ATIS-0x0000x

ATIS Standard on

DRAFT

Parameter Conveyance for Location Determination of Devices Attached To Access Networks

Secretariat

Alliance for Telecommunications Industry Solutions

Approved Month DD, YYYY

Abstract

This technical report introduces concepts to provide a framework and associated protocol(s) to allow a location determination function to obtain the value of relevant network parameters associated with an end device, and from which the location of that end device may be determined. This technical report provides content that may be used as a basis for stage 1 and stage 2 development of a parameter conveyance framework. Future work will include the specific stage 3 protocol to accomplish parameter conveyance.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Emergency Services Interconnection Forum (ESIF) mission is to provide a forum to facilitate the identification and resolution of technical and/or operational issues related to the interconnection of wireline, wireless, cable, satellites, Internet and emergency services networks. ESIF is an open, technical/operational forum with the voluntary participation of interested parties to identify and resolve recognized interconnection issues. The interest of all members will be served by observing the principles of openness, fairness, consensus, and due process. ESIF will liaise with standards and governmental organizations to apprise them of its deliberations and decisions. Discussions will be focused on the FCC's Wireless Phase I and II mandates, and into other areas of emergency services interconnection.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, ESIF Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, ESIF, which is responsible for the development of this Technical Report, had the following members:

COMMITTEE LIST

The current committee list will be added prior to publication.

The Next Generation Emergency Services Subcommittee (NGES-SC) was responsible for the development of this document.

DRAFT

TABLE OF CONTENTS

ATIS-0X0000X I
ATIS STANDARD ON I
SECRETARIAT I
ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS I
ABSTRACT I
FOREWORD II
TABLE OF CONTENTS III
TABLE OF FIGURES IV
TABLE OF TABLES ..... ERROR! BOOKMARK NOT DEFINED.
1 SCOPE, PURPOSE, & APPLICATION 1
1.1 SCOPE 1
1.2 PURPOSE 1
1.3 APPLICATION 2
2 NORMATIVE REFERENCES 2
3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS 3
3.1 DEFINITIONS TO BE ADDED BY NGES EDITOR PRIOR TO FINAL RELEASE IF APPLICABLE 3
3.2 ACRONYMS & ABBREVIATIONS 3
4 INTRODUCTION 4
5. REQUIREMENTS MODEL 4
6. MEASUREMENT MODELS & REQUIREMENTS 5
7. MESSAGE REQUIREMENTS (LDF – AMF) 6
7.1 POLLING FUNCTION REQUIREMENTS 6
7.2 REPORTING FUNCTION REQUIREMENTS 6
8. COMMUNICATION SESSION MANAGEMENT 6
9. PROCEDURAL REQUIREMENTS 7
10. DATA AND SCHEMA FORMULATION REQUIREMENTS 8
11 NETWORK MEASUREMENT CONVEYANCE – ARCHITECTURE AND PROCEDURES (STAGE 2) 9
11.1. FUNCTIONAL ELEMENTS OF LDF 9
11.3 LSIF 9
11.4 AMIF 10
11.5 MCF 10
11.6 LDBF 10
11.7 LCF 10

DRAFT

TABLE OF FIGURES

FIGURE 1 REQUIREMENTS MODEL AND TERMINOLOGY 5
FIGURE 2 LDF FUNCTIONAL ELEMENTS 9
FIGURE 3 HEARTBEAT USING BEEP 12
FIGURE 4 AMIF-AMF CONNECTION STATE MACHINE 12
FIGURE 5 DEMAND POLLING STATE MACHINE.....13
FIGURE 6 PERIODIC POLLING STATE MACHINE 14
FIGURE 7 MEASUREMENT REPORTING STATE MACHINE.....15
FIGURE 8 POLLING MESSAGES 16
FIGURE 9 NOTIFICATION MESSAGES.....16
FIGURE 10 RESYNCHRONIZATION MESSAGES 17

DRAFT

ATIS Standard on –

Parameter Conveyance for Location Determination of Devices Attached To Access Networks

1 SCOPE, PURPOSE, & APPLICATION

1.1 Scope

This technical report introduces concepts to provide a framework and associated protocol(s) to allow a location determination function to obtain the value of relevant network parameters associated with an end device, and from which the location of that end device may be determined. Location determination may be through the application of calculations according to specific algorithms, the association of network parameter values through database enquiry, combinations of these operations, or other operations. These operations, and the process of location determination generally, are outside the scope of this technical report. This technical report provides content that may be used as a basis for stage 1 and stage 2 development of a parameter conveyance framework. Future work will include the specific stage 3 protocol to accomplish parameter conveyance.

1.2 Purpose

The determination of the location associated with a calling device's point of connection to the Internet is an important component of the NENA i2 and i3 emergency service VoIP architectures. The location of the calling device is used for the purposes of call routing, operator display, and emergency responder dispatch. A location determination capability is expected to be commonly available for all forms of Internet access technology even though the manner in which location is determined may vary from technology to technology (reference: NENA VoIP, Recommended Method(s) for Determining Location to Support Emergency Calling Technical Information Document 08-505, December 2006).

A common approach to location determination is to use the value of relevant access network parameters related to the target device to facilitate database lookup and/or actual position calculation. While this approach is common across all access technologies, there exists no common architecture or framework that describes how access-network related location parameters can be sent to or otherwise obtained by a location determination function so that location can be determined.

Network technologies that have an existing location service infrastructure generally already have a specifically defined way of transferring location parameters of this nature from the various network elements to the location determination function (e.g. BSSLAP on the Lb interface in the 3GPP GERAN or PCAP on the Iupc interface in the 3GPP UTRAN – refer to 3GPP specifications 43.059 and 25.305 respectively). However, this functionality is not established for a number of other common access technologies (DSL, Cable, WiMAX for example). It would be advantageous to have a common architecture and framework that could be used with these access networks as opposed to having the same fundamental mechanism defined in idiosyncratic ways on a per-technology basis. The definition of a common conceptual model and framework would facilitate communications between the implementers of location determination functions and access network elements, which in turn would

promote a more rapid deployment of LIS capabilities and successful implementation of the NENA i2 and i3 defined emergency service architectures.

The purpose of this Technical Report is to document the framework and protocol(s) to support a common functionality for Parameter Conveyance for Location Determination of Devices Attached to an Access Network.

1.3 Application

Some network technologies have existing methods of transferring location parameters from the various network elements to the location determination function. However, that functionality is not established for various other common access technologies (DSL, Cable, WiMAX for example). It would be advisable to have a common architecture and framework that could be used with these access networks. The definition of a common conceptual model and framework would facilitate communications between the implementers of location determination functions and access network elements. Doing so would in turn promote a more rapid deployment of Location Information Server (LIS) capabilities. This will help facilitate the successful implementation of the NENA i2 and i3 defined emergency service architectures as well as future commercial location based services.

2 NORMATIVE REFERENCES

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

T1.xxx-YYYY, *Title*.[1] Tba later as they are clearly identified by the team

[1] This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. <http://www.atis.org>

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS

3.1 Definitions To be added by NGES editor prior to final release if applicable

3.1.1 Aaaa: xxxx

3.1.2 Bbbb: xxxx

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
AMF	Access Measurement Function
AMIF	Location Service Interface Function
ATIS	Alliance for Telecommunications Industry Solutions
BEEP	Block Extensible Exchange Protocol
BSSLAP	Base Station System Location Services Assistance Protocol
Cable	Used herein to describe broadband service over coaxial cable, as opposed to DSL
DSL	Digital Subsrciber Line
ESIF	Emergency Services Interconnection Forum
FLAP	Flexible LDF to AMF Protocol
GERAN	GSM/EDGE Radio Access Network
Iupc interface	A logical interface for the interconnection of Standalone A-GPS SMLC (SAS) and Radio Network Controller (RNC) components of the Universal Terrestrial Radio Access Network (UTRAN) for the UMTS system
Lb interface	The link between the Serving Mobile Location Center and the base station controller
LCF	Location Calculation Function
LDBF	Location Database Function
LDF	Location Determination Function
LIS	Location Information Server
LSIF	Location Service Interface Function
MCF	Measurement Cache Function
MSG	Message
NENA	National Emergency Number Association
NENA i2	The transitional stage of emergency service VoIP network architectures as defined by NENA
NENA i3	The (currently) final stage of emergency service VoIP network architectures as defined by NENA
NGES (SC)	Next Generation Eergency Services Subcommittee (author of this TR)
RPY	Reply
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
UMTS	Universal Mobile Telecommunications System
UTC	Coordinated Universal Time
UTRAN	UMTS Terrestrial Radio Access Network
WiMAX	Worldwide Interoperability for Microwave Access,

DRAFT

4 INTRODUCTION

The general requirement is to provide a framework and associated protocol(s) to allow a location determination function to obtain the value of relevant network parameters, associated with an end device, and from which the location of that end device may be determined. Location determination may be through the application of calculations according to specific algorithms, the association of network parameter values through database enquiry, combinations of these operations, or other operations. These operations, and the process of location determination generally, are outside the scope of these requirements.

5. REQUIREMENTS MODEL

An entity labeled a "location determination function" (LDF) is defined which is the recipient of the values associated with specific network parameters. One or more instances of a corresponding entity labeled an "access measurement function" (AMF) is defined which is the source of the values associated with specific network parameters. Associated with the LDF and the AMF entities are target devices which serve as the subject of the parameter values exchanged. It is assumed in the model that the AMF may become "aware" of a target device forming an association with the network and, at any time from which the AMF becomes aware of the device, it will be able to provide the value of network parameters associated with the device.

The model also assumes that the LDF and the AMF entities have prior knowledge of which network parameters are relevant and the manner in which an associated target device may be identified against those parameters. It may also be assumed that the LDF has a priori knowledge of which AMF instance(s) are relevant to it. It is not necessary for the AMF to have prior which LDF instance will be communicating with it.

This model is shown graphically below:

DRAFT

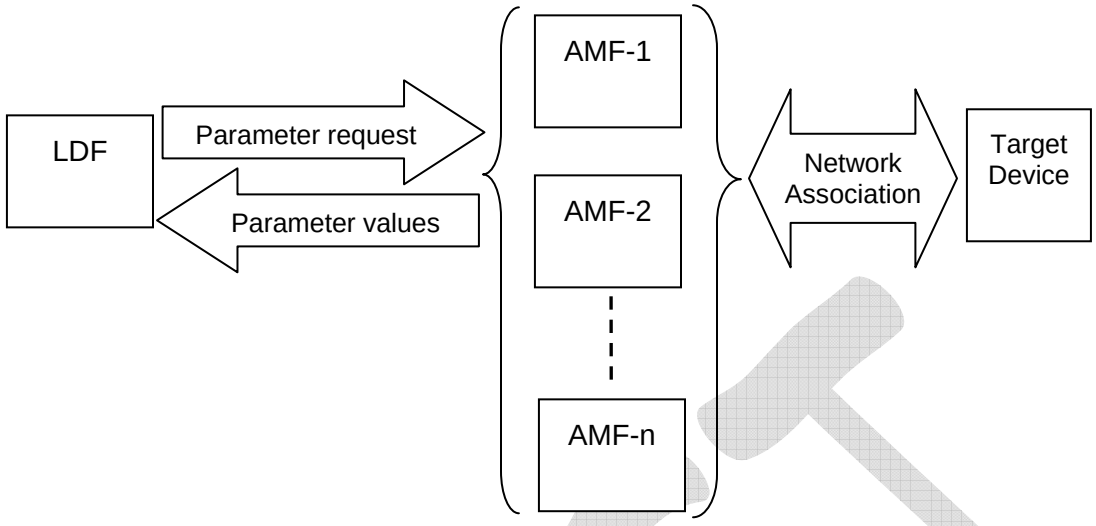

Figure 1 Requirements model and terminology

6. Measurement Models & Requirements

Network measurements may be collected, collated, and stored in a number of ways for the purposes of location determination. This TR assumes the following three models:

A. On-demand polling model

The LDF needs to determine the location of a target device and then immediately polls the relevant AMF instance(s) for the network parameter values associated with the target device.

B. LDF cache with polling model

The LDF periodically polls the relevant AMF instance(s) and for network parameter values associated with all target devices of which the AMF is aware. The LDF caches this information and uses it to calculate the location of a specific target device when required and without polling of the AMF instance(s) solely for the purpose of that location calculation. Synchronization methods are required to bring a cache up to date when an LDF initially comes on line.

C. LDF cache with reporting model

As an AMF becomes aware of significant events related target devices in the network and for which the value of relevant network parameters become established, it reports those values to the LDF. The LDF caches this information and uses it to calculate the location of a specific target device when required and without polling of the AMF instance(s) solely for the purpose of that location calculation. Synchronization methods are required to bring a cache up to date when an LDF initially comes on line.

The following requirements apply to Stage 2:

1. Each model described above must be able to be supported.
2. It must be possible for a specific implementation of a functioning system to be able to apply one or more of the models concurrently.

7. Message Requirements (LDF – AMF)

Functional requirements exist around the ability of the LDF and the AMF to communicate with each other the value of network parameters that correspond to specific target devices. Communications may take the form of polling (one function requests information from the other function) or reporting (one function sends unsolicited information to the other function).

The following requirements apply to the message set defined in Stage 2 in support of LDF and AMF entities.

7.1 Polling function requirements

1. An LDF shall be able to request an AMF to provide the value of network parameters associated with a specific, nominated, target device.
2. An LDF shall be able to request an AMF to provide the value of network parameters associated with all target devices of which the AMF is currently aware.
3. An LDF shall be able to request an AMF to provide the value of network parameters associated with all target devices that the AMF has become aware of, or where parameter values have changed since a nominated point in time.

7.2 Reporting function requirements

1. An AMF shall be able to asynchronously report the value of network parameters associated with a target device.

It is only necessary for any LDF-AMF implementation to support the messages applicable to the measurement models they use.

8. Communication Session Management

An LDF is assumed to be the initiator of communications with AMF instances. The term used to describe the period of time that an LDF and an AMF instance are able to communicate is a "session". The messages used for reporting and polling functions are able to be passed whenever a session exists between an LDF and an AMF.
The following requirements apply to session management:

1. An LDF shall be able to initiate a session with one or more AMF instances concurrently.
2. An LDF shall be able to terminate a session with an AMF at any time.
3. An AMF shall be able to terminate a session with an LDF at any time.
4. Both the LDF and the AMF shall be aware of the existence of sessions and have a mechanism to ensure the session is valid in the absence of polling or reporting messages.
5. There must be a defined way for the communications between the LDF and the AMF to be secure.

9. Procedural Requirements

It is assumed that the establishment of LDF-AMF sessions and the associated messaging will occur in accordance with procedures that are understood between the LDF and the AMF. For example, either polling or reporting may be used as the basis for communicating network parameter values; however both functions have to support the same method, or both methods, in practice.

LDF Procedures

1. On startup, an LDF shall establish sessions with all required and active AMF instances.
2. Where required AMF instances are not active, the LDF shall continue to attempt to establish a session until successful or until exception treatment is applied.
3. When a session is established with an AMF, an LDF may make a request for all network parameter and corresponding target device information known to the AMF.
4. When an LDF has been offline for a known period of time and establishes a session with an AMF, the LDF may make a request for all network parameters and corresponding target device information known to the AMF.
5. An LDF must be able to receive a report from any AMF with which it has a session. The LDF may choose to ignore the contents of the report.

AMF Procedures

1. On startup, an AMF may commence to record the values of network parameters and associated target device information either globally or in response to events that occur within the network. It shall record the time at which each piece of information is recorded.
2. On startup an AMF shall make itself ready to accept the initiation of a session from an LDF.
3. An AMF may apply authentication and authorization mechanisms to the establishment of the session with the LDF.
4. An AMF may support encryption or other channel security mechanisms for session communication.
5. An AMF must respond to a request for network parameter information for a specified target device with one of the following
    a. The requested information together with the time at which the information was determined
    b. A response indicating that the information cannot be provided.
6. An AMF must respond to a request for all currently known network parameter and associated target device information with one of the following
    a. All information currently recorded by the AMF including time of recording

   b. A response indicating there is no such information available
7. An AMF must respond to a request for all network parameter and associated target device information since a nominated point in time with one of the following
   a. All information recorded by the AMF since the nominated point in time and including the time of recording
   b. All information currently recorded by the AMF, regardless of nominated time, and including the time of recording
   c. A response indicating there is no such information available
8. An AMF may at any time asynchronously report the network parameter and associated target device information with corresponding time of determination to an LDF.

10. Data and Schema Formulation Requirements

The protocol used for polling and reporting shall be general and extensible so that any arbitrary data type(s) can be used to convey network parameters and target device identity information. It is assumed that any LDF and AMF instances that are in communication will have a prior common understanding of the number and type of parameters relevant to the exchange of network parameter and target device identification information.

1. A target device shall be able to be identified by any one or more parameters of arbitrary data types.
2. Any one or more parameters of arbitrary data types shall be able to be used to define the network parameters associated with a target device.
3. A given schema for defining the network parameters and corresponding target device identification parameters shall be able to be grouped into a specific measurement class[2].
4. It shall be possible to formulate new schemas by extending the definition of a pre-existing measurement class.

[2] The term "class" is used here in the sense that is common to discussions related to object-oriented analysis. A class describes a generic "object" which has a set of attributes or pieces of data called "members" that characterize it. For example a class "vehicle" may be defined that includes an attribute which is "number of passengers". A new class may be derived from an existing class (a process called "inheritance") by the addition of new attributes. For example the class "car" may be derived from "vehicle" with the addition of new attributes such as "number of doors" while a different class, "airplane", may also be derived from "vehicle" with new attributes such as "number of wings".

11 NETWORK MEASUREMENT CONVEYANCE – ARCHITECTURE AND PROCEDURES (STAGE 2)

11.1. Functional elements of LDF

The LDF contains a number of functional elements as shown in Figure 2. These functions are described to facilitate the description of the LDF procedures associated with AMF interaction. Neither the physical implementation nor the communication interfaces between these functions are prescribed. The key interface which is external to the LDF is the one to the AMF. Details of procedures focus on the messaging across this interface. The protocol used for this messaging is called the Flexible LDF to AMF Protocol (FLAP).

The internal functional elements of the LDF (LSIF, MCF, LCF, AMIF, and LDBF) are described to facilitate the understanding of the procedures described in the subsequent sections. The specific existence of these elements is not mandated by this specification, and the description of their activities is not prescriptive with respect to implementations of an LDF. The purpose is only to clarify the use of FLAP in the specific scenarios and modes of operation governing the interaction between an LDF and one or more instances of an AMF.

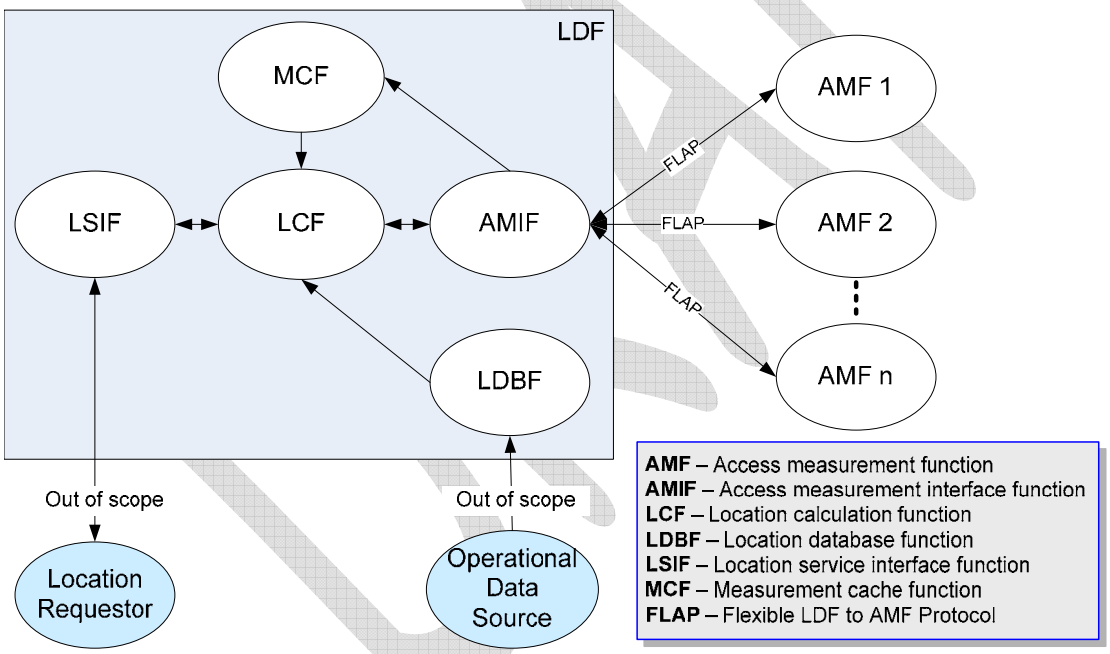

Figure 2 LDF functional elements

11.3 LSIF

The location service interface function (LSIF) interfaces to the location requestor. This may be an application or a LIS or some other function which initiates requests to determine location. The interface protocol to the location requestor is out of scope.

11.4 AMIF

The access measurement interface function (AMIF) provides the connection management and communication support to external AMF entities. The AMIF and the AMF instances communicate using the Flexible LDF-AMF protocol (FLAP).

11.5 MCF

The measurement cache function is a function maintained by the LDF to store measurements which are reported asynchronously from the AMF instances (notification model) and/or storing last known values of network measurement results. The MCF is not used in the on demand model.

11.6 LDBF

The location database function is a storage area for operational data used in conjunction with network measurements in order to calculate location. Examples may include storing the physical end point locations associated with Ethernet switch ports (wire map), or wireless base stations, expressed as either civic addresses or geodetic coordinates or both. The interface protocol to the source of operational data is out of scope.

11.7 LCF

The location calculation function combines measurements retrieved directly via the AMIF and/or from the MCF with data stored in the LDBF to calculate the device location. It embodies the necessary rules and algorithms to perform the location calculation.

12. LDF procedures

The following AMIF-AMF interface procedures are pertinent to the operation of the LDF:

1. The AMIF establishes and maintains connections to the AMF instance(s).

2. The AMIF receives FLAP notifications from AMF instance(s) that implement reporting and stores the reported measurements in the MCF.

3. For an LDF that implements continuous polling, the AMIF initiates the periodic FLAP queries to the relevant AMF instance(s) and stores the query results in the MCF.

4. In response to a location request to the LSIF and the subsequent invocation of the LCF, a request may be made to the AMIF to retrieve new measurement data. This results in the AMIF sending an on-demand FLAP query to the relevant AMF instance(s).

i. Connection and session management

The AMIF knows the identity and network location of the AMF instance(s) with which it will communicate, and is responsible for initiating the network connections and sessions with it/them. The manner in which the AMIF knows this information is out of scope.

FLAP communications occur between the AMIF and the AMF within the context of a session. Session support for FLAP is to be implemented using the Block Extensible Exchange Protocol (BEEP) [Reference: The Blocks Extensible Exchange Protocol Core, M. Rose, IETF RFC3080, March 2001]. BEEP provides a secure, synchronous communication layer that allows for two way communications between clients and servers. Details of the BEEP profile to be used for FLAP session management are defined in [Reference TBD – stage 3 of this spec].

The TCP binding for BEEP [Reference: Mapping the BEEP Core onto TCP, M. Rose, IETF RFC 3081, March 2001] is required to be used for the transport layer of FLAP communication. Where secure communications between the AMIF and AMF are required, TLS should be used. The implementation of security between the AMIF and AMF is not required, therefore support for TLS is optional but recommended. TLS provides a reliable connection with protection from replay, intercept and eavesdropping, and can provide support for authentication. When TLS is used with FLAP, the AMF authenticates the LDF. Specific ciphersuites for use with TLS as a FLAP transport are recommended in [Reference TBD – stage 3 of this spec].

Persistent TCP connections that remain unused for long periods can become inactive without the knowledge of one or other of the peer communicating applications; these being the AMIF and the AMF in this case. This occurs where the underlying operating system which supports the TCP capability does not detect the failure of the using application or where intermediate routing nodes, particularly network address translation (NAT) devices flush the state associated with an apparently idle network connection. To mitigate these issues and consequently improve the reliability of LDF-AMF communications, a heartbeat mechanism is also required as part of the BEEP session management.

The heartbeat mechanism consists of a BEEP "MSG" frame that is sent from the AMIF to the AMF. An active AMF is required to send a BEEP "RPY" frame in response. The use of the "MSG" and "RPY" frames for the heartbeat are shown as steps 1 and 2 respectively in Figure 3. Neither BEEP frame contains any data and consists only of the BEEP frame header and footer. A failure to receive a heartbeat response within the time prescribed by the AMIF is interpreted as a loss of connection and results in exception procedures being exercised by the AMIF as described below. The heartbeat signaling occurs on a dedicated BEEP channel. Details of the BEEP profile used for this channel are defined in [Reference TBD – stage 3 of this spec].

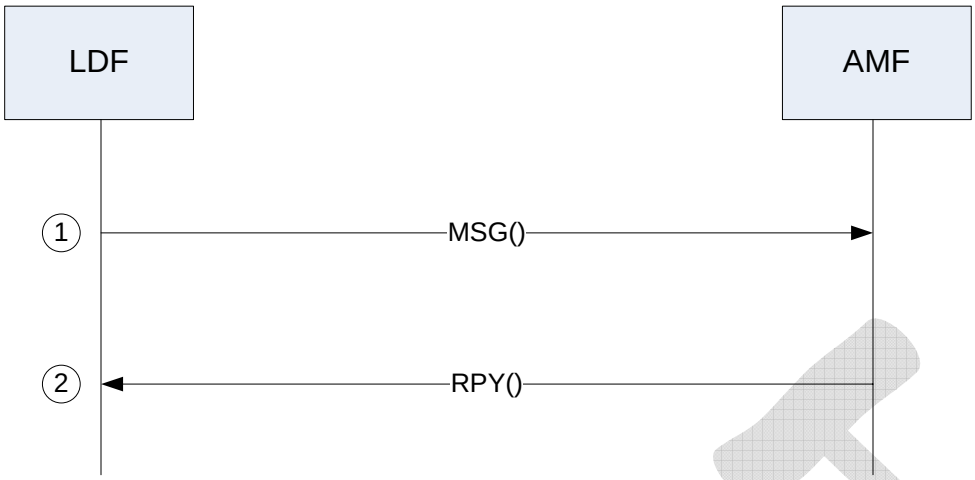

Figure 3 Heartbeat using BEEP

The lifecycle of the connection from the AMIF to each AMF can be described by the state machine shown in Figure 4.

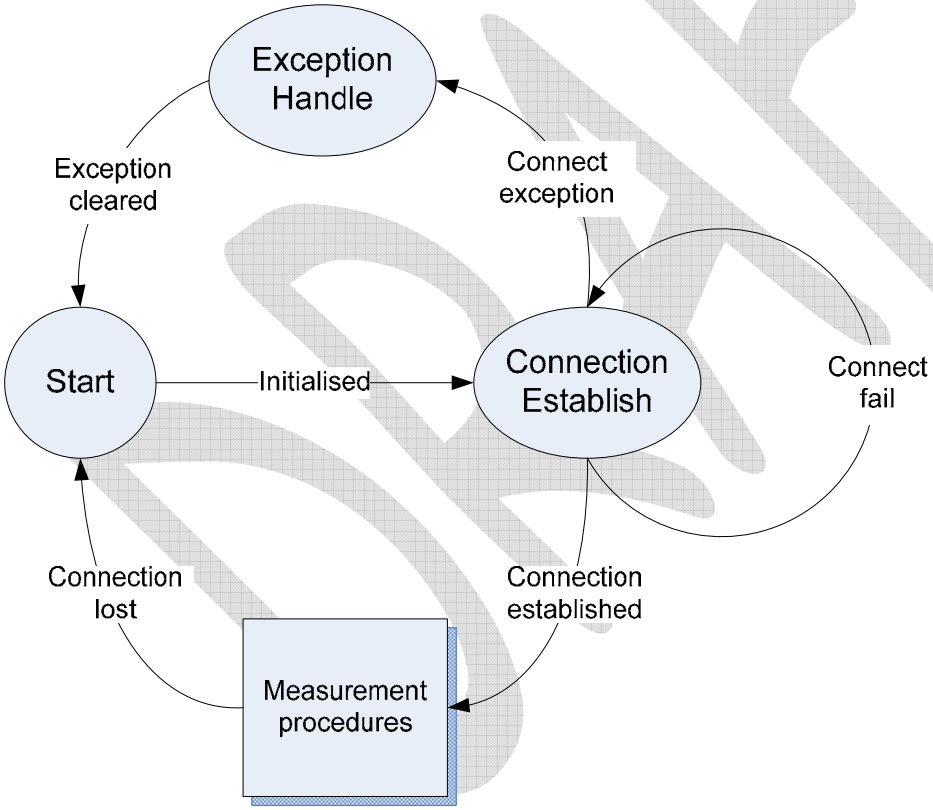

Figure 4 AMIF-AMF connection state machine

The AMIF starts up and is initialized with peer AMF information. Initialization may include manual operations. Once initialized, it enters a connection establishment state in which it periodically attempts to establish a connection with the AMF. This may continue indefinitely until an exception event occurs such as a manual intervention from an operator or a determination that too many failed connection attempts have occurred. Implementation specific processing will occur to reset the exception state and,

if still appropriate, the AMIF will return to the start state and reinitialize before once more attempting connection establishment.

With the successful establishment of a connection, a transition to a state where FLAP messaging procedures are performed will occur. This represents the steady operational state of the AMIF. The specific procedures associated with FLAP messaging will depend on which one or more measurement models the AMF implements; see following descriptions.

Measurement procedures continue until the connection is lost by deliberate operator or system intervention or a failure in the communications. This will result in a transition back to the starting state and subsequent re-initialization.

ii. Demand polling procedure

The state diagram for the demand polling procedure is shown in Figure 5.

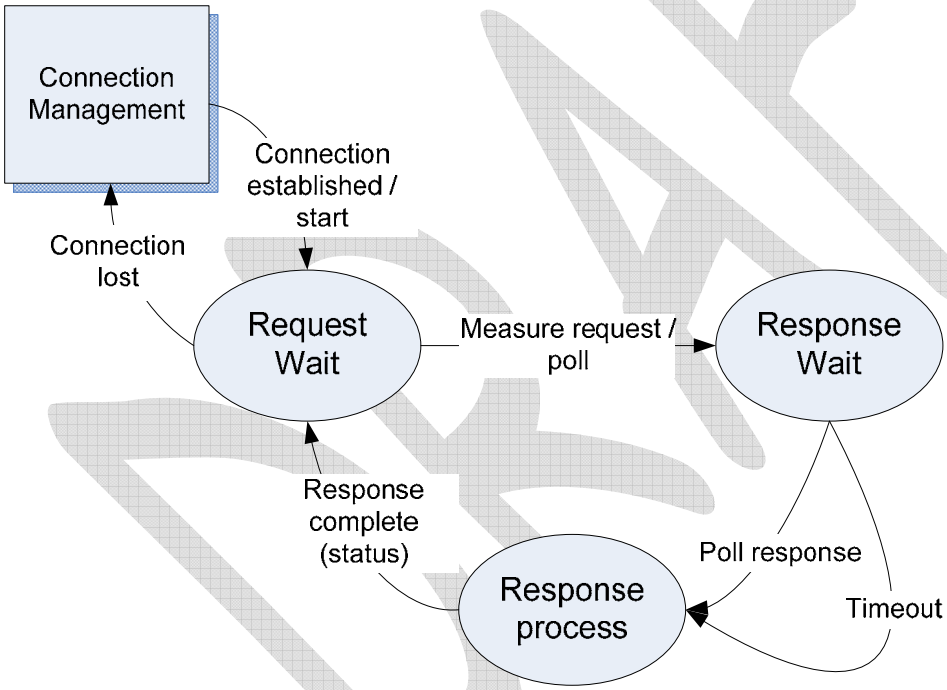

Figure 5 Demand polling state machine

Assuming the AMF connection is in place, the AMIF remains in a wait state until a request for measurement information is received from the LCF. It sends the appropriate FLAP query message to the AMF requesting measurement information. It then waits for a response. When a response is received (or time out occurs) the AMIF processes the result and provides it to the LCF (including status indicating success or failure cause). It then returns to the wait state until the next measurement request is received.

iii. Periodic polling procedure

The state diagram for the periodic polling procedure is shown in Figure 6.

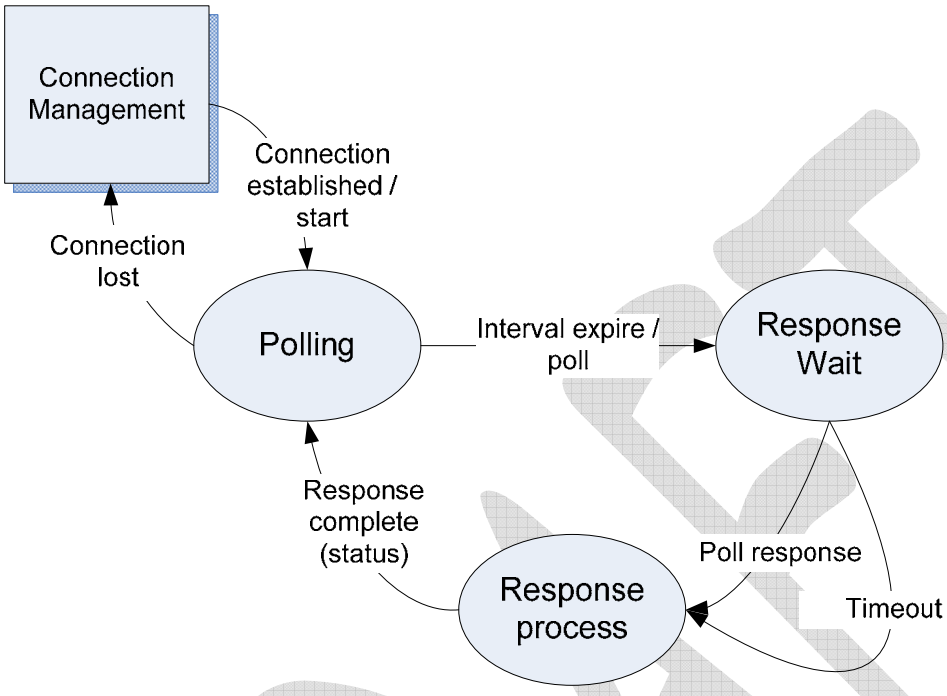

Figure 6 Periodic polling state machine

Assuming the AMF connection is in place, the AMIF initiates a polling interval timer and remains in that state until the polling interval expires. It then sends the appropriate FLAP query message to the AMF requesting measurement information. It then waits for a response. When a response is received (or time out occurs) the AMIF processes the result and stores it in the MCF. It then returns to the polling state and restarts the polling interval timer.

iv. Measurement reporting procedure

The state diagram for the measurement reporting procedure is shown in Figure 7.

DRAFT

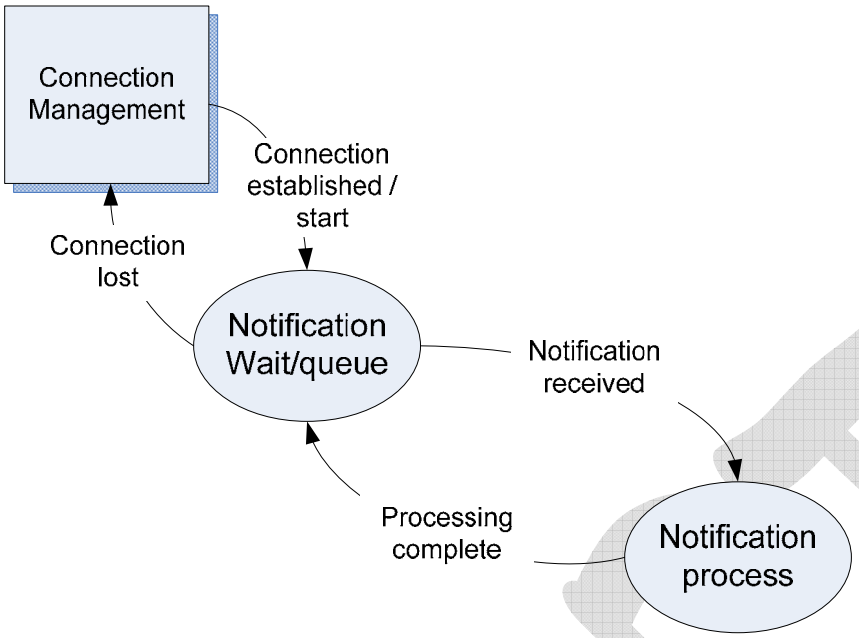

Figure 7 Measurement reporting state machine

Assuming the AMF connection is in place, the AMIF remains in a wait state until a request for measurement notification is received from the AMF. When a notification is received, the AMIF processes the result and stores it in the MCF. It then returns to the wait state until the next measurement notification is received.

13. FLAP Messaging

The following show the exchange of FLAP messages for each mode of operation.

i. Polling

The messaging associated with the polling procedure is shown in Figure 8. The same messages are used for on-demand and periodic polling.

DRAFT

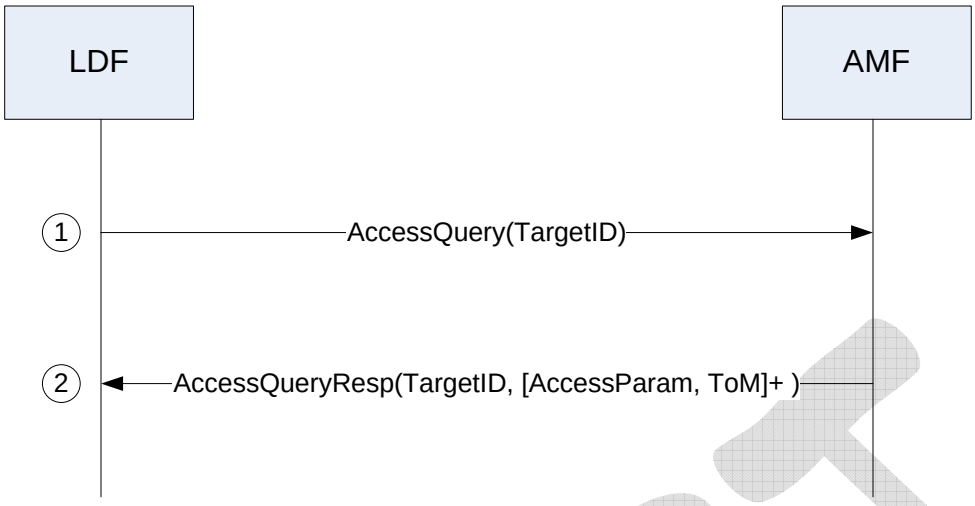

Figure 8 Polling messages

1. Either in response to a location request in on-demand mode or on expiry of the interval timer in polling mode, the AMIF associated with the LDF sends a FLAP *AccessQuery* message to the AMF. The *AccessQuery* message includes the TargetID parameter from which the AMF determines the corresponding access parameter values.
2. The AMF responds with an *AccessQueryResp* message including the values of the access parameters corresponding to the TargetID as well as the time, in Coordinated Universal Time (UTC), at which those values were determined – i.e. "time of measurement" (ToM).

ii. Notification

The messaging associated with the notification mode of operation is shown in Figure 9.

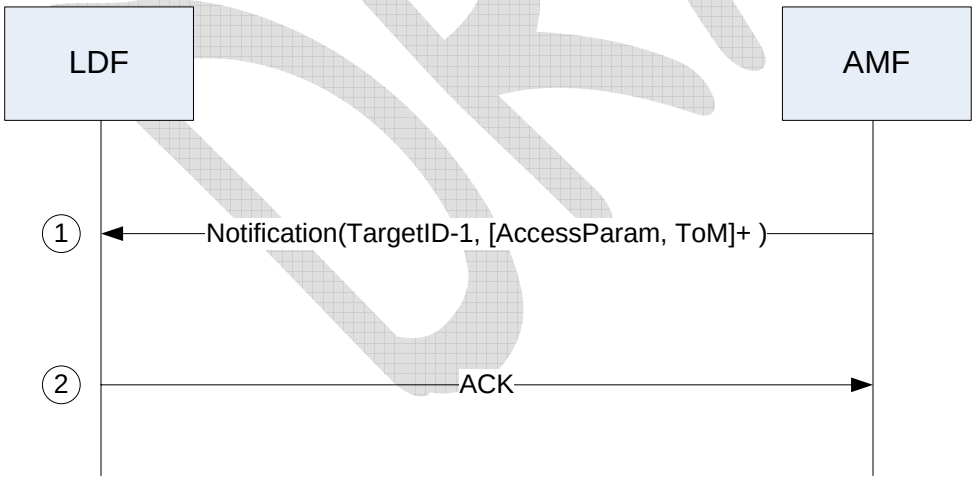

Figure 9 Notification messages

1. The AMF detects a new event resulting in a measurement to be sent to the LDF. It sends a *Notification* message identifying the target to which the parameter values correspond, the values of the parameters, and the UTC value of the time of the measurement (ToM).

2. The AMIF in the LDF sends a simple acknowledgement of receipt of the notification. The AMF may resend the notification if an acknowledgement is not received within a specific time interval. The value and control of the time interval is out of scope.

iii. Resynchronization

Associated with the periodic polling and notification modes of operation is the option to support resynchronization. This occurs when the LDF initializes and wants to populate the MCF with all measurement information known by the AMF instance(s) that has changed since the last time the LDF was receiving measurements. Since previous measurements sent to the LDF have a UTC timestamp provided by the AMF, this time value provides a virtual sequence identifier which the LDF can use to derive the time value in the resynchronization request. The resynchronization messaging is shown in Figure 10.

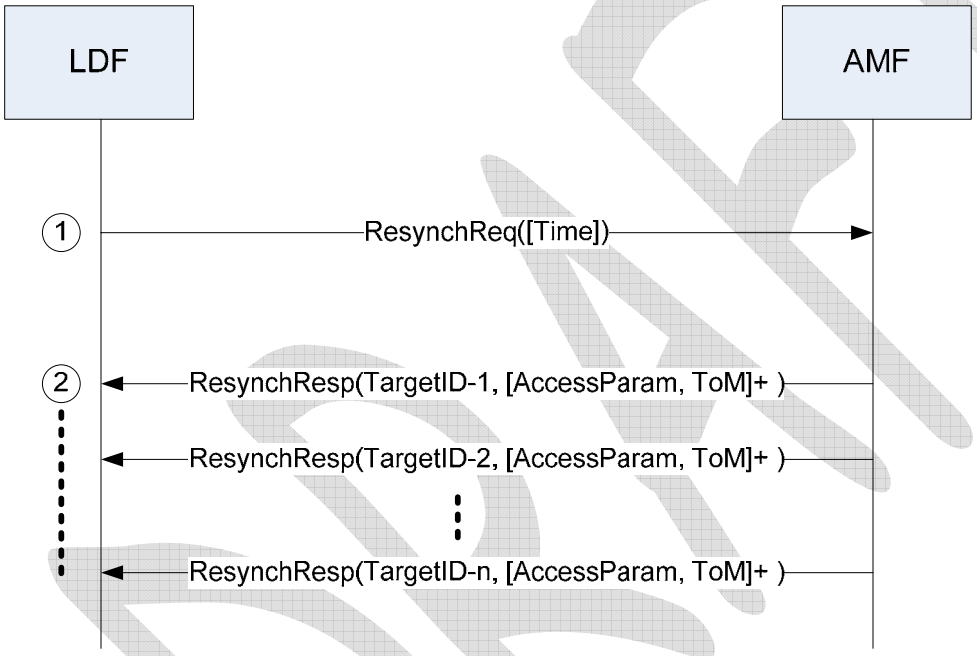

Figure 10 Resynchronization messages

1. The LDF initializes and the AMIF invokes a *ResynchReq* message to the AMF. The *ResynchReq* optionally includes the UTC value of time from which the LDF would like synchronization. That is, if the MCF has data up until a time in UTC, the AMIF may specify that point in time in the *ResynchReq*.
2. The AMF sends a sequence of *ResynchResp* messages with each of the TargetID, and corresponding access parameter values, that are new or have changed value since the nominated time. If the time parameter was not provided in the request all known measurements may be sent. If the AMF does not support the resynchronization service, it sends a cause code indicating this.

14. Data

The key parameters in the FLAP messaging are the TargetID and AccessParam values. These are abstract values defined for the message semantics. The actual components that make up instances of TargetID and AccessParam values depend on the nature of the access network and the AMF instance(s) associated with it.

TargetID and AccessParam become root classes in a hierarchy of derived classes defined for each AMF type. Both root classes are empty. Common derived classes are described in the FLAP specification [ref TBD for the Stage 3 XML schemas].

DRAFT