20], the IOS may reference sections of [20] rather than reproducing much of the text therein. For instance, message and information element formats, extensions, security mechanisms, and codes are borrowed from [20]. Subsequent sections provide explicit references to [20] when text from that document shall be applied.

Note that this standard deviates from [20] in several respects. First, when registering, the PCF uses a fictitious Home Address (= 0.0.0.0). The PDSN acting as an HA shall not attempt to allocate a non-zero IP address, but instead return the Home IP address of 0.0.0.0 in its reply to the PCF. The PDSN uses information in the Session Specific Extension (IMSI and SR_ID) as an identity of the "Mobile Node". Second, this standard specifies messages (Registration Update, Registration Acknowledge, Session Update, and Session Update Acknowledge) not included in [20]. Third, the Registration Request and Registration Reply messages are used not only for performing registrations, but also to exchange other information (e.g., accounting) between the PCF and the PDSN.

1.9 PCF-PDSN Security Association

Security contexts are configurable between every PCF and PDSN pair on the packet data network. Each security context indicates an authentication algorithm and mode, a secret (a shared key, or appropriate public/private key pair), and a style of replay protection in use. Refer to [20] for details.

An index identifying a security context between a pair of PCF and PDSN is called a Security Parameter Index (SPI). SPI values '0' through '255' are reserved, hence not used in any PCF-PDSN security association.

The "Mobile-Home Authentication Extension" and "Registration Update Authentication Extension" provide a means for authenticating the registration messages on the A11 interface. The Authenticator value in the "Mobile-Home Authentication Extension" and "Registration Update Authentication Extension" protects the following fields:

- the UDP payload of registration messages,
- all prior extensions in their entirety, and
- the Type, Length and SPI fields of the extension.

The authentication algorithm uses the default keyed-MD5 ([19]) in the "prefix-suffix" mode to compute a 128-bit "message digest" of the registration message. The Authenticator value is a 128-bit value computed as the MD5 checksum over the following stream of bytes:

- the shared secret defined by the mobility security association between the PCF and the PDSN and by the SPI value specified in the authentication extension, followed by
- the protected fields from the registration message, in the order specified above, followed by
- the shared secret again.

The Authenticator field itself and the UDP header are NOT included in the computation of the Authenticator value. The receiver uses the SPI value within an authentication extension to determine the security context, and to compute the Authenticator value. A mismatch in the Authenticator values results in rejection of the registration message with error code ‘131’ (sending node failed authentication). Refer to [20] for implementation details.

(This page intentionally left blank.)

2.0 Message Procedures

This section describes message procedures for the A10/A11 interface. In the following sections, the term "valid" is used for messages that pass authentication and whose Identification information element is valid (refer to section 4.2.7).

2.1 A10 Connection Establishment, Refresh and Release Procedures

This section describes message procedures to establish, refresh or release an A10 connection. The release of an A10 connection is controlled by the PCF. For PDSN initiated A10 connection release, the PDSN requests that the PCF release the connection.

2.1.1 A11-Registration Request

This message is sent from the PCF to the PDSN to initiate establishment, refresh or release of an A10 connection. In addition, accounting information pertaining to an A10 connection may be included in any A11-Registration Request message for that connection. Refer to section 2.3 for further details.

2.1.1.1 Successful Establishment Operation

When the PCF receives an A9-Setup-A8 message from a BS, the PCF shall initiate setup of an A10 connection as indicated below unless it has an existing A10 connection for the identified user and SR_ID.

- If the A9-Setup-A8 message does not contain a handoff indication, then the PCF shall initiate setup of the A10 connection upon receiving the A9-Setup-A8 message.
- In a fast handoff situation, the (target) PCF shall initiate setup of the A10 connection upon receiving the A9-Setup-A8 message.
- In all other handoff situations, the (target) PCF shall initiate setup of the A10 connection when the (target) BS captures the MS (i.e., upon receiving an A9-AL Connected message from the BS).

The PCF initiates setup of an A10 connection by sending an A11-Registration Request message to the selected PDSN (refer to "PDSN Selection Algorithm" in [13]) with a non-zero Lifetime value. After sending this message, the PCF shall start timer T_{regreq}. The A11-Registration Request message is structured as specified in section 3.1.

If the connection setup request is accepted, the PDSN creates a binding record for the A10 connection by creating an association between the PDSN Session Identifier (PDSN SID) and the IMSI, the MN Session Reference ID and PCF Addresses. If both the PCF and the PDSN support a Session Identifier Version higher than '0', the PDSN may choose any PDSN SID, otherwise the PDSN SID shall be identical to the PCF Session Identifier (PCF SID). In the case of multiple A10 connections for an MS, each A10 connection has its own binding record and Lifetime timer.

The PCF and the PDSN shall use the PCF IP Address (sent in the A11-Registration Request message) and the PDSN IP Address (returned in the A11-Registration Reply message) as the A10 connection endpoints for the transport of user traffic. The PCF IP Address and the PDSN IP Address form the unique link layer ID for each A10

connection. The PCF and the PDSN maintain an association of the MS's IMSI address and MN Session Reference ID with the A10 connection.

When establishing a new A10 connection, the PCF shall include the ANID NVSE with the Current Access Network Identifiers (CANID) as specified in [13]. If the PCF received the ANID from the BS, it shall populate it in the PANID field of the ANID NVSE sent in the A11-Registration Request message.

If the PCF is able to determine that the setup of the A10 connection is due to a dormant handoff or an inter-PCF hard handoff (e.g., the A9-Setup-A8 message included the Access Network Identifiers (ANID) IE or the Data Ready Indicator field in the A9 Indicators IE was set to '0'), the PCF shall include the Mobility Event Indicator (MEI) CVSE in the A11-Registration Request message. The PCF may provide the PDSN with an indication of PCF enabled features for the A10 connection (e.g. short data indication).

In a fast handoff, the (target) PCF shall set the flag bit S to '1', include the Anchor P-P Address and set the Lifetime value to $T_{presetup}$ in the A11-Registration Request message. In other cases the PCF shall set the Lifetime to $T_{rp.}$

2.1.1.2 Successful Refresh Operation

All A11-Registration Request messages with a non-zero Lifetime value sent for an existing A10 connection have the effect of requesting a refresh of that A10 connection. When sending an A11-Registration Request message for an already existing A10 connection, the PCF shall use the same Key value (refer to the Session Specific Extension in section 4.2.12).

- If the A9-Setup-A8 message does not contain a handoff indication, then the PCF shall send an A11-Registration Request message to the PDSN upon receiving the A9-Setup-A8 message.
- In a fast handoff, the (target) PCF shall send an A11-Registration Request message to the PDSN upon receiving the A9-Setup-A8 message.
- In all other handoff situations, the (target) PCF shall send an A11-Registration Request message to the PDSN to initiate setup of the A10 connection when the (target) BS captures the MS (i.e., upon receiving an A9-AL Connected message from the BS).

If the PCF is able to determine that an inter-PCF hard handoff has occurred (e.g., the A9-Setup-A8 message included the Access Network Identifiers (ANID) IE or the Data Ready Indicator field in the A9 Indicators IE is set to '0'), the PCF shall include the MEI CVSE and the ANID NVSE in the A11-Registration Request message.

In a fast handoff case the Lifetime value shall be set to $T_{presetup}$; in all other cases the Lifetime value shall be set to T_{rp}.

If the PCF set the Lifetime value to $T_{presetup}$ in the A11-Registration Request message (i.e., in the case of a fast handoff), then the PCF shall not refresh the A10 connection unless it is notified that the MS has successfully accessed the target BS. At that time, the PCF refreshes the A10 connection with the PDSN by sending an A11-Registration Request message with Lifetime value set to T_{rp}.

If the PCF set the Lifetime value to T_{rp}, then the PCF periodically refreshes the A10 connection with the PDSN by sending an A11-Registration Request message with a non-

zero Lifetime value before the A10 connection registration Lifetime timer expires. After sending this message, the PCF shall start timer T_{regreq}.

2.1.1.3 Successful Release Operation

The PCF may initiate release of the A10 connection by sending an A11-Registration Request message to the PDSN with Lifetime field set to zero. The PCF shall include accounting related and other information in the A11-Registration Request message. After receiving this message, the PDSN shall remove the binding record for the A10 connection and save the accounting related and other information for further processing. The PDSN shall send an A11-Registration Reply message to the PCF with the Lifetime parameter set to '0'; refer to section 2.1.2.3.

2.1.1.4 Failure Operation

Failure detection at the PDSN: If the A11-Registration Request message is invalid, the PDSN shall send an A11-Registration Reply message indicating authentication failure (Code value 83H) or identification mismatch (Code value 85H) and shall then discard the A11-Registration Request message; refer to section 2.1.2. If the PDSN indicates identification mismatch (Code value 85H) in the A11-Registration Reply message, the PDSN shall also include its own time in the 32 high-order bits of the Identification information element of this message to allow the PCF to avoid identification mismatch for subsequent A11-Registration Request messages.

If the Lifetime timer for an A10 connection expires before the PDSN has received a valid A11-Registration Request message from the PCF, then the PDSN shall delete the binding record for the A10 connection.

Failure detection at the PCF: If the PCF does not receive a valid A11-Registration Reply message from the PDSN before timer T_{regreq} expires, the PCF may retransmit the A11-Registration Request message with a new timestamp in the Identification information element and restart timer T_{regreq}. A connection establishment or refresh is considered to have failed if no valid A11-Registration Reply message is received after a configurable number of A11-Registration Request message retransmissions. For a connection refresh or release, on failure to receive a valid A11-Registration Reply message in response to a configurable number of A11-Registration Request message retransmissions, the PCF removes the binding record for the A10 connection.

2.1.2 A11-Registration Reply

The PDSN sends this message to the PCF to acknowledge receipt of an A11-Registration Request message.

2.1.2.1 Successful Establishment Operation

Upon receipt of an A11-Registration Request message with a nonzero Lifetime value, the PDSN shall respond with an A11-Registration Reply message containing the appropriate value in the Code IE. For a valid A11-Registration Request message, if the PDSN accepts establishment of the A10 connection, it shall send a Registration Accepted indication (Code value 00H) and a non-zero Lifetime parameter value in the message. The value of the Lifetime parameter in the A11-Registration Reply message shall be less or equal to the value of the Lifetime parameter received in the A11-Registration Request message. Upon receiving the A11-Registration Reply message, the PCF shall perform

authentication and identification checks. After the message passes the checks, the PCF shall stop timer T_{regreq} and start the Lifetime timer initialized to the value of the returned Lifetime parameter.

If the PDSN has data to send to the PCF when it receives an A11-Registration Request message, the PDSN shall include a Data Available Indication as a CVSE in the A11-Registration Reply message.

If the PDSN accepts a fast handoff request, the A11-Registration Reply message shall include an NVSE containing the Anchor P-P Address value copied from the corresponding A11-Registration Request message. If the PDSN supports fast handoff and becomes the anchor PDSN, the PDSN shall include its Anchor P-P Address in an NVSE in the A11-Registration Reply message.

If the selected PDSN does not accept establishment of the A10 connection, it shall return an A11-Registration Reply message with a reject result code in the Code IE. Upon receipt of this message, the PCF shall stop timer T_{regreq}.

The PDSN may return an A11-Registration Reply message with result code '88H' (Registration Denied – unknown PDSN address). When code '88H' is used, an alternate PDSN address is included in the A11-Registration Reply message. The address of the alternate proposed PDSN shall be returned in the Home Agent field of the A11-Registration Reply message. Upon receipt of this message, the PCF shall stop timer T_{regreq}.

On receipt of an A11-Registration Reply message with code '88H', the PCF shall either initiate establishment of the A10 connection with the proposed PDSN by sending a new A11-Registration Request message as indicated in this section, or it shall use internal algorithms to select a new PDSN.

If the PCF receives a valid A11-Registration Reply message before timer T_{regreq} expires that indicates identification mismatch (Code value 85H), the PCF may adjust the clock that it uses for communication with the PDSN, retransmit the A11-Registration Request message with a newly generated Identification IE, and restart timer T_{regreq}.

On receipt of a valid A11-Registration Reply message with another result code, depending on the result code, the PCF may attempt to re-try setting up the A10 connection with the same or another PDSN; refer to "PDSN Selection Algorithm" in [13].

The PDSN may provide the PCF with an indication of PDSN enabled features for the A10 connection (e.g. flow control).

2.1.2.2 Successful Refresh Operation

Upon receipt of a valid A11-Registration Request message with a nonzero Lifetime value, the PDSN shall respond with an A11-Registration Reply message with an accept indication (Code value 00H), including a Lifetime parameter value less or equal to the value of the received Lifetime parameter and restart the Lifetime timer initialized to the value of the returned Lifetime parameter. Upon receipt of this message, the PCF shall stop timer T_{regreq} and start the Lifetime timer initialized to the value of the returned Lifetime parameter.

If the PCF receives a valid A11-Registration Reply message before timer T_{regreq} expires that indicates identification mismatch (Code value 85H), the PCF may adjust the clock that it uses for communication with the PDSN, retransmit the A11-Registration Request message with a newly generated Identification IE and restart timer T_{regreq}.

On receipt of a valid A11-Registration Reply message that contains a Code other than "Registration accept" (00H) or "Identification mismatch" (85H), the PCF may resend the message with a newly generated Identification IE based on the clock it uses for communication with the PDSN; otherwise the PCF shall initiate release of the A10 connections to this PDSN.

2.1.2.3 Successful Release Operation

Upon receipt of a valid A11-Registration Request message with Lifetime field set to zero, the PDSN shall respond with an A11-Registration Reply message with an accept indication. Upon receipt of this message, the PCF shall remove the binding record for the A10 connection and stops timer T_{regreq}.

If the PCF receives a valid A11-Registration Reply message before timer T_{regreq} expires that indicates identification mismatch (Code value 85H), the PCF may adjust the clock that it uses for communication with the PDSN, retransmit the A11-Registration Request message with a newly generated Identification IE and restart timer T_{regreq}.

On receipt of a valid A11-Registration Reply message that contains a Code other than "Registration accept" (00H) or "Identification mismatch" (85H), the PCF may resend the message with a newly generated Identification IE based on the clock it uses for communication with the PDSN; otherwise the PCF shall initiate release of the A10 connections to this PDSN.

2.1.2.4 Failure Operation

Failure detection at the PCF: If the A11-Registration Reply message is invalid, the PCF shall discard the message.

Failure detection at the PDSN: None.

2.1.3 A11-Registration Update

The PDSN sends this message to the PCF to initiate release of an A10 connection.

2.1.3.1 Successful Operation

The PDSN may initiate release of an A10 connection by sending an A11-Registration Update message to the PCF. The Home Agent field in the A11-Registration Update message is the PDSN Address and the Home Address is set to zero. The PCF Session Identifier and other session specific information are sent within the Session Specific extension. After sending this message, the PDSN starts timer T_{regupd}.

2.1.3.2 Failure Operation

Failure detection at the PCF: If the A11-Registration Update message is invalid, the PCF shall keep the binding for the A10 connection and shall not update its Lifetime timer. The

PCF shall send an A11-Registration Acknowledge message indicating identification mismatch (Status value 85H) or authentication failure (Status value 83H); refer to section 2.1.4.

Failure detection at the PDSN: If the PDSN does not receive a valid A11-Registration Acknowledge message or an A11-Registration Request message (with the Lifetime parameter set to '0' and accounting related information included) before timer T_{regupd} expires, the PDSN may retransmit the A11-Registration Update message with a new timestamp in the Identification information element and restart timer T_{regreq} a configurable number of times.

If the PDSN has not received a valid A11-Registration Acknowledge message with an update accepted status indication (Status value 00H) or an A11-Registration Request message (with Lifetime parameter set to '0' and accounting related information included) after a configurable number of retransmissions, the PDSN shall remove the binding record for the A10 connection.

2.1.4 A11-Registration Acknowledge

The PCF shall send this message to the PDSN to acknowledge receipt of an A11-Registration Update message.

2.1.4.1 Successful Operation

Upon receipt of a A11-Registration Update message, the PCF shall send an A11-Registration Acknowledge message containing the appropriate Status value. For a valid A11-Registration Update message, if the PCF accepts the update, it shall send an 'accept' indication in the message (Status value 00H), and then request the release of the A10 connection by sending an A11-Registration Request message with a zero Lifetime parameter value; refer to section 2.1.1.3. Otherwise, the PCF shall indicate an 'update denied' status. Upon receipt of this message, the PDSN stops timer T_{regupd}.

If the PDSN receives a valid A11-Registration Acknowledge message before timer T_{regudp} expires that indicates identification mismatch (Code value 85H), the PDSN shall not adjust its clock. The PDSN may resend the A11-Registration Update message after updating the timestamp according to its own clock.

If the PDSN receives a valid A11-Registration Acknowledge message that contains a Status value other than "Update accepted" (00H) or "Identification mismatch" (85H), the PDSN may remove the binding record for the A10 connection. If the value of the Status IE in the A11-Registration Acknowledge message is "Update Denied – reason unspecified" (80H) or "Update Denied – poorly formed Registration Update" (86H), the PCF may initiate a graceful release of the A10 connection as specified in section 2.1.1.3 to avoid stale A10 connections at the PCF.

2.1.4.2 Failure Operation

Failure detection at the PDSN: If the A11-Registration Acknowledge message is invalid, the PDSN shall discard the message.

Failure detection at the PCF: None.

2.2 A10-Connection Update Procedures

The PDSN initiates the update of new or additional packet data session parameters on an existing A10 connection with the messages described in this section.

2.2.1 A11-Session Update

The A11-Session Update message is sent from the PDSN to the PCF to add, change, or update session parameters for an A10 connection. It is also sent to update the PCF with the Anchor P-P Address.

2.2.1.1 Successful Operation

The PDSN may update session parameters of an A10 connection or the Anchor P-P Address by sending an A11-Session Update to the PCF. The Home Agent field in A11-Session Update message is the PDSN Address and the Home Address is set to zero. The PCF Session Identifier and other session specific information are sent within the Session Specific Extension.

The A11-Session Update message includes the session parameter(s) or the Anchor P-P Address in NVSE(s). For session parameter(s), the PCF shall update its session parameters or relay the parameters to the BS according to the specified behavior for the particular parameter. The PCF shall relay the Anchor P-P Address to the BS.

After sending the A11-Session Update message, the PDSN shall start timer T_{sesupd}.

2.2.1.2 Failure Operation

Failure detection at the PCF: If the A11-Session Update message is invalid, the PCF shall not update any session parameters. The PCF shall send an A11-Session Update Acknowledge message indicating identification mismatch (Status value 85H) or authentication failure (Status value 83H); refer to section 2.2.2.

Failure detection at the PDSN: If the PDSN does not receive a valid A11-Session Update Acknowledge message before timer T_{sesupd} expires, the PDSN may retransmit the A11-Session Update message with a new timestamp in the Identification information element and restart timer T_{sesupd} a configurable number of times.

If the PDSN has not received an A11-Session Update Acknowledge with an accept indication (Status value 00H) after a configurable number of retransmissions, the PDSN shall consider the update failed and shall maintain the A10 connection.

2.2.2 A11-Session Update Acknowledge

The PCF sends this message to the PDSN to acknowledge receipt of an A11-Session Update message.

2.2.2.1 Successful Operation

When the PCF receives a valid A11-Session Update message with session parameter(s) in NVSE(s), the PCF shall send an A11-Session Update Acknowledge message to the PDSN. If the PCF accepts the update it shall send an ‘accept’ indication (Status value 00H). If the PCF does not accept the update it shall send a ‘denied’ indication (e.g.,

Status value C9H – session parameters not updated). When the PDSN receives this message it stops timer T_{sesupd}.

If the PDSN receives a valid A11-Session Update Acknowledge message before timer T_{sesudp} expires that indicates identification mismatch (Code value 85H), the PDSN shall not adjust its clock. The PDSN may resend the A11-Session Update message after updating the timestamp according to its own clock.

If the PDSN receives a valid A11-Session Update Acknowledge message that contains a Status value other than "Update accepted" (00H) or "Identification mismatch" (85H), the PDSN shall consider the update failed and shall continue to maintain the A10 connection.

2.2.2.2 Failure Operation

Failure detection at the PDSN: If the A11-Session Update Acknowledge message is invalid, the PDSN shall discard the message.

Failure detection at the PCF: None.

2.3 A10 Packet Accounting Procedures

The PCF uses the A11-Registration Request message to send accounting related and other information to the PDSN. The accounting related information is accumulated at the PCF and sent to the PDSN on occurrence of pre-defined triggers, which are listed in Table 2.3-1. The occurrence of these predefined triggers is fully specified in [8]. The A10 connection binding record at the PDSN and the PCF may also be updated appropriately depending on the setting of the Lifetime field.

Table 2.3-1 Accounting Records Generated by the PCF

Airlink Record Type (Y1)	Accounting Records Generated by the PCF
Y1=1	Connection Setup: Setup of A10 connection initiated
Y1=2	Active Start: A10 connection is associated with the traffic channel(s) or new parameters are set.
Y1=3	Active Stop: A10 connection is disassociated from the traffic channel(s) or parameter settings are no longer valid.
Y1=4	A forward or reverse short data burst (SDB) was exchanged with the MS

In addition, the PCF generates an "Active Stop (Y1=3)" accounting record followed by an "Active Start (Y1=2)" accounting record when certain parameters change value. Refer to section 2.3.7 for details. For successful operation, the PDSN saves the accounting related and other information for further processing, and responds with an A11-Registration Reply message containing an accept indication.

The Airlink Record information is transferred from the PCF to the PDSN, as RADIUS protocol encoded attributes, in the Application Data field of a CVSE element. If the PDSN receives an unexpected airlink record it may reject the A11-Registration Request message and the A11-Registration Reply message shall contain the code '86H' (Registration Denied – poorly formed request). If the PDSN does not receive an accounting parameter that is expected, the PDSN may reject the A11-Registration

Request message, and the associated A11-Registration Reply message shall contain either:

- code '8DH' (Registration Denied – unsupported Vendor ID or unable to interpret Application Type or Application Sub Type in the CVSE sent by the PCF to the PDSN), or
- code '86H' (Registration Denied – poorly formed request).

If the PDSN receives a RADIUS attribute that is not expected in a CVSE, the PDSN shall ignore that attribute and process the remainder of the CVSE to the extent possible. Refer to section 4.2.13 for further details.

2.3.1 A10 Connection Setup Airlink Record

The A10 Connection Setup Airlink record shall be included in the A11-Registration Request message at the time of establishment of a new A10 connection. It is also included in the A11-Registration Request message if an A10 connection is pre-setup during fast handoff.

2.3.2 Active-Start Airlink Record

The Active-Start Airlink record shall be included in the A11-Registration Request message under the following circumstances:

1. When a traffic channel is assigned to a packet data service instance: during initial service instance setup when the service instance becomes associated with the air interface, on transition from dormant to active state or during handoff. The Active-Start Airlink record may follow the connection Setup Airlink record in the same A11-Registration Request message (assuming that all the parameters required in the Active-Start Airlink record are made available at the PCF at the time the message is sent).
2. Following an Active-Stop Airlink record when any of the parameters specified in section 2.3.7 are changed. The Active Start Airlink Record shall contain the new set of parameters.

2.3.3 Active-Stop Airlink Record

The Active Stop Airlink Record shall be included in the A11-Registration Request message under the following circumstances:

1. When the traffic channel is disassociated from the packet data service instance: during service instance release, on transition from active state to dormant, or during handoff.
2. When any of the parameters specified in section 2.3.7 are changed.

In the case of (2), the Active Stop Airlink Record shall be sent and followed by an Active Start Airlink Record that shall contain the new set of parameters.

2.3.4 SDB Airlink Record

The SDB Airlink Record is used by the PCF to report to the PDSN the transfer of Short Data Burst information to and from the user.

The PCF should be notified when a successful SDB is delivered to the MS or successfully received by the BS.

2.3.5 Accounting at Re-registration

Reception by the PCF of new accounting information shall trigger an A11-Registration Request message to transfer this accounting information to the PDSN.

2.3.6 Airlink Sequence Numbers

All the airlink records include a sequence number initialized to zero at A10 connection setup for each identification triplet (PCF session ID, MSID, PCF ID). When transmitting an airlink record to the PDSN, the PCF shall increment the sequence number (modulo 256) and insert it into the airlink record. If multiple airlink records are sent in the same message their sequence numbers shall be in ascending order (modulo 256 arithmetic).

In the event of retransmission of the Air Link Record, the PCF shall retransmit with the same sequence number.

2.3.7 Accounting Update Due to Parameter Changes

Certain accounting parameters are specified in [8] as triggering an accounting update if their values change during an active connection. If the value of any of those parameters changes during an active connection, the PCF shall convey an “Active Stop” airlink record, and an “Active Start” airlink record with a new set of parameters to the PDSN, via an A11-Registration Request message.

3.0 Message Formats

3.1 A11-Registration Request

This A11 interface message is sent from the PCF to the PDSN to:

- establish an A10 connection (and identify the associated service option value and MN Session Reference ID);
- periodically re-register an A10 connection;
- clear an A10 connection;
- pass accounting related information per the triggers listed in Table 2.3-1.

The A11-Registration Request messages may contain additional information to:

- indicate that all packet data service instances have gone dormant;
- pass fast handoff related information.
- indicate support of features such as Short Data Indication

Information Element	Section Reference	Element Direction	Type	
A11 Message Type	4.2.1	PCF -> PDSN	M	
Flags	4.2.2	PCF -> PDSN	O	R
Lifetime	4.2.3	PCF -> PDSN	O	R
Home Address	4.2.4	PCF -> PDSN	O	R
Home Agent	4.2.5	PCF -> PDSN	O	R
Care-of-Address	4.2.6	PCF -> PDSN	O	R
Identification	4.2.7	PCF -> PDSN	O	R
Session Specific Extension	4.2.12	PCF -> PDSN	O	R
Critical Vendor/Organization Specific Extension	4.2.13	PCF -> PDSN	O[a,e]	C
Normal Vendor/Organization Specific Extension	4.2.14	PCF -> PDSN	O[a,b,c,d,f,g]	C
Mobile-Home Authentication Extension	4.2.10	PCF -> PDSN	O	R

a. One or more instances of this element may be included.

b During a fast handoff, this element is used to provide the Anchor P-P Address to the target PDSN when the PCF supports fast handoff. If an Anchor P-P Address is included in the message and the PDSN supports fast handoff, then the PDSN shall process the fast handoff request, and disregard the ANID values.

c. If this message contains the Active Stop Airlink Record for the last service instance going dormant (i.e., all packet data service instances for the user are dormant) in the CVSE, then an instance of this element containing the All Dormant Indicator shall be included in this message.

d. This element shall be included when this message is sent for A10 connection setup and the PCF is capable of supporting multiple service instances. It contains the Service Option value received from the BS for the PDSI.

e. During a handoff, this element is used to provide the MEI.

f. During a handoff, this element is used to provide the ANIDs.

g. This element may indicate the features that the PCF has enabled e.g., Short Data Indication.

The following table shows the bitmap layout for the A11-Registration Request message.

3.1 A11-Registration Request

0	1	2	3	4	5	6	7	Octet
⇒ **A11 Message Type** = [01H]								1
⇒ **Flags** = [0AH, 8AH]								1
(MSB)	⇒ **Lifetime** = [00 00H to FF FEH]							1
							(LSB)	2
(MSB)	⇒ **Home Address** = [00 00 00 00H]							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Home Agent** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Care-of-Address** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Identification** = <any value>							1
								2
								3
								4
								5
								6
								7
							(LSB)	8
⇒ **Session Specific Extension:** = [27H]								1
Length = [13H–15H]								2
(MSB)	Protocol Type = [88 81H]							3
							(LSB)	4

3.1 A11-Registration Request

0	1	2	3	4	5	6	7	Octet
(MSB)	Key = <any value>							5
								6
								7
							(LSB)	8
Reserved = [00H]								9
Reserved = [0000 00]						Session ID Ver = [‘00’ (Version 0), ‘01’ (Version 1)]		10
(MSB)	MN Session Reference ID = [00 01H – 00 06H]							11
							(LSB)	12
(MSB)	MSID Type = [00 06H] (IMSI)							13
							(LSB)	14
MSID Length = [06-08H] (10-15 digits)								15
Identity Digit 1 = [0H-9H] (BCD)				Odd/Even Indicator = [0000, 0001]				16
Identity Digit 3 = [0H-9H] (BCD)				Identity Digit 2 = [0H-9H] (BCD)				17
…				…				…
If (Odd/Even Indicator = 0000 (even)) {Identity Digit N+1 = [FH] (BCD)} Else If (Odd/Even Indicator = 0001 (odd)) {Identity Digit N+1 = [0H-9H] (BCD)}				Identity Digit N = [0H-9H] (BCD)				k
⇒ **Critical Vendor/Organization Specific Extension: Type** = [26H]								1
Reserved = [0000 0000]								2
(MSB)	Length = <variable>							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID = [00 00 15 9FH]							5
								6
								7
							(LSB)	8
Application Type = [01H, 02H]								9
IF (Application Type = 01H (Accounting) {1:								
Application Sub Type = [01H]								10
(MSB)	Application Data (contains accounting information)							11
								…
							(LSB)	k
} Application Type = 01H; ELSE IF (Application Type = 02H (Mobility Event Indicator)) {1:								
Application Sub Type = [01H]								m
} Application Type = 02H								

3.1 A11-Registration Request

0	1	2	3	4	5	6	7	Octet
⇒ **Normal Vendor/Organization Specific Extension: Type** = [86H]								1
Length = <variable>								2
(MSB)	Reserved = [00 00H]							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID = [00 00 15 9FH]							5
								6
								7
							(LSB)	8
Application Type = [04H-06H,09H, 0BH] (Access Network Identifiers, PDSN Identifier, Indicators, Service Option, PCF Enabled Features)								9
IF (Application Type = 04H (Access Network Identifiers)) {1:								
Application Sub Type = [01H]								10
(MSB)	Application Data = <any value> (contains PANID and CANID)							11
								…
							(LSB)	20
} Application Type = 04H, ELSE IF (Application Type = 05H (PDSN Identifier)) {1:								
Application Sub Type = [01H (Anchor P-P Address)]								10
(MSB)	Application Data (contains an IPv4 address)							11
								12
								13
							(LSB)	14
} Application Type = 05H; ELSE IF (Application Type = 06H (Indicators)) {1								
Application Sub Type = [01H (All Dormant Indicator)]								10
(MSB)	Application Data = [00 00H]							11
							(LSB)	12
} Application Type = 06H; ELSE IF (Application Type = 09H (Service Option)) {1:								
Application Sub Type = [01H]								10
(MSB)	Application Data (contains Service Option)							11
							(LSB)	12
} Application Type = 09H; ELSE IF (Application Type = 0BH (PCF Enabled Features)){1								
Application Sub Type = [01H (Short Data Indication Supported)]								10
} Application Type = 0BH;								
⇒ **Mobile-Home Authentication Extension: Type =** [20H]								1
Length = [14H]								2
(MSB)	SPI = [00 00 01 00H to FF FF FF FFH]							3
								4

3.1 A11-Registration Request

0	1	2	3	4	5	6	7	Octet
								5
							(LSB)	6
(MSB)	Authenticator = <any value > (keyed-MD-5 authentication)							7
				…				…
							(LSB)	22

1

3.2 A11-Registration Reply

This A11 interface message is sent from the PDSN to the PCF in response to an A11-Registration Request message.

Information Element	Section Reference	Element Direction	Type	
A11 Message Type	4.2.1	PDSN -> PCF	M	
Code	4.2.8	PDSN -> PCF	M	
Lifetime	4.2.3	PDSN -> PCF	M	
Home Address	4.2.4	PDSN -> PCF	M	
Home Agent	4.2.5	PDSN -> PCF	M[a]	
Identification	4.2.7	PDSN -> PCF	M	
Session Specific Extension	4.2.12	PDSN -> PCF	M	
Critical Vendor/Organization Specific Extension	4.2.13	PDSN -> PCF	O[b]	C
Normal Vendor/Organization Specific Extension	4.2.14	PDSN -> PCF	O[c,d,e,f,g,h]	C
Mobile-Home Authentication Extension	4.2.10	PDSN -> PCF	O	R

a. This element can also be used to identify the IPv4 address of an alternative PDSN.

b. This element is included if the PDSN has data available.

c. This element is used by the anchor PDSN to provide an Anchor P-P Address when the PDSN supports fast handoff.

d. One or more instances of this element may be included.

e. During a fast handoff, the target PDSN includes the Anchor P-P Address to indicate that the fast handoff request was accepted.

f. This element is used to send a Radio Network Packet Data Inactivity Timer (RN-PDIT) to the PCF when supported.

g. When an Always-on Indicator is present at the PDSN, the PDSN shall include the NVSE with an Always-on indicator.

h. This element is used by the PDSN to indicate that flow control is enabled for the packet data service instance.

The following table shows the bitmap layout for the A11-Registration Reply message.

3.2 A11-Registration Reply

0	1	2	3	4	5	6	7	Octet
⇒ **A11 Message Type** = [03H]								1
⇒ **Code** = [00H (Registration Accepted), 80H (Registration Denied – reason unspecified), 81H (Registration Denied – administratively prohibited), 82H (Registration Denied – insufficient resources), 83H (Registration Denied – PCF failed authentication), 85H (Registration Denied – identification mismatch), 86H (Registration Denied – poorly formed request), 88H (Registration Denied – unknown PDSN address), 89H (Registration Denied – requested reverse tunnel unavailable), 8AH (Registration Denied – reverse tunnel is mandatory and 'T' bit not set), 8DH (Registration Denied – unsupported vendor ID or unable to interpret Application Type or Application Sub Type in the CVSE sent by the PCF to the PDSN.)]								1
(MSB)	⇒ **Lifetime** = [00 00H to FF FEH]							1
							(LSB)	2
(MSB)	⇒ **Home Address** = [00 00 00 00H]							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Home Agent** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Identification** = <any value>							1
								2
								3
								4
								5
								6
								7
							(LSB)	8
⇒ **Session Specific Extension: Type** = [27H]								1
Length = [13H – 15H]								2
(MSB)	Protocol Type = [88 81H]							3

3.2 A11-Registration Reply

0	1	2	3	4	5	6	7	Octet
							(LSB)	4
(MSB)	Key = <any value>							5
								6
								7
							(LSB)	8
Reserved = [00H]								9
Reserved = [0000 00]						Session ID Ver = [‘00’ (Version 0), ‘01’ (Version 1)]		10
(MSB)	MN Session Reference ID = [00 01H – 00 06H]							11
							(LSB)	12
(MSB)	MSID Type = [00 06H] (IMSI)							13
							(LSB)	14
MSID Length = [06-08H] (10-15 digits)								15
Identity Digit 1 = [0H - 9H] (BCD)				Odd/Even Indicator = [0000, 0001]				16
Identity Digit 3 = [0H - 9H] (BCD)				Identity Digit 2 = [0H - 9H] (BCD)				17
…				…				…
If (Odd/Even Indicator = 0000 (even)) {Identity Digit N+1 = [FH] (BCD)} Else If (Odd/Even Indicator = 0001 (odd)) {Identity Digit N+1 = [0H - 9H] (BCD)}				Identity Digit N = [0H - 9H] (BCD)				21-23
⇒ **Critical Vendor/Organization Specific Extension: Type** = [26H]								1
Reserved = [0000 0000]								2
(MSB)	Length = [00 06H]							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID = [00 00 15 9FH]							5
								6
								7
							(LSB)	8
Application Type = [03H] (Data Availability Indicator)								9
Application Sub Type = [01H]								10
⇒ **Normal Vendor/Organization Specific Extension: Type** = [86H]								1
Length = <variable>								2
Reserved = [00 00H]								3
								4
(MSB)	3GPP2 Vendor ID = [00 00 15 9FH]							5
								6

3.2 A11-Registration Reply

0	1	2	3	4	5	6	7	Octet
								7
							(LSB)	8
Application Type = [05H (PDSN Identifier, 08H (Session Parameter), 0AH (PDSN Enabled Features)]								9
IF (Application Type = 05H (PDSN Identifier)){1								
Application Sub Type = [01H (Anchor P-P Address)]								10
(MSB)	Application Data (contains an IPv4 address)>							11
								12
								13
							(LSB)	14
} Application Type = 05H; ELSE IF (Application Type = 08H (Session Parameter)){1								
Application Sub Type = [01H (RN-PDIT), 02H (Always-on)]								10
IF (Application Sub Type = 01H (RN-PDIT)) {1								
(MSB)	Application Data = [01H–FFH]						(LSB)	11
} Application Sub Type =01H, } Application Type = 08H; ELSE IF (Application Type = 0AH (PDSN Enabled Features)){1								
Application Sub Type = [01H (Flow Control Enabled)]								10
} Application Type = 0AH;								
⇒ **Mobile-Home Authentication Extension: Type** = [20H]								1
Length = [14H]								2
(MSB)	SPI = [00 00 01 00H to FF FF FF FFH]							3
								4
								5
							(LSB)	6
(MSB)	Authenticator = <any value > (keyed-MD-5 authentication)							7
				…				**…**
							(LSB)	22

1

3.3 A11-Registration Update

This A11 interface message is sent from the PDSN to the PCF to release an A10 connection.

Information Element	Section Reference	Element Direction	Type	
A11 Message Type	4.2.1	PDSN -> PCF	M	
Reserved <3 octets>	None	PDSN -> PCF	M[a]	
Home Address	4.2.4	PDSN -> PCF	M	
Home Agent	4.2.5	PDSN -> PCF	M	
Identification	4.2.7	PDSN -> PCF	M	
Session Specific Extension	4.2.12	PDSN -> PCF	M	
Normal Vendor/Organization Specific Extension	4.2.14	PDSN -> PCF	O[b]	C
Registration Update Authentication Extension	4.2.11	PDSN -> PCF	M	

a. This field is set to zero by the PDSN and ignored by the PCF.

b. This element is used by the PDSN to provide a PDSN code to the PCF.

The following table shows the bitmap layout for the A11-Registration Update message.

3.3 A11-Registration Update

0	1	2	3	4	5	6	7	Octet
⇒ **Message Type** = [14H]								1
⇒ **Reserved** = [00 00 00H]								1
								2
								3
(MSB)	⇒ **Home Address** = [00 00 00 00H]							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Home Agent** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Identification** = <any value>							1
								2
								3
								4
								5

3.3 A11-Registration Update

0	1	2	3	4	5	6	7	Octet
								6
								7
							(LSB)	8
⇒ **Session Specific Extension: Type** = [27H]								1
Length = [13H – 15H]								2
(MSB)	Protocol Type = [88 81H]							3
							(LSB)	4
(MSB)	Key = <any value>							5
								6
								7
							(LSB)	8
Reserved = [00H]								9
Reserved = [0000 00]						Session ID Ver = [‘00’ (Version 0), ‘01’ (Version 1)]		10
(MSB)	MN Session Reference ID = [00 01H – 00 06H]							11
							(LSB)	12
(MSB)	MSID Type = [00 06H] (IMSI)							13
							(LSB)	14
MSID Length = [06-08H] (10-15 digits)								15
Identity Digit 1 = [0H-9H] (BCD)				Odd/Even Indicator = [0000, 0001]				16
Identity Digit 3 = [0H-9H] (BCD)				Identity Digit 2 = [0H-9H] (BCD)				17
…				…				…
If (Odd/Even Indicator = 0000 (even)) {Identity Digit N+1 = [FH] (BCD)} ELSE (If Odd/Even Indicator = 0001 (odd)) {Identity Digit N+1 = [0H-9H] (BCD)}				Identity Digit N = [0H-9H] (BCD)				k
⇒ **Normal Vendor/Organization Specific Extension: Type** = [86H]								1
Length = <variable>								2
(MSB)	Reserved = [00 00H]							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID = 00 00 15 9FH							5
								6
								7
							(LSB)	8
Application Type = [07H (PDSN CODE)]								9
Application Sub Type = [01H]								10

3.3 A11-Registration Update

0	1	2	3	4	5	6	7	Octet
Application Data = [C1H-C8H, CAH]								11
⇒ **Registration Update Authentication Extension: Type =** [28H]								1
Length = [14H]								2
(MSB)	SPI = [00 00 01 00H to FF FF FF FFH]							3
								4
								5
							(LSB)	6
(MSB)	Authenticator = <any value > (keyed-MD-5 authentication)							7
				…				**…**
							(LSB)	22

1

3.4 A11-Registration Acknowledge

This A11 interface message is sent from the PCF to the PDSN in response to an A11-Registration Update message.

Information Element	Section Reference	Element Direction	Type
A11 Message Type	4.2.1	PCF -> PDSN	M
Reserved <2 octets>	None	PCF -> PDSN	M[a]
Status	4.2.9	PCF -> PDSN	M
Home Address	4.2.4	PCF -> PDSN	M
Care-of-Address	4.2.6	PCF -> PDSN	M
Identification	4.2.7	PCF -> PDSN	M
Session Specific Extension	4.2.12	PCF -> PDSN	M
Registration Update Authentication Extension	4.2.11	PCF -> PDSN	M

a. This field is set to zero by the PCF and ignored by the PDSN.

The following table shows the bitmap layout for the A11-Registration Acknowledge message.

3.4 A11-Registration Acknowledge

0	1	2	3	4	5	6	7	Octet
⇒ **Message Type** = [15H]								1
⇒ **Reserved** = [00 00H]								1
								2
⇒ **Status =** [00H (Update Accepted) 80H (Update Denied – reason unspecified) 83H (Update Denied – sending node failed authentication) 85H (Update Denied – identification mismatch) 86H (Update Denied – poorly formed registration update)]								1
(MSB)	⇒ **Home Address** = [00 00 00 00H]							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Care-of-Address** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Identification** = <any value>							1
								2

3.4 A11-Registration Acknowledge

0	1	2	3	4	5	6	7	Octet
								3
								4
								5
								6
								7
							(LSB)	8
⇒ **Session Specific Extension: Type =** [27H]								1
Length = [13H – 15H]								2
(MSB)	Protocol Type = [88 81H]							3
							(LSB)	4
(MSB)	Key = <any value>							5
								6
								7
							(LSB)	8
Reserved = [00H]								9
Reserved = [0000 00]						Session ID Ver = [‘00’ (Version 0), ‘01’ (Version 1)]		10
(MSB)	MN Session Reference ID = [00 01H – 00 06H]							11
							(LSB)	12
(MSB)	MSID Type = [00 06H] (IMSI)							13
							(LSB)	14
MSID Length = [06-08H] (10-15 digits)								15
Identity Digit 1 = [0H-9H] (BCD)				Odd/Even Indicator = [0000, 0001]				16
Identity Digit 3 = [0H-9H] (BCD)				Identity Digit 2 = [0H-9H] (BCD)				17
…				…				…
If (Odd/Even Indicator = 0000 (even)) {Identity Digit N+1 = [FH] (BCD)} Else If (Odd/Even Indicator = 0001 (odd)) {Identity Digit N+1 = [0H-9H] (BCD)}				Identity Digit N = [0H-9H] (BCD)				k
⇒ **Registration Update Authentication Extension: Type** = [28H]								1
Length = [14H]								2
(MSB)	SPI = [00 00 01 00H to FF FF FF FFH]							3
								4
								5
							(LSB)	6
(MSB)	Authenticator = <any value > (keyed-MD-5 authentication)							7

3.4 A11-Registration Acknowledge

0	1	2	3	4	5	6	7	Octet
…								…
							(LSB)	22

1

2

3.5 A11-Session Update

This A11 interface message is sent from the PDSN to the PCF to add new or update parameters of an A10 connection. It is also sent to update the PCF with the Anchor P-P Address.

Information Element	Section Reference	Element Direction	Type	
A11 Message Type	4.2.1	PDSN -> PCF	M	
Reserved <3 octets>	None	PDSN -> PCF	M[a]	
Home Address	4.2.4	PDSN -> PCF	M	
Home Agent	4.2.5	PDSN -> PCF	M	
Identification	4.2.7	PDSN -> PCF	M	
Session Specific Extension	4.2.12	PDSN -> PCF	M	
Normal Vendor/Organization Specific Extension	4.2.14	PDSN -> PCF	O[b, c, d]	C
Registration Update Authentication Extension	4.2.11	PDSN -> PCF	M	

a. This field is set to zero by the PDSN and ignored by the PCF.

b. This element is used by the PDSN to provide an RN-PDIT value to the PCF.

c. When an Always-on Indicator is present at the PDSN, the PDSN shall include the NVSE with an Always-on indicator.

d. This element is included by the PDSN to update the PCF with an Anchor P-P Address for fast handoff.

The following table shows the bitmap layout for the A11-Session Update message.

3.5 A11-Session Update

0	1	2	3	4	5	6	7	Octet
⇒ **Message Type** = [16H]								1
(MSB)	⇒ **Reserved** = [00 00 00H]							1
								2
							(LSB)	3
(MSB)	⇒ **Home Address** = [00 00 00 00H]							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Home Agent** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Identification** = <any value>							1

3.5 A11-Session Update

0	1	2	3	4	5	6	7	Octet
								2
								3
								4
								5
								6
								7
							(LSB)	8
⇒ **Session Specific Extension: Type** = [27H]								1
Length = [13H – 15H]								2
(MSB)	Protocol Type = [88 81H]							3
							(LSB)	4
(MSB)	Key = <any value>							5
								6
								7
							(LSB)	8
Reserved = [00H]								9
Reserved = [0000 00]						Session ID Ver = [‘00’ (Version 0), ‘01’ (Version 1)]		10
(MSB)	MN Session Reference ID = [00 01H – 00 06H]							11
							(LSB)	12
(MSB)	MSID Type = [00 06H] (IMSI)							13
							(LSB)	14
MSID Length = [06-08H] (10-15 digits)								15
Identity Digit 1 = [0H-9H] (BCD)				Odd/Even Indicator = [0000, 0001]				16
Identity Digit 3 = [0H-9H] (BCD)				Identity Digit 2 = [0H-9H] (BCD)				17
…				…				…
If (Odd/Even Indicator = 0000 (even)) {Identity Digit N+1 = [FH] (BCD)} ELSE (If Odd/Even Indicator = 0001 (odd)) {Identity Digit N+1 = [0H-9H] (BCD)}				Identity Digit N = [0H-9H] (BCD)				k
⇒ **Normal Vendor/Organization Specific Extension: Type** = [86H]								1
Length = <any value>								2
(MSB)	Reserved = [00 00H]							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID = [00 00 15 9FH]							5
								6

3.5 A11-Session Update

0	1	2	3	4	5	6	7	Octet
								7
							(LSB)	8
Application Type = [05H (PDSN Identifier), 08H (Session Parameter)]								9
IF (Application Type = 05H (PDSN Identifier)){1								
Application Sub Type = [01H (Anchor P-P Address)]								10
(MSB)	Application Data = (contains an IPv4 address)							11
								12
								13
							(LSB)	14
} Application Type = 05H; ELSE IF (Application Type = 08H (Session Parameter)) {1								
Application Sub Type = [01H (RN-PDIT), 02H (Always-on)]								10
IF (Application Sub Type = 01H (RN-PDIT)) {1								
(MSB)	Application Data = [01H–FFH]						(LSB)	11
} Application Sub Type =01H, } Application Type = 08H;								
⇒ **Registration Update Authentication Extension: Type =** [28H]								1
Length = [14H]								2
(MSB)	SPI = [00 00 01 00H to FF FF FF FFH]							3
								4
								5
							(LSB)	6
(MSB)	Authenticator = <any value > (keyed-MD-5 authentication)							7
…								…
							(LSB)	22

1

3.6 A11-Session Update Acknowledge

This A11 interface message is sent from the PCF to the PDSN in response to an A11-Session Update message.

Information Element	Section Reference	Element Direction	Type
A11 Message Type	4.2.1	PCF -> PDSN	M
Reserved <2 octets>	None	PCF -> PDSN	M[a]
Status	4.2.9	PCF -> PDSN	M
Home Address	4.2.4	PCF -> PDSN	M
Care-of-Address	4.2.6	PCF -> PDSN	M
Identification	4.2.7	PCF -> PDSN	M
Session Specific Extension	4.2.12	PCF -> PDSN	M
Registration Update Authentication Extension	4.2.11	PCF -> PDSN	M

a. This field is set to zero by the PCF and ignored by the PDSN.

The following table shows the bitmap layout for the A11-Session Update Acknowledge message.

3.6 A11-Session Update Acknowledge

0	1	2	3	4	5	6	7	Octet
⇒ **Message Type** = [17H]								1
⇒ **Reserved** = [00 00H]								1
								2
⇒ **Status =** [00H (Update Accepted) 80H (Update Denied – reason unspecified) 83H (Update Denied – sending node failed authentication) 85H (Update Denied – identification mismatch) 86H (Update Denied – poorly formed registration update) C9H (Update Denied – session parameters not updated)]								1
(MSB)	⇒ **Home Address** = [00 00 00 00H]							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Care-of-Address** = <any value>							1
								2
								3
							(LSB)	4
(MSB)	⇒ **Identification** = <any value>							1

3.6 A11-Session Update Acknowledge

0	1	2	3	4	5	6	7	Octet
								2
								3
								4
								5
								6
								7
							(LSB)	8
⇒ **Session Specific Extension: Type =** [27H]								1
Length = [13H – 15H]								2
(MSB)	Protocol Type = [88 81H]							3
							(LSB)	4
(MSB)	Key = <any value>							5
								6
								7
							(LSB)	8
Reserved = [00H]								9
Reserved = [0000 00]						Session ID Ver = [‘00’ (Version 0), ‘01’ (Version 1)]		10
(MSB)	MN Session Reference ID = [00 01H – 00 06H]							11
							(LSB)	12
(MSB)	MSID Type = [00 06H] (IMSI)							13
							(LSB)	14
MSID Length = [06-08H] (10-15 digits)								15
Identity Digit 1 = [0H-9H] (BCD)				Odd/Even Indicator = [0000, 0001]				16
Identity Digit 3 = [0H-9H] (BCD)				Identity Digit 2 = [0H-9H] (BCD)				17
…				…				…
If (Odd/Even Indicator = 0000 (even)) {Identity Digit N+1 = [FH] (BCD)} Else If (Odd/Even Indicator = 0001 (odd)) {Identity Digit N+1 = [0H-9H] (BCD)}				Identity Digit N = [0H-9H] (BCD)				k
⇒ **Registration Update Authentication Extension: Type** = [28H]								1
Length = [14H]								2
(MSB)	SPI = [00 00 01 00H to FF FF FF FFH]							3
								4
								5
							(LSB)	6

3.6 A11-Session Update Acknowledge

0	1	2	3	4	5	6	7	Octet
(MSB)	Authenticator = <any value > (keyed-MD-5 authentication)							7
…								…
							(LSB)	22

(This page intentionally left blank.)

4.0 Information Element Definitions

This section contains the coding of the information elements used in the messages defined in section 3.0.

The following subsections define information element formats and ranges for parameter values. In the event that text in this section conflicts with text in section 3, the text in section 3 shall take precedence. Parameter usage may vary per message in that only a subset of the defined values may be applicable in a particular message. Therefore, the allowed values are specified per message in the subsections of section 3.0.

4.1 Generic Information Element Encoding

4.1.1 Conventions, Coding, and Interpretation Rules for Information Elements

The following conventions are assumed for the sequence of transmission of bits and bytes:

- Each bit position is marked as 0 to 7. For the A10/A11 interface, bit 0 is the **most** significant bit and is transmitted first. Note that for all other interfaces, bit 0 is the **least** significant bit and is transmitted first.
- In a message, octets are identified by number. Octet 1 is transmitted first, then octet 2, etc.

For variable length elements, a length indicator is included. This indicates the number of octets following in the element.

Information elements shall always use the same Information Element Identifier for all occurrences on a specific A11 interface. Insofar as possible, the same Information Element Identifier shall be used for a given information element when it is used on more than one interface.

The order of appearance for each information element and the definition of whether an information element is mandatory or optional are specified in section 3.0.

For future expansion purposes, some of these information elements have fields within them that have been reserved. All reserved bits are set to 0, unless otherwise indicated. To allow compatibility with future implementation, messages shall not be rejected simply because a reserved bit is set to ‘1’. The **extensions** for the A11 interface messages are defined in the TLV (Type-Length-Value) format. The Type field indicates the type of the extension. Length field indicates the length (in octets) of the extension, not including the Type and Length fields. The value field contains the information specific to the Type of the extension.

4.1.2 Information Element Identifiers

The following table contains a list of all information elements that make up the messages defined in section 3.0. The table is sorted by the Information Element Identifier (IEI) coding which distinguishes one information element from another. The table also

includes a reference to the section where the information element coding can be found. A listing of information elements, sorted by name, is included in Table 4.1.3-1, which also specifies the messages in which each information element is used.

A11 interface information elements, other than the extensions, are position specific, and hence do not include the IEI. The A11 interface extensions are, however, identified by a Type field, which distinguishes one extension from the others.

Table 4.1.2-1 A11 Information Element Identifiers Sorted by Value

Element Name	Identifier	Reference
A11 Message Type	None	4.2.1
Care-of-Address	None	4.2.6
Code	None	4.2.8
Flags	None	4.2.2
Home Address	None	4.2.4
Home Agent	None	4.2.5
Identification	None	4.2.7
Lifetime	None	4.2.3
Status	None	4.2.9
Mobile-Home Authentication Extension	20H	4.2.10
Critical Vendor/Organization Specific Extension	26H	4.2.13
Session Specific Extension	27H	4.2.12
Registration Update Authentication Extension	28H	4.2.11
Normal Vendor/Organization Specific Extension	86H	4.2.14
All other values are reserved.		

4.1.3 Cross Reference of Information Elements With Messages

The following table provides a cross reference between the elements defined in this specification and the messages defined herein.

Table 4.1.3-1 Cross Reference of Information Elements with Messages

Information Element	Reference	IEI	Used in These Messages	Reference
A11 Message Type	4.2.1	None	A11-Registration Request	3.1
			A11-Registration Reply	3.2
			A11-Registration Update	3.3
			A11-Registration Acknowledge	3.4
			A11-Session Update	3.5
			A11-Session Update Acknowledge	3.6
Care-of-Address	4.2.6	None	A11-Registration Request	3.1
			A11-Registration Acknowledge	3.4
			A11-Session Update Acknowledge	3.6
Code	4.2.8	None	A11-Registration Reply	3.2
Critical Vendor/Organization Specific Extension	4.2.13	26H	A11-Registration Request	3.1
			A11-Registration Reply	3.2
Flags	4.2.2	None	A11-Registration Request	3.1
Home Address	4.2.4	None	A11-Registration Request	3.1
			A11-Registration Reply	3.2
			A11-Registration Update	3.3
			A11-Registration Acknowledge	3.4
			A11-Session Update	3.5
			A11-Session Update Acknowledge	3.6
Home Agent	4.2.5	None	A11-Registration Request	3.1
			A11-Registration Reply	3.2
			A11-Registration Update	3.3
			A11-Session Update	3.5
Identification	4.2.7	None	A11-Registration Request	3.1
			A11-Registration Reply	3.2
			A11-Registration Update	3.3
			A11-Registration Acknowledge	3.4
			A11-Session Update	3.5
			A11-Session Update Acknowledge	3.6
Lifetime	4.2.3	None	A11-Registration Request	3.1
			A11-Registration Reply	3.2

Table 4.1.3-1 Cross Reference of Information Elements with Messages

Information Element	Reference	IEI	Used in These Messages	Reference
Mobile-Home Authentication Extension	4.2.10	20H	A11-Registration Request	3.1
			A11-Registration Reply	3.2
Normal Vendor/Organization Specific Extension	4.2.14	86H	A11-Registration Request	3.1
			A11-Registration Reply	3.2
			A11-Registration Update	3.3
			A11-Session Update	3.5
Registration Update Authentication Extension	4.2.11	28H	A11-Registration Update	3.3
			A11-Registration Acknowledge	3.4
			A11-Session Update	3.5
			A11-Session Update Acknowledge	3.6
Session Specific Extension	4.2.12	27H	A11-Registration Request	3.1
			A11-Registration Reply	3.2
			A11-Registration Update	3.3
			A11-Registration Acknowledge	3.4
			A11-Session Update	3.5
			A11-Session Update Acknowledge	3.6
Status	4.2.9	None	A11-Registration Acknowledge	3.4
			A11-Session Update Acknowledge	3.6

1

4.2 Information Elements

4.2.1 A11 Message Type

This one octet element identifies the type of the A11 interface message. The structure of the element conforms to [20], and is shown below.

4.2.1 A11 Message Type

0	1	2	3	4	5	6	7	Octet
A11 Message Type								1

The A11 interface message types are listed in Table 4.2.1-1. These values shall remain coordinated with the values assigned by the IETF for the Mobile IP protocol.

Table 4.2.1-1 A11 Interface Message Types

A11 Interface Message Name	A11 Message Type Value	Section Reference
A11-Registration Request	01H	3.1
A11-Registration Reply	03H	3.2
A11-Registration Update	14H	3.3
A11-Registration Acknowledge	15H	3.4
A11-Session Update	16H	3.5
A11-Session Update Acknowledge	17H	3.6

4.2.2 Flags

The structure of this element conforms to [20], and is shown below. The setting of the Flags bits determines how an A11 interface message is interpreted by the receiving entity, and also the characteristics of the A10 connection.

4.2.2 Flags

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Octet**
S	B	D	M	G	V	T	Reserved	1

For the A11-Registration Request message, the Flag bits are set as specified in Table 4.2.2-1. The 'S' bit is used for fast handoff. It is coded as specified in [8].

Table 4.2.2-1 Setting of A11-Registration Request Message Flags

0	1	2	3	4	5	6	7	Bit Position
S	**B**	**D**	**M**	**G**	**V**	**T**	**RES**	**Bit Identifier**
0/1								Simultaneous Bindings
	0							Broadcast Datagrams
		0						Decapsulation by mobile node
			0					Minimal Encapsulation
				1				GRE Encapsulation
					0			V.J. Compression
						1		Reverse Tunneling
							0	Reserved Bit

4.2.3 Lifetime

This two-octet element indicates the longest lifetime measured in seconds that the sending entity is willing to accept before registration for an A10 connection is considered expired. The structure of the element conforms to [20] and is shown below.

4.2.3 Lifetime

0	1	2	3	4	5	6	7	Octet
(MSB)	Lifetime							1
							(LSB)	2

4.2.4 Home Address

This information element does not carry valid information for this interface and is ignored. However, it shall be included in all A11 messages and the information element conforms to [20].

4.2.4 Home Address

0	1	2	3	4	5	6	7	Octet
(MSB)	Home Address							1
								2
								3
							(LSB)	4

Table 4.2.4-1 shows the setting of the Home Address field for various A11 interface messages.

Table 4.2.4-1 Setting of Home Address Field

A11 Interface Message	Home Address
A11-Registration Request	00 00 00 00H
A11-Registration Reply	00 00 00 00H
A11-Registration Update	00 00 00 00H
A11-Registration Acknowledge	00 00 00 00H
A11-Session Update	00 00 00 00H
A11-Session Update Acknowledge	00 00 00 00H

4.2.5 Home Agent

This element identifies the IPv4 address of the PDSN that terminates the A10 connection. The structure of the element conforms to [20] and is shown below.

4.2.5 Home Agent

0	1	2	3	4	5	6	7	Octet
(MSB)	Home Agent							1
								2
								3
							(LSB)	4

4.2.6 Care-of-Address

This element identifies the IPv4 address of the PCF that terminates the A10 connection. The structure of the element conforms to [20] and is shown below.

4.2.6 Care-of-Address

0	1	2	3	4	5	6	7	Octet
(MSB)	Care-of-Address							1
								2
								3
							(LSB)	4

4.2.7 Identification

This element is used by the PCF and the PDSN for matching the A11-Registration Request messages with A11-Registration Reply messages, A11-Registration Update messages with A11-Registration Acknowledge messages, and A11-Session Update messages with A11-Session Update Acknowledge messages. It also protects against replay attacks using timestamps in the information element. The PCF and the PDSN should have access to an accurate time-of-day clock. The margin of error should be a configurable parameter. To avoid an identification mismatch "deadlock" at the PCF, whereby the PCF considers the two entities to be out of synchronization, but the PDSN does not, the margin of error at the PDSN should be less than the margin of error at the PCF.

For the Identification IE to be valid in A11-Registration Request, A11-Registration Update, and A11-Session Update messages, it shall be within the error tolerance specific to the security association between the PCF and PDSN from the receiving entity's time of day (refer to section 1.9). It shall be formatted as specified by [20], and shall be greater than any previously accepted values, as the receiving entity uses this value also as a sequence number. The low-order 32 bits represent fractional seconds, and those bits that are not available from a time source may be generated from a good source of randomness.

In order for the Identification IE to be valid in a response message (A11-Registration Reply, A11-Registration Acknowledge, or A11-Session Update Acknowledge message), it shall be identical to the Identification IE of the corresponding request message (A11-Registration Request, A11-Registration Update, or A11-Session Update message), except when the A11-Registration Reply message reports an identification mismatch (Code value is 85H). In that case, the 32 low-order bits of the Identification IEs in the A11-Registration Request and the A11-Registration Reply messages shall match, and the 32 high-order bits in the Identification IE of the A11-Registration Reply message shall indicate the time of day of the PDSN clock. This information may be used by the PCF to adjust its clock.

The structure of the element conforms to [20] and is shown below.

4.2.7 Identification

0	1	2	3	4	5	6	7	Octet
(MSB)	Identification							1
								2
								3
								4
								5
								6
								7
							(LSB)	8

4.2.8 Code

This element identifies the result of processing an A11-Registration Request message. The element includes codes from [20] and is shown below.

4.2.8 Code

0	1	2	3	4	5	6	7	Octet
Code								1

The supported Code values are listed in Table 4.2.8-1.

Table 4.2.8-1 A11 Code Values

Hex Value	Decimal Value	Code
00H	0	Registration Accepted
09H	9	Reserved
80H	128	Registration Denied – reason unspecified
81H	129	Registration Denied – administratively prohibited
82H	130	Registration Denied – insufficient resources
83H	131	Registration Denied – PCF failed authentication
85H	133	Registration Denied – identification mismatch
86H	134	Registration Denied – poorly formed request
88H	136	Registration Denied – unknown PDSN address
89H	137	Registration Denied – requested reverse tunnel unavailable
8AH	138	Registration Denied – reverse tunnel is mandatory and ‘T’ bit not set
8DH	141	Registration Denied – unsupported Vendor ID or unable to interpret Application Type or Application Sub Type in the CVSE sent by the PCF to the PDSN
All other values reserved		

4.2.9 Status

This element identifies the result of processing an A11-Registration Update message or an A11-Session Update message.

4.2.9 Status

0	1	2	3	4	5	6	7	Octet
Status								1

The supported Status values are listed in Table 4.2.9-1.

Table 4.2.9-1 A11 Status Values

Hex Value	Decimal Value	A11 Status
0	0	Update Accepted
80H	128	Update Denied – reason unspecified
83H	131	Update Denied – sending node failed authentication
85H	133	Update Denied – identification mismatch
86H	134	Update Denied – poorly formed registration update
C9H	193	Update Denied – session parameters not updated
All other values reserved		

4.2.10 Mobile-Home Authentication Extension

This element is present in all A11-Registration Request and A11-Registration Reply messages. This element marks the end of the authenticated data in these messages. The structure of the extension conforms to [20] and is shown below.

4.2.10 Mobile-Home Authentication Extension

0	1	2	3	4	5	6	7	Octet
A11 Element Identifier (Type)								1
Length								2
(MSB)	SPI							3
								4
								5
							(LSB)	6
(MSB)	Authenticator							7
								•••
							(LSB)	22

Type:

20H.

Length:

This field indicates the number of octets in this element following the Length field. This field is set to 4 plus the number of bytes in the authenticator.

SPI:

This four octet field is set to the Security Parameter Index, as described in Section 1.6, [20].

Authenticator:

For keyed-MD-5 authentication, the Authenticator field is set to the 128-bit “message digest” value obtained by applying the keyed-MD-5 algorithm in the “prefix+suffix” mode on the protected fields. Refer to section 1.9 for details. The default authenticator algorithm shall also protect the SPI value.

4.2.11 Registration Update Authentication Extension

This element is present in all A11-Registration Update, A11-Registration Acknowledge, A11-Session Update and A11-Session Update Acknowledge messages. This element marks the end of the authenticated data in these messages.

4.2.11 Registration Update Authentication Extension

0	1	2	3	4	5	6	7	Octet
A11 Element Identifier (Type)								1
Length								2
(MSB)	SPI							3
								4
								5
							(LSB)	6
(MSB)	Authenticator							7
								...
							(LSB)	22

Type:

28H

Length:

This field indicates the number of octets in this element following the Length field. This field is set to 4 plus the number of bytes in the authenticator.

SPI:

This four octet field is set to the Security Parameter Index, as described in Section 1.6, [20].

Authenticator:

For keyed-MD-5 authentication, the Authenticator field is set to the 128-bit “message digest” value obtained by applying the keyed-MD-5 algorithm in the “prefix+suffix” mode on the protected fields. Refer to section 1.9 for details. The default authenticator algorithm shall also protect the SPI value.

4.2.12 Session Specific Extension

This element is present in all A11-Registration Request, A11-Registration Reply, A11-Registration Update, A11-Registration Acknowledge, A11-Session Update and A11-Session Update Acknowledge messages. This element includes the mobile identity and session specific information.

4.2.12 Session Specific Extension

0	1	2	3	4	5	6	7	Octet
A11 Element Identifier (Type)								1
Length								2
(MSB)	Protocol Type							3
							(LSB)	4
(MSB)	Key							5
								6
								7
							(LSB)	8
Reserved								9
Reserved						Session ID Ver		10
(MSB)	MN Session Reference ID							11
							(LSB)	12
(MSB)	MSID Type							13
							(LSB)	14
MSID Length								15
Identity Digit 1				Odd/Even Indicator				16
Identity Digit 3				Identity Digit 2				17
…				…				…
Identity Digit N+1				Identity Digit N				Variable

Type:

27H

Length:

This field indicates the number of octets following the Length field.

Protocol Type:

This two octet field identifies the type of the link layer protocol/network layer protocol in use at the mobile node. The supported ‘Protocol Type’ values are listed below:

Table 4.2.12-1 A11 Protocol Type Values

Protocol Type	Value
Unstructured Byte Stream	88 81H

Key:

This field indicates to the receiver the value to use in the GRE header Key field when sending traffic frames on the A10 connection. Refer to [21] and [24].

Reserved:

This field is not used at present. It is set to zero by the sending entity and ignored by the receiving entity.

Session ID Ver:

This field is used to negotiate the Session Identifier Version to be used. A one step negotiation is used where the initiating entity (the PCF) indicates the highest version it supports, and the replying entity (the PDSN) indicates the highest version it supports that is less than or equal to the version received from the initiating entity.

If the negotiated Session Identifier Version is '0', the replying entity shall send the same Key value received by the initiating entity.

If the negotiated Session Identifier Version is '1', the replying entity may select a Key value different from the one received from the initiating entity.

Values greater than '1' are reserved.

MN Session Reference ID:

This field is used to uniquely identify a packet data service instance in the MS. The MN Session Reference ID shall be set to the SR_ID associated with the PDSI.

MSID Type:

This field indicates the type of the address used by the mobile node. The field is coded as shown in Table 4.2.12-2. Note only the least significant bits are shown, all other bits are set to zero.

Table 4.2.12-2 Mobile Identity - Type of Identity Coding

Binary Values	Meaning
000	No Identity Code
010	Reserved
101	Reserved
110	IMSI

MSID Length:

This field indicates the number of octets in this element following the MSID Length field.

Odd/Even Indicator:

This field is set to '0000' for an even number of identity digits and to '0001' for an odd number of identity digits.

Identity Digits:

The identity digits are coded as follows:

The International Mobile Subscriber Identifier fields are coded using BCD coding format. If the number of identity digits is even then bits 0 to 3 of the last octet shall be filled with an end mark coded as ‘1111’.

4.2.13 Critical Vendor/Organization Specific Extension (CVSE)

This element may be present in the A11-Registration Request message to convey accounting information from the PCF to the PDSN. This element may also be present in the A11-Registration Request message to convey the Mobility Event Indicator from the PCF to the PDSN during dormant handoffs and active/hard handoffs. The coding format of the CVSE defined herein conforms to [25].

This element may be present in the A11-Registration Reply message to convey the Data Available Indicator (DAI) from the PDSN to the PCF during handoff.

This element reflects Application Type and Application Sub-Types supported in IOS v4.0. New Application Type or Application Sub-Types shall be added to the Normal Vendor/Organization Specific Extension (NVSE) (refer to section 4.2.14).

When used to convey accounting information, the accounting records are contained within the Application Data field of this element. The accounting records conveyed from the PCF to the PDSN conform to the specifications in [8]. Each application type 01H (Accounting) CVSE contains one and only one airlink record as specified by Tables 4.2.13-2 through 4.2.13-5, and shall include all the parameters listed in the corresponding table unless otherwise specified. For transmission of multiple airlink records in the same A11-Registration Request message, multiple instances of accounting type CVSEs are used.

4.2.13 Critical Vendor/Organization Specific Extension (CVSE)

0	1	2	3	4	5	6	7	Octet
A11 Element Identifier (Type)								1
Reserved								2
(MSB)	Length							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID							5
								6
								7
							(LSB)	8
Application Type								9
Application Sub Type								10
(MSB)	Application Data							11
								12
								...
								...
							(LSB)	k

Note that the Application Type and the Application Sub Type together correspond to the Vendor- CVSE-Type as defined in [25].

Type:

26H

Length:

This field indicates the number of octets in this element following the Length field.

3GPP2 Vendor ID:

00 00 15 9FH

Application Type:

This field indicates the type of application to which the extension relates. The supported values are listed in Table 4.2.13-1.

Application Sub Type:

This one octet field indicates the Application sub-type within the Application Type. The supported values are listed in Table 4.2.13-1.

Table 4.2.13-1 Application Type and Sub Type

Application Type		**Application Sub Type**		**Used in Message**	**Reference**
Name	Value	Name	Value		
Accounting	01H	RADIUS	01H	A11-Registration Request	3.1
		DIAMETER	02H	Not used	
		All other values are reserved			
Mobility Event Indicator	02H	Mobility	01H	A11-Registration Request	3.1
		All other values are reserved			
Data Available Indicator	03H	Data Ready to Send	01H	A11-Registration Reply	3.2
		All other values are reserved			
All other values are reserved					

Application Data:

For Application Type 01H (Accounting), this field contains all the accounting parameters contained in one airlink record conveyed from the PCF to the PDSN as specified in [8]. In this version of this standard, only Application Sub Type = RADIUS is used. Each of the accounting parameters is structured in the format of RADIUS attributes specified in [22] and [23]. Refer to the following text for more details.

For Application Type 02H (Mobility Event Indicator), this field is zero bytes in length.

For Application Type 03H (Data Available Indicator), this field is zero bytes in length.

For Application Type 01H (Accounting), all 3GPP2 specific Accounting Parameters are coded using RADIUS Vendor-Specific-Attribute format as follows:

1	2	3	4	5	6	7	8	Octet
Type								1
Length								2
(MSB)	3GPP2 Vendor-Id							3
								4
								5
							(LSB)	6
Vendor-Type								7
Vendor-Length								8
(MSB)	Vendor-Value (variable number of octets)							9
								10
								...
							(LSB)	k

Type:

1AH

Length:

Type (1 octet) + Length (1 octet) + 3GPP2 Vendor Id (4 octets) + { Vendor-Type (1 octet), Vendor-Length (1 octet), Vendor-Value (variable octets) of the 3GPP2 specific parameter comprising the airlink record being coded.}

Vendor ID:

00 00 15 9FH

Vendor Type:

Sub-Type value from the Airlink Record tables below.

Vendor-Length:

Vendor-Type (1 octet) + Vendor-Length (1 octet) + Payload Length (in octets) from the Airlink Record tables below.

Vendor-Value:

Payload of the accounting parameter.

For Application Type 01H (Accounting) all RADIUS specific Airlink Record Parameters are coded as follows:

1	2	3	4	5	6	7	8	Octet
Type								1
Length								2
(MSB)	Value (variable number of octets)							3
								4
								…
							(LSB)	k

Type:

Type value from the Airlink Record tables below.

Length:

Type (1 octet) + Length (1 octet) + Payload Length (in octets) from the Airlink Record tables below.

Value:

Payload of the accounting parameter.

Table of Fields that may be present in Airlink Records:

Table 4.2.13-2 A10 Connection Setup Airlink Record (Connection Setup)

Parameter	Type	Sub-Type	Max. Payload Length (octet)	Format
Airlink Record Type = 1 (Setup)	26	40	4	Integer
A10 Connection ID	26	41	4	Integer[a]
Airlink Sequence number	26	42	4	Integer
MSID	31	N/A	15	String[b]
ESN	26	52	15	String[d,f]
MEID	26	116	14	String[e,f]
Serving PCF	26	9	4	Ip-addr
BSID (SID+NID+Cell Identifier)	26	10	12	String[c]

a. This parameter shall be set to the same value as the Key field in the Session Specific Extension information element sent in the A11-Registration Request message.

b. Each digit is encoded an American Standard Code for Information Interchange (ASCII) character.

c. The string is the result of the concatenation of SID+NID+ Cell Identifier (Type 2), where each item is encoded using four hexadecimal uppercase ASCII characters.

d. The string consists of the 8-bit ASCII encoding of the uppercase hexadecimal representation of the ESN.

e. The string consists of the 8-bit ASCII encoding of the uppercase representation of the Mobile Equipment Identifier. If the network operator uses MEID, this parameter is included if the MEID is available at the Radio Access Network (RAN) at the time of A10 connection establishment.

f. Inclusion of ESN, MEID or both parameters in this record is a network operator decision.

Table 4.2.13-3 Active Start Airlink Record

Parameter	Type	Sub-Type	Max. Payload Length (octet)	Format
Airlink record type = 2 (START)	26	40	4	Integer
A10 Connection ID	26	41	4	Integer
Airlink Sequence number	26	42	4	Integer
MEID	26	116	14	String[d]
BSID (SID+NID+Cell Identifier)	26	10	12	String
User Zone	26	11	4	Integer[a]
Forward FCH Mux Option	26	12	4	Integer[b]
Reverse FCH Mux Option	26	13	4	Integer[b]
Service Option	26	16	4	Integer
Forward Traffic Type (Primary, Secondary)	26	17	4	Integer
Reverse Traffic Type (Primary, Secondary)	26	18	4	Integer
FCH Frame Size (0/5/20ms)	26	19	4	Integer[c]
Forward FCH RC	26	20	4	Integer[b]
Reverse FCH RC	26	21	4	Integer[b]
DCCH Frame Size (0/5/20 ms)	26	50	4	Integer[c]
Forward PDCH RC	26	83	4	Integer[b]
Forward DCCH Mux Option	26	84	4	Integer[b]
Reverse DCCH Mux Option	26	85	4	Integer[b]
Forward DCCH RC	26	86	4	Integer[b]
Reverse DCCH RC	26	87	4	Integer[b]
Reverse PDCH RC	26	114	4	Integer[b]
Airlink Priority	26	39	4	Integer

a. This parameter shall either be set to 00 00 00 00H or not be included if the PCF does not have the information available.

b. This parameter shall not be included if the corresponding physical channel type is not part of the current channel configuration.

c. This parameter shall be set to zero if the corresponding physical channel type is not part of the current channel configuration.

d. If the network operator uses MEID, this parameter is included if the MEID is available at the RAN. The string consists of the 8-bit ASCII encoding of the uppercase representation of the Mobile Equipment Identifier.

Table 4.2.13-4 Active Stop Airlink Record

Parameter	Type	Sub-Type	Max. Payload Length (octet)	Format
Airlink record type = 3 (STOP)	26	40	4	Integer
A10 Connection ID	26	41	4	Integer
Airlink Sequence number	26	42	4	Integer
MEID	26	116	14	String[a]
Active Connection Time in Seconds	26	49	4	Integer

a. If the network operator uses MEID, this parameter is included if the MEID is available at the RAN. The string consists of the 8-bit ASCII encoding of the uppercase representation of the Mobile Equipment Identifier.

Table 4.2.13-5 SDB Airlink Record

Parameter	Type	Sub-Type	Max. Payload Length (octet)	Format
Airlink record type = 4 (SDB)	26	40	4	Integer
A10 Connection ID	26	41	4	Integer
Airlink Sequence number	26	42	4	Integer
Mobile Orig./Term. Indicator	26	45	4	Integer
SDB Octet Count	26	31/32[a]	4	Integer

a. Subtype 31 is for terminating SDB octet count, and subtype 32 is for originating SDB octet count.

An example coding of the Active Stop Airlink Record within the CVSE element is illustrated below:

0	1	2	3	4	5	6	7	Octet
A11 Element Identifier = 26H								1
Reserved								2
(MSB)	Length = 36H							3
							(LSB)	4
(MSB)	3GPP2 Vendor ID = 00 00 15 9FH							5
								6
								7
							(LSB)	8
Application Type = 01H								9
Application Sub Type = 01H								10
Parameter Name: Airlink Record Type = 3 (Active Stop)								
Type = 1AH								11
Length = 0CH								12

0	1	2	3	4	5	6	7	Octet
(MSB)	3GPP2 Vendor-Id = 00 00 15 9FH							13
								14
								15
							(LSB)	16
Vendor-Type = 28H								17
Vendor-Length = 06H								18
MSB	Vendor-Value = 3 (Active Stop)							19
								20
								21
							(LSB)	22
Parameter Name: A10 Connection ID								
Type = 1AH								23
Length = 0CH								24
(MSB)	3GPP2 Vendor-Id = 00 00 15 9FH							25
								26
								27
							(LSB)	28
Vendor-Type = 29H								29
Vendor-Length = 06H								30
(MSB)	Vendor-Value = PCF Session Identifier							31
								32
								33
							(LSB)	34
Parameter Name: Airlink Sequence Number								
Type = 1AH								35
Length = 0CH								36
(MSB)	3GPP2 Vendor-Id = 00 00 15 9FH							37
								38
								39
							(LSB)	40
Vendor-Type = 2AH								41
Vendor-Length = 06H								42
(MSB)	Vendor-Value = Sequence Number							43
								44
								45
							(LSB)	46
Parameter Name: Active Connection Time								

0	1	2	3	4	5	6	7	Octet
Type = 1AH								47
Length = 0CH								48
(MSB)	3GPP2 Vendor-Id = 00 00 15 9FH							49
								50
								51
							(LSB)	52
Vendor Type = 31H								53
Length = 06H								54
(MSB)	Value = Active Connection Time (in seconds)							55
								56
								57
							(LSB)	58

1

4.2.14 Normal Vendor/Organization Specific Extension (NVSE)

This element may be included in the A11-Registration Request, A11-Registration Reply, A11-Registration Update, and A11-Session Update messages to convey information between the PCF and the PDSN. Any new Application Types or Application Sub-Types supported after IOS v4.0 shall be added to this element. The coding format of the NVSE defined herein conforms to [25].

This element may be included in the A11-Registration Request message to convey the Previous and Current Access Network Identifiers (PANID, CANID) to the PDSN.

This element may be included in A11-Registration Reply, A11-Registration Request, or A11-Session Update messages to convey the Anchor PDSN Address for fast handoff when the PCF establishes an A10 connection. When sent by the PCF, the Anchor P-P Address is the address received in the fast handoff request from the source BS/PCF. When sent by the PDSN, the Anchor P-P Address value is copied from the corresponding A11-Registration Request if the PDSN accepts a fast handoff request. It is the PDSN's own P-P address if the PDSN supports fast handoff and becomes the anchor PDSN.

If the receiver does not recognize the NVSE Vendor-ID or the NVSE Application Type or Application Sub Type, it shall ignore the NVSE and process the remainder of the message to the extent possible.

This element may be included in the A11-Registration Request message to send the All Dormant Indicator for the case of an MS in fast handoff. The serving PCF shall send the All Dormant Indicator to its supporting PDSN when all service instances for the MS become dormant. The PCF shall send this indication in the same message as the Active Stop Airlink Record for the last service instance that becomes dormant.

This element may be included in the A11-Registration Update message to indicate the reason the PDSN initiated the release of the packet data session.

This element may be included in the A11-Registration Reply or A11-Session Update messages to change the value of a session parameter.

This element may be included in the A11-Registration Request message to indicate the service option of a service instance.

This element may be included in the A11-Session Update message to indicate a PDSN Identifier.

This element may be included in the A11-Registration Request message to indicate the features enabled by the PCF.

This element may be included in the A11-Registration Reply message to indicate the features enabled by the PDSN.

4.2.14 Normal Vendor/Organization Specific Extension (NVSE)

0	1	2	3	4	5	6	7	Octet
A11 Element Identifier (Type)								1
Length								2
(MSB)	Reserved							3

4.2.14 Normal Vendor/Organization Specific Extension (NVSE)

0	1	2	3	4	5	6	7	Octet
							(LSB)	4
(MSB)	3GPP2 Vendor ID							5
								6
								7
							(LSB)	8
Application Type								9
Application Sub Type								10
(MSB)	Application Data							11
								12
								...
								...
							(LSB)	k

Note that the Application Type and the Application Sub Type together correspond to the Vendor- NVSE-Type as defined in [25].

Type:

86H

Length:

This field indicates the number of octets in this element following the Length field.

3GPP2 Vendor ID:

00 00 15 9FH.

Application Type:

This field indicates the type of application to which the extension relates. The supported values are listed in Table 4.2.14-1.

Application Sub Type:

This one octet field indicates the Application sub-type within the Application Type. The supported values are listed in Table 4.2.14-1.

Table 4.2.14-1 Application Sub Type

Application Type		Application Sub Type		Used in Message	Reference
Name	Value	Name	Value		
Access Network Identifiers (ANID)	04H	ANID	01H	A11-Registration Request	3.1
		All other values are reserved			
PDSN Identifier	05H	Anchor P-P Address	01H	A11-Registration Request A11-Registration Reply A11-Session Update	3.1 3.2 3.5
		All other values are reserved			
Indicators	06H	All Dormant Indicator	01H	A11-Registration Request	3.1
		All other values are reserved			
PDSN Code	07H	PDSN CODE	01H	A11-Registration Update	3.3
		All other values are reserved			
Session Parameter	08H	RN-PDIT	01H	A11-Registration Reply A11-Session Update	3.2 3.5
		Always-On	02H	A11-Registration Reply A11-Session Update	3.2 3.5
		All other values are reserved			
Service Option	09H	Service Option Value	01H	A11-Registration Request	3.1
		All other values are reserved			
PDSN Enabled Features	0AH	Flow Control Enabled	01H	A11-Registration Reply	3.2
		All other values are reserved			
PCF Enabled Features	0BH	Short Data Indication Supported	01H	A11-Registration Request	3.1
		All other values are reserved			
All other values are reserved					

Application Data:

For Application Type 04H (Access Network Identifiers), this field contains the PANID of the source PCF in the PANID field (octets 11-15) and the ANID of the target PCF in the CANID field (octets 16-20). The PANID and CANID fields are formatted as specified for the Access Network Identifiers element (refer to [16]) from octet 3-7. If PANID information is not available, it shall be coded as all zeros. The CANID field shall be populated with the PCF's own ANID.

For Application Type 05H (PDSN Identifier), this field contains an IPv4 address in octets 11-14. This is the Anchor P-P Address. The Anchor P-P Address is the P-P interface address (refer to [8]) of the anchor PDSN.

For Application Type 06H (Indicators), this field contains the All Dormant Indicator in octets 11-12. A value of '00 00H' indicates that

all MS packet data service instances are dormant. All other values are reserved.

For Application Type 07H (PDSN CODE), the field contains a PDSN Code indicating the reason the packet data connection is being released by the PDSN. The PDSN Code values and their meanings are listed in Table 4.2.14-2.

Table 4.2.14-2 PDSN Code Values

Hex Value	Decimal Value	PDSN Code
C1H	193	Connection Release - reason unspecified
C2H	194	Connection Release - PPP time-out
C3H	195	Connection Release - registration time-out
C4H	196	Connection Release - PDSN error
C5H	197	Connection Release - inter-PCF handoff
C6H	198	Connection Release - inter-PDSN handoff
C7H	199	Connection Release - PDSN OAM&P intervention
C8H	200	Connection Release - accounting error
CAH	202	Connection Release - user (NAI) failed authentication
All other values reserved		

For Application Type 08H (Session Parameter) and Application Sub-Type 01H, the Application Data field contains the Radio Network Packet Data Inactivity Timer (RN-PDIT) value in seconds. This field is one octet in length and has range 01H–FFH, corresponding to timer values 1–255 seconds. For Application Sub Type 02H (Always-on indicator), the Application Data is zero bytes in length.

For Application Type 09H (Service Option), this field contains the Service Option value for the service instance associated with the A10 connection, in octets 11-12.

For Application Type 09H, the Application Data field is coded as follows:

0	1	2	3	4	5	6	7	Octet
(MSB)	Service Option							11
							(LSB)	12

Service Option:

Table 4.2.14-3 Service Option Values

Service Option Value (hex)	Description
0021H	3G High Speed Packet Data
003CH	Link Layer Assisted Header Removal
003DH	Link Layer Assisted RObust Header Compression

For Application Type 0AH (PDSN Enabled Features) and Application Sub-Type 01H (Flow Control Enabled), the Application Data field is zero bytes in length. This Application Sub-Type is included if the PDSN enables flow control for the corresponding A10 connection.

For Application Type 0BH (PCF Enabled Features) and Application Sub-Type 01H (Short Data Indication Supported), the Application Data field is zero bytes in length. This Application Sub-Type is included by the PCF in the A11-Registration Request message to request Short Data Indications via the GRE header.

(This page intentionally left blank.)

5.0 Timer Definitions

5.1 Timer Values

The following table is in units of seconds unless otherwise noted.

Table 5.1-1 Timer Values and Ranges Sorted by Name

Timer Name	Default Value	Range of Values	Granularity	Section Reference
$T_{presetup}$	10	0-255	1	5.2.4
T_{regreq}	1	1 – 5	1	5.2.1
T_{regupd}	1	1 – 5	1	5.2.2
T_{rp}	1800	60 – 65,534	1	5.2.3
T_{sesupd}	3	1-10	1	5.2.5

5.2 Timer Definitions

5.2.1 T_{regreq}

The PCF timer T_{regreq} is started when the A11-Registration Request message is sent, and stopped when the A11-Registration Reply message is received.

5.2.2 T_{regupd}

The PDSN timer T_{regupd} is started when the A11-Registration Update message is sent, and stopped when the A11-Registration Acknowledge message is received.

5.2.3 T_{rp}

This configurable parameter represents the longest lifetime that the PCF is willing to accept before registration for an A10 connection is considered expired. It is used to set the Lifetime parameter in the A11-Registration Request message.

5.2.4 $T_{presetup}$

This configurable parameter represents the longest lifetime that the PCF is willing to accept before a fast handoff pre-registration for an A10 connection is considered expired. It is used to set the Lifetime parameter in the A11-Registration Request message.

5.2.5 T_{sesupd}

The PDSN timer T_{sesupd} is used when a packet data session update occurs. It is set when the PDSN sends the A11-Session Update message with any new or updated packet data

session parameters, and stopped when an A11-Session Update Acknowledge message is received from the PCF indicating the results of processing the new session parameters.