3GPP TR 23.888 V11.0.0 (2012-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System improvements for Machine-Type Communications (MTC) (Release 11)

Keywords
3GPP, Architecture, Machine-to-machine

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This Technical Report studies and evaluates architectural aspects of the System Improvements for Machine Type Communications requirements specified in TS 22.368 [2].

Specifically, the following system improvements are considered:

- Architectural enhancements to support a large number of Machine-Type Communication (MTC) devices in the network;
- Architectural enhancements to fulfil MTC service requirements;
- Support combinations of architectural enhancements for MTC, though not all combinations may by possible.

The end-to-end aspects of communication between MTC devices and MTC servers (which can be located outside or inside the network operator's domain) are out of the scope of this study. However, the transport services for MTC as provided by the 3GPP system and the related optimizations are considered in this study. In addition, the aspects needed to ensure that MTC devices and/or MTC servers and/or MTC applications do not cause peak loads of short duration (e.g. a "busy minute" rather than a "busy hour") are within the scope of this TR.

Even though some provided solutions may be beneficial for communications from a MTC Device towards another MTC Device, this particular type communication has not been explicitly considered in this Technical Report.

This Technical Report analyzes architectural aspects to achieve these objectives and to gather technical content until it can be included in the relevant technical specifications.

NOTE: Some aspects in this feasibility study have led into normative specification in TS 23.682 [20], TS 23.060 [21], TS 23.401 [5], TS 23.221 [22] and TS 23.272 [23]. The text of the present document was not updated to align with normative specifications.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.368: "Service Requirements for Machine-Type Communications".

[3] NAT Traversal through Tunnelling (NATTT) available at: http://www.cs.arizona.edu/~bzhang/nat/nattt.htm

[4] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based services and Packet Data Networks (PDN)".

[5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[6] 3GPP TS 23.040: "Technical Realization of the Short Message Service (SMS)".

[7] ITU-T Recommendation E.118: "Operation, numbering, routing and mobile service – International operation – General provisions concerning Administrations".

[8] ETSI TS 102 221: "UICC-Terminal interface; Physical and logical characteristics".

[9] 3GPP TS 23.142: "Value-added Services for SMS (VAS4SMS)".

[10] Void.

[11] 3GPP TS 23.251: "Network sharing; Architecture and functional description".

[12] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[13] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3".

[14] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[15] 3GPP TS 23.204: "Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2".

[16] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[17] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[18] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[19] 3GPP TS 29.272: "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[20] 3GPP TS 23.682: "Architecture Enhancements to facilitate communications with Packet Data Networks and Applications".

[21] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[22] 3GPP TS 23.221: "Architectural requirements".

[23] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 22.368 [2], and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

External Identifier: Identifier used from outside the 3GPP system (e.g. at the MTCsp interface), to refer to a UE using a subscription (or the subscription itself e.g. when UE is not registered).

Internal Identifier: Identifier used within the 3GPP system to uniquely identify a UE using a subscription (or the subscription itself e.g. when the UE is not registered). In Rel-11, IMSI is the internal identifier in the 3GPP network for mapping to/from an external identifier.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

MTC Machine Type Communications
M2M Machine-to-Machine

4 Architectural Considerations

4.1 Architectural requirements

Editor's note: Contributions to this clause should follow after agreements are achieved in the Required Functionality clause s of individual Key Issues.

1) The 3GPP Core Network can communicate with the MTC Server. An intermediary entity may be used for the control plane communication for topology hiding or protocol translation purposes. Any intermediary entity for the user plane communication is out of scope of 3GPP standardization.

2) Both mobile terminated and mobile originated communication shall be supported. To initiate mobile terminated communication, an MTC Server shall be able to uniquely identify an MTC Device.

Editor's note: Unique identification of an MTC Device when the UE comprises multiple TEs may imply further requirements.

3) The mobile network shall provide security mechanisms that can be used to:

- ensure that an MTC Server can only communicate with certain UEs used for MTC;

NOTE: This requirement does not imply that it applies to all MTC Server communication to UEs used for MTC. Some scenarios allowing for less restricted communication have been considered.

Editor's note: The association of an MTC Server to certain UEs used for MTC for means of restricting communication (e.g. between an MTC User and the MTC Subscriber) is FFS.

- ensure that only authorized PDN entities can communicate with the UEs used for MTC;

- ensure that a UE used for MTC can only communicate with the MTC Server(s) of its subscriber, and that communication with any other entity is not possible.

The existing 3GPP security functions e.g. authentication and encryption shall be unaffected by the above security measures.

4) It shall be possible to provide secure and encrypted communication between PLMN and MTC Server.

5) The reference points between the MTC Server and the PLMN shall enable message exchange to support the following services:

a. Device Triggering

b. …

6) Architectural enhancements for MTC shall be designed to work in network sharing environments for all sharing configurations described in TS 23.251 [11].

4.1A. Architecture Principles

Editor's note: This clause captures principles that can be agreed in discussion of architecture. Once agreed, these principles will guide further work in the TR.

1) Communication at the application level between the MTC Device and the MTC Application is out of scope of 3GPP standardization.

4.2 Architecture Model

Different models are foreseen for machine type of traffic in what relates to the communication between the MTC Application and the 3GPP network. In a so called Direct Model, the MTC Application communicates with the UE for MTC directly as an over-the-top application on 3GPP network. This is shown as Figure 4.2-1(A).

In a complementary way, several sub models are foreseen for an Indirect model, in which the MTC Application communicates with the UE for MTC by making use of additional services provided by the 3GPP network:

1. The MTC Application would make use of an MTC Server, for additional value added services, provided by a third party Service Provider, that is, outside the 3GPP responsibility. The interface between the MTC server and the MTC application is totally out of the scope of 3GPP. The MTC server communicates with the 3GPP network by means of an interface or set of interfaces. This is shown as Figure 4.2-1(B).

2. The MTC Application makes use of an MTC Server, again for additional value added services, provided by the 3GPP operator (which becomes a Service Provider). The interface between the MTC Server and the MTC application remains still out of the scope of 3GPP, whilst the communication between the MTC server and the 3GPP network becomes internal to the PLMN. This is shown as Figure 4.2-1(C),

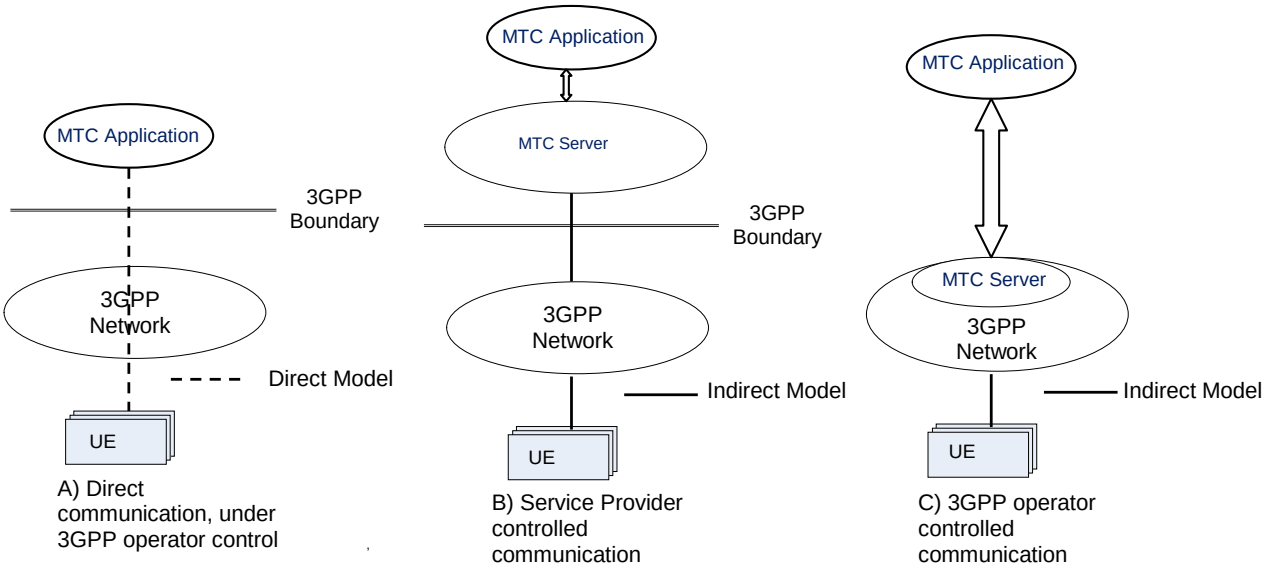


Figure 4.2-1: MTC Application to UE for MTC Communication Models

3 Since the sub models in the indirect scenario are not mutually exclusive but just complementary, it is possible for a 3GPP operator to combine them for different applications. Next figure provides a high level model in which the 3GPP operator provides value added services to an MTC Application and in addition, offers telecom services to a third party Service provider. This is shown as Figure 4.2-2.

The communication between the MTC server and 3GPP network is, as in bullet #1, within the scope of 3GPP, including when that communication becomes internal to the network, as in bullet #2. The communication between the MTC Application and the MTC Server is out of the scope of 3GPP.

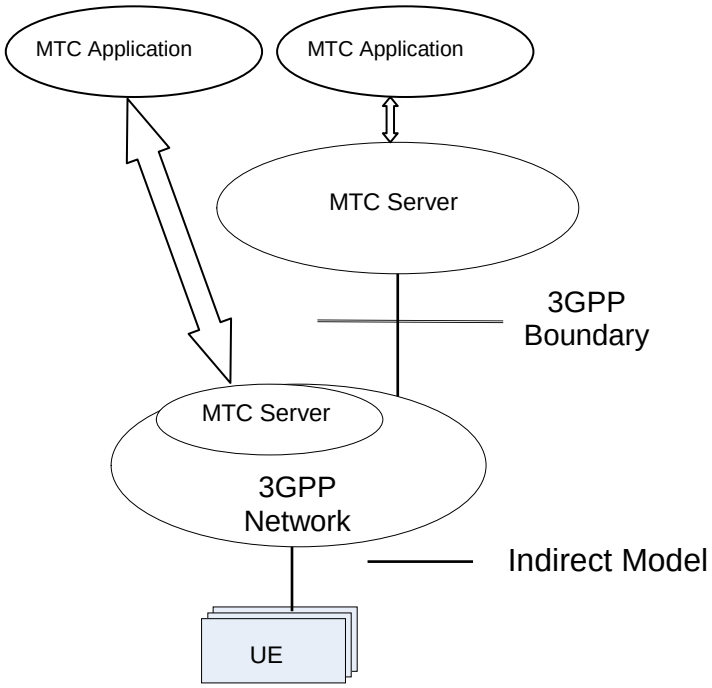


Figure 4.2-2: Multiple MTC Applications using Diverse Communication Models

NOTE: The services provided by the MTC server within the 3GPP network maybe either:

- different from those offered by the external MTC Server;
- the same as those in the external MTC Server;
- a subset/superset of those offered by the external MTC Server;
  - The functionality provided by either MTC Server is out of the scope of this document.
- a subset/superset of those offered by the external MTC Server.
  - The functionality provided by either MTC Server is out of the scope of this document.

4.3 Architectural Reference Model for MTC

The end-to-end application, between the UE used for Machine Type Communication (MTC) and the MTC Application, uses services provided by the 3GPP system, and optionally services provided by an MTC Server. The 3GPP system provides transport and communication services (including 3GPP bearer services, IMS and SMS) including various optimizations that can facilitate MTC.

Figure 4.3-1 shows a UE used for MTC connecting to the 3GPP network (UTRAN, E-UTRAN, GERAN, I-WLAN, etc) via the Um/Uu/LTE-Uu interface. The architecture covers the various architectural models described in Clause 4.2.

- Direct Model - Direct Communication provided by the 3GPP Operator: The MTC Application connects directly to the operator network without the use of any MTC Server;
- Indirect Model - MTC Service Provider controlled communication: The MTC Server is an entity outside of the operator domain. The MTCsp and MTCsms are external interfaces (i.e. to a third party M2M service provider);
- Indirect Model - 3GPP Operator controlled communication: The MTC Server is an entity inside the operator domain. The MTCsp and MTCsms are internal to the PLMN;
- Hybrid Model: The direct and indirect models are used simultaneously in the hybrid model e.g. connecting the user plane using the direct model and doing control plane signalling using the indirect model.

Editor's note: Considerations for hybrid scenarios and for security and scalability for the direct model is FFS.

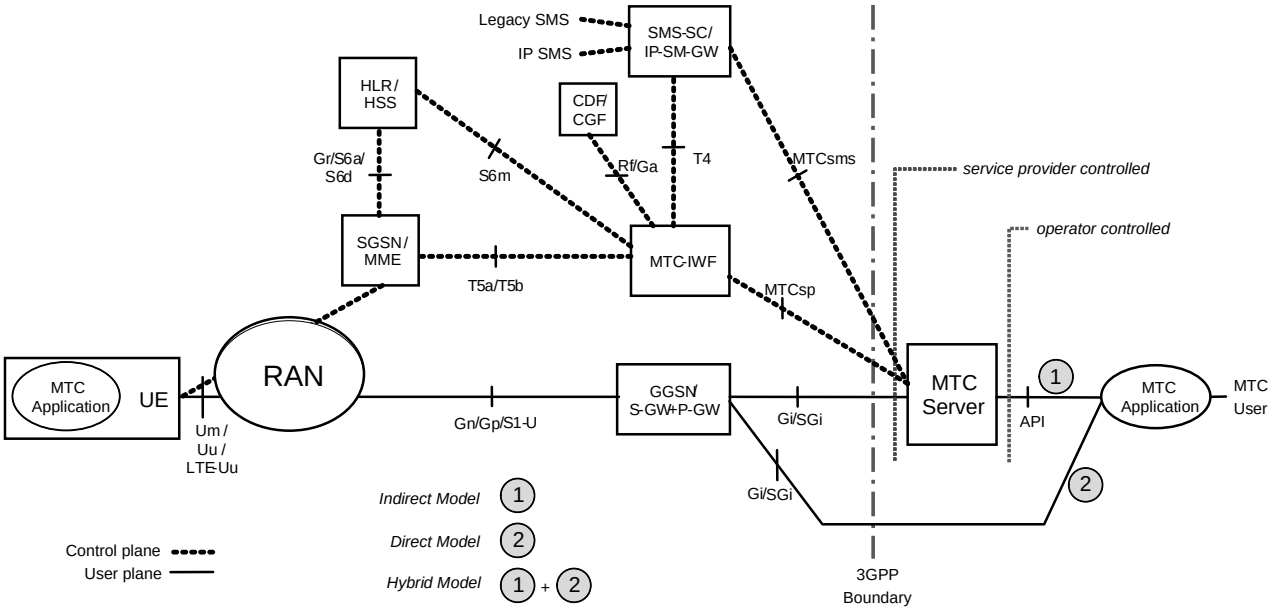


Figure 4.3-1: Non-Roaming Architecture for 3GPP Architecture for Machine-Type Communication

The 'MTC Application' entities and the reference point API in the figure are outside of 3GPP scope. They are solely used as abstracts to show the end-to-end view for MTC and simplify mapping to MTC specifications of other standardization organizations. The MTC Application can be collocated with the MTC Server.

The MTC Server is an entity which connects to the 3GPP network to communicate with UEs used for MTC and nodes in the PLMN.

The 3GPP Architecture supports roaming scenarios in which the UE used for MTC obtains service by means of Um/Uu/LTE-Uu in a VPLMN.

For the roaming UE in the visited network, the MTC-IWF shall have the connection with HSS/HLR and SMS-SC within the home network only and with serving SGSN/MME in the visited network.

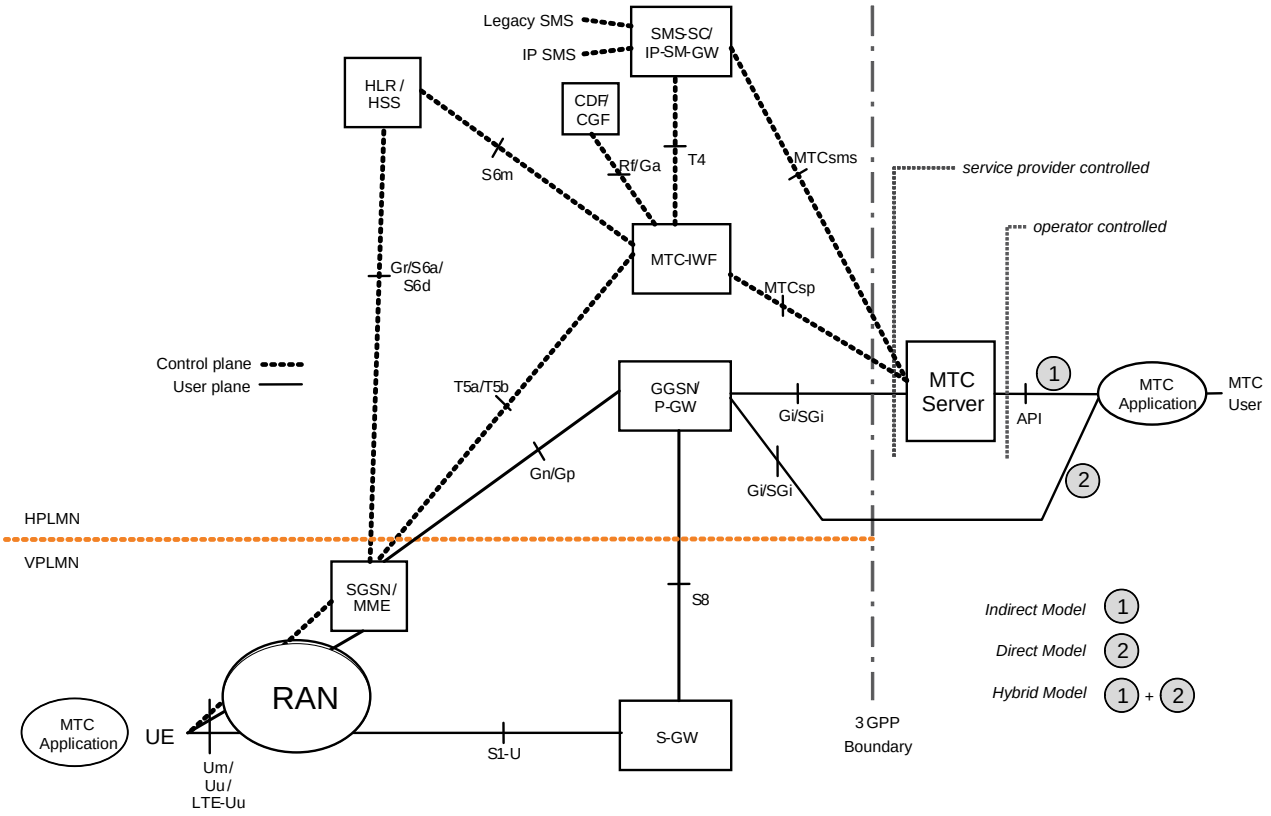


Figure 4.3-2: Roaming Architecture for 3GPP Architecture for Machine-Type Communication for Home Routed scenario

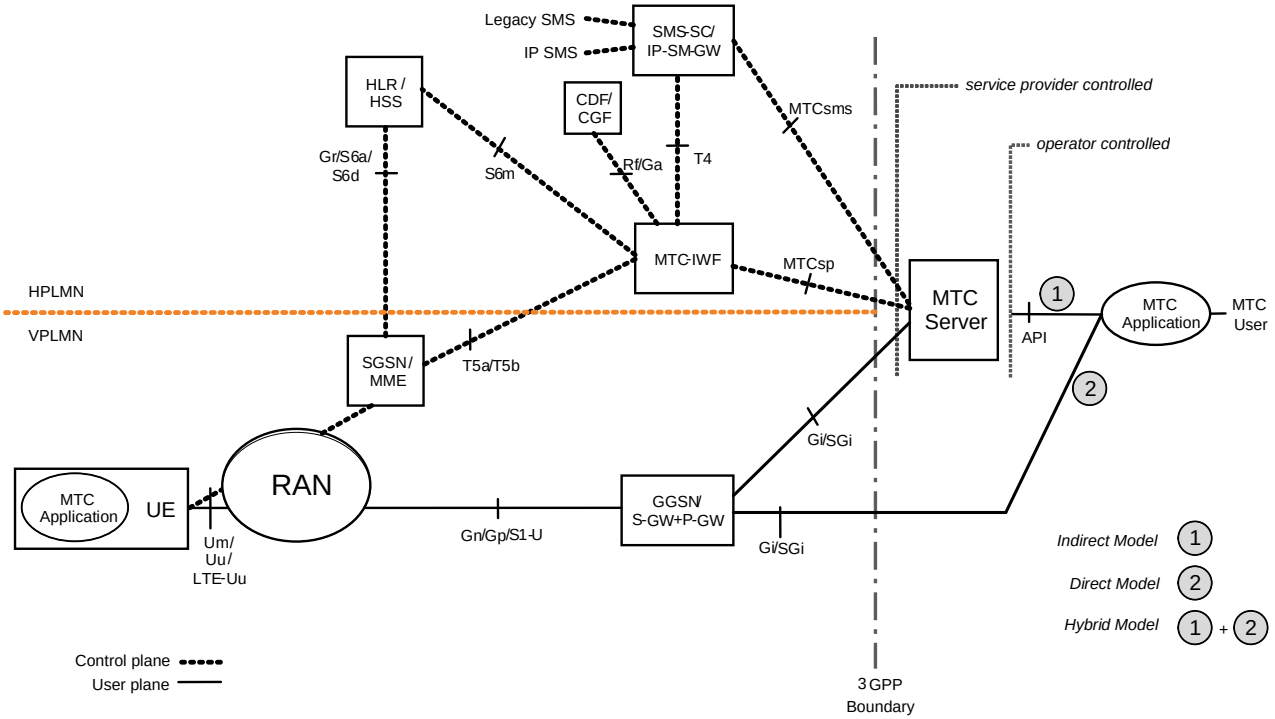


Figure 4.3-3: Roaming Architecture for 3GPP Architecture for Machine-Type Communication for Local Breakout scenario

Editor's note: Constraints on any MTC specific functionality for Local Breakout scenario is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

Editor's note: Any additional entities or interfaces to be added to the MTC architecture figures are FFS and are dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.4 Network Elements

4.4.1 General

The following 3GPP network elements provide functionality to support the Indirect and Hybrid models of MTC. Additionally, IMS network elements may provide functionality to support the Indirect and Hybrid models of MTC.

NOTE: As further development of the MTC architecture takes place as well as when additional MTC common functionality and features are addressed, further network elements may be defined.

Editor's note: The final naming of any new entities added as part of the SIMTC work is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.4.2 MTC-IWF

To support the Indirect and Hybrid models of MTC, one or more instances of an MTC InterWorking Function (MTC-IWF) reside in the HPLMN. An MTC-IWF could be a standalone entity or a functional entity of another network element. The MTC-IWF hides the internal PLMN topology and relays or translates signaling protocols used over MTCsp to invoke specific functionality in the PLMN.

The functionality of the MTC-IWF includes the following:

- terminates the MTCsp , S6m, T5a, T5b, T4 and Rf/Ga reference points;
- may authenticate the MTC Server before communication establishment with the 3GPP network;
- may authorize control plane requests from an MTC Server;
- support the following control plane messaging from an MTC Server:
  - receive device trigger request.
- support the following control plane messaging to an MTC Server:
  - may report device trigger request acknowledgement;
  - device trigger success/failure delivery report;

Editor's note: Additional request messages between the MTC Server and the MTC-IWF are FFS and are dependent on the solutions selected as part of the conclusions reached for SIMTC.

- an HSS resolution mechanism for use when multiple and separately addressable HSSs have been deployed by the network operator (see e.g. the SLF / Diameter Proxy agent specified in clause 5.8 TS 23.228 [14]);
- interrogation of the appropriate HLR/HSS, when needed, to map E.164 MSISDN or external identifier to the IMSI of the associated UE subscription and gather UE reachability information;

Editor's note: The set of UE reachability information utilized for MTC-IWF for device triggering is FFS and is dependent on the solutions selected as part of the conclusions reached for SIMTC.

- selection of the most efficient and effective device trigger delivery mechanism and shielding this detail from MTC Server based on;
  - current reachability information of the UE;
  - the possible device trigger delivery services supported by the HPLMN and, when roaming, VPLMN;
  - the device trigger delivery mechanisms supported by the UE;
  - any MNO device trigger delivery policies; and/or
  - any information received from the MTC Server.

- perform protocol translation, if necessary, and forwarding towards the relevant network entity (i.e. serving SGSN/MME or SMS-SC inside HPLMN domain) of a device trigger request to match the selected trigger delivery mechanism;
- generation of device trigger CDRs and forwarding to CDF/CGF over new instance of Rf/Ga;
- may support secure communications between the 3GPP network and the MTC server.

Editor's note: Solutions for the security related functionality described in the three bullets above are in the scope of SA WG3.

The characteristics of the MTC-IWF includes the following:

- multiple MTC-IWFs can be used with a HPLMN;
- system shall be robust to single MTC-IWF failure.

Editor's note: Additional MTC functionality in the MTC-IWF is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.4.3 HLR/HSS

HLR and HSS specific functionality to support the Indirect and Hybrid models of MTC.

Functionality for triggering includes the following:

- termination of the S6m reference point where MTC-IWFs connect to the HLR/HSS;
- stores and provides the mapping/lookup of E.164 MSISDN or external identifier(s) to IMSI, routing information (i.e. serving MME/SGSN/MSC address), configuration information and UE reachability information to the MTC-IWF.

Editor's note: The specific configuration information used by MTC-IWF for device triggering is FFS and dependent on the final conclusions reached for SIMTC.

Editor's note: Specific MTC functionality in the HLR/HSS is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.4.4 GGSN/PGW

GGSN and PGW specific functionality to support the Indirect and Hybrid models of MTC:

Editor's note: Specific MTC functionality for the GGSN/PGW is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.4.5 SGSN/MME

SGSN and MME specific functionality to support the Indirect and Hybrid models of MTC includes the following:

- SGSN terminates the T5a reference point;
- MME terminates the T5b reference point;
- receives device trigger from MTC-IWF and optionally stores it;
- encapsulates device trigger delivery information in NAS message sent to the UE used for MTC.

Editor's note: Additional MTC functionality for the SGSN/MME is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.5 Reference Points

4.5.1 General

The following 3GPP reference points support the Indirect and Hybrid models of MTC.

NOTE: As further development of the MTC architecture takes place as well as when additional MTC common functionality and features are addressed, further reference points may be added.

4.5.2 List of Reference Points

The description of the MTC related reference points:

MTCsms: It is the reference point an entity outside the 3GPP system uses to communicate with UEs used for MTC via SMS.
MTCsp: It is the reference point an entity outside the 3GPP system uses to communicate with the MTC-IWF related control plane signalling.
T4: Reference point used by MTC-IWF to route device trigger to the SMS-SC in the HPLMN.
T5a: Reference point used between MTC-IWF and serving SGSN.
T5b: Reference point used between MTC-IWF and serving MME.
S6m: Reference point used by MTC-IWF to interrogate HSS/HLR for E.164 MSISDN or external identifier mapping to IMSI and gather UE reachability and configuration information.

Protocol assumption:

- User plane communication with MTC Server, for Indirect and Hybrid models, and MTC Application, for Direct and Hybrid models, is achieved using existing protocols over Gi and SGi reference points. Existing control plane protocols over those reference points such as RADIUS/Diameter as specified in TS 29.061 [4] can also be supported towards the MTC Server.

- S6m may be based on pre-existing protocols e.g. RADIUS/Diameter/MAP.

4.5.3 Reference Point Requirements

4.5.3.1 MTCsp Reference Point Requirements

The MTCsp reference point shall fulfil the following requirements:

- connect a MTC-IWF to one or more MTC Servers;

- supports following services:

  - reception of a device trigger request from MTC Server;

  - may report to the MTC Server the acknowledgement of the device trigger request; and

  - report to the MTC Server the success or failure of a device trigger request.

Editor's note: Additional message exchange support is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

- optional security and privacy protection for communication between the MTC-IWF and MTC Server.

Editor's note: Solutions for the security related functionality described in the above bullet are in the scope of SA WG3.

- Domain Name System procedures similar to what is specified in TS 29.303 [13] may be used by the MTC Server for lookup and selection of which specific MTC-IWF to be used.

- the protocol used on the MTCsp should support repetitions and switching MTC-IWF to ensure operation if one MTC-IWF fails;

- the protocol used on the MTCsp should allow the MTC-IWF and the MTC Server to detect duplicated trigger request and response messages.

Editor's note: Additional MTC reference point requirements are FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.5.3.2 T4 Reference Point Requirements

The T4 reference point shall fulfil the following requirements:

- connect the MTC-IWF to SMS-SC inside HPLMN domain;
- transfer of device trigger,addressed by either an MSISDN or IMSI from MTC-IWF to SMS-SC inside HPLMN domain;
- report back to MTC-IWF the success or failure of delivering a device trigger to UE.

Editor's note: Additional message exchange support is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.5.3.3 T5a/T5b Reference Point Requirements

The T5a/T5b reference point shall fulfil the following requirements:

- T5a connects the MTC-IWF to the serving SGSN;
- T5b connects the MTC-IWF to the serving MME.

Editor's note: The specific requirements of these reference points are FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.5.3.4 S6m Reference Point Requirements

The S6m reference point shall fulfil the following requirements:

- connect the MTC-IWF to HSS/HLR containing UE subscription information;
- support interrogation of HSS/HLR to map external identifier to IMSI and gather UE reachability and configuration information.

Editor's note: Additional message exchange support is FFS and dependent on the solutions selected as part of the conclusions reached for SIMTC.

4.6 High Level Functions

4.6.1 General

The following functions describe the MTC functions performed within this system.

Editor's note: The set of functions for MTC specific logic are FFS and are dependent on the solutions selected as part of the conclusions reached for SIMTC.

NOTE: As further development of the MTC architecture takes place as well as when additional MTC common functionality and features are addressed, further functions may be defined.

4.7 Authorization and Security

Authorization and security measures may be applied to MTC reference points when communication extends beyond the boundary of the 3GPP system.

Editor's note: The authorization and security measures needed are to be studied and specified in SA WG3.

4.8 Protocol Stacks

4.8.1 User plane

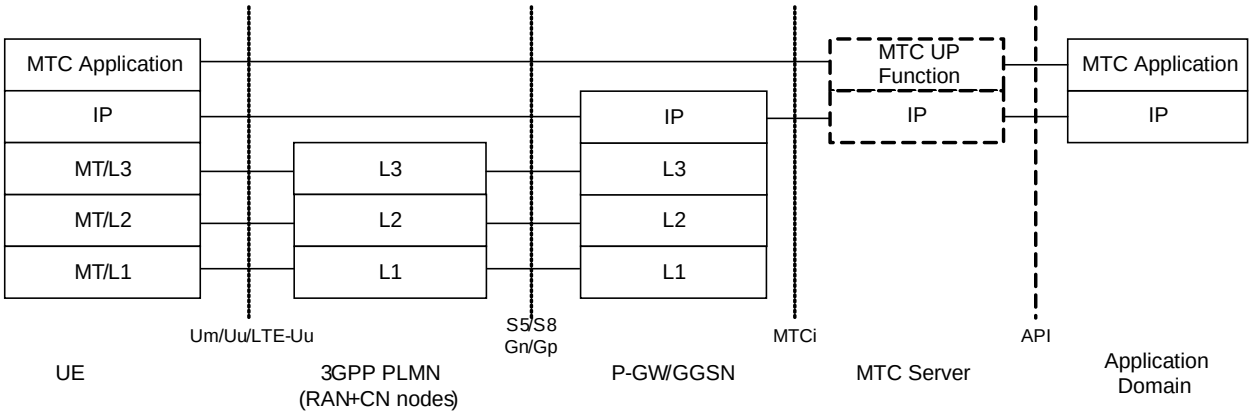


Figure 4.8.1-1: User plane stack for Machine Type Communication architecture

NOTE 1: Both transparent and non-transparent models as defined in TS 29.061 [4] can be used in the connectivity with the PDN where the MTC Server is.

NOTE 2: The internal user plane architecture of the MTC Server is out of scope of 3GPP, the MTC UP Function is optional and is shown for illustration purposes in order to indicate that if such entity exists it resides in the domain of MTC Server.

Editor's note: Impacts on the protocol stack in the internal nodes, when 3GPP UE is acting as a capillary network are FFS.

4.8.2 Control plane

4.8.2.1 MTC Server-MTC-IWF MTCsp reference point

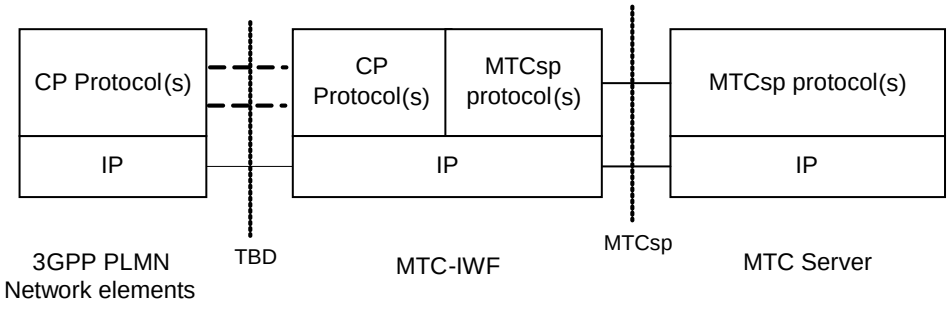


Figure 4.8.2.1-1: MTCsp protocol stack for Machine Type Communication architecture

NOTE 1: The MTCsp reference point can map to a protocol or number of protocols.

Editor's note: Whether the interface between the MTC-IWF and the various 3GPP PLMN Network Elements can map to a number of protocols that may be same or different from the ones used in MTCsp is FFS. In this respect it is also FFS whether the MTC-IWF simply proxies requests from MTC Server or performs protocol translation.

Editor's note: It is FFS whether the protocol stack of MTC-IWF remains the same in case of direct and indirect model as described in section 4.2.

4.8.2.2 MTC Server-SMS SC MTCsms reference point

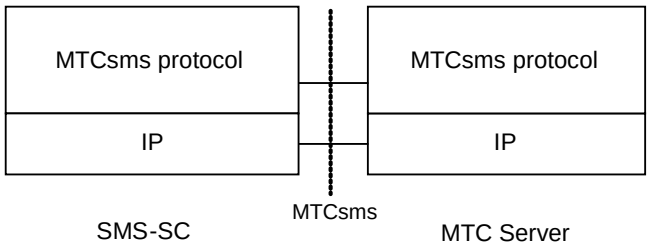


Figure 4.8.2.2-1: MTCsms protocol stack for Machine Type Communication architecture

Editor's note: It is FFS whether MTCsms is within the scope of 3GPP to specify.

5 Description of envisioned System Improvements for Machine Type Communication, use cases

Editor's note: This clause is intended to provide an overview of the alternative architecture fulfilling the requirements. Architecture solutions may apply to all or only some scenarios.

5.1 Key Issue - Group Based Optimization

5.1.1 Use case description

Editor's note: Expand upon the Service Description use case, including technical constraints and interpretations.

MTC Devices can be grouped together for the control, management or charging facilities etc. to meet the need of operators. This optimization may provide easier mode to control/update/charge the MTC devices, in a granularity of group, which may decrease the redundant signalling to avoid congestion. Also the network resource could be saved by using group based optimization when the number of MTC devices is large. The MTC devices within the same group can be in the same area and/or have the same MTC features attributed and/or belong to the same MTC user, which provides the flexibility to allocate a group. Moreover, each of the MTC devices is visible from the network perspective.

Editor's note: Group based optimization may include many optimizations. E.g. group based charging, group based signalling saving etc. It is not clear whether the solutions for these optimizations will be independent to each other or not. Whether this key issue will be split for evaluation is FFS.

5.1.2 Required Functionality

Editor's note: Capture agreements on requirements for solving the key issue. This clause may be omitted if deemed unnecessary.

5.1.3 Evaluation

5.2 Key Issue - MTC Devices communicating with one or more MTC Servers

5.2.1 Use case description

A MTC subscriber may have one or more MTC servers that communicate with the subscriber's MTC devices through the PLMN, which is optimized for machine-type communications. This key issue focuses on the common service requirements as specified in TS 22.368 [2] (e.g. addressing, identifiers, charging, security, etc.) for communication between MTC devices and MTC servers.

5.2.2 Required Functionality

To enable communication between MTC devices and MTC servers the following requirements shall be met:

- It shall be possible to use one or more MTC servers for communicating with the MTC devices of a MTC subscriber.
- The PLMN shall allow transactions between an MTC device and an MTC server, either initiated by the MTC device or the MTC server.
- The PLMN shall be able to authenticate and authorize an MTC device before the device can communicate with an MTC server.
- It shall be possible to uniquely identify an MTC device.
- It shall be possible to uniquely identify an MTC Group i.e. a collection of MTC devices belonging to the same MTC subscriber.

5.3 Key Issue - IP Addressing

5.3.1 Use case description

This key issue focuses on the common service requirements regarding IP addressing as specified in TS 22.368 [2] for communication between UEs used for MTC and MTC servers. The key issue relates to communication in the user plane i.e. the SGi/Gi reference point.

For some MTC Applications, there is a need for the MTC Server to be the initiator of communications between the MTC Server and the UE used for MTC (e.g. due to the need for centralized control).

It is expected in Rel-11 timeframe that the UE used for MTC and the MTC Server are assigned IPv6 addresses, and are thus in the same routable address space (see figure 5.3.1-1). For IPv6 addressing, the number of available IPv6 prefixes is abundant and thus there is no limitation for the IPv6 address space.

When IPv4 addressing is used, the UE used for MTC is normally assigned a private IPv4 address due to the limitation of the public IPv4 address space. The MTC Server may reside in the same private IPv4 address space as the UE, or the MTC Server may reside in public IPv4 address space (see figure 5.3.1-2). In the former case, the UE used for MTC and the MTC Server are in the same routable address space. In the latter case, the UE used for MTC and the MTC Server are located in different non-routable address spaces.

For both IPv4 and IPv6 addressing, the network may employ network topology security techniques that are intended to thwart unauthorized mobile terminated communications over a pre-existing globally routable IP connection. These security techniques are employed by the network operator to address various security goals. These security goals may include, but are not limited to, the desire for end-system privacy (e.g. to prevent device profiling), topology hiding (e.g. to mitigate scanning attacks) and to prevent unauthorized or unwanted communications with the UE used for MTC.

Editor's note: The security solutions that may be needed for MTC are specified by SA WG3.

The following scenarios must be specifically targeted for MTC addressing (the large ovals in the figures depict routable address spaces):

A. The MTC Server and the UE used for MTC are both located in the IPv6 address space. The UE used for MTC is assigned an IP address by the MNO.

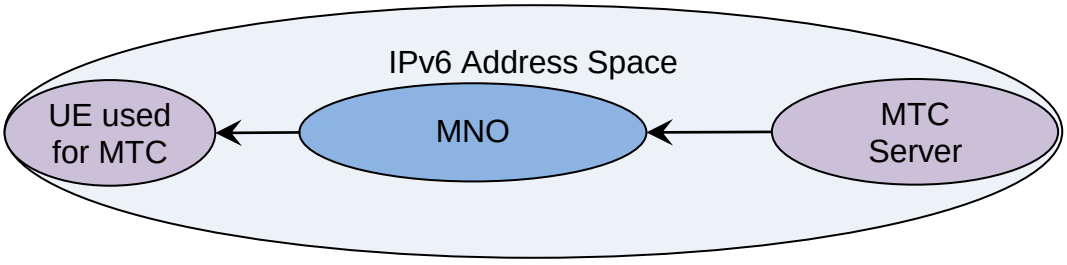


Figure 5.3.1-1: MTC Server and the UE used for MTC in the IPv6 address space

NOTE 1: IPv6 based addressing for both UEs used for MTC and MTC Servers is considered the primary addressing solution and is preferred to ensure future proof and scalable deployments.

NOTE 2: Middleboxes (e.g. firewalls) may be deployed by the MNO in an IPv6 address space to thwart unauthorized mobile terminated communication.

B. The MTC Server is located in a public IPv4 address space. The UE used for MTC is assigned a private IPv4 address from an address pool that is owned and managed by the MNO.

C. The MTC Server is located in a private IPv4 address space. The UE used for MTC is assigned by the MNO a private IPv4 address corresponding to the same IPv4 address space the MTC Server belongs to.

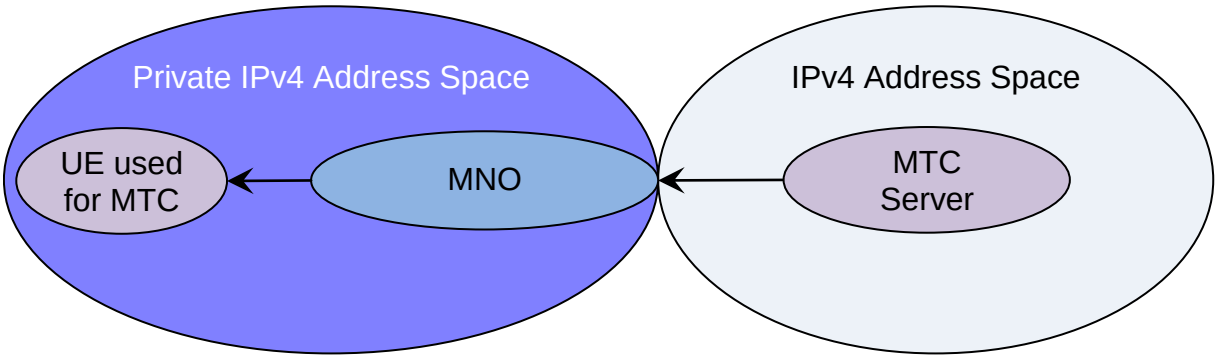


Figure 5.3.1-2: MTC Server in a public or private IPv4 address space, UE used for MTC in a private IPv4 address space

NOTE 3: IPv4 based addressing solutions are considered transition solutions and are deprecated but not precluded.

5.3.2 Required Functionality

The system shall provide communication between the MTC Server and the UE used for MTC in the scenarios described in clause 5.3.1. For any used addressing mechanism:

- The mechanism shall be scalable;
- The mechanism shall minimize the required configuration by the MNO and the MTC User;
- The mechanism shall minimize the required messaging transactions by the MTC Server to initiate MT communications;
- The mechanism shall minimize the messaging sent over the air to the UE used for MTC;
- The mechanism shall minimize any additional user plane latency;
- The mechanism shall minimize any additional security threats to the UE used for MTC.

5.3.3 Evaluation

IPv6 based addressing for both UEs used for MTC and MTC Servers is considered the primary addressing solution and is preferred to ensure future proof and scalable deployments. IPv4 based addressing solutions are considered transition solutions and are deprecated.

Solutions for the Key issue IP addressing have been selected by:

1) focusing on the most important and realistic deployment scenarios as per clause 5.3.1;
2) maximizing the reuse of existing 3GPP standards and minimizing the impact on the 3GPP System;
3) using IPv6 as the primary solution for IP addressing of UEs used for MTC. IPv4 based addressing is deprecated.

NOTE: The scenario where the MTC Server and/or the end-to-end connection between the MTC Server and the mobile operator's domain are pure and only IPv4 is becoming unlikely, especially in Rel-11 timeframe. However an IPv6 capable MTC Server (i.e. dual-stack) in an IPv4 public address space can still be a valid scenario for some years. For such scenarios when there is no end-to-end IPv6 connectivity, well known transition mechanisms can be used. This is considered normal network design and should be transparent to 3GPP specifications. Therefore an MTC Server using IPv6 addressing connected to IPv6 MTC Devices over a public IPv4 address space is considered an IPv6 scenario (i.e. scenario A in clause 5.3.1).

The use of dedicated APNs (clause 6.29.2) with tunnelling towards the MTC Server can be used in all the IP Addressing scenarios and satisfies the above required selection criteria, required functionality and other criteria as outlined in Table x APN Tunnel Evaluation below. It is especially suited when the Indirect model is used. There may be scalability and configuration concerns when the Direct or Hybrid models are used. The solution should be documented as an IPv4 addressing solution, and can also be used as an IPv6 solution to fulfil other requirements such as security.

This approach eliminates any IPv4 Address limitations, allows full use of private IPv4 addressing space and allows overlapping IPv4 address pools. IP address assignment can be handled by the MNO or controlled by the M2M enterprise providing for either static or dynamic addressing assignment.

MT Communication can be initiated by the MTC Server without the need for issuing a request to the 3GPP system to trigger attached MTC devices using the always on model. This is solved by the relaying of RADIUS/Diameter accounting start/stop messages (clause 6.29.3) to provide an indication of the presence and IP address of MTC Device towards MTC Server. For other connection models, like PDP/PDN connections on demand, device trigger requests may be used in together with RADIUS/Diameter updates of MTC Device presence and IP address.

Solution can be achieved with no or minimal standards impacts using existing 3GPP capabilities and VPN techniques (e.g. MPLS VPN, IPSec Tunnel, and other Layer 2 and Layer 3 tunnelling techniques) over Gi/SGi.

Table 5.3.3-1: APN Tunnel Evaluation

Criteria	Solution: Dedicated APN tunnels (i.e. 6.29.2, 6.29.3, 6.29.4)
The mechanism shall be scalable	A GGSN/P-GW can typically support a large number of APNs. Operators may have different policies for usage of dedicated APNs. No IPv4 Addressing limitations. Allows for overlapping and full use of private IPv4 address space. This eliminates scalability constraints also for always-connected scenarios. Some considerations about scalability issues may be needed for events that affect large amounts of the always-on PDN/PDP connections like a need for (re-)balancing due to O&M measures for network nodes or when there is a recovery/restoration. No scalability issues are expected during normal operation when the Indirect model – Operator Controlled (i.e. single dedicated APN/IPSec tunnel per MTC Server and GGSN/PDN-GW combination) is used. When the Direct, Indirect model – Service Provider Controlled and Hybrid models are used, scalability will be an issue when there are multiple MTC Applications communicating with UEs directly (requiring dedicated APN/VPN tunnel per MTC Application and GGSN/PGW combinations) or indirectly via the MTC Server (i.e. problem of public IP address resolution for addressing by MTC Application pushed from mobile network onto MTC Server). When the Indirect model – Service Provider Controlled are used, it is FFS if scalability will be an issue when a MTC Server is communicating with a set of UEs whose subscriptions are spread across multiple MNOs
The mechanism shall minimize the required configuration by the MNO and the MTC User;	IPSec tunnel with IKE (Internet key Exchange) can be used for dynamic setting of IPSec Security associations minimizing configuration by operator. UE needs APN configuration. Dedicated APN configuration required per APN and MTC Server or MTC Application. When a high numbers of VPN tunnels are required per MTC Server this will cause significant configuration burden for MTC Server. For Hybrid model, when a high number of VPN tunnels are required per MTC Application, this will cause significant configuration burden for MTC Applications.
The mechanism shall minimize the required messaging transactions by the MTC Server to initiate MT communications;	With always on support no additional message transactions required for MT terminated communication, besides perhaps for some specific situations where triggering may be used e.g. to recover the (always-on) PDP/PDN connection from error cases or to set triggers for devices that are out of coverage. MTC Server can be aware of presence of MTC device and assigned Private IP address as described using techniques as described in 6.29.3 and 6.29.4 For PDP/PDN connections not using always on, triggering should be used similar to any non-always-on solution. Triggering may also be used e.g. to recover the PDP/PDN connection from error cases or to set triggers for devices that are out of coverage.
The mechanism shall minimize the messaging sent over the air to the MTC Device;	For the always-on model there is no new signalling induced or alternate communication channels (e.g. SMS) for delivery of a "push" stimulus to an attached MTC device with an established PDN connection is required. For PDP/PDN connections not using always on, triggering should be used similar to any non-always-on solution.
The mechanism shall minimize any additional user plane latency;	For the always-on model there is no change to user plane latency in core network and radio interface.
The mechanism shall minimize any additional security threats to the MTC Device	Traffic Separation achieved with IPSec tunnel. Additional security provided with dedicated APNs. Only MT communication originating from the MTC server or emanating from the MTC enterprise network can be initiated towards MTC device. Similar level of security provided as per existing 3GPP deployments providing corporate access to corporate APNs
Direct Model - Direct Communication provided by the 3GPP Operator: The M2M Application connects directly to the operator network without the use of any MTC Server;	Supported Instead of terminating in the MTC Server, the tunnel could terminate into another node (IPSec GW) with Public IP interface in the MTC enterprise network. Otherwise, there will be scalability issue (see scalability criteria above).
Indirect Model – MTC Service Provider controlled communication: The MTC Server is an entity outside of the operator domain.	Supported with traffic separation over public Internet e.g. using IPSec tunnel. Tunnel terminated at the MTC Server. When MTC Server communicates with multiple HPLMNs, there will be scalability issues (see scalability criteria above).
Indirect Model – 3GPP Operator controlled communication: The MTC	Tunnelling within operators domain towards MTC Server can be achieved with other existing VPN techniques such as MPLS VPN

Criteria	Solution: Dedicated APN tunnels (i.e. 6.29.2, 6.29.3, 6.29.4)
Server is an entity inside the operator domain	
Hybrid model	Supported with traffic separation over public Internet e.g. using IPSec tunnel. Tunnel terminated at the MTC Application. There may be a scalability issue (see scalability criteria above).
MTC Server Complexity	MTC Server could serve as tunnel endpoint as IPSec/IKE supported by common OS (e.g. Linux/FreeBSD). Alternately the MTC enterprise network tunnel endpoint could be served by readily available infrastructure (IPSec GW) instead of MTC Server. Dedicated APN configuration requirements and public IP address resolution burden (see scalability criteria above).
Impacts to Standards	For the always-on model there is none. Reuse of existing 3GPP features (e.g. dedicated APNs, Private IPv4 addressing, Traffic Separation over Gi/SGi using well known VPN techniques (e.g. IPSec Tunnel, MPLS VPN), Radius/Diameter accounting to relay presence of and IP address of MTC Device towards MTC Server
Support for roaming	Roaming is supported via HPLMN. Not suitable for local breakout scenarios.
Deployment solutions	Various solutions based on dedicated APN and tunnelling exists today for the enterprise domain.
Terminal complexity	If the MTC Device needs to have simultaneous access to MTC Servers associated with different APNs, the solution requires that the MTC device support multiple PDN connections (i.e. multiple IP addresses)
Added complexity to the 3GPP network elements	Uses existing function in the existing 3GPP system.
Dependency on other SDOs before the solution is deployable	None.

5.4 Key Issue - Small Data Transmission

5.4.1 Use case description

Editor's note: Expand upon the Service Description use case, including technical constraints and interpretations.

MTC Devices with Small Data Transmission send or receive only small amounts of data. The exact amount that is considered to be small may differ per individual system improvement proposal. It is the amount of data where a specific system improvement proposal still provides its benefits.

For online small data transmission it is assumed that data transfer can happen any time when needed by the application. Before the transmission of the small data, the MTC device may be attached to or detached from the network.

5.4.2 Required Functionality

Editor's note: Capture agreements on requirements for solving the key issue. This clause may be omitted if deemed unnecessary.

The following functionalities are required for Small Data Transmission:

- It shall be possible to transmit small amounts of data with very efficient resource.
- Before transmission of small amount of data, the MTC Device may be attached or detached to/from the network.
- The definition of a small amount of data shall be configurable per subscription or by network operator policy.

Editor's note: Considerations for solutions should include the small data upper limit that the solution is suitable for.

Editor's note: Considerations for solutions should include the frequency of small data transmissions that the solution is suitable for.

Editor's note: Considerations for solutions should include support for mobility management or retransmission of lost data.

Editor's note: Need to determine charging requirements.

Editor's note: Need to determine subscription aspects related to small amount data transmission.

5.4.3 Evaluation

5.5 Void

5.6 Key Issue - Low Mobility

5.6.1 Use case description

Editor's note: Expand upon the Service Description use case, including technical constraints and interpretations.

For MTC Device with low mobility, several use cases should be captured in this TR as follows:

- not move frequently and may move only within small area: e.g. health monitoring at home.
- not move frequently but may move within wide area: e.g. mobile sales terminals.
- not move normally, i.e. with fixed location: e.g. water metering.

For this kind of MTC Device, it is studied how to reduce the frequency of mobility management procedures and how to optimize the paging.

5.6.2 Required Functionality

The required functionality for low mobility should result in:

- reduction in resource usage for low mobility MTC Devices (e.g. paging, location management signalling, mobility context in MME/SGSN/MSC)

5.6.3 Evaluation

5.7 Key Issue - MTC Subscriptions

5.7.1 Use case description

Based on stage1 requirements, MTC Features are subscribed and controlled by subscription.

Any usage of the subscribed MTC features is activated by default at the time of the subscribing the feature.

It should be possible to allow the MTC Subscribers to activate the unsubscribed MTC Features or deactivate the subscribed MTC Features based on the operator policy. The mechanisms used for activation/deactivation are outside the scope of 3GPP. The MTC solution shall make it possible to provision the home PLMN with MTC subscriptions and allow one or more MTC Devices to share this subscription. This key issue aims at specifying the architectural requirements related to MTC subscriptions as well as the relationship between MTC subscriptions, MTC Devices and MTC architecture enhancements.

5.7.2 Required Functionality

MTC Features are controlled by subscription in HSS.

NOTE: MTC Features should be subscribed by already existing methods; It is normally out of scope of 3GPP standardisation e.g. via the provisioning interface or via a web interface.

The capability to subscribe/unsubscribe MTC Features is provided to the MTC Subscriber. The subscription information (i.e. MTC Feature is subscribed) of the MTC Feature shall be stored in the relevant 3GPP CN entities.

It is also possible for a network operator to restrict incompatible MTC Feature subscription (according to network operator policy.) During the activation/deactivation, if the MTC Subscriber request results in a set of incompatible MTC Features (according to network operator policy), it shall be possible for the operator to reject the request.

Upon attachment or subscription update, it shall be possible for the SGSN/MME to support only a subset of the subscribed MTC features based on network capability and/or MTC device capability.

Editor's note: It is FFS how the device capability can be known to the network.

Editor's note: It is FFS, if MTC feature(s) may be designated as "essential". In which case, the MME/SGSN informs the MTC device and detaches the device when the MTC Features cannot be supported.

A feature is considered as essential if a MTC device cannot operate normally when the feature is not enabled.

A feature is considered as mandatory when the home operator forbids attachment to the network when this feature is not/cannot be enabled.

Editor's note: Upon attachment or subscription update when the MTC device is in roaming, it may be possible for the visited network operator to inform the home operator of the features are not supported.

It may be possible for the network operator to inform the MTC Device enabled/disabled status of the MTC features.

Editor's note: It is FFS which MTC features' enabled status may be notified to the MTC device.

The following requirements are relevant to MTC subscriptions:

- It shall be possible to provision the home PLMN with MTC Subscriptions, each one shared by one or more MTC Devices.
- Each MTC Device shall be associated to one MTC subscription and shall have a device subscription including the security credentials used to authenticate the device.
- An MTC subscription shall indicate MTC Features that are subscribed by the MTC Devices sharing this subscription.
- It shall be possible for all MTC Devices sharing the same MTC subscription to use all subscribed MTC Features belonging to this subscription.

Editor's note: As it is assumed that subscribed MTC Features are activated whenever supported by the network, the above requirement may be redundant.

5.8 Key Issue - MTC Device Trigger

5.8.1 Use case description

For many M2M applications there may be an interest to have poll model for communications between MTC devices and the MTC Server. This may be because the MTC User wants to be in control of communication from MTC Devices, and does not allow MTC Devices to randomly access the MTC Server. Also for applications where normally the MTC Devices initiate communications, there may occasionally be a need for the MTC Server to poll data from MTC devices.

If an MTC Server has an IP address available for the device it needs to poll data from, it tries to communicate with the device using the IP address. If the communications fails, or if no IP address is available for the device, the MTC Server can use the MTC Device Trigger to try to establish the communication. This may cause a PDP/PDN connection to be established if it didn't exist or re-established if it wasn't working e.g. after an error condition in the network. It is important that it can be guaranteed to the MTC User that MTC Devices can only be triggered by authorized MTC Servers. If the network is not able to trigger the MTC Device, e.g. due to network congestion, the network may report the trigger failure to the MTC Server. The MTC Device Trigger is a service provided by the 3GPP system for the MTC server over control plane signalling.

Triggering of MTC Devices is based on the use of an identifier identifying the MTC Device that needs to be triggered. The identifier used by the MTC User in the triggering request to the MTC Server can be different from the identifier used by the MTC Server in the triggering request to the PLMN network.

5.8.2 Required Functionality

The following functionality is required to trigger MTC Devices:

- The PLMN shall be able to trigger MTC Devices to initiate communication with the MTC Server based on a trigger indication from the MTC server.
  - The network shall provide a mechanism such that the MTC Device can only receive trigger indications from authorized MTC Servers.
  - Upon receiving a trigger indication from a source that is not an authorised MTC Server, the network shall be able to provide the details of the source (e.g. address) to the MTC User.
  - The network shall provide a mechanism to the MTC User to provide a set of authorized MTC Server(s).
  - The trigger mechanism shall be able to provide a scalable transmission of trigger request and trigger response messages for multiple MTC Devices in the PLMN and on the interfaces to the MTC Server.
  - The main characteristic of the device trigger feature is the *control plane* interaction between the MTC Server and the 3GPP system that initiates all necessary functions or procedures within the 3GPP system and towards the MTC Server to enable the MTC Server to send user plane data towards the MTC Device. Any triggering activity on MTC application level, which results in traffic being transferred by the 3GPP system transparently as user plane data, is not considered as device trigger (feature).
- A MTC Device shall be able to receive trigger indications from the network and establish communication with the MTC server when receiving the trigger indication. Possible options are:
  - Receiving trigger indication in detached state and establish communication.
  - Receiving trigger indication in attached state and the MTC device has no PDP/PDN connection.
  - Receiving trigger indication in attached state and the MTC device has a PDP/PDN connection.

NOTE 1: There are currently available solutions to trigger MTC Devices (e.g. unanswered CS call attempts, sending an SMS). However, these have disadvantage when used at a large scale (e.g. they are based on MSISDNs), and work only for attached MTC Devices. This key issue will investigate possible improvements over the currently available means for triggering.

NOTE 2: In reference to the three sub-bullets above (beginning with "*Receiving trigger indication in…*"), the trigger indication denotes a control plane indication specific to the MTC Device Trigger feature, including the case of the MTC device having a PDP/PDN connection. Reasons for recurring to device triggering in the latter case are e.g. when the MTC Server does not know the IP address assigned to the MTC Device, or when the MTC device does not respond after using MT IP communication e.g. due to network problems or that the IP address has become obsolete, or when the MTC device is not user plane reachable by a MTC Server over the currently established PDP/PDN connections, or because of other reasons where user plane communication needs to be initiated from the MTC device side.

- A HPLMN supporting the MTC device trigger feature shall provide an interface for reception of a trigger indication into the PLMN in order to be delivered by the network to the addressed MTC device. This MTCsp interface:
  - shall be globally consistent (i.e. the same) across PLMNs supporting the MTC device trigger feature.
  - shall not require the MTC server to have prior knowledge of the current reachability state (e.g. attachment and PDP context/PDN connection states) of the targeted MTC device.
  - shall allow for providing a validity or life time that indicates how long the network should store the trigger request when it cannot be delivered to the UE, e.g. when the UE is not reachable or when load control prevents immediate delivery
  - PLMNs supporting the MTC device trigger feature shall be able to collect appropriate CDRs for each trigger delivered to a UE.

NOTE 3: This interface does not preclude an MTC server from interrogating/monitoring the network for the current reachability state of a MTC device.

NOTE 4: For backwards compatibility reasons, this interface does not preclude a MTC server from using a pre-existing interface (e.g. submitting an SMS-based trigger indication directly to an SMS-SC). However, the intention would be for MTC service providers to migrate towards utilizing this new interface for device triggering.

- The network shall be able to report the success or failure of the trigger (e.g. due to network congestion) to the MTC server, if so requested by the MTC Server.

- It shall be possible to provide a load control mechanism for the trigger requests, e.g. controlling the ingress rate of triggers from a specific MTC server at the MTC-IWF or the aggregate ingress rate from all MTC servers at the MTC-IWF or by some other means to reduce the load on the network.

- NAS level congestion control assumes that the network will not trigger the UE as long as the particular congestion situation remains. Trigger load control mechanisms shall ensure that the network congestion is not exacerbated by UEs that respond to triggers.

Editor's note: It is FFS how existing or new congestion control mechanism works with the selected triggering solution to control trigger requests.

- In the triggering request to the PLMN the MTC Server shall use an external identifier to indicate the UE used for MTC that is required to be triggered.

NOTE 5: The identifier used by the MTC User in the triggering request to the MTC Server can be a different identifier than the one used by the MTC Server in the triggering request to the PLMN. The identifier used by the MTC User is out of scope of 3GPP standardisation and may e.g. be an application specific identifier.

5.8.3 Evaluation

5.8.3.1 Comparison of the MTC Device Trigger solutions

Evaluation characteristic → Solution ↴	***Impact on existing system and UE***	***Possibility to trigger device without MSISDN***	***Possibility to trigger device without CS subscription***	***Possibility to trigger device behind a middle box (NAT/firewall)***	***Load on CS nodes***	***Complexity (incl. issues like need for new entities)***	***Efficiency***	***Migration (incl. issues like roaming or interoperation with legacy, MSISDN-less, PS only, triggering when device becomes reachable)***	***Comment (specific issues not covered by other columns)***
6.6 Solution - Triggering of non-attached MTC Devices based on location information provided by MTC User									
6.39 Solution – Triggering MTC devices via HSS and NAS signalling									
6.41 Solution – Triggering of attached MTC Devices by reusing Network Requested PDP Context Activation procedure									
6.42 Solution - Triggering of attached MTC Device via Pre rel-11 SMS									
6.43 Solution - Triggering of attached MTC Device via intermediate node									
6.44 Solution – Device Triggering reuse of MT SMS WAP Push									
6.45 Solution									

– Device trigger gateway solution									

5.8.3.2 Delivery of device trigger information from 3GPP system to UE

When it is possible for an MTC device to receive MT-SMS (e.g., currently over E-UTRAN requires a CS or IMS subscription) and to be associated with an individual MSISDN, for reasons of minimizing impact on the existing system, keeping complexity low and facilitating migration from triggering solutions used today, an MT-SMS based solution shall be supported for delivering trigger information from 3GPP system to the device. This would also allow roaming in other PLMNs without any upgrade in the visited network.

A 3GPP network may support more than one trigger delivery methods, e.g. a pre-Rel-11 SMS delivery without any system enhancements and another trigger delivery method to cope with different capability and deployment conditions, e.g. for triggering an MTC device to which no E.164-MSISDN is assigned.

Editor's note: Whether any additional trigger delivery mechanisms are to be supported in Rel-11 is FFS.

5.8.3.3 Submission of device trigger requests from MTC server to 3GPP system

The 3GPP network shall support standardized control signalling between the MTC Server and the 3GPP system via the MTCsp reference point for submission of the device trigger requests. The MTCsp is provided by an MTC-IWF.

In order to provide an automated, reliable and scalable mechanism for an MTC Server to determine the address/route of the assigned MTC-IWF(s) for a UE used for MTC to be triggered, e.g. DNS resolution of the address of assigned MTC-IWF for each UE used for MTC that can be triggered over MTCsp shall be supported.

The MTC-IWF performs PLMN related control functionality such as MTC Server authentication, trigger request authorization and charging, and shields the MTC Server from the actual trigger delivery mechanism used within the PLMN.

The protocol used from the MTC Server for submitting device trigger requests to the 3GPP system (and subsequent protocols within the PLMN) should support an option where the UE can be identified without the use of an E.164-MSISDN.

MTCsp shall always be provided by the HPLMN and the MTC-IWF will only accept a device trigger for a UE subscribed with the HPLMN. This removes the need for the MTC-IWF in the VPLMN to map the external identifier and forward the trigger request to the HPLMN of a roaming device.

Additionally, the 3GPP network shall support control signalling between the MTC Server and the 3GPP system via the MTCsms reference point for submission of the device trigger requests as part of user data of a MT-SMS. The MTCsms is provided by an SMS-SC.

5.8.3.4 3GPP system internal handling of device triggers

The protocols within the PLMN should support an option where the UE can be identified without the use of an E.164-MSISDN. A PLMN may support delivery of MT-SMS with an IMSI as destination address instead of an E.164-MSISDN. However, in order to avoid exposure of IMSI outside the MNO domain, this shall only be allowed for SMEs located in the MNO domain.

The MTC-IWF interrogates HLR/HSS, when needed, to map external identifier to IMSI and gather UE reachability and configuration information, selects the trigger delivery mechanism and performs protocol translation if necessary, e.g. to reformat the triggered request to match the selected trigger delivery method, and routes the request towards the relevant network entity. Validity time is used for the delivery of device trigger requests to the UE.

Synergies might be possible with MTC Small data transmission where MT-SMS or other trigger delivery services are also a candidate for small data transmission.

Editor's note: The MT-SMS should be further detailed, including how E.164-MSISDN-less operation is done. This detailing may include both the existing MT-SMS and possible future evolutions.

5.9 Key Issue –Time Controlled

5.9.1 Use case description

MTC Devices with Time Controlled MTC Feature send / receive data only at certain pre-defined time periods. Network operators can pre-define / alter the time period based on criteria (e.g. daily traffic load) and only allow MTC Devices to access the network (attach to the network or send / receive data) during the pre-defined time period. The key issue aims at describing how to restrict MTC Device's access to the network and avoid unnecessary network load outside these pre-defined time periods. The home network operator may restrict altering the time period by the visited network operator e.g. to avoid traffic when the MTC server is in maintenance by means of a 'forbidden time interval.' During this forbidden interval, the network shall reject access requests per MTC Device. This allows for maintenance, e.g. of the MTC Server.

Editor's note: The interaction of PAM and Time Control are FFS.

Typically, an MTC User agrees with an operator on a predefined time period for a group of MTC Devices. The time in which access is permitted is termed a 'grant time interval.' The network shall communicate the (altered) grant time interval to the MTC Device and may also do so to the MTC Server and MTC User. A 'grant time interval' does not overlap with a 'forbidden time interval.'

In roaming scenarios, the local network operator may alter the access grant time interval based on local criteria, e.g. (daily traffic load, time zones) but the forbidden time interval may not be altered.

It is desirable that access of MTC Devices with the same access grant interval is distributed across this interval in a manner to reduce peaks in the signalling and data traffic.

For many applications, individual MTC Devices do not need the total duration of this predefined time period to communicate with the MTC Server. Typically a 5-10 minutes communication window is sufficient for an individual MTC Device. The network operator may limit the duration of these communication windows. To avoid network overload, signalling and data traffic the communication windows of the devices shall be distributed over the pre-defined time period e.g. through randomization of the start time of the individual communication windows. For a network operator, it can be beneficial that the MTC Devices are not attached outside their communication window. Therefore, the network operator should be able to enforce detach of an MTC Device from the network at the end of the communication window of a device.

The network operator may allow MTC Devices to exchange signalling and send and receive data outside of defined time intervals but charge differently for such traffic.

Time Control terminology is illustrated in Figure 5.9.1-1.

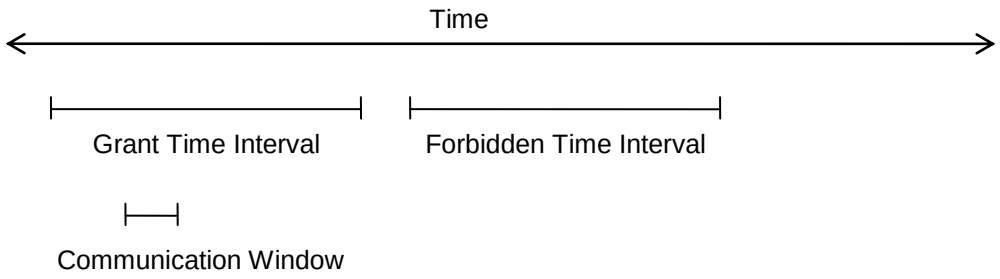


Figure 5.9.1-1: Time Control Terminology

NOTE: The Communication Window can be expressed as a start and stop time, a start time and duration, an offset from the beginning of the Grant Time Interval and a duration, etc dependent on the solution.

The MTC Device may defer access of the network until it will originate communication, provided that the MTC Device's upper layers do not require reception of mobile terminated communication during the period of time the MTC Device remains Detached.

5.9.2 Required Functionality

The following requirements can be derived from the Time Controlled MTC feature requirements specified in TS 22.368 [2]:

- the network operator shall be able to allocate for a group of MTC devices time periods during which signalling or user plane traffic to/from the network is allowed. This is termed 'grant time interval';
- the network operator shall be able to further restrict the time during which signalling or user plane traffic to/from the network is allowed for individual MTC devices in the group to a time window with a defined duration;
- the network shall be able to inform the MTC Device of the (altered) time periods during which signalling or user plane traffic to/from the network is allowed. The network may communicate the (altered) time periods to the MTC Server or MTC User;
- enforcement of a detach of an MTC Device from the network at the end of the of the Device's communication window shall be supported;
- roaming shall be supported for MTC devices with Time Controlled Feature. The local network operator (in roaming scenarios) may alter the grant time interval based on local criteria;
- the network shall be able to alter above time periods;
- the network operator shall be able to allocate for a group of MTC devices a time period during which signalling or user plane traffic to/from the network is disallowed. This is termed 'forbidden time interval.' A forbidden time interval and a grant time interval shall not overlap. The forbidden interval shall not be altered. The home network operator or MTC User use the 'forbidden interval' to restrict the extent to which change of the time periods is allowed by the (visited) network operator (e.g. to avoid traffic when the MTC server is in maintenance);
- peaks in traffic (including signalling traffic) shall be avoided (e.g. by randomization of the time during which the MTC Devices communicate.).

NOTE: It is possible for the network operator to allow or reject the MTC device's access to the network according to the operator policy, when it is out of time period.

5.9.3 Evaluation

5.10 Key Issue - MTC Monitoring

5.10.1 Use case description

MTC Devices may be deployed in locations with high risk, e.g. possibility of vandalism or theft of the communication module. For those MTC Devices, it is desirable that the network detects and reports events (including location) caused by those devices that may result, for example, from vandalism or theft of the communication module. If such an event is detected, the network might be configured to perform special actions, e.g. limit the access or reduce the allocated resource.

5.10.2 Required Functionality

The following functionalities are required for MTC monitoring:

- It shall be possible for the MTC User to configure the monitoring events, e.g. monitoring the association of the MTC Device and UICC, misalignment of the MTC feature, change in the point of attachment, loss of connectivity.
- The MTC User shall configure the action to be executed by the network.
- It shall be possible for the network to detect monitoring events.
- It shall be possible for the network to report the detected events to the MTC User or the appropriate MTC Server and optionally to perform action to reduce services provided to the MTC Device.

- It shall be possible to configure the maximum time between the actual loss of connectivity and its detection in the MTC subscription. The maximum detection time can be in the order of 1 minute to 1 hour.

5.11 Key Issue - Decoupling MTC Server from 3GPP Architecture

5.11.1 Use Case Description

Machine to machine communications exist today, over a variety of access systems. These essentially make use of particular features exposed by individual access systems, devices and aggregation services to build a unique 'vertical system' to support an application for an end customer. Examples include logistics, point of sale and power metering.

The current direction of the industry is to eventually provide general service interfaces to enable a new class of 'layered' applications that can work with diverse MTC devices, network operators, accesses and diverse business logic components without requiring a unique 'from scratch' system integration effort.

The current abstraction shown in the SA1 service aspects specification TS 22.368 [2] represents the MTC server as an entity with which the 3GPP PLMN and the MTC Device directly communicate. This depicts a service delivery representation well, but has very misleading implications if accepted as a basis for the MTC architecture,

Two potential deployment scenarios exist for MTC Services – either under the control of a mobile network operator or by a third party.

To support MTC services deployed by third parties, it is assumed that additional interaction between MTC service logic components and the 3GPP PLMN are required, beyond data communications (SMS and packet domain communication.), These interactions include at least the ability for service logic components to securely interact with the 3GPP PLMN and the ability for the service logic components to obtain certain information regarding MTC Subscriptions and modifying this information (if allowed by the network operator).

Some service logic components only interact with MTC Devices by means of established user plane communication (e.g. SMS or TCP/IP based applications). These service logic components may have no direct means to interact with or become aware of MTC Features. For example, there are existing M2M applications that employ GPRS and/or SMS to communicate with MTC Devices. For such service logic components, no additional mediating interfaces as proposed in this key issue shall be required.

A 3GPP MNO can restrict or deliberately allow access to information, resources and services in the core network by means of the Service Abstraction Layer.

5.11.2 Required Functionality

MTC Service Logic components may be deployed within a mobile network operator's control or externally.

The Baseline Architecture in clause 4.3 shall be updated with additional interfaces for secure communications between MTC Service Logic Components and the 3GPP PLMN as well as for MTC Service Logic Components to query or possibly update MTC subscription information.

It is desirable to minimize the requirements for MTC Service Logic components to support 3GPP interfaces and 3GPP-specific configuration. This facilitates the design of MTC services that function over multiple access systems.

5.12 Key Issue - Signalling Congestion Control

5.12.1 Use Case Description

MTC related signalling congestion and overload is an urgent issue that network operators are currently facing. Not only network operators that are providing MTC services, but also network operators in which MTC Devices are roaming can be affected by MTC related signalling congestion and overload.

MTC related signalling congestion and overload can be caused by:

- a malfunctioning in the MTC application and/or MTC Server.

  This cause leads to a congestion situation for which the operator wants to protect its network without affecting other MTC users.

- an external event triggering massive numbers of MTC Devices to attach/connect all at once.

  This cause leads to an overload situation for which the operator wants to prevent its network from a complete collapse. As the overload situation relates to abnormal usage from a multitude of applications and customers, a protection mechanism will affect all or a significant number of MTC applications.

- recurring applications that are synchronised to the exact (half/quarter) hour.

  This cause leads to a peak load situation for which the operator wants to spread the required capacity over time with the goal of reducing the investment needed to fulfil the required capacity demand.

Though some of the signalling congestion issues could be avoided if MTC applications behave more mobile network operator friendly, there is little a network operator can do to influence the application developers. It is important that the mobile network operator has the capability to control signalling network congestion independent of the application providers.

Signalling network nodes that may suffer from MTC related signalling congestion include all PS domain control plane nodes and gateways. With large scale attach requests, mainly the SGSN/MME is vulnerable. With connection requests, also the SGSN/MME is vulnerable as this node has a relative large load per connection request. GGSNs/PGWs are especially vulnerable as often M2M applications use a dedicated APN which may be terminated at one GGSN/PGW unless DNS and load balancing mechanisms are used. All connection requests for that particular application will then have to be handled by a single GGSN/PGW. MTC devices may concurrently attempt signalling interaction only in a limited area. That means the signalling congestion could occur just at one or several particular signalling links and no overall congestion appears on network nodes.

In order to combat signalling congestion, network nodes shall be able to reject or prevent attach or connection requests. The challenge is to block the traffic of the particular MTC application(s) that is causing the congestion, without restricting non-MTC traffic or traffic from other MTC applications that are not causing a problem. A dedicated APN or a MTC Group Identifier are possible identifiers to indicate particular large scale MTC applications. How to identify applications that are causing recurring signalling congestion (e.g. mail applications, buddy finders, etc) that are often downloaded applications on a smart phone is still a challenge.

Care shall be taken that rejecting connection requests or attach requests does not result in a MTC Device immediately re-initiating the same request. The network should be able to instruct MTC Devices not to initiate a similar request until after a back off time. This back off time may also be used to instruct MTC Devices with recurring applications to change their timing of attach/connection requests.

Care shall be taken that preventing attachment or connection requests by a targeted group of MTC Devices does not immediately or sometime thereafter result in the same group of MTC Devices almost simultaneously attempting signalling or data interactions with the same or different PLMN. Randomization should be applied to spread any resultant network access attempts by the group.

5.12.2 Required Functionality

The required functionality depends on the identified congestion and overload situation.

Congestion control provides means to manage the network load from a particular MTC group and/or related to a specific APN. Congestion control requires the following functionalities:

Editor's note: Further architecture work is required on the MTC Group concept before it is possible to progress solutions depending on MTC Group Identifiers.

- It shall be possible to reduce signalling load (Attach, PDP/PDN Activation, Service Request, …) from MTC devices related to a specific APN or from MTC Devices belonging to a particular MTC Group.

- Congestion control per APN or MTC group shall be possible with a granularity of a single SGSN, MME, GGSN or PGW.

- In order to reduce network load due to congestion situation, it shall be possible for the network to detach MTC devices belonging to a particular MTC Group and/or related to a specific APN and/or deactivate the bearers belonging to a specific APN or to a particular MTC device group.

- In order to avoid network congestion, it shall be possible for the network to prevent MTC devices related to a specific APN and/or belonging to a particular MTC group from too frequent initiation of attach and/or connection requests.

Congestion control shall also be taken with a granularity of a single signalling link between BSC/RNC and SGSN or eNodeB and MME, or a signalling link set which contain all links connecting to a single BSC, RNC, eNodeB, RA or TA(List).

Overload control provides means to manage the network load from all MTC devices independently from other devices. Overload control requires the following functionalities:

- It shall be possible to reduce signalling load caused by MTC Devices independently from signalling load caused by non-MTC devices.
- Overload control shall be possible with a granularity of a single SGSN, MME, GGSN and/or PGW.
- In order to reduce network load due to overload situation, it shall be possible for the network to detach MTC devices selectively and/or deactivate the bearers selectively among APNs or MTC device groups.
- In order to avoid network overload, it shall be possible for the network to prevent MTC Devices from too frequent initiation of attach and/or connection requests.

NOTE 1: It is for further study how it can be prevented that large numbers of devices re-initiate their deferred attach and/or connection requests at (almost) the same time to avoid excessive network congestion.

Peak shaving requires the following functionalities:

- It shall be possible to reduce (quarter/half) hourly signalling peaks from recurring MTC applications
- It shall be possible to spread over time signalling load of requests from all MTC Devices.

NOTE 2: The relation of this key issue with the key issue Time controlled is for further study especially regarding the treatment of MTC devices that are sending/signalling during their assigned time period is for further study.

5.12.3 Evaluation

5.12.3.1 General

Editor's note: The evaluations for this clause were approved distinctly and are complimentary. They are provided without any attempt to merge them.

5.12.3.2 Evaluation for Congestion Control

For congestion control, a combined solution from "Solution - Rejecting connection requests by the SGSN/MME", see clause 6.22, and "Solution - Broadcasting MTC Access Control by RAN", see clause 6.28, provides the most complete, fast and efficient means to manage the network load from a particular MTC group and/or related to a specific APN.

At the immediate onset of a congestion scenario, the first few MTC Devices from the congesting MTC Group/APN requesting RRC and/or NAS access can be rejected assuming there are enough signalling resources available to receive and reject the RRC and/or NAS access requests. To prevent the remaining MTC Device from the congesting MTC Group/APN from sending any access requests during the remainder of the congestion scenario, MTC access barring can be broadcast by the RAN to efficiently bar the specific congesting MTC Group/APN from attempting access. The RRC and/or NAS rejection back-off times and MTC access barring randomization can successful prevent the rejected/barred MTC Devices from almost simultaneously initiating access attempts after the congestion scenario has subsided.

Given this solution is dependent on the implementation of MTC Groups, it does not provide for a low impact on existing 3GPP standards and products and thus is not feasible in Rel-10.

5.12.3.3 Evaluation for Overload Control

For overload control, a combined solution from "Solution – Rejecting connection requests by the SGSN/MME", see clause 6.22, "Solution - Rejecting RRC Connection and Channel Requests by the eNodeB/RNC/BSS", see clause 6.26, and "Solution - Broadcasting MTC Access Control by RAN", see clause 6.28, provides the most complete, fast and efficient means to manage the network load from all MTC Devices independently from other devices.

At the immediate onset of an overload scenario, the first few MTC Devices requesting RRC and/or NAS access can be rejected assuming there are enough signalling resources available to receive and reject the RRC and/or NAS access requests. To prevent the remaining MTC Device from sending any access requests during the remainder of the overload

scenario, MTC access barring can be broadcast by the RAN to efficiently bar all MTC Devices, low-priority MTC Devices, and/or MTC Devices of a PLMN type from attempting access. The RRC and/or NAS rejection back-off times and MTC access barring randomization can successful prevent the rejected/barred MTC Devices from almost simultaneously initiating access attempts after the overload scenario has subsided.

Given this solution is not dependent on the implementation of MTC Groups, it provides for a low impact on existing 3GPP standards and products that may be feasible in Rel-10.

5.12.3.4 Comparison of Each Solution

The pros and cons of each solution are as follows.

1. Access Control by the RAN (eNB/RNC/BSS) as per 6.28.
   a. Pros :

      There is no wasted signalling with the MTC devices

      It can be used for controlling the overload of the RAN node and also for the CN node with the extension of the S1AP: Overload Start and Stop message.

   b. Cons:

      For applying the barring with the finer granularity such as per group, the more information should be broadcasted in the system information.

NOTE 1: The randomized barring computed as T303= (0.7+ 0.6 * rand) * ac-BarringTime may decrease the possibility that a large number of MTC devices simultaneously access the network. But the possibility still exists. Due to this possibility, we may need to enhance the current RACH mechanism that limits the number of the UE identifying the opportunities at the same time. For the other two solutions, it is also required to enhance the current RACH mechanism.

2. Rejecting RRC connection and channel requests by the eNB/RNC/BSS as per 6.26.
   a. Pros:

      This solution wastes the smaller number of signals than rejecting the request by the SGSN/MME.

   b. Cons:

      It is possible to use the solution for finer granularity control, such as per group. But, per group, the group ID should be included and then the RRC message; that is, including the group ID in the RRC connection setup complete rather than the RRC connection request. This is needed because the RRC connection request message is sent using CCCH before the dedicated control channel to the UE. Hence, for the finer granularity control, more signals (Precisely, RRC connection request, RRC connection setup, RRC Connection Setup complete) are wasted.

NOTE 2: When a low priority cause value in the RRC connection request is used as the low priority MTC device indicator, the network may experience confusion in deciding the policy for the low priority normal UE and the low priority MTC device. The details of the argument is in S2-103122.

3. Rejecting connection requests by the SGSN/MME as per 6.22 (and S2-103120 for Mobile Terminated communication.)
   a. Pros:

      The mechanism can be implemented without any change on the RAN node.

      The SGSN/MME can consider various conditions (such as roaming restriction, group, APN etc.) in order to determine whether to accept or reject the request from the MTC device.

   b. Cons:

Before the SGSN/MME receives the NAS message from the MTC device, the network and the MTC device exchange the many signals (RRC signals for connection establishment, S1AP/RNANP message from the RAN to the SGSN/MME.) All these exchanged signals may be wasted just for rejecting the request from the MTC device.

Congestion/overload control solutions proposed so far describe mechanisms that start to block signalling traffic or transactions when the system load reaches certain thresholds. There are three basic solutions:

- Broadcast based solutions that prevent any access from MTC (or low priority) devices, and
- reject based solutions that imply some MTC device individual signalling. The reject based solution may be further categorised into:
  - Reject by RAN, and
  - Reject by CN nodes.

Table 5.12.3.4-1 collects pros and cons for the three solution alternatives: broadcast based, reject by RAN and reject by SGSN/MME. The reject by GGSN/PGW can be considered as covered by the reject by SGSN as the functionality is similar and the rejection to the MTC device is finally the SGSN/MME may need to send.

Table 5.12.3.4-1: Pros and Cons for the three solution alternatives

	Broadcast control	Reject by RAN	Reject by SGSN/MME
pros	Reduces load without any signalling with the device. It is the only solution that allows for preventing any signalling from MTC devices. Also suitable for cell/RAN node overload control.	Reduces load by rejecting already the first RRC message of the device (assuming proper criteria are available with first RRC message, like the proposed "low priority" indication). Also suitable for cell/RAN node overload control. RAN node can quickly start to reduce load by rejection. Suited for SGSN/MME MTC load control on higher granularity as RAN based reject can be started by SGSN/MME, e.g. as specified for MME overload. Load control granularity per SGSN/MME, per shared PLMN and also per low/high priority is possible.	Reduces load by rejecting NAS requests (MM or SM) of the device (ideally rejecting already the first message when proper criteria are available) SGSN/MME can have group/APN information, and therefore suited for controlling load with group/APN granularity. Load control granularity per certain PLMN or roaming conditions and also per low/high priority are also possible, specifically when it can be derived from already existing signalling.
cons	Reacts slower on load than reject solutions as it depends on frequency of sending and reading the control information. (How slow in absolute figures?) Less suited for reducing load per group/APN or per CN node as extensive broadcast information seems needed to indicate a group/APN.	Less suited for reducing load per group/APN. Requires device individual RRC signalling. Some interference with NAS timers and repetitions might occur when the proposed long wait timers are longer than the NAS timers.	Requires certain amount of device individual signalling: first RRC setup needs to be performed and at least some initial NAS signalling before the SGSN/MME can reject. Without further enhancements the SGSN/MME needs more signalling before it can reject an attach, e.g. get subscriber data from HSS, to know the group/APN of the device.
others	Additional mechanism may be needed to avoid that all devices start immediately when the broadcast indication changes to allow access.	Some new identity handling is proposed (e.g. indicate IMSI when re-selecting PLMN) to provide specific criteria fro deciding on reject. RNC could also reject based on establishment cause, e.g. "background traffic".	NAS/MM (e.g. attach) may need extensions to allow for rejecting already first NAS message Some delay/wait mechanism is needed in addition (e.g. the proposed back-off timer) to prevent frequent retry from device If SGSN/MME stores all MM contexts from MTC devices after detach then the SGSN/MME may have sufficient information to reject group/APN based already with initial NAS message.

The only safe method to block MTC signalling load without impacting other traffic is the broadcast mechanism. As it is hard to predict whether reject mechanisms alone would be able to manage all potential situations it seems useful to adopt a broadcast solution. The granularity would be rather high so that some reject solution may be needed in addition to perform a more fine granular control.

Broadcast control granularity could be all MTC or with some high granularity it could prevent access from devices that change PLMN. Allowing access again may cause many devices to access at the same time. Some load distribution mechanism may be needed in addition.

The adoption of a reject mechanism in addition to a broadcast mechanism seems useful for more fine granular load control. As the RAN reject seems not suited to control based on group/APN the SGSN/MME based rejection may be used in addition to it. Also here some wait time is needed before the UE is allowed to retry.

However, as the eNodeB reject mechanism exists already it may be enhanced with reasonable effort to reduce an MME's MTC load. The MME could request the eNodeB to reject MTC devices before it request to reject all UEs besides emergency services. Applying this mechanism for GERAN/UTRAN may need further study.

5.13 Key Issue - MTC Identifiers

5.13.1 Use Case Description

The amount of MTC Devices is expected to become 2 orders of magnitude higher than the amount of devices for human to human communication scenarios. This has to be taken into account for IMSI, IMEI and MSISDN. Regulatory bodies indicate shortages of IMSIs and MSISDNs.

The MTC Feature PS Only in TS 22.368 [2] includes a requirement that PS Only subscriptions shall be possible without an MSISDN. In principle an MSISDN is not used in any of the PS based signalling procedures. However, it will have to be assured that all PS procedures indeed work and subscriptions can be uniquely identified without providing an MSISDN. Furthermore, TS 22.368 [2] specifies that remote MTC Device configuration shall be supported for PS only subscriptions without an MSDISDN assigned. Current remote MTC Device configuration solutions (i.e. Device Management and Over-the-Air configuration) are based on SMS, which assumes the use of MSISDNs. So a solution to support remote MTC Device configuration that does not require the use of MSISDNs is needed.

The identifiers can be categorised into:

- Internal Identifiers: used within the 3GPP system to identify a UE using a subscription (or the subscription itself e.g. when the UE is not registered).

- External Identifiers: used from outside the 3GPP system (e.g. at the MTCsp interface), to refer to a UE using a subscription (or the subscription itself e.g. when the UE is not registered).

5.13.2 Required Functionality

- It shall be possible to uniquely identify the ME.

NOTE 1: This requirement relates to the ME which is generally identified by the IMEI.

- It shall be possible to uniquely identify the UE using a subscription or the subscription itself.

NOTE 2: The two requirements above also apply to human-to-human communications. However, for Machine-Type Communication identifiers will have to be able to cater for a number of identifiers up to two orders of magnitude higher than for human-to-human communications.

- It shall be possible to use the following identifiers:

  1. IMSI, for internal usage within the 3GPP operator domain, and either

  2. E.164 MSISDN, for usage outside the 3GPP operator domain, or

  3. Unique identifier (e.g. FQDN), other than E.164 MSISDN, for usage outside the 3GPP operator domain.

NOTE 3: Use of IMSI outside the 3GPP operator domain is an operator option (i.e. not subject to standardization)

- If no (unique or common) MSISDN is assigned to a PS only subscription, the Internal Identifier (IMSI) shall be used as charging identifier.

- It shall be possible to associate one or more External Identifiers to the same Internal Identifier (e.g. several MSISDNs associated with the same IMSI).

- Globally unique External Identifiers shall be supported for identifying UEs used for MTC that must be globally reachable (i.e. irrespective of which mobile operator owns the subscription)
- Operator specific External Identifiers (e.g. based on a private numbering plan) may be supported for identifying UEs used for MTC that have to be reachable only from the operator domain to which they are subscribed.
- The Internal Identifier shall be globally unique.
- Remote MTC Device configuration shall still be supported for subscriptions without an MSISDN.

NOTE 4: Current remote MTC Device configuration solutions (i.e. Device Management and Over-the-Air configuration) are based on SMS, which assumes the use of MSISDNs.

5.13.3 Evaluation

5.14 Key Issue - Potential overload issues caused by Roaming MTC devices

5.14.1 Use Case Description

5.14.1.1 What is the likelihood of M2M devices being roamers?

In many cases (possibly the vast majority of cases) M2M devices will be used as part of a contract between one network operator (or network operator group with operations in multiple countries) and a large (possibly multi-national) company.

Coverage:

One of the key aspects that the operator will "sell" to the corporate customer is coverage. The use of "national roaming" obviously improves geographic coverage, but, its utilisation poses several challenges. An obvious solution to some of these national roaming challenges is for the operator to use "international roaming", either with a SIM from a different company within the same operator group, or, by using a SIM with "non-geographic" Mobile Country Code (e.g. MCC 901).

Both of these options appear to already be in use, and are likely to be used widely in the future.

Multi-national customer:

Typically a multi-national customer will want to be delivered devices and choose in which country they are used. This inevitably leads to 'roaming' for their M2M devices.

This situation is exacerbated by the use of factory "pre-fitted" SIMs.

Chance of Roaming Summary:

Overall, for devices sending low data volumes, there seem to be some strong reasons to expect most devices to be camped on a PLMN that is different to their IMSI's PLMN-ID, i.e. it may be that MOST M2M devices ARE ROAMING.

5.14.1.2 What are the consequences if most M2M devices are roaming?

5.14.1.2.1 Commercial arrangements

Currently, most roaming agreements seem to implicitly assume some degree of balance/mutual benefit between the two operators.

However, the subscribers of a network with a non-geographic Mobile Country Code are "all outbound roamers". And, the outbound roaming M2M devices are likely to generate very little traffic per device but still generate 'normal' levels of signalling and occupy 'normal' levels of VLR space. This "imbalance" might lead to the VPLMN operator being "unhappy".

At the moment the only 3GPP-standards consequence of this would seem to be, that, we should ensure that the VPLMN has sufficient counters and capabilities to measure the level of "imbalance".

5.14.1.2.2 Devices that only power-up/attach when they need to do something

If the M2M devices with foreign SIMs are normally not-attached to the network, then the VPLMN may only discover that these devices are in its territory when an event happens that causes the device to report back to the "MTC server".

If a large set of such devices get activated by the same event (e.g. burglar alarms with foreign SIMs responding to a power cut or earthquake) then the VPLMN may suddenly get loaded by huge numbers of M2M devices: yet, potentially, the VPLMN would have been totally unaware of the existence of (millions of) these devices.

Without prior knowledge of the number of inactive devices in the geographic area, network capacity planning is close to impossible.

Such scenarios lead to the need for a VPLMN to be able to "survive" a potentially massive increase in unplanned /unpredicted signalling load.

Some "tools" in the 3GPP standards may be needed to help manage this scenario.

5.14.1.2.3 Failure of "M2M partner" network

It is likely that many M2M "roaming" devices will be using the network of a PLMN within the same operator group, but not necessarily the same operator within a certain country.

For example, "OperatorX UK" might have a contract to supply 5 million electricity meters in the South of England. To 'enhance' their coverage area, they could equip them with SIM cards from their partner network "OperatorX in country A".

But what then happens if the "OperatorX UK" network fails? These devices will NOT have "OperatorY UK" as a forbidden PLMN and so, when their periodic update fails, they are likely to change network, and, over a potentially fairly short time period, up to 5 million new devices appear on the "OperatorY UK" network.

Again, we need "tools" in the 3GPP standards to permit networks to "survive" these situations.

5.14.2 Required Functionality

Tools are required to protect a VPLMN from any overload caused by the failure of one (or more) other networks in that country. However, it should be noted that a degree of co-operation from the HPLMN is still likely to be required.

The following tools needed to be ***investigated*** further:

a) counters/alarms (on e.g. a per MCC and MNC basis) to detect unusual increases in the number of roaming devices in a VPLMN;

b) the ability to remotely configure M2M devices to indicate that they are "low value" M2M devices;

c) signalling from the UE to the RAN to permit the IDNNS function in the RAN to steer "low value" M2M devices towards Core Network nodes with large VLR/storage capacity and/or large processing capacity, especially in the CS domain;

d) "access class barring" functionality that can be used to bar e.g.:

- low value" M2M devices that are not on their HPLMN or a PLMN in the (U)SIM's preferred PLMNs list;
- low value" M2M devices that are not on their HPLMN or an Equivalent HPLMN;
- low value" M2M devices that are not on their HPLMN;
- low value" M2M devices;

e) control of the "more preferred PLMN background search timer" so that M2M devices do not return too rapidly to a failed PLMN, and/or do not scroll through multiple different PLMNs in that country;

f) minimising M2M device to network signalling at inter-PLMN change, e.g. by using Attach rather than RAU/TAU and using IMSI rather than a temporary ID;

g) slowing down the rate at which "low value" M2M devices detect network failure, e.g. by having mechanisms to give "low value" M2M devices relatively long CS and PS domain periodic update timers;

h) modifications to the existing specification of how the M2M device reacts to some MM/GMM/EMM reject cause values such as "IMSI unknown in HLR"; "illegal ME"; and "PLMN not allowed";

i) inclusion of a "low value" M2M device indicator in the M2M device to RAN signalling to permit the RAN to provide special handling to such devices in times of congestion (e.g. by rejecting them with a back off time);

j) inclusion of a "low value" M2M device indicator in the M2M device to Core Network signalling to permit the CN to provide special handling to subsets of such devices in times of congestion (e.g. by checking the IMSI and/or APN and/or MTC group ID and rejecting certain groups with a back off time);

k) specification of new MM/GMM/EMM functionality (e.g. reject cause values or "abuse" of the Accept message) that causes new UE behaviour (e.g. a cause value that says "LA not allowed, but stay in this LA for X deci-hours before searching for another PLMN", or, sending RAU accept with a 20 minute PRU timer value and locally loading a "no services permitted" subscription into the SGSN's database);

l) modification of signalling to/from the EIR to permit the EIR e.g. to allow rejection/parking of an M2M device without overloading the inter-operator signalling links;

m) the specification of a new Network Mode of Operation that permits the VPLMN to offer NMO=II to their existing devices while minimising signalling from "low value" M2M devices by getting those M2M devices to use NMO=I.

5.14.3 Evaluation

5.14.3.1 Evaluation for M2M "access class barring" functionality

The "PLMN type" option from "Solution - Broadcasting MTC Access Control by RAN", see clause 6.28, defines the required mechanisms for barring MTC Devices based on their current PLMN type (e.g. not in HPLMN, PLMN in the (U)SIM's preferred PLMNs list, Equivalent HPLMN, etc). Given this solution is not dependent on the implementation of MTC Groups and can use a very efficient encoding of the PLMN type to take advantage of spare bits in pre-existing system information messages, it provides for a low impact on existing 3GPP standards and products that may be feasible in Rel-10.

NOTE: The detailed "PLMN type" indication parameters should be specified in stage 3.

Editor's note: Text to be added for remaining functionality requirements

5.15 Key Issue - Low Power Consumption

5.15.1 Use case description

For some types of MTC Devices, operation with very low power consumption is a critical requirement. For some devices, such as those used for gas metering and animal, cargo, prisoner, elderly and children tracking, low power consumption is critical because it is not easy to re-charge or replace the battery, This creates the need for system enhancements that would minimize the power consumption of MTC Devices.

5.15.2 Required Functionality

It shall be possible to save battery energy consumption for UEs.

5.15.3 Evaluation

6 Solutions

Editor's note: Solutions to all Key Issues are listed here. Under Problem Solved / Gains Provided, please list the Key Issue(s) that are addressed by the solution.

6.1 Solution - FQDN Identifier Solution

6.1.1 Problem Solved / Gains Provided

See Key Issue 5.2 "MTC Devices communicating with one or more MTC Servers".

6.1.2 General

MTC devices relying on IP communications that need to be reachable for mobile terminated communications are assigned a static unique "host name" (i.e. an FQDN identifier specific to the MTC device). The "host name" is assigned in addition to any EPS-level identity (such as IMSI or MSISDN) of the MTC device.

NOTE 1: The "host name" may be defined via the EPS-level identity. For instance, assuming that the MTC device has an IMSI as the EPS-level identity, the "host name" can be defined as "mtc.IMSI.pub.3gppnetworks.org". The exact definition of the "host name" is a Stage 3 matter.

The "host name" is used as the primary addressing identifier for mobile terminating communications.

Upon attachment to the PLMN the MTC device that relies on IP communications is assigned dynamic IP address. In roaming scenarios the dynamic IP address may be assigned in the Visited PLMN.

The association between the "host name" and the dynamically assigned IP address is stored in the authoritative DNS server in the Home PLMN.

When the MTC device is assigned a dynamic IP address, the authoritative DNS server is kept up-to-date using DNS Update mechanisms.

The entity performing DNS updates is preferably located in the Home PLMN in order to reduce the number of trusted interfaces to the DNS server.

The call flow depicted in Figure 6.1.2-1 describes how MT communication with MTC devices inside public IP address space works in step by step fashion:

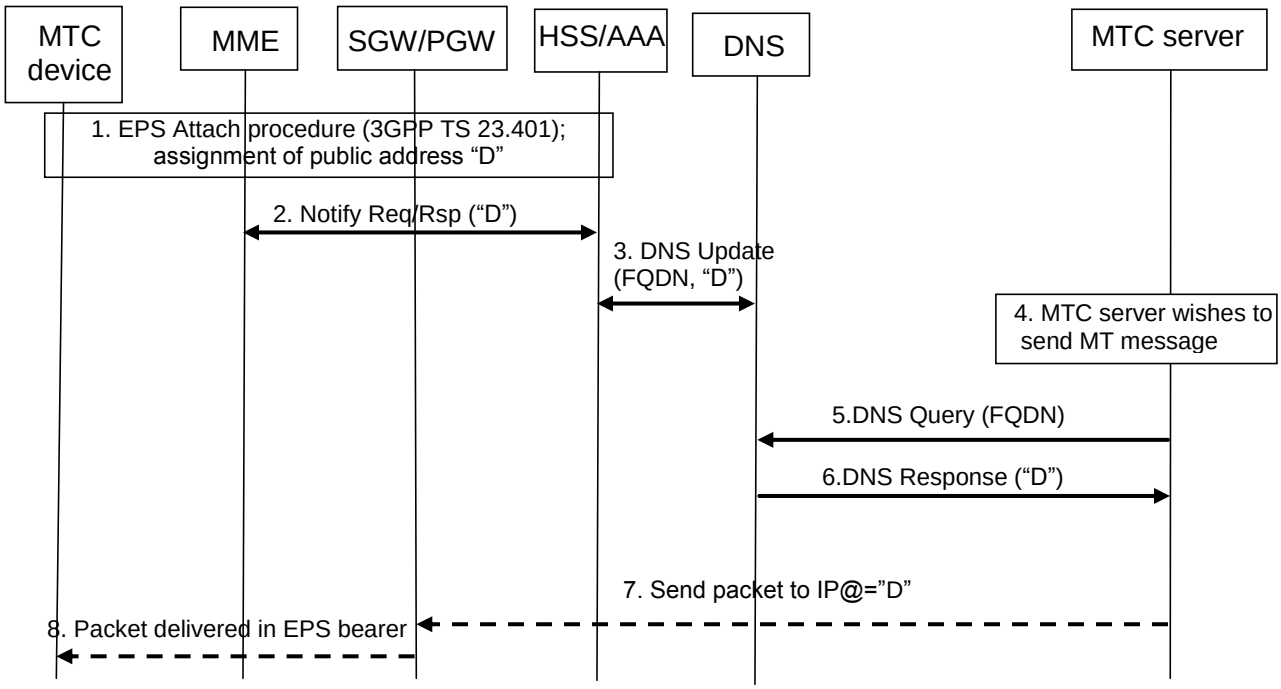


Figure 6.1.2-1: Call flow for MT communication with MTC device inside public IP address space

1. MTC device performs the EPS Attach procedure as described in TS 23.401 [5]. As part of the EPS Attach procedure the MTC device is assigned a public IP address, referred to here shortly as "D". The S5/S8/S11 Create Session Response message (not shown) is used to convey "D" from the PGW to the MME.

NOTE 2: For IPv6 it is assumed that the MTC device relies on DHCPv6 for stateful address allocation, or uses the solution described in clause 6.49.

2. As part of the previous step, or at the end of the EPS Attach procedure, the MME notifies the HSS/AAA with "D". Currently there is no direct interface between the PGW and the HSS/AAA, which is why the Notification is sent from the MME.

NOTE 3: If an interface between the PGW and the HSS/AAA is defined in the future, the MTC device's IP address "D" can be notified directly without passing through the MME.

3. The association between the "host name" of the MTC device and the dynamically assigned IP address "D" is stored in the authoritative DNS server in the Home PLMN. The HSS/AAA sends a DNS Update to the authoritative DNS server.

4. At some point the MTC server wishes to send a Mobile terminated (MT) message to the MTC device whose unique identifier is FQDN.

5. MTC server sends a DNS query that eventually reaches the authoritative DNS server.

6. The DNS response of the authoritative DNS server includes "D".

7. MTC server sets the Destination IP address in the packet it wishes to send to the MTC device to "D".

8. The PGW hosting the MTC device's public IP address delivers the packet to the MTC device via an appropriate EPS bearer.

The proposed solution also applies to GERAN and UTRAN devices, in which case MME and PGW are replaced with SGSN and GGSN.

It also applies to MTC device-to-device communications, where both MTC devices are located inside public IP address space. In this case it is the source MTC device itself that performs the DNS query to resolve the FQDN of the target MTC device.

Editor's note: If the MTC device has multiple PDN connections, it is FFS which IP address the MTC Server selects for sending packets to the MTC device.

NOTE 4: Further details on mobile terminated communications to MTC devices inside a private Ipv4 address space are described as a separate key issue, see clause 5.3 "IPv4 Addressing."

6.1.3 Impacts on existing nodes or functionality

For IP address assignment via DHCPv4, the PGW needs to notify the SGSN/MME of the assigned IPv4 address outside of the Attach procedure (e.g. via the Bearer Modification procedure).

SGSN/MME needs to notify the HSS of the device's IP address "D" (e.g. new parameter in the Notify Request message).

HSS need to perform DNS updates of the authoritative DNS server that stores the association between the "host name" of the MTC device and the dynamically assigned IP address "D".

6.1.4 Evaluation

Benefits:

- Low impact on existing Core Network nodes;
- Generic IP-level solution that does not rely on application-level identifiers (e.g. SIP URI);
- Works in all scenarios (non-roaming, roaming with home routed traffic, roaming with local breakout);
- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a "push" stimulus;
- Works also for device-to-device communication;
- Compatible with the solution for Mobile Terminated communication into private IPv4 address space (refer to clause 6.18).

Drawbacks:

- For IPv6 the solution requires stateful address configuration via DHCPv6.

6.2 Solution - Transfer of device trigger or data via SMS

6.2.1 Problem Solved / Gains Provided

See clause 5.4 "Key Issue – Online Small Data Transfer" and clause 5.8 "Key Issue - MTC Device Trigger".

6.2.2 General

MTC Devices with low data usage send or receive data utilizing SMS via SGSN/MSC or SMS over SGs. The MTC Server connects with the SM-SC or behaves as a SM-SC (e.g. has an integrated SM-SC) to send or receive MTC service data or send device trigger message encapsulated in short message. SMS transfer is suited for MTC users that infrequently transfer amounts of data that can be carried by SMS(s) and where SMS transfer generates less system load compared to the usage of packet data bearers.

Editor's note: The impact of storing and forwarding nature of SMS delivery on MTC service is FFS.

The SGSN/MME is aware that the MTC Device has the low data usage feature (e.g. the usage of that feature is known from the HLR/HSS subscription data). The MME and MTC Device will not create any EPS bearer for MTC service.

NOTE 1: In the current pre Rel-11 E-UTRAN it is not possible to establish NAS signalling connection without establishing at least the default EPS bearer. Clause 6.52 describes some potential optimisations to SMS transmission without establishing the EPS bearer.

NOTE 2: According to stage 1 requirements the small data upper limit can be around 1000 octets.

Editor's note: Need to address how this solution can support subscription and operator policy on data size.

Editor's note: The frequency of small data transmissions that can be supported with this solution needs to be described.

6.2.3 Impacts on existing nodes or functionality

a) Extensive use of SMS for transmission of small data puts additional load on control plane nodes (e.g., MME, SGSN, MSC Server, SMS-GMSC, SMS-IWMSC, SMS-SC) in order to transport user data.

6.2.4 Evaluation

6.3 Solution - Paging within configured area

6.3.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility".

6.3.2 General

For MTC devices that do not move frequently or move only within a small area, the paging area (e.g. TAI, CGI, ECGI) is configured in the HLR/HSS as a part of the subscription of the MTC subscriber. The SGSN/MME stores the paging area as part of the subscriber data as received from HLR/HSS.

During the mobile terminated service, the SGSN/MME pages the MTC Device within the specific area. The configured paging area is assumed to be smaller than typical paging areas for other UEs. Thereby paging traffic can be reduced.

An issue might be needed for reconfiguring subscription data when the network reconfigures some cells or the MTC Device is roaming.

6.3.3 Impacts on existing nodes or functionality

6.3.4 Evaluation

6.4 Solution - Paging stepwise

6.4.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility".

6.4.2 General

For the MTC Device with low mobility, the SGSN/MME stores the RAI/TAI(s) like for any other UE and in addition the last known cell (i.e. CGI/ECGI) or last known service area (i.e. SAI) as provided by RAN in S1/Iu/Gb signalling. For low mobility MTC devices the MME preferentially includes only one TAI for TAI List in the accept message.

During the mobile terminated service, the SGSN/MME may page stepwise, e.g. first in the last known cell (i.e. CGI/ECGI) or last known service area (i.e. SAI) and if there is no response the SGSN/MME pages the MTC Device in a wider area, i.e. within the RAI or TAI List allocated to the MTC Device.

6.4.3 Impacts on existing nodes or functionality

6.4.4 Evaluation

6.5 Solution - Paging within reported area

6.5.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility".

6.5.2 General

For the MTC Device with fixed location (i.e. not move normally), which can be deduced by the SGSN/MME when receiving the same area identifier (e.g. CGI, ECGI, SAI, RAI or TAI) via S1/Iu/Gb signalling during a predefined period or receiving a explicit report from the MTC Device. The SGSN/MME stores the area identifier and pages the MTC Device within the specific area.

When the MTC Device moves (e.g. for maintain purpose), the SGSN/MME detects the moving and pages within the new area which is reported by RAN or by the MTC Device explicitly.

6.5.3 Impacts on existing nodes or functionality

6.5.4 Evaluation

6.6 Solution - Triggering of non-attached MTC Devices based on location information provided by MTC User

6.6.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger".

6.6.2 General

With non-attached MTC Devices, the network has no knowledge of the location of the MTC Device. However, in many cases the MTC User does have knowledge about the location of the MTC Device. In these cases the MTC User can provide the PLMN with information on the location of the MTC Device. Based on that information the PLMN can then broadcast a trigger message in a relevant cell or group of cells. The MTC Device, while not attached, will still listen to the broadcast channel of the PLMN.

A possible solution to broadcast the triggers may be by using the Cell Broadcast Service (CBS) as specified in TS 23.041. A Cell Broadcast Center (CBC) is under control of a mobile network operator and connected to the radio network i.e. to the BSCs in case of GSM and to the RNCs in case of UMTS. Connected to a CBC are one or more Cell Broadcast Entities (CBEs) which may originate CBS messages. A mobile network operator may make available the interface on the CBC to trusted 3rd parties to interconnect their CBE to the CBC of the mobile network operator. The MTC Devices are programmed to monitor a preset CB channel(s), even when they are not attached to the network, and have assigned a Unique Paging Identity (UPID). This way the MTC Server of the 3rd party is able to send CBS messages, including one or more UPIDs, to its MTC Devices in certain areas based on location information available in the MTC Server. But also other broadcast solutions (such as using the BCCH) can be considered to trigger the MTC Devices that are not attached to the network to attach and establish PDP/PDN connectivity. Solutions to reduce the amount of trigger request and trigger response messages to be transmitted through these broadcast solutions shall also be considered together.

6.6.3 Impacts on existing nodes or functionality

6.6.4 Evaluation

6.7 Solution – Network access control by the PLMN

6.7.1 Problem Solved / Gains Provided

See clause 5.9 "Key Issue - Time Controlled"; clause 5.12, "Key Issue - Signalling Congestion Control".

6.7.2 General

The 3GPP network supports policing of the MTC Device's access to the network to prevent or allow (e.g. with specific charging) traffic to/from the network during unauthorized time periods. This may be accomplished as follows:

i) the operator provisions the access duration, grant time interval and forbidden time interval within the MTC subscription in the HLR/HSS;

ii) the SGSN/MME receives the access duration, grant time interval and forbidden time interval periods from the HLR/HSS during the Attachment, Routing Area Update or Tracking Area Update procedure;

iii) the SGSN/MME alters the grant time interval periods for MTC devices base on the value received from HLR/HSS or local operator policies, e.g. due to locally determined congestion overload conditions;

a. SGSN/MME randomly determines a communication window within the grant time interval to improve uniform utilization of the network and reduce the chance of overload at the beginning or end of the grant time interval

b. The length of the communication window shall not be less than the Access Duration agreed between the MTC Subscriber and network operator, though it could be longer.

iv) The SGSN/MME provides the communication window to the GGSN/P-GW, e.g. for the purpose of specific charging rate, or stopping data transmission when outside of the authorized time period.

v) the SGSN/MME police the MTC Device's access to the network to prevent or allow (e.g. with specific charging) traffic to/from the network outside of the communication window. In the former case, the SGSN/MME reject the access request message (e.g. Attach Request or Tracking Area Update Request) or Service Requests initiated by the MTC device outside of the communication window. In all cases, the SGSN/MME indicates the communication window to the MTC device in the accept or reject message.

Editor's note: It is FFS whether the network detaches MTC devices which remain attached to the network when the communication windowexpires.

Editors note: It is FFS whether the network should let MTC Devices attach to the network outside of the communication window, but reject session management requests (e.g. Activate PDP Context Request in GPRS).

The network may inform the MTC Devices of the communication window as follows:

i) the network provides the communication window to the MTC Server; the MTC Server distributes them to the MTC Devices via application level data; this approach has however the following drawbacks:

- a modification of the communication window may generate important signalling/traffic between the MTC Server and a possibly significant number of MTC Devices;

- MTC Devices' accesses to the network may be rejected or unduly charged until the MTC Server communicates them the communication window in-use in the Mobile Network.

Or

ii) the SGSN/MME provides the communication window directly to the MTC Devices via NAS signalling, e.g. the first time the MTC Device registers to the network, and upon subsequent NAS signalling from the MTC Device if the communication window has changed. Following an operator's update of the communication window, the MTC Device might initiate NAS signalling outside of the new communication window. In that case, the network may either:

- reject the MTC Device request and return the new communication window in the response; or accept the first access outside of the new communication window and provide at that time the new communication window for subsequent accesses. E.g. the MME/SGSN could store both the 'Time-Intervals In-Use' (i.e. the last time intervals communicated to the MTC Device) and the 'Subscribed Time-Intervals' received from the HLR/HSS, and accept the first access of the MTC Device during the 'Time-Intervals In-Use'.

In all cases where a communication window is supplied to the MTC Device, a timestamp is also provided to aid in synchronization.

6.7.3 Impacts on existing nodes or functionality

The HLR/HSS need to support provisioning of authorized time periods (i.e. access duration, grant time interval and forbidden time interval) in MTC subscriptions.

The SGSN/MME needs to determine the communication window and grant time interval for MTC devices based on the value received from the HLR/HSS randomization or the local operator policies, e.g. due to locally determined congestion or overload conditions.

The SGSN/MME needs to police the MTC Device's access to the network according to the authorized time periods.

The SGSN/MME needs to provide the MTC Devices with the communication window and timestamp information in NAS signalling (if NAS signalling is used to inform MTC Devices of the communication window).

The SGSN/MME needs to store both the new and last communication window. The SGSN/MME uses both the last and new communication windows to authorize the MTC device access to the network (e.g. reject or accept access request of the MTC Device) until the MTC device is updated with the new communication window.

MTC Devices need to store the communication window and check the stored communication window before accessing the network.

NOTE: This implies some time management and possibly buffering in the MTC Device to defer* the sending of application traffic until the next authorized time period.

Editor's note: PGW impact is still FFS. If some information needs to be transferred to PGW from MME/SGW, the information is expected to be sent using GTP if S5/S8-GTP is used, or using PCC infrastructure if S5/S8-PMIP is used.

6.7.4 Evaluation

Network Access control by the PLMN satisfies all requirements listed in clause 5.9.2. The access duration, grant time interval and forbidden interval are taken into consideration. Randomization occurs for access to prevent non-uniform utilization of the network and peaks in traffic. The VPLMN policy can be accommodated by means of applying local policy at the serving SGSN or MME. Use of the network can be enforced as required, either by detaching the MTC Device, refusing to allow it to attach or surcharging it, outside of the authorized time period.

This solution introduces some complexity in that the MTC Device and the network must agree to time periods allowed for communication. This synchronization should not be needed in the ordinary case, as the communication window is retained by both the MTC Device and the network and can be reused.

6.8 Solution - Introduction of a 3GPP MTC Service Abstraction Layer

6.8.1 Problem Solved / Gains Provided

See clause 5.11 "Key Issue – Decoupling the MTC Server from 3GPP Architecture".

6.8.2 General

A) Add additional terminology to clause 3.1:

MTC Service Logic Components: Business logic, configuration, data and other elements that implement an MTC Application and provide service to the MTC User. MTC Service Logic Components communicate with MTC Devices and may be deployed under or external to mobile network operator control.

3GPP MTC Service Abstraction Layer: A functional entity that shares reference points with network elements in the 3GPP PLMN that are specified by 3GPP. The Service Abstraction Layer also exposes interfaces to PDNs to allow Service Logic Components to communicate with MTC Devices and services offered by mobile network operators to support interaction with MTC Devices.

B) Modify clause 4.3 Architecture Baseline, as follows:

The end to end application, between the MTC device and the MTC server, uses services provided by the 3GPP system. The 3GPP system provides transport and communication services (including 3GPP bearer services, IMS and SMS) optimized for the Machine-Type Communication. For the purposes of 3GPP standardization, the MTC Server - including its internal state, operations and interfaces remain out of scope.

As shown in Figure 4.3.1, MTC Device connects to the 3GPP network (UTRAN, E-UTRAN, GERAN, etc) via MTCu interface. MTC Device communicates with MTC Service Logic Components by means of an MTC Service Abstraction Layer or other MTC Devices using MTC Functions, 3GPP bearer services, SMS and IMS Application Servers provided by the PLMN. The MTC Server is an entity which connects to the 3GPP network via a Generic Service Layer API which remains out of scope of 3GPP standardisation. The MTC Service Abstraction Layer separates the MTC Service Logic Components from access specific interfaces. The MTC Service Abstraction Layer presents generic capabilities that map to concrete ones offered by the specific access. For example, communication capabilities in the 3GPP access are supplied using the MTCi/MTCsms interfaces and thus communicates with MTC Devices. MTC Server Logic Components may be outside of the operator domain or inside an operator domain.

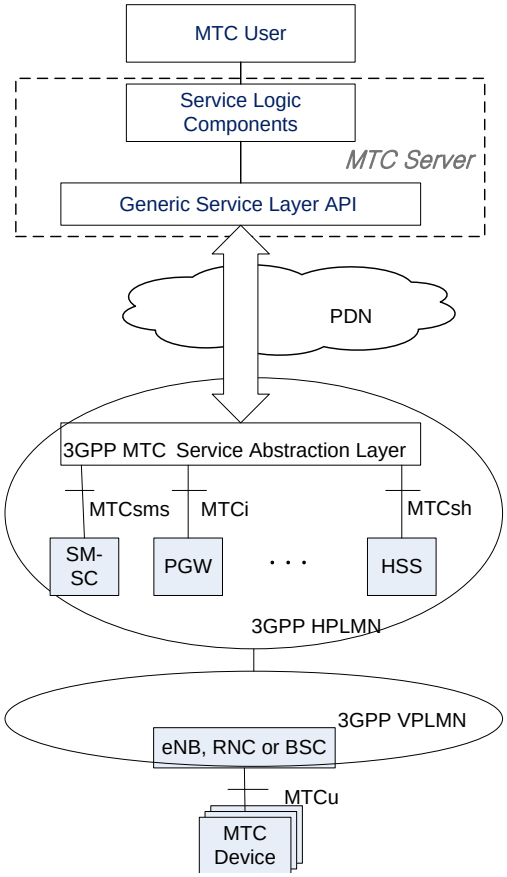


Figure 4.3-1: MTC Service Abstraction architecture

The reference points are listed as below:

MTCu: It provides MTC Devices access to 3GPP network for the transport of user plane and control plane traffic. MTCu interface could be based on Uu, Um, Ww and LTE-Uu interface.

MTCi: It is the reference point that MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP bearer services/IMS. MTCi could be based on Gi, Sgi, and Wi interface.

MTCsms: It is the reference point MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP SMS.

NOTE: Both MTCi and MTCsms may be defined in such a way as to traverse the Service Abstraction Layer transparently.

MTCsh: It provides transport of service-related data (opaque to the 3GPP system) as well as user / subscriber related data. This reference point may be based upon Sh.

Additional reference points between the 3GPP PLMN and the 3GPP MTC Service Abstraction Layer (e.g. for IMS) are FFS.

It is FFS whether the 3GPP MTC service abstraction layer applies to pre-release 8 3GPP core networks and I-WLAN.

6.8.3 Impacts on existing nodes or functionality

6.8.4 Evaluation

6.9 Solution - MTC Monitoring - General

6.9.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring".

6.9.2 General

The MTC Monitoring events are configured in the HLR/HSS as part of the MTC subscription. The related criteria (e.g. the mapped IMSI/IMEI or the allowed location area) for reporting purpose are configured together with the event as well unless the event type is self explanatory, e.g., loss of connectivity. For those configured MTC Monitoring events, default action can be predefined as well, e.g. detaching the MTC Device when the IMEI and IMSI are not mapped.

According to the requirement, the following MTC Monitoring events shall be configured in the HLR/HSS:

1. Monitoring the association of the MTC Device and UICC.

   In this case, the HLR/HSS shall also configure the mapped IMSI and IMEI as the criteria together with this event.

2. Monitoring the alignment of the MTC feature.

   In this case, the activated MTC features and the expected behavior for the special MTC Device, which is configured in the HLR/HSS as part of the MTC subscription, apply for this monitoring event.

3. Monitoring change in the point of attachment.

   In this case, the allowed location information may also need to be configured as the criteria in the HLR/HSS (e.g. the Low Mobility feature is also activated for the MTC Device).

4. Monitoring loss of connectivity.

The network shall be able to detect such configured MTC monitoring events. The following alternatives (i.e. solution 1 to solution 3) can be used for the detecting purpose. The alternatives (solution 6.24 to solution 6.25) can be used for the MTC Event Reporting entity to get the MTC Server identity.

Editor's note: It is FFS whether other alternatives can be used for the event detecting purpose.

Editor's note: It is FFS whether MTC Device can be used for assisting in MTC monitoring.

When such event is detected, the network shall be able to report to the MTC Server and/or MTC User. The following alternatives (solution 4 to solution 7) can be used for the reporting purpose.

Editor's note: It is FFS for whether other alternatives can be used for the reporting purpose.

When any event is detected, the network may also trigger MTC Monitoring actions accordingly, i.e. reduce services provided to the MTC Device or restrict access of the MTC Device or detach the MTC Device completely. When default action is predefined in the MTC subscription, the network triggers the default action (s). Dynamic action indication from the MTC server/user is not supported.

When the MTC monitoring action "reduce services provided to the MTC device" is triggered, the SGSN initiates the PDP Context Modification procedure or the MME initiates the Modify Bearer Command to the Serving GW with included modified QoS parameters for the reduced service.

When the MTC monitoring action "restrict access of the MTC Device" is triggered, in order to restrict the access of an MTC Device in idle mode, the SGSN rejects based on access restriction the Routing Area Update procedure or the MME rejects based on access restriction the Tracking Area Update procedure initiated by the MTC device. In order to restrict the access of an MTC Device in active mode, the SGSN or MME informs the RAN about the access restriction during the attach procedure or TAU/RAU procedure (the allowed location). The RAN restricts the handover only to allowed locations.

When the MTC monitoring action "detach the MTC Device" is triggered, the SGSN or MME initiates the Detach procedure.

Editor's note: How to handle the roaming scenario for this monitoring key issue is FFS.

Editor's note: How to guarantee a MTC Monitoring action will not restrict network access to the MTC Device in a way that prevents the network or MTC Server to update the MTC Device to resolve the issue that triggered the MTC Monitoring action is FFS.

6.10 Solution – SGSN/MME based detection

6.10.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring - General".

6.10.2 General

For this solution, the SGSN/MME is responsible for detecting monitoring event, so the configured MTC monitoring events along with the related criteria and default action are downloaded from the HLR/HSS to the SGSN/MME during the Insert Subscription procedure along with the MTC subscription e.g. during Attach procedure.

Basically, the SGSN/MME monitors the MTC Device behavior according to the MTC monitoring event trigger and performs corresponding action. The following table shows the procedures of the SGSN/MME.

Table 6.10.2-1: SGSN/MME based detection

Monitoring Event	Procedures
Monitoring the association of the MTC Device and UICC	The SGSN/MME asks for the MTC Device IMEI (e.g. Identity procedure). 2> The SGSN/MME checks whether the IMEI provided by the device is the same as the configured IMEI. 3> If not, the SGSN/MME shall trigger the reporting.
Monitoring the alignment of the MTC feature	The SGSN/MME checks whether the MTC Device behavior is aligned with the activated MTC features for the device. 2> If not (e.g. the MTC Device with low mobility feature performs RAU/TAU or handover procedure frequently), the SGSN/MME shall trigger the reporting.
Monitoring change in the point of attachment	The SGSN/MME checks whether there is change in point of attachment by comparing the location area information from RAN against the configured location area information from the HLR/HSS (e.g. the allowed location area information). 2> If yes, the SGSN/MME shall trigger the reporting.
Monitoring loss of connectivity	The SGSN/MME checks whether the MTC Device is offline. 2> If yes, the SGSN/MME shall trigger the reporting.

6.10.3 Impacts on existing nodes or functionality

Impacts on HLR/HSS:

- Support configuring and provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) in MTC subscription.

Impacts on SGSN/MME:

- Support storing the monitoring related information (e.g. monitoring event, criteria, default action and etc) for a particular MTC Device.
- Support monitoring detecting behaviour.
- Support executing monitoring action, e.g. according to the pre-defined action.

6.10.4 Evaluation

All events can be detected and the signals to obtain the information for detecting the events can be optimized.

However the load of the SGSN/MME may increase depending on the number of events and actions.

6.11 Solution - HLR/HSS based detection

6.11.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring - General".

6.11.2 General

For this solution, the HLR/HSS is responsible for detecting monitoring event with the assistance of other nodes. The MTC monitoring events along with the related criteria and default action are configured in the HLR/HSS. The HLR/HSS monitors the MTC Device behaviour according to the MTC monitoring event trigger and performs corresponding action.

The following table shows the procedures of the HLR/HSS.

Table 6.11.2-1: HLR/HSS based detection

Monitoring Event	Procedures
Monitoring the association of the MTC Device and UICC	1. The SGSN/MME provides the MTC Device IMEI together with the IMSI to the HLR/HSS. 2> The HLR/HSS checks whether the IMEI provided by the SGSN/MME is the same as the configured IMEI for the MTC Device. 3> If not, the HLR/HSS shall trigger the reporting.
Monitoring the alignment of the MTC feature	1. The HLR/HSS checks whether the MTC Device behaviour is aligned with the activated MTC features for the device. 2> If not (e.g. the HLR/HSS is aware that the MTC Device with low mobility feature changes the serving SGSN/MME), the HLR/HSS shall trigger the reporting.
Monitoring change in the point of attachment	1. The SGSN/MME reports the UE location (e.g. RAI, TAI, CGI, E-CGI and etc) to the HLR/HSS during MM procedure. 2> The HLR/HSS checks whether the UE location is allowed comparing to the configured location. 3> If not, the HLR/HSS shall trigger the reporting.
Monitoring loss of connectivity	1. The HLR/HSS checks whether the MTC Device is offline, e.g. the GGSN/P-GW information for the M2M APN is deleted, or receives Purge message. 2> If yes, the HLR/HSS shall trigger the reporting.

6.11.3 Impacts on existing nodes or functionality

Impacts on HLR/HSS:

- Support configuring monitoring related information (e.g. monitoring event, criteria, default action and etc) in MTC subscription.

- Support monitoring detecting behaviour.

Impacts on SGSN/MME:

- Support reporting location information to the HLR/HSS so that the HLR/HSS can detect a change by comparing with a subscribed location, or by comparing with the earlier stored location.

- Support registering GGSN/P-GW information to the HLR/HSS. To detect loss of connectivity quicker the SGSN/MME may need to configure very short periodic update timers, which increases MM signalling considerably.

- Support reporting MTC Device IMEI to the HLR/HSS.

6.11.4 Evaluation

Without any impacts on other nodes or signalling the HLR/HSS is able to detect when another device (IMEI) uses the UICC (IMSI). Also an action (e.g. cancel location or invalidate UICC) can be added and affects only the HLR/HSS.

Monitoring of feature activation clearly requires additional functions in other nodes and related signalling. Also monitoring of the point of attachment by the HLR/HSS requires additional functions in other nodes and related signalling.

Monitoring of the connectivity is not necessarily suited for the HLR/HSS as other HLR/HSS signalling is much less frequent. Detection of lost connectivity may require frequent indications to the HLR/HSS that connectivity exists.

6.12 Solution - GGSN/P-GW based detection

6.12.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring - General".

6.12.2 General

For this solution, the GGSN/P-GW is responsible for detecting monitoring event with the assistance of other nodes. The GGSN/P-GW obtains such information from the HLR/HSS, and monitors the MTC Device behavior according to the MTC monitoring event trigger and performs corresponding action.

The following table shows the procedures of the GGSN/P-GW.

Table 6.12.2-1: GGSN/P-GW based detection

Monitoring Event	Procedures
Monitoring the association of the MTC Device and UICC	1. The SGSN/MME provides the MTC Device IMEI together with the IMSI to the GGSN/P-GW during the bearer establishment procedure. 2> The GGSN/P-GW obtains the mapped IMEI and IMSI pair from e.g. the HLR/HSS. 3> The GGSN/P-GW checks whether the IMEI and IMSI provided by the SGSN/MME is matches with the configured IMEI and IMSI pair. 4> If not, the GGSN/P-GW shall trigger the reporting.
Monitoring the alignment of the MTC feature	1. The GGSN/P-GW checks whether the MTC Device behaviour is aligned with the activated MTC features for the device. 2> If not (e.g. the GGSN/P-GW is aware that the MTC Device with low mobility feature changes location), the GGSN/P-GW shall trigger the reporting.
Monitoring change in the point of attachment	1. The GGSN/P-GW activates the MS Info Change Reporting Action when PDN connection is created. 2> The SGSN/MME reports the UE location (e.g. RAI, TAI, CGI, E-CGI and etc) to the GGSN/P-GW during bearer management procedure. 3> The GGSN/P-GW checks whether the UE location is allowed comparing to the configured location. 4> If not, the GGSN/P-GW shall trigger the reporting.
Monitoring loss of connectivity	1. The GGSN/P-GW checks whether the MTC Device is offline, e.g. the PDN connection for the M2M APN is deactivated. 2> If yes, the GGSN/P-GW shall trigger the reporting.

6.12.3 Impacts on existing nodes or functionality

Impacts on HLR/HSS:

- Support configuring monitoring related information (e.g. monitoring event, criteria, default action and etc) in MTC subscription.

Impacts on SGSN/MME:

- Support provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) to the GGSN/P-GW.

Impacts on GGSN/P-GW:

- Support monitoring detecting behaviour.

Impacts on PCRF/BBERF/PCEF:

- Support provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) to the P-GW, if PMIP is used over S5/S8.

6.12.4 Evaluation

With a proper subscription it can be prevented that a UICC can be used for anything else than the PDP/PDN connection provided for MTC. PDP/PDN connections are then only possible with the subscribed APN/P-GW/GGSN. The

GGSN/P-GW can refuse PDP/PDN activation when the IMEI does not match. Compared to the HLR/HSS with the existing signalling the GGSN/P-GW cannot detach the device and also not invalidate the UICC.

The GGSN/P-GW gets location information by setting "the MS Info Change Reporting Action" to start in the create session response to the MME and then the GGSN/P-GW can monitor change of the point of attachment using the existing procedure of the MS info change reporting procedure.

If the MTC device has only one PDN connection, the P-GW may detect the monitoring of the connectivity by detecting the PDN disconnection, but when the multiple PDN connections is used, a PDN disconnection does not imply that the UE is detached and the connectivity with the UE is lost. Hence, the GGSN/P-GW is not necessarily suited for detecting lost connectivity.

Editor's note: Evaluation for PMIP based S5/S8 is FFS.

6.13 Solution - Reporting by SGSN/MME

6.13.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General".

6.13.2 General

For this solution, the SGSN/MME is responsible for reporting the event.

This solution can only be used for solution 1, i.e. the SGSN/MME is responsible for detecting (clause 6.10.)

When the event is detected, the SGSN/MME reports towards the MTC Server

6.13.3 Impacts on existing nodes or functionality

The SGSN/MME needs to provide a new reference point for event reporting.

6.13.4 Evaluation

6.14 Solution - Reporting by HLR/HSS

6.14.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring – General".

6.14.2 General

For this solution, the HLR/HSS is responsible for reporting the event. When the event is detected, the HLR/HSS reports towards the MTC Server.

This solution can be used with solution 1 and 2, i.e. the SGSN/MME or the HLR/HSS is responsible for detecting. The following table shows the procedures for different detecting solution.

Table 6.14.2-1: HLR/HSS based Reporting

Detecting solution	Procedures
Solution 1: SGSN/MME based detection (clause 6.10)	The SGSN/MME reports the event related information (e.g. event type, MTC Device identifier) to the HLR/HSS. The HLR/HSS forwards the warning notification request message to the MTC Server. 3> The HLR/HSS receives the warning notification acknowledgement message from the MTC Server and forwards it to the SGSN/MME.
Solution 2: HLR/HSS based detection (clause 6.11)	The HLR/HSS sends the warning notification request message to the MTC Server, which includes the event related information (e.g. event type, MTC Device identifier). 2> The HLR/HSS receives the warning notification acknowledgement message from the MTC Server.

6.14.3 Impacts on existing nodes or functionality

The path between the HLR/HSS and the MTC Server needs to be updated in order to exchange the warning notification.

For solution 1, the message between SGSN/MME and the HLR/HSS e.g. Notify Request message, also needs to be updated.

6.14.4 Evaluation

6.15 Solution - Reporting by GGSN/P-GW

6.15.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General".

6.15.2 General

For this solution, the GGSN/P-GW is responsible for reporting the event. The GGSN/P-GW reports towards the MTC Server.

This solution can be used with solution 1 and 3, i.e. the SGSN/MME or the GGSN/P-GW is responsible for detecting. The following table shows the procedures for different detecting solution.

Table 6.15.2-1: GGSN/P-GW based Reporting

Detecting solution	Procedures
Solution 1: SGSN/MME based detection (clause 6.10)	The SGSN/MME reports the event related information (e.g. event type, MTC Device identifier) to the GGSN/P-GW through S-GW via GTP-C message (e.g. reusing the Change Notification Request message) for GTP based S5/S8. Those information are transferred to PGW via PCC for PMIP based S5/S8. The GGSN/P-GW encapsulates and sends the warning notification request message to the MTC Server. 3> The SGSN/MME receives the warning notification acknowledgement message from the MTC Server and forwards it to the SGSN/MME via the GTP-C path.
Solution 2: GGSN/P-GW based detection (clause 6.12)	The GGSN/P-GW sends the warning notification request message to the MTC Server, which includes the event related information (e.g. event type, MTC Device identifier). 2> The GGSN/P-GW receives the warning notification acknowledgement message from the MTC Server.

6.15.3 Impacts on existing nodes or functionality

The GGSN/P-GW needs to be updated to communicate with the MTC Server.

For solution 1, the GTP-C message also needs to be updated to transfer the warning notification. For PMIP based S5/S8, PCRF/BBERF/PCEF: shall support provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) to the P-GW, if PMIP is used over S8.

6.15.4 Evaluation

6.16 Solution - Reporting by PCRF

6.16.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General".

6.16.2 General

For this solution, the GGSN/P-GW or S-GW (PMIP based) is responsible for reporting the event via PCRF. The GGSN/P-GW/S-GW exchanges warning notification message with the PCRF, and the PCRF reports towards the MTC Server.

This solution can be used with solution 1 and 3, i.e. the SGSN/MME or the GGSN/P-GW is responsible for detecting. The following table shows the procedures for different detecting solution

Table 6.16.2-1: PCRF based Reporting

Detecting solution	Procedures
Solution 1: SGSN/MME based detection (clause 6.10)	The SGSN/MME reports the event related information (e.g. event type, MTC Device identifier) to the GGSN/P-GW through S-GW via GTP-C message (e.g. reusing the Change Notification Request message) for GTP based S5/S8. For PMIP based S5/S8, the SGSN/MME reports the event to the S-GW. For GTP based S5/S8 case, the GGSN/P-GW encapsulates and sends the warning notification request message to the PCRF by reusing the IP-CAN session modification request message. For the PMIP based S5/S8 case, the S-GW directly informs the PCRF by reusing Gateway Control session modification message. The PCRF reports the event to the MTC Server and obtains acknowledge from the MTC Server. The PCRF forwards the acknowledgement message to the GGSN/P-GW or S-GW (i.e. PMIP based S5/S8). 5> The GGSN/P-GW or S-GW forwards the warning notification acknowledgement message to the SGSN/MME.
Solution 2: GGSN/P-GW based detection (clause 6.12)	The GGSN/P-GW sends the warning notification request message to the PCRF by reusing the IP-CAN session modification request message. The PCRF forwards the warning notification request message to the MTC Server, which includes the event related information (e.g. event type, MTC Device identifier). 3> The PCRF receives the warning notification acknowledgement message from the MTC Server and forwards it to the GGSN/P-GW.

6.16.3 Impacts on existing nodes or functionality

The PCC related messages needs to be updated to transfer warning notification.

For solution 1, the GTP-C message also needs to be updated to transfer the warning notification.

For solution 2, PCC/BBERF/PCEF need to be updated to transfer the warning notification if PMIP is used over S8.

NOTE: PCRF impacts are expected to be the same as GTP based S5/S8.

6.16.4 Evaluation

6.17 Solution – Allowed Time Period after TAU/RAU

6.17.1 Problem Solved / Gains Provided

See clause 5.9 "Key Issue –Time Controlled" and clause [TBD] "Key Issue – Extra Low Power".

6.17.2 General

The solution specified in this clause can be used for Extra-low power consumption, possibly together with Time-controlled MTC communications.

The basic idea behind the solution is that downlink data transfer is only possible during an allowed time period after the MTC Device performed a TAU/RAU procedure. During that allowed time period the MTC server can communicate with the MTC device. After the allowed time period the MTC device may switch off the receiver and communication is not possible.

Editor's note: It is FFS how this solution can cope with MTC Devices with low mobility, which may perform the TAU/RAU procedure very rarely.

Editor's note: It is FFS how this solution can cope with MTC Devices performing TAU/RAU often during network-determined forbidden time interval (i.e., assuming that TAU/RAU is allowed during the forbidden time).

After the MTC Device performs a TAU/RAU procedure the MTC Device may stay in power-up mode and inform the MTC Server that is available for communication so that the MTC Server(s) can forward all buffered traffic to the device. The MTC Device may be configured not to inform the MTC Server after every TAU/RAU procedure and thus reduce the frequency of allowed time periods based on the applicable time-controlled requirements. How often an allowed time period occurs is thus configurable. For example, the MTC Device may be configured to stay in power-up mode after a TAU/RAU and inform the MTC Server about its availability only between 1am – 5am every day.

The MTC Server buffers downlink traffic for the MTC Device until the MTC Device informs the server that is ready for MTC communications.

NOTE 1: Since this solution requires downlink traffic buffering, it is appropriate for time-tolerant MTC applications.

The EPS network configures the MTC Device as to initiate allowed-time periods (after a RAU/TAU) according to the operator requirements and the MTC subscription options. Normally, downlink traffic does not occur outside of an allowed time period because the MTC Server(s) expect the device to send first a message to announce its availability for MTC communications. However, if downlink traffic for the MTC Device occurs outside an allowed time period, then the EPS network rejects/drops this traffic (i.e. the EPS network does not page the MTC Device outside the allowed time period).

6.17.3 Impacts on existing nodes or functionality

6.17.4 Evaluation

6.18 Solution - MT Communication with NATTT

6.18.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue – Ipv4 Addressing".

6.18.2 General

What follows below are some additional considerations, beyond the FQDN Identifier Solution described in clause 6.1, when the assigned Ipv4 address belongs to the range of private Ipv4 addresses. Depicted in Figure 6.18.2-1 is a general MTC scenario with MTC device roaming in a VPLMN. The MTC device is assigned a private IP address (referred to as "D") that is hosted on the PGW node residing in the VPLMN (i.e. Local breakout). All the relevant EPS nodes are located in the VPLMN, except for the HSS/AAA node that resides in the HPLMN.

The MTC server wishing to establish a Mobile Terminated (MT) communication may be owned by the HPLMN, by the VPLMN or by a third party. It is located somewhere on the Internet, which is why a Network Address Translation (NAT) device is needed at the public/private boundary.

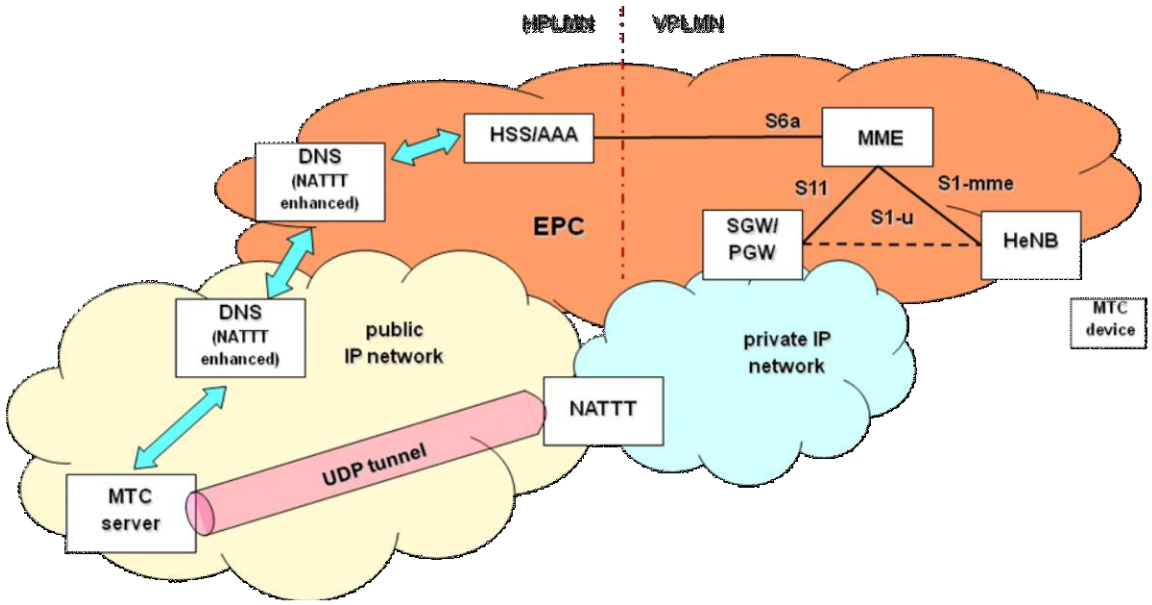


Figure 6.18.2-1: NATTT applied to the MTC context

In order to support MT communications to MTC devices inside private IP address space, the NAT device on the public/private boundary is replaced by a NATTT-capable device ([3]) i.e. a NAT device capable of UDP encapsulation for packets exchanged on the "public" side (i.e. to/from the MTC server), in addition to its traditional role as a NAT device. The reason for using UDP encapsulation (instead of simple IP-in-IP encapsulation) is because the NATTT device relies on a well-known UDP port number to identify the encapsulated packets.

The call flow depicted in Figure 6.18.2-2 describes how MT communication with MTC devices inside private IP address space works in step by step fashion:

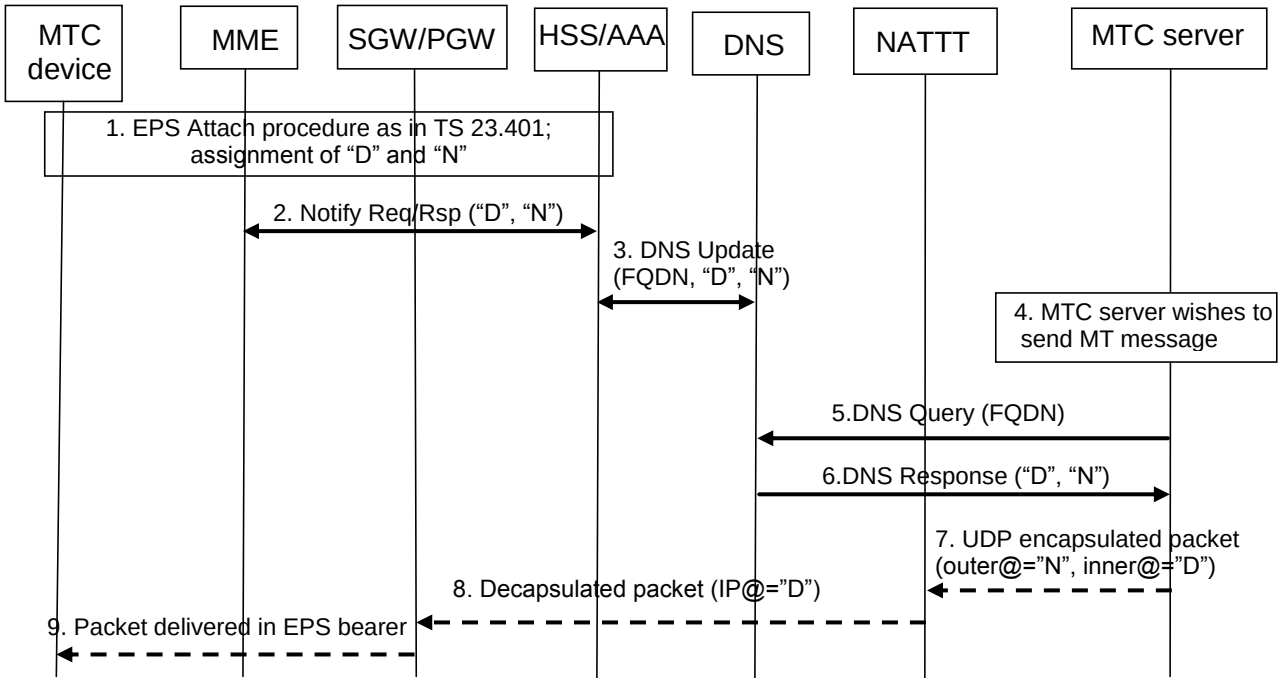


Figure 9.18.2-2: Call flow for MT communication with MTC device inside private IP address space

1. MTC device performs the EPS Attach procedure as described in TS 23.401 [5]. As part of the EPS Attach procedure the MTC device is assigned a private IP address, referred to here shortly as "D". Also as part of this procedure, the PGW node returns the public IP address of the NATTT device ("N") through which the private address "D" is reachable. If there are several NATTT devices on the border of the private IP network, the PGW

selects any that provides access to the private address "D". The S5/S8/S11 Create Session Response message (not shown) is used to convey both "D" and "N" from the PGW to the MME.

2. As part of the previous step, or at the end of the EPS Attach procedure, the MME notifies the HSS/AAA with "D" and "N". Currently there is no direct interface between the PGW and the HSS/AAA, which is why the Notification is sent from the MME.

3. The HSS/AAA sends a DNS Update to the authoritative DNS server in order to associate "D" and "N" with the DNS record for the MTC device (the latter being referenced via its unique FQDN). This requires a new type of DNS record.

4. At some point in time the MTC server wishes to send a Mobile terminated (MT) message to the MTC device whose unique identifier is FQDN.

5. MTC server sends a DNS query that eventually reaches the authoritative DNS server.

6. The DNS response of the authoritative DNS server includes "D" and "N".

7. MTC server performs UDP encapsulation of the IP packet it wishes to send to the MTC device. The destination IP address in the outer IP header is set to "N". The destination IP address in the inner IP header is set to "D". The UDP port in the UDP encapsulation header is set to a well known value, as described in [3]. The source IP address in both the inner and outer IP headers is set to the public IP address of the MTC server.

8. The NATTT device identifies the packet as a NAT tunnelled packet because it arrives on a well-known UDP port. It strips off the outer IP/UDP header and forwards the inner IP packet on the private IP network.

9. The inner IP packet reaches the PGW hosting the MTC device's private IP address. The PGW delivers the packet to the MTC device via an appropriate EPS bearer.

The proposed solution also applies to GERAN and UTRAN devices, in which case MME and PGW are replaced with SGSN and GGSN.

It also applies to MTC device-to-device communications, where either or both MTC devices are located inside private IP address space. In this case it is the source MTC device itself that performs the DNS query to resolve the FQDN of the target MTC device (i.e. to obtain the private IP address of the target MTC device, as well as the public address of the NATTT device in the target network). It is also the source MTC device that performs the packet encapsulation.

NOTE: It is FFS how to prevent unwanted traffic from being sent to the MTC device.

6.18.3 Impacts on existing nodes or functionality

The PGW needs to notify the SGSN/MME of the NAT device's public address "N" (e.g. new parameter in the Create Session Response message).

For IP address assignment via DHCPv4, the PGW needs to notify the SGSN/MME of the assigned IPv4 address outside of the Attach procedure (e.g. via the Bearer Modification procedure).

SGSN/MME needs to notify the HSS of the MTC device's private address "D" and the NAT device's public address "N" (e.g. new parameters in the Notify Request message).

HSS needs to perform DNS updates of the authoritative DNS server that stores the association between the "host name" of the MTC device on one hand, and the dynamically assigned private IP address "D" plus the NAT device's public address "N" on the other.

Requires definition of a new DNS record, capable of storing the NAT device's IP address "N".

6.18.4 Evaluation

Benefits:

- Low impact on existing Core Network nodes;

- Generic IP-level solution that does not rely on application-level identifiers (e.g. SIP URI);

- Works in all scenarios (non-roaming, roaming with home routed traffic, roaming with local breakout) to an attached MTC device with an established PDN connection;

- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a "push" stimulus;
- Works also for device-to-device communication;
- The solution is based on the generic FQDN Identifier solution described in clause 6.1, but the public DNS functionality needs to be extended.

Drawbacks:

- Requires support of a new DNS record (supporting D and N addresses) in the public DNS infrastructure, this DNS record needs to be standardised by the IETF and globally deployed as part of the public DNS infrastructure. Such a deployment may take a relatively long period of time.

Editor's note: A solution may exist not requiring support of the new DNS record by the public DNS infrastructure, whereby the private IP address "D" would be transferred in the DNS infrastructure via transparent strings. This is FFS.

- If the failure of a NATTT box requires to modify the public IP address "N" through which the private address "D" is reachable, then all the DNS entries of all MTC devices served by this NATTT must be updated (via the MME in this case). In addition the DNS cache entries at the MTC Server need to be cleared, generally after a timeout of few minutes (depending on the implementation).
- additional complexity in the MTC Server to support new DNS records and UDP/IP encapsulation (according to [3] this may require the support of a NAT Daemon in the MTC Server which intercepts DNS queries and user plane traffic to hide the DNS extension and UDP/IP encapsulation to the application).

6.19 Solution - MT Communication with Micro Port Forwarding

6.19.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue – IP Addressing".

6.19.2 General

The general concept of this solution is that during initial PDP context / PDN connection establishment, the network will setup special very narrow port forward rule(s) (i.e. a Micro Port Forward rule) with the NAT to allow MT messages only from a defined MTC Server(s). Not only is the port forward narrowed based on the MTC Server IP address, it is further narrowed by only allowing specific source and destination port numbers. This effectively creates the same size pinhole in the NAT that UE used for MTC creates with a normal outbound packet. The difference being that this pinhole is now more specifically managed.

When NAPT (Network Address and Port Translation) port forwarding only uses a mandated SRC IP address (i.e. public MTC Server IP address) and DST port number (i.e. public UE port number), this yields only 65,536 (2^16) unique port forwarding rules per public UE IP address per public MTC Server IP address. However, when the port forward rule is extended to a MPF rule (additionally mandate of the SRC port number (i.e. public MTC Server port number), this yields ~4 billion (2^32) unique port forwarding rules per public UE IP address per public MTC Server IP address.

More than one MPF rule may be established for a particular UE used for MTC. The UE needs a MPF rule for each MTC Server it requires MT messaging support for.

The set of MPF rule configuration parameters that can be specified as input into the NAT entity establishing a new MPF rule could include the following:

- Per UE subscription:
  - default MPF enablement flag;
  - default set of authorized MTC Server public IP address(es) that can use an established PDP context / PDN connection for IP communications;
  - default private UE DST port # range (optional)(Eases the requirement on the UE to only have to listen to pre-configured static ports);

  - public MTC Server port # range (optional);
  - protocol constraints (optional);
  - lease time (time for the NAT to maintain the MPR rule) (optional).
- Per authorized MTC Server public IP address (optional configuration parameters that overrides the default above):
  - reference to the authorized MTC Server public IP address;
  - private UE DST port # range constraints (optional);
  - public MTC Server port # range constraints (optional);
  - protocol constraints (optional);
  - lease time (time for the NAT to maintain the MPR rule) (optional).
- Per APN configuration / PDN subscription context (optional configuration paremeter that overrides the default above);
  - reference to APN configuration / PDN subscription context;
  - MPF enablement flag;
  - references to the subset of authorized MTC Server public IP address(es) that can use an established PDP context / PDN connection for IP communications.

These MPF rule configuration parameters could be configured in the UE used for MTC (e.g. by the MTC Server through Device Management procedures) and/or in the subscription data for the UE in the HSS/HLR. If there is a conflicting parameter value between a parameter stored both in the UE and the HSS/HLR, the subscription data value in the HSS/HLR will have priority over the value stored in the UE. Furthermore, if there is still a conflicting parameter value between the default value and a MTC Server or APN configuration / PDN subscription context specific value, the latter will have priority over the default value.

An established MPF rule contains the following parameters:

- reference to the established PDP context / PDN connection;
- set of authorized MTC Server public IP address(es) that can use the established PDP context / PDN connection for IP communications;
- public UE IP address;
- public MTC Server port number;
- public UE port number.
- private UE IP address;
- private UE port number;
- lease time (optional);
- protocol constraints (optional).

Once a MPF rule is established, the methods to communicate the public portion of the MPF rule to the MTC Server so that it can be used for MT communications includes:

1) UE used for MTC sends MPF rule to MTC Server - The UE used for MTC receives the public portion of the MPF rule from the network during the PDN connection establishment procedure. Then the UE used for MTC sends a message(s) to the MTC Server(s) containing the information regarding the public portion of the MPF rule that was created. The UE used for MTC can do this by simply sending a transport layer (e.g. UDP or TCP) message using the appropriate IP address and port numbers. Alternatively, the UE used for MTC can send this information via an application layer message;

2) MTC Server request MPF rule from DNS server - This option uses the FQDN Identifier Solution described in clause 6.1. When the MTC Server wants to send a MT message it will do a DNS query of the FQDN of the UE used for MTC. The DNS response will contain the information defining the public portion of the MPF rule;

3) MTC Server obtains MPF rule from DT-GW - This option uses the MT communications address resolution via DT-GW solution described in clause 6.46. When the MTC Server wants to send a MT message to a UE used for MTC and the address of the assigned DT-GW is not known, the MTC Server will first perform a DNS query of the hostname of the UE. The DNS response will contain the IP addresses of the assigned DT-GW for the UE. Once the address of the assigned DT-GW for the UE is known, the MTC Server communicates with the DT-GW to ascertain the public portion of the MPF rule.

Figure 6.19.2-1 illustrates how the IP address(es) and port numbers of a MPF rule are then used to route a MT IP packet from the MTC Server to the UE used for MTC in both the public and private address space.

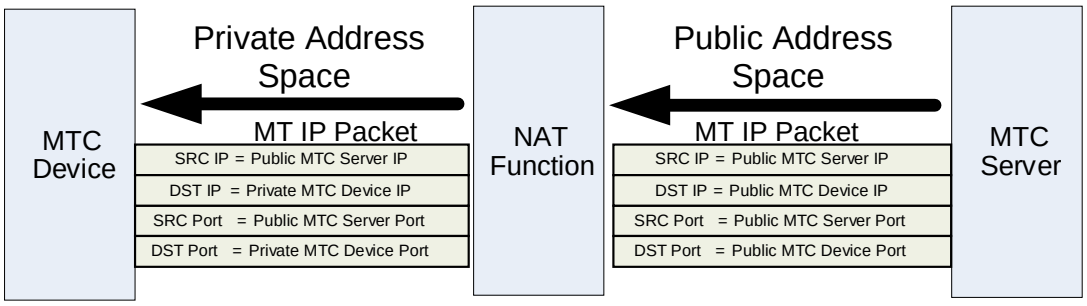


Figure 6.19.2-1: MT message sent into a private IPv4 address space using Micro Port Forwarding

Figure 6.19.2-2 illustrates how a MPF rule is established for a new PDN connection, communicated to the MTC Server and utilized for MT communications.

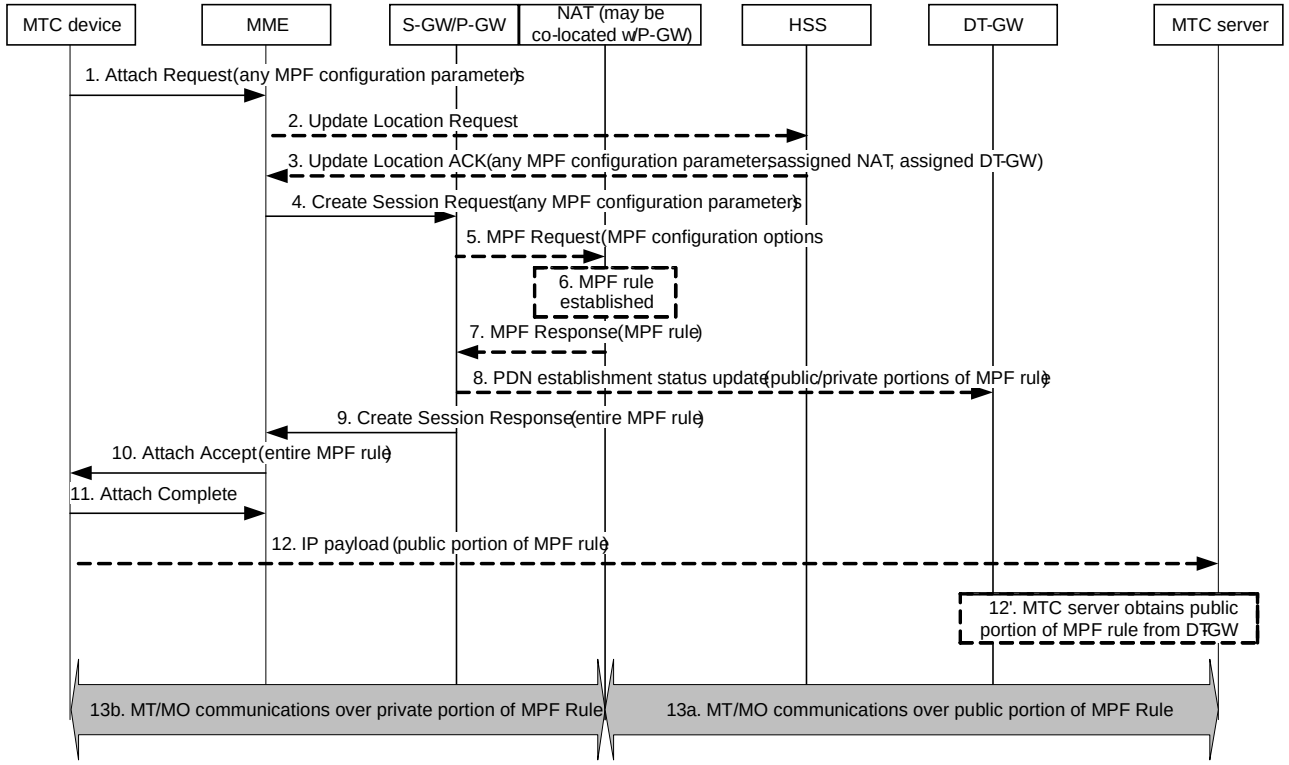


Figure 6.19.2-2: Call flow for MPF rule establishment for a PDN connection

1. UE used for MTC sends initial attach request specifying any MPF configuration preferences for the default PDN connection e.g. that may have been configured using Device Management procedures by the MTC service provider.

2. If the MME does not have the subscription data for the UE, the Update Location request is sent to the HSS.

3. The HSS sends the Update Location ACK to the MME containing subscription data for any MPF configuration parameters and, if a DT-GW is employed for the UE, the assigned NAT entity for the new PDN connection, if not co-locate with the P-GW and the assigned DT-GW. The MME resolves any duplicate and conflicting MPF configuration parameter values by applying the appropriate priority.

4. The MME and S-GW include any MPF configuration parameters in their respective Create Session requests.

5. If the MPF enablement flag is set for the new PDN connection and the NAT entity and P-GW are not co-located, the P-GW sends a MPF request to the NAT entity responsible for the establishing the MPF rule for the new PDN connection.

6. NAT entity establishes the MPF rule for the new PDN connection using any specified MPF configuration parameters.

7. If a MPF rule was established and the NAT entity and P-GW are not co-located, the NAT entity includes the entire MPF rule (both public and private portions) in the MPF response to the P-GW.

8. If a DT-GW is assigned for the UE, the P-GW sends a PDN establishment status update to the assigned DT-GW containing the complete MPF rule.

9. If a MPF rule was established, the P-GW and S-GW includes the entire MPF rule in their respective Create Session responses.

10. If a MPF rule was established, the MME includes the entire MPF rule in the Attach Accept message.

11. UE responds with the Attach Complete message.

12. The UE used for MTC sends a transport layer (e.g. UDP or TCP) message using the appropriate IP address and port numbers. Alternatively, the MTC device can send this information via an application layer message.

12'. In an alternative to step 12, the MTC server obtains the public portion of the MPF rule from the DT-GW.

13a. When the NAT entity receives an incoming packet from the MTC server that matches the MPF rule (i.e. public MTC Server SRC IP and port #, public UE DST IP and port #), it performs the normal NAPT on the public UE device IP address and DST port #.

13b. The NAT entity then forwards the packet to the UE.

6.19.3 Impacts on existing nodes or functionality

Impacts on CN nodes:

- NAPT functionality is extended to employ MPF (addition of the SRC port number to the port forwarding rule);

- If NAT entity is not co-located with the GGSN/P-GW, a new interface and messaging between the GGSN/P-GW and NAT entity is required to establish MPF rules;

- HSS/HLR additional storage of MPF configuration parameters as part of subscription data;

- PDP context / PDN establishment procedure messaging to be extended to include MPF configuration parameters and MPF rule;

- if DT-GW is used for MTC Server to obtain public portion of MPF rule, the "MT communications address resolution via DT-GW" solution described in clause 6.46 shall be supported.

6.19.4 Evaluation

Benefits:

- Increases the number of possible unique port forwarding rules per public UE IP address per public MTC server IP address from 65,536 (2^16) to ~4 billion (2^32);

- For security, reduces scanning attack success rate from malicious network entities.

- Works in all scenarios (non-roaming, roaming with home routed traffic, roaming with local breakout);
- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a "push" stimulus to an attached MTC device with an established PDN connection, but this requires the network to periodically re-new the MPF rule in the NAT entity;

Drawbacks:

- MPF rule adds additional port forwarding requirements on NAPT in network;
- MPF rule adds additional subscription data and/or UE configuration.
- If the application payload need to transport IP addresses then there is a need for ALG (Application Level Gateway), which may not be possible if the payload is encrypted end to end; If no encryption is used then the NAT needs to parse the application level payload.
- NAT single point of failure (the MPF rules are lost if the NAT box fails) but this is similar to traditional port forwarding;
- MTC Device needs an explicit protocol to discover the NAT and also set the MPC filter in the NAT.

6.20 Solution - Optimizing periodic LAU/RAU/TAU Signalling

6.20.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility," clause 5.12 "Key issue – Signalling Congestion Control", clause 5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices" and clause [TBD] "Key Issue – Extra Low Power".

6.20.2 General

This solution can be used for low mobility and/or extra low power MTC devices (CS and PS domain specific systems), MTC devices that indicate "Low-Priority-Access" (PS domain specific system) (see clause 6.23), and for signalling congestion control and potential overload issues caused by roaming MTC devices.

For CS domain specific systems, MTC devices can be pre-provisioned with MTC_T3212 _Multiplier. If provisioned, the MTC device shall calculate the periodic LAU timer by multiplying T3212 (received from BCCH) with MTC_T3212 _Multiplier. MTC_T3212_Multiplier is also configured at MSC/VLR in order to derives new implicit detach timer. Alternatively, MTC_T3212_Multiplier may be part of an MTC subscription data stored in HLR/HSS and downloaded to MSC/VLR during attach procedure.

NOTE: The MTC device may need to be configured to apply the specific timer, e.g. whether to adopt the special timer value from broadcast information.

Editor's note: It is FFS if dynamic synchronization of MTC_T3212_Multiplier is needed between MSC/VLR and MTC device.

Alternatively, a separate setting for the T3212 timer can be added into the LAU procedure. Details for such solution including whether to add specific MS capability sent from the MTC device can be decided in stage 3.

For PS domain specific systems, in order to reduce periodic RAU/TAU signalling the granularity of T3312/T3412 and Mobile reachable timer can be increased. New binary coding can be added for example to indicate GPRS timer value is incremented in multiple of 10 or 100 decihours.

Editor's note: Exact changes to coding of the GPRS timer value is FFS and will be specified as part of stage-3 specification.

A long periodic RAU/TAU timer (T3312/T3412) or specific coding to deactivate the timers may be part of an MTC subscription data stored in HLR/HSS and downloaded to the SGSN/MME during the Attach procedure. During Attach and periodic RAU/TAU procedures the SGSN/MME sets the device's periodic RAU/TAU timer and the mobile reachable timer to long values or deactivate the timers according to the parameter received from the MTC subscription data. Alternatively, if periodic RAU/TAU timer is not stored as part of MTC subscription data, or if SGSN/MME is experiencing overload situation, or if MTC device indicates "Low priority Access", SGSN/MME may decide to set them to higher values or decide to deactivate them.

If the subscribed periodic timer changes the SGSN/MME provides the MTC device with the new timer value during the next RAU/TAU procedure. Alternatively the SGSN/MME can initiate an SGSN/MME-Initiated Detach procedure with a re-attach indication to enforce an Attach procedure and provide the MTC device with the new timer value.

For M2M devices that support both the PS and CS domains, an alternative implementation is that these devices are commanded to use Network Mode of Operation (NMO) I and use a long PRU timer in the PS domain. With NMO=I, the MSC deactivates its implicit detach functionality and the device only performs periodic updates to the PS domain. By using a new broadcast indication, the network operator can maintain the use of NMO=II for existing devices and only use NMO=I for M2M devices.

6.20.3 Impacts on existing nodes or functionality

Impacts to HLR/HSS:

- Support configuring and provisioning of periodic LAU/RAU/TAU information (e.g. MTC_T3212_Multiplier, T3312/T3412 timer value or special encoding to disable them) as part of MTC subscription.

Impacts on SGSN/MME:

- Support configuring and storing the periodic RAU/TAU information (e.g. T3312/T3412 timer value or special encoding to disable them) and mobile reachable timer for a particular MTC Device, according to the parameter received from the HSS/HLR.
- Support modification of periodic RAU/TAU and mobile reachable timer values, if the subscribed periodic timer value changes, and provide the MTC device with the new timer value during the next RAU/TAU procedure or by initiating detach with "re-attach indication".
- Support configuring longer timer values for RAU/TAU or disable them based on local configuration, if periodic timer is not present in subscription information, or if SGSN/MME is experiencing overload situation, or if the device indicates "low priority access".
- Support for an extended coding of the timers (e.g. T3312/T3412)

Impacts on MSC/VLR:

- Support configuring and storing the periodic LAU information (e.g. MTC_T3212_Multiplier).
- Using MTC_T3213_Multiplier to derive new implicit detach timer.
- Downloading MTC_T3213_Multiplier during the attach procedure, if it is stored as part of subscription data.

Impact on the MTC Device / UE

- Support pre-configuring MTC_T3213_Multiplier and calculating the periodic LAU timer.
- Configuration flag on whether to use MTC_T3213_Multiplier or special periodic timer value from broadcast information.
- MTC devices need to be able to read the NMO I indication in the broadcast information

Impacts on the RAN/GERAN:

- New broadcast indication telling specifically MTC devices to use NMO I (In UTRAN this can be an existing spare bit in one of the 'transparent containers' of NAS information that the UTRAN broadcasts),
- For CS domain system, generation of special periodic timer value in the broadcast information

6.20.4 Evaluation

Following conclusion can be drawn:

- For the protection of other networks in the case of one network's failure, long periodic timers seem to be useful in slowing down the rate at which low activity mobiles detect the network failure. Hence mechanisms with the minimal impact on VPLMN equipment are desirable.

- Extending the periodic timer in one domain (e.g. PS) and not the other (e.g. CS) will not slow down the rate at which mobiles detect network failure unless NMO=1 is used.

- Proposed solution does not avoid overload or provide a congestion control mechanism, but it provides a simple way to limit the signalling load in the network.

- Extending the existing periodic LAU/RAU/TAU timers and defining configuration of new parameter (MTC_T3212 _Multiplier) is fairly simple.

- MTC device indication of "Low Priority Access" to SGSN/MME can be added by using new IE on existing NAS messages.

- HLR/HSS control of the periodic timer ranges is useful longer term functionality. Operator can control the frequency of the periodic update performed by MTC devices by configuring the periodic timer related parameters in the MTC subscription database.

- Adding the new timer values or indication to broadcast information may have an impact on RAN and GERAN. In general Broadcast channels are a scarce resource.

Based on the above conclusion following items are proposed for normative work:

- Add normative stage 2 requirements for enabling the long periodic LAU/RAU/TAU update timer for MTC devices.

- Add encoding of the extended periodic LAU/RAU/TAU timers and MTC_T3212_Multiplier.

- Standardization and encoding for new subscription parameters in HLR/HSS for extended periodic LAU/RAU/TAU timers and MTC_T3212_Multiplier.

- Standardization of mechanism for MTC device to indicate "Low priority Access" to SGSN/MME/MSC.

- GERAN broadcast information and the existing NAS information broadcast by UTRAN is modified so that M2M devices can be commanded to use NMO=I (Gs interface) while existing devices use NMO=II.

6.21 Solution - Randomized triggering of time-controlled MTC operations

6.21.1 Problem Solved / Gains Provided

See clause 5.9, "Key Issue – Time Controlled"; clause 5.12, "Key Issue – Signalling Congestion Control."

6.21.2 General

Simultaneous operations by too many MTC devices especially at the beginning of the time period may cause serious network or MTC server overload. Therefore, the triggering of time-controlled MTC operations needs to be randomized.

The time-controlled operation can be triggered by MTC device or the network including MTC server. When triggered by the network, the operation of MTC device can be started after receiving paging from the network elements (e.g. SGSN/MME) or application-level data from the MTC server directly if the MTC device is online.

Therefore, two alternatives to randomize triggering point of time-controlled operation can be considered:

1) Randomization of triggering at the MTC device – The MTC device randomizes triggering of the operation over the authorized time-controlled period informed by the network or MTC server.

NOTE: The MTC devices shall not trigger operations due to signalling congestion/overload situations, e.g. based on access control by RAN via broadcast system information.

2) Randomized triggering from the MTC server – Based on the poll model for communications between MTC devices and the MTC server, the MTC server randomizes the initiation of communication for the MTC devices during the time-controlled period provided by the network.

NOTE: The MTC server shall quit triggering operations if indicated from the network due to signalling congestion/overload situations.

Editor's note: It is FFS how the MTC server can communicate with VPLMN when the MTC device is roaming.

Editor's note: It is FFS if applying the two above-mentioned approaches concurrently would be more beneficial. In other words, it is FFS if the operation of the MTC device should start immediately after the MTC device is paged or if it would be beneficial that the operation starts only after a randomly selected time.

6.21.3 Impacts on existing nodes or functionality

6.21.4 Evaluation

6.22 Solution – Rejecting connection requests by the SGSN/MME

6.22.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion and Overload Control", more specifically congestion control.

6.22.2 General

The solution is applied for both GTP and PMIP based EPC. A number of variants of rejecting connection requests by the SGSN/MME can be distinguished:

Rejecting connection requests per APN

The SGSN/MME and/or GGSN/PGW can reject connection requests targeted at a particular APN. When the MTC application uses a dedicated APN, the specific MTC application can be targeted that causes the congestion.

Rejecting connection requests and attach requests per MTC Group

The SGSN/MME can reject connection requests targeted at a particular MTC Group. With the attach procedure the MTC Group Identifier can be downloaded as part of the service profile from the HSS into the SGSN/MME. When a connection request is received by the SGSN/MME, the SGSN/MME can find in the service profile if the particular MTC Device is part of a MTC Group that causes congestion. In case only the GGSN/PGW is congested, the SGSN/MME need to be informed about which MTC Group is causing that congestion.

The SGSN/MME can reject attach requests on the basis of MTC Group is the only option. One option is that the MTC Group is downloaded from the HSS during the attach procedure. However this implies the service profile is only downloaded when most of the attach procedure is already done.

Another option would be to add the MTC Group ID to the connection requests and attach requests from the MTC Device. That way the SGSN/MME can easily identify that a particular request comes from a MTC Application that is causing congestion.

Rejecting service request and attach attempts based on MTC Device provided low priority access indication

With availability of an access priority indication from the MTC Device the SGSN/MME can take an early decision to reject the request. Depending on internal SGSN/MME congestion mechanisms the SGSN/MME can appropriately treat the "low priority access" (e.g. used by Time Tolerant MTC device) in comparison to other accesses.

The treatment can be performed without inducing or consuming further load in the SGSN/MME and the network as it could be performed prior to the download of the service profile from the HSS. The treatment could include returning an extended back-off time to the MTC Device requesting the "low priority access".

When using SGSN/MME level rejection of devices, care is needed to guard against the possibility that the devices use the result as a soft (or hard) trigger for network reselection. This is because triggering network reselection can lead to the device repeatedly, cyclically attempting access on all the local competing networks and adding load to all of them.

Providing a back-off time and a reject indication to the MTC Device

To avoid a MTC Device from re-initiating a connection request or attach request immediately after a reject to an earlier request, the SGSN/MME can provide a back off time to the MTC Device in the reject message. If it is the GGSN/PGW that sent the reject originally, the SGSN/MME may append a back off time to the reject message.

In case of large number of MTC Devices, to avoid them from re-initiating access requests simultaneously, the back off time should be randomized. SGSN/MME may randomize the back off time with certain range and assign it to each individual MTC Device directly.

Alternatively, SGSN/MME may just send "back-off time" to MTC device and the MTC device can randomize its local back-off time.

The reject message from the SGSN/MME may contain a reject indication informing the MTC Device about the reject cause. For example a reject indication could inform that there is a signalling congestion at the SGSN/MME, or overload at the GGSN/PGW, or restricted access per requested APN, or the QoS requirements of the requested PDN connection cannot be fulfilled etc.

The reject indication may inform the MTC Devices capable of dealing with multiple connections how to proceed when establishing additional connections. In one example the MTC Devices could be informed that no additional connection to a particular APN shall be established. In another example when the resources at the GGSN/PGW are limited per MTC Device, if the MTC Device has an existing connection and initiates an additional connection establishment, the reject indication can inform the MTC Device about the limited available resources. Additionally the MTC Device may be allowed to keep the already existing PDN connection(s) at time, and/or the MTC Device is allowed to establish multiple connections within the limited resources and/or number of possible PDN connections. In this case, if the MTC Device has an existing connection and has higher priority data to send over new connection, the MTC Device may decide to share the resources among the existing and additional connections or to release the existing connection and establish the new one. When the reject message contains reject indication together with a back off time, the reject indication is valid only during the back off time.

The MTC Device shall not re-initiate a similar request during the back off time depending on the reject indication.

The SGSN/MME may store the back off time for a particular MTC Device and immediately reject any subsequent requests from that MTC Device before the back off time is expired. A new (longer) back off time may be provided to further deter the MTC Device from repeated attempts before its back off time is expired.

Providing a back off time could also be a solution to the issue of recurring (quarter/half) hourly applications. If the MTC Device could identify the recurring applications, it could delay attach request or connection requests for these applications with the back off time. How to identify such recurring applications is unclear.

6.22.3 Impacts on existing nodes or functionality

Impact on the SGSN/MME:

Additional functionality for SGSN/MME with this solution includes:

- Rejection of a connection request targeted at a particular APN.
- Rejection of attach and connection requests by MTC Devices belonging to a particular MTC Group.
- Detection if an MTC Device is part of a particular MTC Group (e.g. based on subscription information requested from the HSS/HLR).
- Determining the MTC Group or APN that causes congestion, within SGSN/MME, or upon reception of indication from GGSN/PGW.
- Providing a reject cause including a back off time in the reject messages.
- Providing a reject indication in the reject message.
- Randomization of the back off time that is applicable for a particular MTC Device.
- Determination of the reject indication that is applicable for a particular MTC Device and connection.
- (For SGSN) Indicating MTC Group ID to GGSN.

- (For MME) Indicating MTC Group ID to SGW.
- In the case that the MTC device supports the Time Controlled feature and the subscriber data is available, based on implementation the SGSN/MME may take this into consideration when calculating a wait time.
- In the case of the SGSN/MME rejecting a service request the Mobile Reachable Timer may be compensated by the extended wait time to take into consideration that a periodic TAU/RAU may be suppressed during this period.

Impact on the MTC Device / UE:

Additional functionality for the communication module in MTC Device / UE with this solution includes:

- Not re-initiating further attach or connection requests before the back off time is expired, if timer value is provided by the network.
- Possibly needing to randomize the local back off time according to the back off time received in reject signalling, if such information is provided by the network.
- Determining how the MTC Device deals with additional connections depending on the reject indication.
- Handling of reject causes such that network reselection is not triggered.
- Capability to configure the device with a low priority indication.

Impact on the SGW:

Additional functionality for SGW with this solution includes:

- Forwarding MTC Group ID received from MME to PGW.
- Forwarding low priority device indication to PGW.
- Forwarding the overload/congestion situation indication received from PGW to MME for a particular APN or MTC Group.
- Forwarding a reject cause in the reject messages received from PGW to MME.
- Forwarding a reject indication in the reject messages received from PGW to MME.

Impact on the GGSN / PGW:

Additional functionality for the GGSN and PGW with this solution includes:

- Detecting the overload/congestion.
- Determining the MTC Group or APN that causes overload/congestion.
- Rejection of a connection request targeted at a particular APN.
- Rejection of connection requests by MTC Devices belonging to a particular MTC Group, possibly taking the low priority device indication into account.
- Indicating the overload/congestion situation to SGSN/MME for a particular APN or MTC Group.
- Suggesting value of back off time to SGSN/MME.
- Providing a reject cause in the reject messages.

Impact on the HSS/HLR:

Additional functionality for HSS/HLR with this solution includes:

- Storing the MTC Group Identifier as part of the subscription profile of an MTC Device.

Impact on the PCC:

- Forwarding MTC Group ID received from MME to PGW (via BBERF, PCRF, PCEF).

Editor's note: It is FFS how PGW exactly indicates the congestion situation back to MME and how SGW (BBERF) correlates such information.

Editor's note: It is FFS if PCC needs to be used. PMIP mobility related information may be used instead.

6.22.4 Evaluation

In the case that the MTC device also supports the Time Controlled feature and the subscriber data is unavailable, the calculated wait time may coincide with a Time Controlled "Forbidden Time Interval". This is not considered significant as the MTC device as per Time Control implementation would access the network at the next available Grant Time Interval.

Benefits:

- Low impact on existing 3GPP RAN standards and products.
- Allows for CN node specific load control in flex or sharing scenarios (in UTRAN and E-UTRAN, but not GSM)
- For roaming scenarios, the SGSN/MME rejects or accepts the connection requests of roaming MTC device based on the load situation and operator's policy.
- Within the network, only requires changes to core network nodes
- By using back-off time, devices are prohibited from generating any more signalling traffic, both in the core network and in the radio network, from requests that would be denied anyway.
- Back-off times allow for peak shaving; making more efficient use of existing capacity.

Drawbacks:

- This solution consumes the RAN and CN resource even at the congestion and overload situation.
- Requires updates to mobiles (their behaviour while a MM/GMM/EMM and/or CM/SM/ESM back off timer is running needs to be defined, specified and tested).

6.23 Solution – Low Priority Access Indication

6.23.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control", more specifically overload control; and 5.14 "Key Issue - Potential overload issues caused by Roaming MTC devices".

6.23.2 General

This solution introduces the concept that access attempts from certain MTC devices or applications (e.g. "time tolerant" utility meters) can be treated as a low priority requests.

In the abnormal case of congestion due to many simultaneous connection requests it is of benefit that the connection requests are rejected as early on in the access procedures such that resources are not consumed or induced further into the network.

NOTE: It is assumed that the network is appropriately dimensioned i.e. congestion or close to maximum resource usage is an abnormal situation.

This solution addresses (unexpected) unacceptable high load resulting from MTC devices in the Low-Priority-Access category. High load resulting from MTC devices out of this category is not covered.

This is a solution that avoids problems in the network that affects both MTC devices that do and MTC devices (in the Low-Priority-Access category) that do not generate an unacceptable high load.

At a high level the following stages occur for UE access from RRC Idle state:

1. Read broadcasted System Information
2. Identifying a RACH opportunity

3. RRC Connection Establishment (E-UTRAN/UTRAN), Channel Request/EGPRS Packet Channel Request (GERAN)

4. Service Request, EPC ATTACH Procedure or GPRS ATTACH/PDP Context Activation)

At step 1 the access class barring mechanism can protect the network.

At step 2 contention based random access procedure exists for identifying an access opportunity on acquiring the Random Access Channel.

At step 3 reception of a priority indication at the access attempt can be used to manage access attempts in RAN (GERAN, UTRAN, E-UTRAN) prior to knowing (decoding and authentication) of the specific identity of the accessing MTC device.

At step 4, reception of a priority indication at the access attempt can be used to manage the requests received in the MME/SGSN early on in the process, i.e. prior to decoding any NAS messages of the accessing "time tolerant" MTC device is attempted. If the request is admitted the indication can also possibly be used to verify the behaviour towards subscription data for the MTC user. An extended use case of the indication can also be to propagate the information for charging purposes.

A priority indication allowing for "Low-Priority-Access" can be used to determine whether to reject the service request or attach attempt depending on the current load.

This indication can be used by MTC devices (e.g. "time tolerant" utility meters) during their normal operating access or access attempts following a power failure (i.e. mass simultaneous registration scenario) as means to request a "Low-Priority-Access". Note that in other scenarios these same devices when accessing the network could use other priorities as required. For example this may be the case of a MTC device supporting multiple MTC applications requiring different priorities (i.e. the MTC application will determine the priority to be indicated during an access attempt).

In the case of overload condition in the RAN, where RACH overload isn't a factor, the RAN may take the decision to reject these requests without further propagating signalling into the core network. In addition, the RAN can use the "low-Priority-Access" indicator to signal a longer back off time to a "low priority access" device compared to any back-off time sent to a normal UE (e.g. one attempting a voice call).

The MME/SGSN can initiate gradual overload procedures by first reducing low priority traffic. The MME/SGSN can notify the RAN to allow all traffic except low priority, using a similar overload mechanism as defined currently for requesting the RAN to reject all non-emergency traffic by sending the OVERLOAD START message.

In the absence of overload condition in the RAN or notification to RAN, the request is eventually transported to the SGSN/MME. Depending on internal MME/SGSN congestion mechanisms the MME/SGSN can appropriately treat the "Low-Priority-Access" request in comparison to other priorities. The treatment can be performed without inducing or consuming further load in the SGSN/MME and for example could be performed prior subscriber profile retrieval.

Also, the "Low-Priority-Access" should be passed to the GGSN/S-GW/P-GW. For Mobile Originating communication, in the absence of overload condition in the RAN and the SGSN/MME and the signal screening at the SGSN/MME for GGSN/S-GW/P-GW, the GGSN/S-GW/P-GW can appropriate treat the request related with the existing session marked as "Low-Priority-Access". For Mobile Terminating call, the S-GW can decide whether to send downlink data notification or not for the existing session marked as "Low-Priority-Access"

This indication conveyed by MTC Devices at the access attempt implies the MTC application is less critical. It can be used as a criterion by the network to determine which MTC Devices/bearers should be detached / deactivated prior to others in case of congestion. When the network status is normal without congestion, the "low priority" MTC Devices will be accepted by the network and bearers will be established. When the network starts to get congested, the already attached "low priority" MTC Devices or established "low priority" MTC bearers can be detached / deactivated first.

This Low Priority Access Indication can be used in combination with Group ID or APN, e.g. when the network decided to detach devices/deactivate bearers belonging to a certain group, the "low priority" MTC Devices within the group can be detached/bearers deactivated first, followed by the remaining devices in the group.

6.23.3 Impacts on existing nodes or functionality

In E-UTRAN a new RRC Establishment cause could be introduced. The purpose of the *RRC Establishment Cause* IE is to indicate to the eNB the reason for RRC Connection Establishment (ref TS 36.331 clause 6.2.1 - "RRCConnectionRequest" message). Existing values can indicate emergency, highPriorityAccess, mt-Access, mo-

Signalling, mo-Data. Following this model of "normal", emergency and high priority causes it is proposed that some MTC device accesses could be viewed as "Low-Priority-Access" as compared to the existing establishment causes. The *RRC establishment cause* IE is as currently specified (ref TS 36.413 clause 9.1.7.1) forwarded to the MME in the "Initial UE message" over the S1-AP protocol.

In the UTRAN case a new *establishment cause* could be used by MTC "time tolerant" devices in the RRC Connection Request. Signalling would be impacted to include the establishment cause such that SGSN can be made aware of a low priority access (e.g. by a MTC "time tolerant" device).

NOTE 1: the existing UTRAN establishment cause "Originating Low Priority Signalling" is used for mobile originating SMS and is unsuitable for re-use as this code-point.

For the GERAN case a priority indication may be introduced in the access message (e.g. EGPRS Packet Channel Request or by partial re-coding of the existing Channel Request message) to indicate when an access is attempted by an MTC device and the priority of the corresponding MTC message requiring transmission. The priority indication should allow for the equivalent of a "Low-Priority-Access". MM/GMM Signalling would be impacted to include a priority indication such that MSC/SGSN can be made aware of a low priority access (e.g. by a MTC "time tolerant" device).

NOTE 2: The above mechanisms are provided as examples. If the solution is supported, it is the responsibility of the RAN/GERAN to specify the messages and parameters in which the low priority indicator would be passed.

For E-UTRAN/UTRAN/GERAN, the OVERLOAD START message would need to support the ability to request RAN to reject low priority access requests.

For E-UTRAN, UTRAN and GERAN it is likely that the "low priority access" codepoint should be used for EMM, GMM and MM signalling as well as for initiating data transfer/responding to paging. However, some further study on this aspect may be needed.

The SGSN/MME should include the "Low Priority Access" indicator in the session create message in order to notify it to GGSN/S-GW/P-GW. A GGSN/S-GW/P-GW that experience overload, may decide to reject any additional "Low Priority" session creation requests in order not to increase its number of sessions and any potential traffic related to these sessions. If a GGSN/S-GW/P-GW reject a session create request due to an overload condition, a specific reject cause shall be indicated back to the SGSN/MME so that the SGSN/MME can take appropriate action (e.g. try another GGSN/S-GW/P-GW instead or reject with a wait time).

A low priority access indication usage control parameter may be pre-configured (e.g. at manufacturing) or set via OMA device management in the MTC Device SIM/USIM to allow for:

- MTC Device that uses the low priority access indication for all its access attempts
- MTC Device that uses the low priority access indication for all its delay tolerant accesses attempts, but which may use other priorities for services that require immediate response

The MTC Device low priority indication usage could be according to the Service Level Agreement (SLA) established between the mobile operator and the MTC service provider.

SGSN/MME/GGSN/P-GW are required to store the "Low-Priority-Access" indication for each attached MTC Device. SGSN/MME need to forward this indication to GGSN/P-GW.

6.23.4 Evaluation

Benefits:

- Should be possible to easily add parameters/mechanisms to the UTRAN and E-UTRAN RRC protocol and to GERAN although the network's support/non-support for these new parameters may probably need to be broadcast.

NOTE: Whether necessity to broadcast network's support/non-support for these new parameters should be decided at the stage 3.

- Works in a roaming environment. A network upgraded with "low priority" functionality can take advantage of this as soon as there are terminals also supporting this regardless if terminals are roaming or not.
- Low impact on existing 3GPP standards and products and may be feasible in Rel-10.

- allows for CN node specific load control in flex or sharing scenarios

- Initially provides, from the time RAN decides to start rejecting low-priority-access requests until the first low-priority-access barring is broadcast in system information, a faster way to protect from overload compared to mechanisms relying on broadcasted system information (e.g. ACB)

- Allows GGSN/S-GW/P-GW to handle signalling overload appropriately

- Allows the UE flexible access to the network by indicating the priority that is suitable for use (e.g., low priority MTC service vs normal priority when not in MTC low priority mode).

- Provides a criterion for the network to determine the MTC Devices to be detached / bearers to be deactivated for congestion control.

Drawbacks:

- Doesn't allow to switch off specific groups or applications (vs. broadcasting in system information which can prevent low-priority-access requests from devices that have not received access rejections).

- the node specific load control or network sharing specific control might not work if the device signals the IMSI instead of temporary IDs e.g. during PLMN changes

- As it bases on UE individual signalling it might not be possible to completely avoid Radio Resource congestion. There are also related work in RAN e.g. usage of concentrators.

- In the case that the MTC device also supports the Time Controlled feature, the calculated wait time may coincide with a Time Controlled "Forbidden Time Interval". This is not considered significant as the MTC device as per Time Control implementation would access the network at the next available Grant Time Interval.

6.24 Solution - Directly Reporting to MTC Server from CN entity

6.24.1 Problem Solved / Gains Provided

In the MTC Monitoring solution, clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General", the MTC Event Reporting entity (e.g. SGSN/MME or GGSN/PGW or PCRF) is not aware of the MTC Server identity, thus it cannot send the MTC Event Report to the MTC Server.

6.24.2 General

In this solution, the MTC Server identity (e.g. FQDN or IP address) is stored in the HLR/HSS as part of MTC subscription per MTC device or per MTC group, and is downloaded to the SGSN/MME through Insert Subscription Data procedure. The SGSN/MME then stores this MTC Server identity.

If the CN entity for MTC Event Reporting is the GGSN/PGW, the SGSN/MME transfers the MTC Server identity to the GGSN/PGW through Create PDP Context Request / Create Session Request, or carries the MTC Server identity within the MTC Event Report when it sends MTC Event Report to the GGSN/PGW, and PCEF may send the Event Report to PCC if GTP is used over S5/S8. If PMIP is used, these information are transferred via PCC i.e. BBERF sends MTC Event Report to PCRF.

If the CN entity for MTC Event Reporting is the PCRF, after receiving the MTC Server identity, the GGSN/PGW then transfers the MTC Server identity to the PCRF through PCC procedure, or carries the MTC Server identity within the MTC Event Report when it sends MTC Event Report to the PCRF. The PCRF uses the MTC Server identity to send MTC Event Report.

If the MTC server is out of the operator control, a security connection between the CN entity and the MTC server may be needed.

Editor's note: It is FFS how to setup a security connection to the MTC Server, and where the security connection information is stored and how to establish the secure connection.

Editor note: It is FFS how to report MTC events to multiple MTC servers.

6.24.3 Impacts on existing nodes or functionality

HLR/HSS:

- The HLR/HSS stores the MTC Server identity as part of MTC subscription.

SGSN/MME:

- SGSN/MME stores the MTC Server identity
- The SGSN/MME includes the MTC Server identity in the Create PDP Context Request / Create Session Request.

GGSN/PGW:

- The GGSN/PGW includes the MTC Server identity during the Gx session procedure to the PCRF.

SGW(BBERF)

- The BBERF forwards the MTC Server identity during the Gxx session procedure to the PCRF, if PMIP is used over S5/S8.

PCRF

- The PCRF receives MTC Server Identity from PCEF (if GTP is used over S5/S8) and from BBERF (if PMIP is used over S5/S8)
- The PCRF uses the MTC Server identity to send MTC Event Report.

6.24.4 Evaluation

6.25 Solution - Reporting to MTC Server through the intermediate node

6.25.1 Problem Solved / Gains Provided

See clause 6.24.1.

6.25.2 General

In this solution, there is an operator controlled intermediate node (e.g. MTC Monitoring GW or IWKF) deployed to collect MTC event reports. The CN entity for MTC event reporting (e.g. the SGSN/MME or GGSN/PGW or the PCRF) sends MTC Event Report to this intermediate node, and the intermediate node then gets the corresponding MTC server identity and forwards the MTC Event Report to that MTC server.

The CN entity for MTC event reporting can get the identity of this intermediate node through the following methods:

A) Static configuration based on the local configuration for the home PLMN or the roaming agreement for the visited PLMN.

B) The MTC subscription from HLR/HSS.

The CN entity for MTC event reporting needs not know where the MTC server is, the intermediate node will find MTC server through the following methods:

The intermediate node locally configures the MTC Server identity.

Or, the MTC Server(s) contact the Intermediate Node (e.g. the3GPP PLMN-MTC Server IWK Function) and register. The Intermediate node then requires no configuration or information from the CN to locate the MTC Server(s).

If the MTC server is out of the operator control, the security connection between the intermediate node and the MTC Server may be needed.

Editor's note: It is FFS how to setup a security connection to the MTC Server, and where the security connection information is stored.

Editor's note: Whether there are changes to the roaming architecture and message flow are FFS.

Editor's note: It is FFS whether new interface between the CN entity and the intermediate node is introduced.

Editor's note: It is FFS how to report MTC events to multiple MTC servers.

6.25.3 Impacts on existing nodes or functionality

HLR/HSS:

- The HLR/HSS stores the intermediate node identity as part of MTC subscription if the CN entity for MTC event reporting gets the intermediate node identity from HLR/HSS.

CN nodes for MTC event reporting (SGSN/MME, GGSN/PGW, PCRF):

- The CN entity for MTC event reporting shall send MTC Event report to the intermediate node (e.g. MTC Monitoring GW or IWKF) located in the HPLMN.

- A new network entity (e.g. MTC Monitoring GW) may be introduced and new interfaces are introduced.

Editor's note: Whether there are additional impacts in roaming scenario is FFS.

6.25.4 Evaluation

6.26 Solution – Rejecting RRC Connection and Channel Requests by the eNodeB/RNC/BSS

6.26.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control", more specifically overload control, and 5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices".

6.26.2 General

This solution introduces the concept that accesses from certain MTC devices (e.g. "time tolerant" Utility meters) can be treated as a low priority access and could be rejected with an extended wait time.

In the abnormal case of massive simultaneous connection requests it is of benefit that the connection requests be rejected as early on as possible in the access procedure such that resources are not consumed or induced further into the network.

NOTE: It is assumed that the network is appropriately dimensioned i.e. congestion or close to maximum resource usage is an abnormal situation.

This solution addresses (unexpected) unacceptable high load resulting from MTC devices in the Low-Priority-Access category. High load resulting from MTC devices out of this category is not covered.

This is a solution that avoids problems in the network that affects both MTC devices that do and MTC devices (in the Low-Priority-Access category) that do not generate an unacceptable high load.

In the case of priority indication being received from the MTC Device the RAN (E-UTRAN, UTRAN, GERAN) has the opportunity to reject the connection request with a wait time that is appropriate for the access priority indicated by the MTC Device.

It is proposed that the existing wait time range in the rejection messages be extended to allow better control of such MTC "Time Tolerant" devices.

It is proposed that a new "extended wait time" could potentially range in the order of minutes or even hours.

With this potentially wide timer range the RAN could have for example the logic to assign a wait time ranging from 5 to 60 minute or even from 1- 24 hours to better control the MTC devices and ensure an even distribution of future incoming requests of low priority accesses into the system.

Some care is needed to ensure that these rejections do not lead to network reselection attempts that repeatedly load the local competing networks.

To ensure an even distribution of the re-initiated access attempts by a large group of "low priority access" MTC Devices, it is proposed that, when allocating the extended wait time for a MTC Device, eNB/RNC/BSS could apply randomization of the extended wait time within the overall maximum allowed wait time, and optionally allocate longer wait times to "low priority access" MTC Devices compared to that for normal MTC Devices.

The randomized wait times allocated to MTC Devices should be different from one another as much as possible. On the other hand, for each MTC Device, the start time of re-initiation is the current time of rejection + randomized wait time. When the wait time is being randomized, the current time of rejection should also be taken into account to ensure that the start time of re-initiation of different MTC Devices is sufficiently different from one another.

Alternatively, eNB/RNC/BSS could send one "reference wait time" to the MTC Devices, and each MTC Device calculates its own randomized offset time independently. Then for each MTC Device, the start time of re-initiation could be calculated as current time of rejection + reference wait time (from the network) + randomized offset (calculated by individual MTC Device).

6.26.3 Impacts on existing nodes or functionality

The E-UTRAN, UTRAN and GERAN would be impacted by the introduction of an extended and randomized wait time whose range would extend beyond the following documented values:

- For E-UTRAN the RRC Protocol Spec (36.331 v.9.1.0) shows a waitTime of between 1-16 seconds for the RRCConnectionReject.
- For UTRAN the RNC (25.331 RRC UTRAN) can return an RRC Connection Reject which includes a waitTime of between 0-15 seconds.
- For GERAN the BSS (TS 44.018 RRC) can return an IMMEDIATE ASSIGNMENT REJECT which includes wait indication octet (i.e. 0-255 seconds).

E-UTRAN, UTRAN and GERAN devices and networks extended and randomized wait time support would benefit from support of the Low priority access value (see solution "Low Priority Access Indication") that is indicated by the MTC Device when the MTC Device attempts to connect to the network and evaluated by the RAN when allowing/rejecting the request.

MME/SGSN in the case of MTC devices shall set the mobile reachable timer to be longer than the periodic update timer used by an MS and may take into consideration (i.e. through configuration) the value of the extended wait time that the RAN may use when rejecting channel requests in overload conditions.

MTC Devices receiving an extended wait time shall start any necessary the periodic update procedure following expiration of the extended wait time.

Impact on the MTC Device/UE

Additional functionality for the communication module in MTC Device/UE for this solution includes:

- Possibly randomizing the local offset time according to the reference wait time received in RRCConnectionReject/ IMMEDIATE ASSIGNMENT REJECT, if such information is provided by the network.
- Not re-initiating further attach/connection requests before the extended wait time is expired.

6.26.4 Evaluation

Benefits:

- Based on an existing concept of a wait time parameter in the E-UTRAN, UTRAN and GERAN protocols.
- Works in a roaming environment as solution is not dependent on coordinating any specific MTC application level identifiers between operators. Instead broad control is possible in the serving network based on devices

making access attempts as a low-priority-access. If a rejection is required an extended wait time can be returned for those accesses.

- Low impact on existing 3GPP standards and products and may be feasible in Rel-10.
- allows for CN node specific load control in flex or sharing scenarios (in UTRAN and E-UTRAN, but not GSM)
- Provides a faster way to react to varying levels of overload/unused capacity compared to mechanisms relying on broadcasted system information (e.g. ACB.

Drawbacks:

- Doesn't allow to target specific MTC groups or applications
- Allows each unique low-priority-access device to send a connect request followed by a corresponding reject sent by the RAN, thus adding to the current congestion load in the RAN (vs, broadcasting which can prevent the remaining low-priority-access devices from sending any access requests).
- In the case that the MTC device also supports the Time Controlled feature, the calculated wait time may coincide with a Time Controlled "Forbidden Time Interval". This is not considered significant as the MTC device as per Time Control implementation would access the network at the next available Grant Time Interval.
- Doesn't protect the core/centralized network elements in the case that, say, two M2M mobiles per cell access every cell in the network at the same time.

6.27 Time Control Solution Summary

This solution considers the Time Control MTC Feature Solutions thus far included in the TR and several that have not yet been included. The goal is to make progress towards understanding the solution space better and facilitating a comparison of alternatives. This solution neither replaces other existing solutions in the TR nor do the summarized solutions necessarily suffice as a 'key issue solutions.'

Table 6.27-1

Solution	Status	Randomization of Communication Window in the Grant Time Interval	Informs MTC Device of altered Grant Time Interval	Informs MTC Server or User of altered Grant Time Interval	Enforcement of Grant Time Interval and Forbidden Interval	Information Storage of Grant Time Interval and Forbidden Interval
1) Network Access Control by the PLMN	6.7	Not considered in solution 6.7 yet.	(1) The MTC Server via application level data (2) MME/SGSN via NAS initially or when the time period changes (accepting the first access outside the interval or informing when to use the network.)	"The network provides the information."	GGSN/P-GW (for charging and stopping data transmission.) MME/SGSN may prevent access outside of the Grant Time Interval.	HLR/HSS, SGSN/MME may alter the Grant Time Interval to conform with local policies.
2) "Randomized Time Control" [S2-102404]	tdoc	Either in the HSS or in the MME or SGSN (if local policy is applied.) A time window is selected within the Grant Time Interval to uniformly distribute access	(1) O&M procedure (2) NAS procedures as per 6.7 or during Grant Time Interval initiated by the MME/SGSN (notifying the MTC Device). Also synchronizes the device with respect to the MME/SGSN.	Not discussed	As 6.7	In HSS/HLR (the time window is stored along with the grant time interval and forbidden interval).
3) "Time control for MTC Time Controlled" [S2-102588]	tdoc	The MME or SGSN selects a random start time and duration. Local policy may reset the start time and duration to a new value.	NAS procedure communicate the time window during attach or connection request. A time stamp may be added by the network to synchronize the MTC Device to the network	Not discussed	As 6.7	In HSS/HLR (the grant time interval and forbidden interval)
4) "Allowed Time Period after TAU/RAU" [S2-102572]	6.17	The TAU or RAU will occur randomly within the Grant Time Interval.	"The EPS network configures the MTC Device ... according to operator requirements and MTC subscription options." NAS will be used	Not discussed	Not discussed	Presumably in the HSS/HLR for subscription options.

Solution	Status	Randomization of Communication Window in the Grant Time Interval	Informs MTC Device of altered Grant Time Interval	Informs MTC Server or User of altered Grant Time Interval	Enforcement of Grant Time Interval and Forbidden Interval	Information Storage of Grant Time Interval and Forbidden Interval
			to inform the length of the communication window.			
5) "Randomized triggering of time-controlled MTC operations"	6.21	1) the MTC Device 2) the MTC server	interval from the network or the MTC Server	by the network	Not discussed	Not discussed
6) PCRF based network access control [S2-102475]	tdoc	not discussed	The PCRF informs the MTC Device during IP CAN session establishment	The PCRF receives the grant time interval from the SPR	The PCRF rejects IP CAN sessions outside of the grant time interval or terminates IP CAN sessions that exceed the time limit.	SPR
7) Time control according to MTC Device Identifiers [S2-102330]	tdoc	Use of MTC Identifier to randomly distribute at a fixed point (based on a known start time and a randomized offset)	not discussed	not discussed	not discussed	not discussed
8) Time controlled feature via Operator and MTC Business Agreements [S2-102436]	tdoc	not discussed (It is asserted that the application will be 'well behaved' and randomize communication through the grant time interval.)	not discussed	off-line (the MTC User informs the MTC Server)	not discussed	not discussed
9) MTC Request to Release Resources [S2-102519]	tdoc	not discussed	the network sends this using NAS as part of detach or S1 release. The MTC Device may propose a time.	"The network then ... forwards the ... notification to the MTC User"	not discussed	not discussed
10) Proactive congestion control [S2-102225]	tdoc	Randomization algorithm in the device	Periodically through broadcast	not discussed (the network or the UE may notify the MTC Server/User when communication is granted)	not discussed (as 6.7)	Not necessary when this method is used.

6.28 Solution - Access Control by RAN

6.28.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control", more specifically congestion control and overload control and clause 5.14, "Key Issue – Potential overload issues caused by Roaming MTC devices."

6.28.2 General

To avoid and handle the overload situations caused by MTC Devices, the MME/SGSN can send OVERLOAD START message to the RAN node, O+M action can be directed to the RAN node, and/or internal congestion alarm in RAN node can trigger the broadcasting of access control for MTC Devices to avoid further access to the network. The OVERLOAD START message, O+M action and internal congestion alarm in the RAN can include specific MTC Access Class Barring (ACB) overload actions as follows:

- Coarse-grained access control for MTC Devices with "Low-Priority-Access". MME/SGSN, O+M action and/or internal RAN congestion alarm will request MTC access control with indication of "Low-Priority-Access". Based on that, RAN will broadcast "access barring for MTC Devices with Low-Priority-Access" in system information.

- Fine-grained access control for MTC Devices with specific group. MME/SGSN O+M action and/or internal RAN congestion alarm will provide group related access control information, (e.g. an MTC Group or specific APN,) to RAN node. Based on that, RAN node will broadcast "access barring for MTC Devices with specific group" in the system information; or

- Coarse-grained access control for MTC Devices with specific "PLMN type". MME/SGSN, O+M action and/or internal RAN congestion alarm will provide PLMN type related control information, i.e. "MTC Devices that are not on their HPLMN or a PLMN in the (U)SIM's preferred PLMNs list", "MTC Devices that are not on their HPLMN or an Equivalent HPLMN", "MTC Devices that are not on their HPLMN" and "all MTC Devices" ,, to RAN node and/or RAN will determine from internal. Based on that, RAN node will broadcast "access barring for MTC Devices with specific PLMN type" in the system information.

MTC access control with different granularities could be triggered by signalling thresholds in the RAN, SGSN/MME and/or GGSN/PGW. In the case of the GGSN/PGW, the GGSN/PGW informs the SGSN/MME when a congestion threshold is exceeded. P-GW/GGSN can reject the connection request for a particular MTC group, e.g. a specific APN, when the congestion control policy is trigged, and indicates a delay value to the MME/SGSN in the reject message. The delay value is set by P-GW/GGSN for the requested MTC group. By receiving the reject message, MME/SGSN can reject the connection request described under "6.22 Solution – Rejecting connection requests by the SGSN/MME" for the corresponding MTC group until the delay value expires, and the MME/SGSN can also be triggered to provide the congestion indication to RAN nodes.

NOTE 1: This functionality is supported for both PMIP and GTP based S5/S8.

Editor's note: It is FFS if and how access control for MTC Devices with specific groups can be triggered by signalling thresholds in the RAN.

Editor's note: This functionality is supported for both PMIP and GTP based S5/S8. It is FFS how PGW informs its congested status to the SGSN/MME.

When a SGSN/MME needs to trigger a MTC access control due to the MME/SGSN's load situation or the congestion indication received from P-GW/GGSN,, the SGSN/MME sends the specific OVERLOAD START message to the RANs (eNodeBs/RNCs/BSCs) specifically for MTC Devices, i.e. OVERLOAD START message with an indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group (e.g. MTC Group Identifier) of MTC access to be barred and any load status information.

Similar to general MME overload control procedures in TS 23.401 [5], the set of eNodeBs/RNCs/BSCs to send an OVERLOAD START message should be randomly selected (so that if two SGSNs/MMEs within a pool area are overloaded, they do not both send OVERLOAD START messages to exactly the same set of eNodeBs/RNCs/BSCs) and, in total, be proportional to reflect the amount of load that the SGSN/MME wishes to reduce. In addition, the set of eNodeBs/RNCs/BSCs to consider sending an OVERLOAD START message may be limited to a particular location area or subset of eNodeBs/RNCs/BSCs (e.g. where MTC Devices of the targeted type are registered).

The RAN uses the information from the SGSN/MME in the OVERLOAD START message, from the O+M action or from the internal RAN congestion alarm t to determine if and when to broadcast the corresponding MTC ACB information in the system information to the Ues. Any barring factor and/or barring time or functional equivalent included in the barring information will be derived internally by RAN (similar to general ACB) but should take into consideration any load status information provided by the SGSN/MME or input from the O+M action.The RAN uses the information from the SGSN/MME in the OVERLOAD STOP message, from the O+M action, or from internal RAN congestion alarms to determine if and when to stop broadcasting the corresponding MTC ACB information in the system information to the Ues. The RAN should not have to wait for indication from or be prevented by SGSN/MME from starting or stopping the broadcast of a particular MTC ACB action.

NOTE 2: OVERLOAD START/STOP messages from SGSNs/MMEs to RAN are considered amongst other inputs that can influence the decisions RAN ultimately makes in management of MTC access barring.

When using pooling of CN nodes, the RAN shall only broadcast a SGSN/MME-triggered MTC overload action when all connected MMEs/SGSNs from the same pool area have enabled the MTC overload action. When only a subset have triggered the MTC overload action, the RAN shall instead reject RRC connection requests, as described in clause 6.26, for specific access to a barring SGSN/MME from a MTC Device type or group that the SGSN/MME is barring. An O+M or internally RAN-triggered MTC overload action can be broadcasted regardless of the set of SGSNs/MMEs that have enabled the same MTC overload action.

The MTC Device which is going to access the network will receive the broadcasted system information for MTC access barring and uses this information to determine whether this access is barred or not. If so the corresponding MTC Devices will delay the access to the network. Subsequent initial access attempts to the network will be randomized by each MTC Device using the last barring time or equivalent value(s) provided by the RAN.

Editor's note: Broadcasting access control barring information in a large area, e.g. whole PLMN, caused by GGSN/PGW congestion should be avoided.

A MTC Device priority (i.e. "low" or "normal") shall be configured in a MTC Device in order to determine when "Low-Priority-Access" is barred by the network,

Editor's note: It is FFS how to configure the MTC access priority in the MTC Device, e.g. SIM OTA or OMA DM.

Editor's note: It is FFS how MTC Device priority will be applied to all applications on the device for Rel-10.

The operator may configure in a MTC Device (using OMA DM) a penalty level to be applied (i.e. weighted) to the received barring factor and/or barring time or equivalent when MTC Low-Priority-Access is barred by all MTC Devices.

NOTE: When using a penalty level, computed barring values should not be less than originally ordered by RAN in order to prevent an MTC Device from gaining an advantage in access.

6.28.3 Impacts on existing nodes or functionality

Impact on the RAN:

Additional RAN functionality for RAN-triggered solution includes:

- For coarse-grained MTC access barring:
  - Determining when overall congestion situation within the RAN warrants starting/stopping a particular MTC ACB action
  - Broadcasting MTC access barring with the indication of the type (i.e. "Low-Priority-Access or one of the "PLMN type" options)
- For fine-grained MTC access barring:
  - Determining the MTC Group or APN that is causing congestion within RAN.
- Determine the barring time and/or barring factor or equivalent for a new MTC access barring start operation.
- Broadcasting MTC access barring with the indication of the type or group of MTC access to be barred, barring time and/or barring factor or equivalent in the system information to the Ues.

- Control via O+M input to the RAN node is less 'automatic' but impacts fewer network entities and may attract the human/management attention needed to handle cases of very high overload.

Additional RAN functionality for CN-triggered solution includes:

- Receive the OVERLOAD START/STOP messages from the SGSN/MME with the indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group of MTC access to be barred.
- Determine if CN provided OVERLOAD START/STOP request influences MTC ACB and/or RRC rejection operations for the requesting CN node and other CN nodes sharing a pool area with the requesting CN node.
- Determine the barring time and/or barring factor or equivalent for a new MTC access barring start operation.
- Broadcasting MTC access barring with the indication of the type (i.e. " Low-Priority-Access" or one of the "PLMN type" options) or group of MTC access to be barred, barring time and/or barring factor or equivalent in the system information to the Ues.

Impact on the SGSN/MME

Additional SGSN/MME functionality for CN-triggered solution includes:

- For coarse-grained MTC access barring:
  - Determining when overall congestion situation, within SGSN/MME or upon reception of congestion indication from GGSN/PGW, warrants starting/stopping a particular MTC ACB action.
- For fine-grained MTC access barring:
  - Determining the MTC Group or APN that is causing congestion, within SGSN/MME, or upon reception of indication from GGSN/PGW.
  - (For GGSN/PGW-triggered) Indicating MTC Group ID to GGSN/SGW
- Determining the proportion and specific set of RANs to send a new MTC ACB action.
- Sending the OVERLOAD START/STOP messages to the targeted RANs specifically for MTC Devices with the indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group of MTC access to be barred.
- For penalty level configuration:
  - A mechanism is required to configure a penalty level in the MTC Device to be used for processing MTC access barring information for Low-Priority-Access attempts by the MTC Device.

NOTE: The detailed message name and indication parameters should be specified in stage 3.

Impact on the HSS/HLR

Additional HSS/HLR functionality for CN-triggered solution includes:

- For fine-grained MTC access control:
  - Storing the MTC Group Identifier as part of the subscription profile of an MTC Device.

Impact on the SGW

Editor's note: It is FFS whether such information may be transferred via PCC, if PMIP is used on S5/S8.

Additional SGW functionality for PGW-triggered solution includes:

- For coarse-grained MTC access barring:
  - Forwarding the overall PGW congestion situation indication received from PGW to MME
- For fine-grained MTC access barring:
  - Forwarding MTC Group IDs received from MME to PGW

- Forwarding the congestion situation indication received from PGW to MME for a particular MTC Group or APN

Impact on the GGSN/PGW

Additional GGSN and PGW functionality for GGSN/PGW-triggered solution includes:

- The GGSN/PGW needs to provide the different overload actions for MTC Devices to the SGSN/MME node.
- For coarse-grained MTC access control:
  - Detecting the overall GGSN/PGW congestion condition.
  - Indicating the overall GGSN/PGW congestion situation to SGSN/MME.
- For fine-grained MTC access control:
  - Receiving MTC Group ID from SGSN/SGW.
  - Determining the MTC Group or APN that is causing congestion within GGSN/PGW.
  - Indicating the congestion situation within GGSN/PGW to the SGSN/SGW for a particular MTC Group or APN.

Impact on the MTC Device / UE

Additional functionality for the communication module in MTC Device / UE with this solution includes:

- The MTC Device needs to recognize the different MTC specific access control types and groups that are applicable to it.
- The MTC Device uses the latest received MTC access barring information to determine if, and for how long, not to initiate any access requests.
- For penalty level configuration:
- A mechanism is required to configure a penalty level in the MTC Device to be used for processing MTC access barring information for Low-Priority-Access attempts by the MTC Device.

6.28.4 Evaluation

Benefits:

- RAN and core network resource consumption can be avoided during congestion situation and there will be no further AS and NAS signalling initiated from the targeted, access barred MTC Devices.
- Can be used for both congestion control as well as overload control as described in clause 5.12.
- Can reuse existing UE functionality (e.g. GSM Immediate Assignment Reject already specifies Wait Times out to 255 seconds).
- With broadcasting MTC access barring it may be possible to completely stop congestion even if RRC and/or NAS signalling are almost instantaneously overwhelmed with access attempts.
- Different combinations of MTC ACB actions provides for a low impact on existing 3GPP standards and products that may be feasible in Rel-10 (e.g. coarse-grained via RAN and/or SGSN/MME triggering) while allowing reuse for expanded functionality in Rel-11 (e.g. fine- and coarse-grained via RAN, SGSN/MME and/or GGSN/PGW).
- Complements RRC and NAS access request rejection mechanisms i.e. initial few requests rejected and remaining subsequent requests prevented through MTC access barring.
- Barring time randomization or equivalent prevents simultaneous subsequent initial access attempts by a previously blocked group.
- Provides solution for "unhappy" VPLMN operator to handle signalling and VLR space congestion from roaming MTC Devices.

- For RAN triggered options:
  - Does not impact CN entities (coarse-grained options).
  - Permits the VPLMN to activate barring because of a situation reported by another PLMN operator and/or due to severe abnormalities in the levels of core network signalling to particular HSS(s).
- For CN triggered options:
  - Allows aggregated MTC specific congestion at the SGSN/MME and/or GGSN/PGW to be stopped and/or prevented without guaranteed signalling bandwidth for worse-case individualized access request rejections.
- For O+M triggered options:
  - An effective yet relatively simple solution for catastrophic overload is probably the use of O+M controlled "access class barring" functionality that can be used to bar e.g.:
    - "low value" M2M devices that are not on their HPLMN or a PLMN in the (U)SIM's preferred PLMNs list;
    - "low value" M2M devices that are not on their HPLMN or an Equivalent HPLMN;
    - "low value" M2M devices that are not on their HPLMN;
    - "low value" M2M devices;
  - This may be achievable with just 2 broadcast bits. Reducing the core network load by X% can be achieved by the O+M barring of X% of the base stations/Node Bs/eNodeBs.
- For coarse-grained options:
  - Not dependent on implementation of MTC Group Identifier support.
  - Allows for efficient encoding of MTC access barring information that should fit in the spare bits of pre-existing System Information messages used for Access Class Barring.
- For fine-grained options:
  - Does not impact/block MTC applications that are not causing a problem.
  - When a MTC application uses a dedicated APN, the specific MTC application that causes the congestion can be targeted.
- For penalty level configuration:
  - When broadcast MTC barring information includes uniform barring info toward all MTC Devices, a penalty level can be used to discriminate some MTC Devices (i.e. this selectively assigns MTC Devices an advantage or disadvantage).

Drawbacks:

- The broadcast information for access barring needs to be enhanced to restrict the further MTC device access with different granularity triggered by RAN, SGSN/MME or GGSN/PGW.
- Initially, from the time determined to start rejecting and barring connect requests from MTC Devices from a particular group until the barring is broadcast, not as fast as RRC and NAS signalling access request rejections.
- For CN-triggered options:
  - When using pooling of core network nodes, care is needed in the use of ACB functionality as it can limit load on all MMEs/SGSNs/MSCs in the pool.
  - Added complexity during MME/SGSN overload to determine cause of overload type (e.g. Group/APN, PLMN type and/or "Low-Priority-Access") in order to request specific MTC overload action when not combined with rejecting connection requests by the SGSN/MME in clause 6.22 (can uses same mechanisms within CN to make this determination).

  - Added complexity in RAN to evaluate CN MTC overload action request amongst status of other CNs, O+M request and internal RAN MTC overload process.

- For coarse-grained options:
  - Impacts MTC applications that are not causing a problem.
- For fine-grained options:
  - Requires enhancements for broadcasting one or more unique MTC Group Identifiers.
  - Requires enhancements to HLR/HSS to store the MTC Group Identifier as part of the subscription profile of an MTC Device
  - Requires new mechanisms for detecting and indicating between nodes the MTC Group or APN that is causing congestion

6.29 Solution – IP address assignment mechanisms

6.29.1 Problem Solved / Gains Provided

See clause 5.3. "Key Issue – Ipv4 addressing".

NOTE: The stage 1 requirement that an MTC Server in a public address space can successfully send a mobile terminated message to the MTC Device inside a private Ipv4 address space is not addressed by this solution.

6.29.2 General approach based on existing standards

This solution shows how the key issue Ipv4 addressing can be addressed based on the mechanisms in the existing standards. Minor further optimization might be required. The alternatives outlined should be seen as examples and additional alternatives or variants may exist. An operator can choose to deploy one of the configurations for all its customers or deploy different configurations for different customers.

The MTC server is either deployed by the PLMN operator or by an application provider who owns an MTC Server and uses a specific APN assigned by the PLMN. In both cases a tunnelling mechanism is used between the GGSN/P-GW and the PDN of the MTC server to allow carrying the IP packets enabling assignment of private IP addresses to the MTC Devices. The tunnelling allows for connecting the PLMN with the MTC server(s) using public IP networks. Furthermore that tunnelling allows for setting up private network with multiple GGSNs/P-GWs and multiple MTC servers where every GGSN, P-GW or MTC server can be deployed at a different location. By using a separate APN per application (provider) the MTC servers from different applications can use the same overlapping private IP addresses as needed without the need for the network to implement a NAT function as the MTC devices and MTC servers belonging to one application share the same private IP address space.

Such a segregation of the traffic also reduces the motivation for subscribers to try to use this subscription for other purposes (e.g. free Internet service) since they cannot reach the public Internet. It also helps to simplify other operational issues, such as monitoring that all the MTC devices obey potential access restrictions like being active only during the network's low traffic periods. Traffic within this private intranet at other times would indicate the devices or applications are not working properly.

A PGW/GGSN can serve one or multiple APNs. A GGSN/PGW can be configured to use an AAA server for address allocation and protocol configuration options notification. When serving multiple APNs the PGW/GGSN may be configured with an AAA server per APN. The use of the AAA server and the communication and security feature needed to dialogue with this / those AAA server(s) e.g. tunnel, IPSec security association are specified in TS 29.061 [4].

The following figure shows just one MTC server per PDN/APN. There may be however multiple MTC Servers in the same PDN/APN.

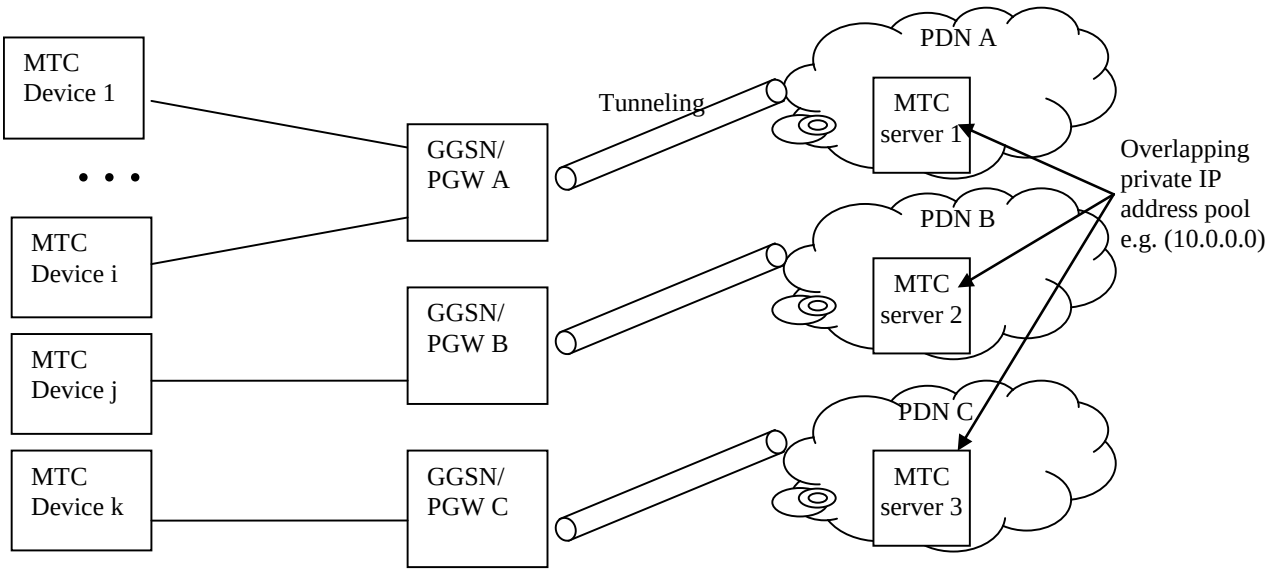


Figure 6.29.2-1: IP address assignment when the MTC Server is owned by the MNO or by a M2M Application Provider using a specific dedicated APN

In clause 6.29.5, the MTC Server is located on Internet (i.e. using an APN providing Internet connectivity) and hence no tunnelling is required between the GGSN/PGW and the MTC Server. This solution in clause 6.29.5 also assumes no NAT is used and is hence optimized for usage of Ipv6 addresses or public Ipv4 addresses.

6.29.3 IP address assignment by the PDN of the MTC server

A RADIUS or Diameter client at the GGSN/P-GW can obtain an IP address from the MTC server (providing an AAA server) upon receiving a PDP context/PDN connection request with the APN corresponding to the MTC server and assign that address to the MTC Device. The GGSN/P-GW indicates an MTC device provided PDN specific ID, an MSISDN or an IMSI to the MTC server when obtaining an IP address. Thereby the MTC server knows the IP address for an MTC device.

The application in the MTC Device may provide a PDN specific id potentially together with a related password in e.g., the PCO IE at PDP Context /PDN Connection establishment. Alternatively a PDN specific ID may be provided by the SGSN/MME at PDP Context /PDN Connection establishment. The PDN specific ID or the MSISDN or the IMSI are used to identify the MTC device. The ID is conveyed to the MTC Server when an IP address is requested via a RADIUS or Diameter interface from the MTC Server. The IP address assigned can be a private or public IP address. Overlapping IP address ranges can be handled by using different APNs.

A separate AAA server can be used to enable multiple MTC servers to forward MT data to an MTC device. The GGSN/P-GW obtains IP addresses from the AAA server and the AAA server updates the DNS entries of the DNS server functionality administered by the PDN with the assigned IP address. The MTC servers or other entities of the MTC User query the DNS server for the IP addresses of the MTC devices.

NAT functionality (along with related ALG) can be implemented by the MTC Server or on a separate entity if needed by the MTC business logic.

6.29.4 IP address assignment by the GGSN/P-GW

This is an alternative for the address allocation described in 6.29.3. In difference to the IP address allocation by an AAA server from the MTC specific PDN here the IP address is assigned by the GGSN/P-GW from a specific private or public address pool that is used for this particular APN. In the case when the address is a private, traffic will be tunnelled to the MTC Server(s).

The rest of the approach is the same as for 6.29.3. The application in the MTC Device may provide its PDN specific device id in e.g., the PCO IE at PDP Context /PDN Connection establishment. Alternatively a PDN specific ID may be provided by the SGSN/MME at PDP Context /PDN Connection establishment. The PDN specific ID, or IMSI or MSIDN are used as identity for the MTC device. Although the IP address is assigned locally, there can be RADIUS or Diameter signalling providing the AAA server with the IP address and the identity, which triggers the AAA server to update the DNS entry of the DNS server functionality administered by the PDN with a domain name including the

identity and the IP address. The same mechanism needs to be used to update the MTC Device DNS entry once the IP address is released by the GGSN/P-GW.

An alternate to the use of DNS is that the MTC Server receives AAA accounting messages from the GGSN/P-GW. The AAA accounting messages provide the MTC Server with the IP address assigned to the UE. From that the MTC server can also deduce the presence of the device (at accounting start) as well as when it is no longer available (e.g. accounting stop). This may for example be used by the MTC Server to decide when device triggering is required or not.

6.29.5 MTC Server located on Internet and public IP addresses for MTC devices

For this scenario a dedicated APN with public IP addresses is used for the MTC Server. A general APN for Internet access might not be used as the AAA server needs to provide a special interface towards MTC servers and also because updating an AAA server by a GGSN/P-GW is not necessarily required for every Internet APN. The IP address allocation is done by either the GGSN/PGW or by an AAA server within the PLMN domain. When the MTC device application registers its ID (PDN specific ID, IMSI, MSISDN) at the MTC server the MTC server can use an S_{MTC} interface to verify with the AAA server whether the MTC device with the specific ID got the IP address allocated.

The basic idea of the proposal is that it is left for the application layer in the MTC Device and the MTC Server to do the necessary registration of the MTC device and make an MTC device ID and its IP address known in the MTC Server. The 3GPP system provides the communication connection and a means to verify that the IP address is assigned to a specific ID (IMSI, MSISDN, PDN specific ID). A notification of bearer releases can optionally be provided to the MTC Server, e.g. for cases when the MTC Device cannot deregister because of lost coverage. Existing protocols and nodes are used in the 3GPP system and enhanced for this scenario here. This scenario assumes public Ipv4 addresses or Ipv6 addresses.

Editor's note: In case MTC Monitoring is part of Rel-10, the optional notification of bearer releases mentioned above may be replaced by corresponding MTC Monitoring features.

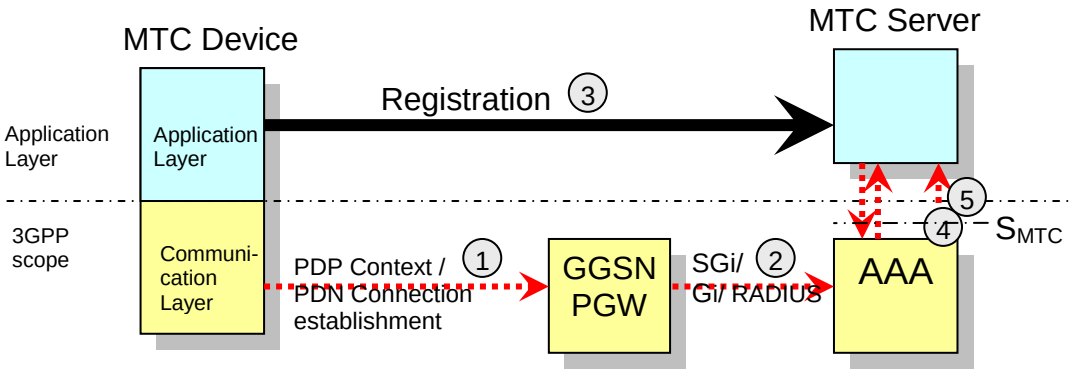


Figure 6.29.5-1: MTC Device doing registration at the MTC Server, authenticating the IP address, and subscribing to bearer releases from the network

The flow of events in the figure above:

1. The device establishes its communication connection by attaching to the network and creating a PDP Context or PDN Connection.

2. The Sgi/Gi/RADIUS protocol as specified in TS 29.061 [4] clause 16 is used to provide the IP address of the device to a AAA server. The AAA server stores the IP address as long as the bearer is active together with an ID (IMSI, MSISDN, PDN specific ID provided by MTC device in PCO). Optionally the PGW/GGSN may let the AAA do the IP address allocation. If a PDN specific ID is used the AAA server needs to be configured with a PDN specific ID for each MSISDN or IMSI. If a PDN specific ID is used the AAA server needs to verify that the UE provided ID matches the GGSN/P-GW provided IMSI or MSISDN. However the effort of configuring the UE might be avoided and the configuration of the AAA server, which is needed for verifying a UE provided ID, can directly be used to map the PLMN internal IMSI to an ID that can be used by the MTC application.

   The AAA Server is deployed in the PLMN.

3. The application in the MTC Device registers at the MTC Server. At a minimum the PDN specific ID or the IMSI or the MSISDN and the IP address of the device is provided.

Editor's note: It is FFS how to handle communication scenarios with multiple MTC Servers belonging to the same application/APN/PDN.

4. The MTC Server checks at the AAA Server the relationship between the IP address and the MTC Device provided ID thus checking the validity of the MTC Device provided id. This checking is the same mechanism as the GIBA mechanism that is already specified in TS 33.203. Only the PDN specific ID allocation needs to be managed in a different way.

NOTE: Similar restrictions and limitations apply as with GIBA, e.g. the IP address spoofing needs to be prevented.

5. A notification may optionally be sent to the MTC Server at a later stage when the PDP Context/PDN Connection is released and the IP address of the Device becomes invalid.

6.29.6 Impacts on existing nodes or functionality

This solution has a low impact on the existing mobile system as:

- RADIUS client is already part of the GGSN/P-GW as per TS 29.061 [4];
- Need to add a mechanism to dynamically update the DNS function in the MTC Server or on a separate DNS server. The existing RADIUS client in the GGSN (accounting message) may be used; in that case, the AAA server may need new functionality if not located on the MTC server.

An MTC device that needs to support simultaneous access to different MTC Servers associated with different APNs establishes multiple PDN connections and support multiple IP addresses.

6.29.7 Evaluation

Benefits:

- Avoids the need for NAT in the operator network as overlapping private IP addresses can be used among different MTC Servers on different APNs;
- Minimum or no impact on the existing standard/ existing Core Network nodes;
- the solutions described in 6.29.3 and 6.29.4 are generic IP-level solution that does not rely on application-level identifiers (e.g. SIP URI);
- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a "push" stimulus to an attached MTC device with an established PDN connection;

Drawbacks:

- requires tunnelling mechanism to be used between the GGSN/P-GW and the PDN of the MTC Server to enable assignment of private IP addresses to the MTC Devices;
- if the MTC device needs to have simultaneous access to MTC Servers associated with different APNs, the solutions described in 6.29.3 and 6.29.4 require that the MTC device support multiple PDN connections (i.e. multiple IP addresses);
- the solutions described in 6.29.3 and 6.29.4 may not be suitable for local breakout scenarios;
- the solution in 6.29.5 works with Ipv6 and public Ipv4 addresses only.

6.30 Solution - MME/SGSN overload control by DL MTC traffic throttling

6.30.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control".

6.30.2 General

An MME or SGSN starting to experience overload should be able to trigger partial or complete throttling of the signalling traffic generated by low priority MTC devices/applications while still allowing normal operations for other traffic (e.g. voice, data, signalling).

This solution specifically addresses throttling of DL traffic received on low priority PDN connections for MTC devices in ECM-Idle state or PMM-Idle mode, i.e. traffic for which the SGW would normally send a Downlink Data Notification message to the MME/S4-SGSN to trigger a network-initiated service request procedure.

An S4-SGSN or MME starting to experience overload (i.e. whose load exceeds a threshold to start MTC low priority traffic throttling) may reduce its load by requesting the SGW to throttle DL low priority MTC traffic for MTC devices in idle mode according to a throttling factor (%) and for a throttling delay specified in the request, e.g. within the Downlink Data Notification Ack message.

During that throttling delay, the SGW drops DL packets received on all its PDN connections marked as low priority served by that MME/S4-SGSN and without an S1/12 bearer in proportion to the throttling factor, and sends a Downlink Data Notification message to the MME/S4-SGSN only for the non throttled PDN connections.

The SGW resumes normal operations at the expiry of the throttling delay. The last received value of the MTC throttling factor and throttling delay supersedes any previous values received from that MME/S4-SGSN. The reception of an "MTC throttling delay" restarts the SGW timer associated with that MME/S4-SGSN.

When dropping a DL IP packet the SGW may send an ICMP packet (e.g. ICMP "destination un-reachable") that should tell the source that there is no use in repeating the packet.

When setting up the PDN connection, the MME/S4-SGSN signal to the SGW whether the PDN connection is for low priority MTC traffic or not.

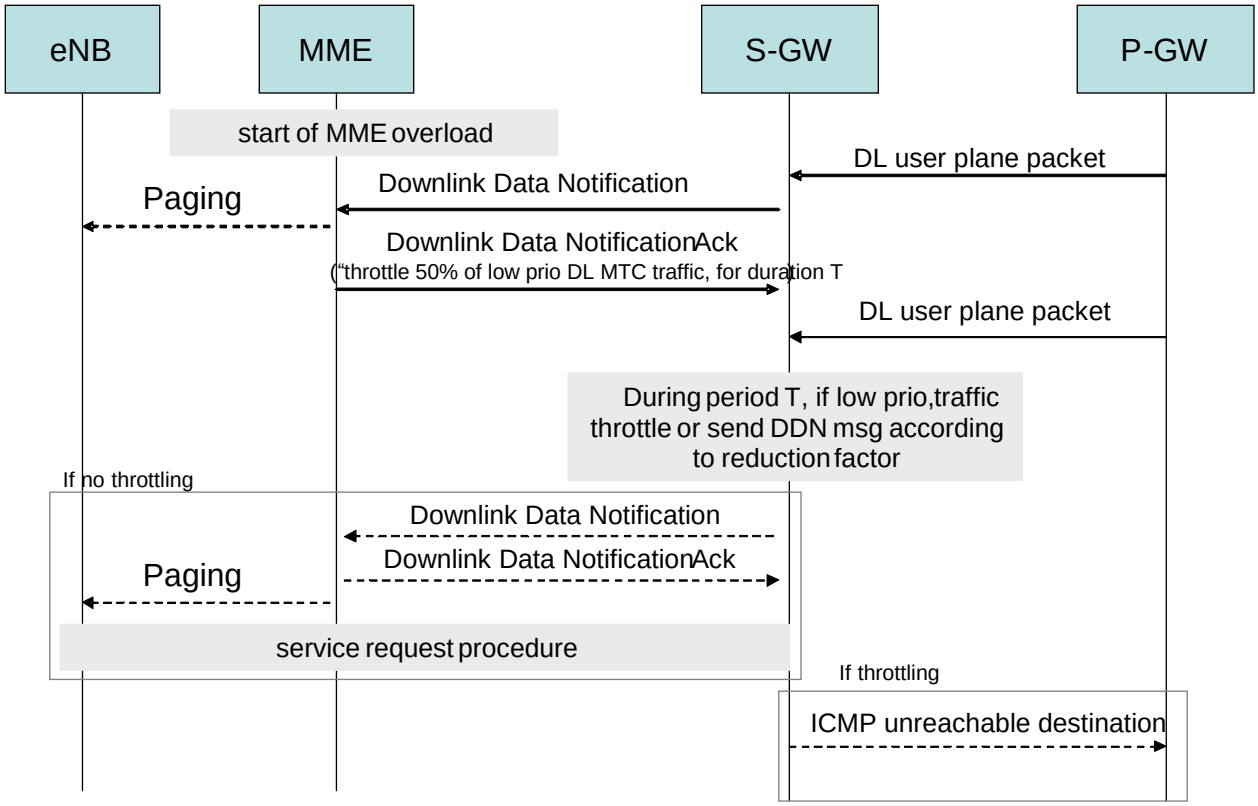


Figure 6.30.2-1

Editor's note: Any relation to ARP for the throttling mechanism in SGW is FFS.

Editor's note: Throttling in GPRS core is FFS.

This solution allows selective throttling of low priority DL MTC traffic in case of overload in the EPS Network, at the closest point of the source of the DL traffic. This allows to reduce immediately the load in MME/SGSN induced by low priority DL MTC traffic. It also allows to stop the sending of further DL packets by the application.

6.30.3 Impacts on existing nodes or functionality

MME/S4-SGSN signals MTC throttling parameters to the SGW.

The SGW throttles DL low priority MTC traffic according to the MME/S4-SGSN request.

6.30.4 Evaluation

This approach enables an MME/SGSN to reduce its load by reducing the signalling traffic resulting from DL user traffic received for PDN connections marked as low priority for MTC devices in ECM-Idle state or PMM-Idle mode (Downlink Data Notification / Downlink Data Notification Ack messages on S11/S4, paging and service request procedures).

It provides mainly benefits by protecting MME/S4-SGSN from massive simultaneous push or poll transactions from ("badly implemented") MTC server for devices with established low priority PDN connections.

It is complementary to an UL MTC signalling traffic throttling approach.

6.31 Solution – Rejecting connection requests at partial signalling links

6.31.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion and Overload Control", more specifically congestion control.

6.31.2 General

MTC devices maybe concurrently attempt signalling interaction only in a limited area. That means the signalling congestion could occur just in one or several particular signalling links and no overall congestion appears on network elements. For example, in 2G network, the link congestion would be met frequently for Gb interface over Frame Relay because of limited capacity of the interface protocol. It is not appropriate to reject all the MTC related signalling requests receiving from every signalling link for the control of the congestion existed only at partial signalling links.

Editor's note: It is FFS whether this problem can be addressed purely as a network element implementation issue or by means of an effect application of mechanisms available through SCTP, to be further studied in stage 3.

Rejecting signalling requests at separate signalling links

The signalling link could be the connection between BSC/RNC and SGSN or eNodeB and MME. SGSN/MME or other network functions (e.g. OAM) shall detect whether the congestion caused by MTC devices just occurs at the partial signalling links or the overall network node. Upon the congestion of the partial links, SGSN/MME can reject MTC related signalling requests received from other network nodes at one or several signalling links.

Rejecting signalling requests at a single signalling link set

A signalling link set contains all links connecting to a single BSC, RNC, eNodeB, RA or TA (List). The SGSN/MME or other network functions (e.g. OAM) shall detect whether the signalling congestion caused by MTC devices just occurs within one kind of link set or not. If yes, SGSN or MME can reject all MTC related signalling requests belonging to a BSC, RNC, eNodeB, RA or TA (List).

The mechanism of back-off time to the MTC Device as described in the clause 6.22 is also applicable for this solution.

6.31.3 Impacts on existing nodes or functionality

Possible impacts on SGSN/MME

- Rejection of a connection request targeted at a particular signalling link

- Rejection of a connection request targeted at signalling links connecting to a BSC, RNC, eNodeB, RA or TA(List).
- Detection if the congestion only occurs on one or several signalling links.
- Detection if the congestion only occurs on signalling links belonging to one BSC, RNC, eNodeB, RA or TA(List).
- Providing a reject cause including a back off time in the reject messages (same as the solution specified in 6.22),
- Determination of the back off time that is applicable for a particular MTC Device (same as the solution specified in 6.22).

Possible impact on the MTC Device / UE

- Same as the solution specified in 6.22.

6.31.4 Evaluation

Benefits

Avoids that most innocent MTC signalling requests are rejected when congestion only occurs on partial signalling links.

Drawbacks

MME/SGSN will make more complex detections for the congestion.

6.32 Solution – Rejecting connection requests based on request types

6.32.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion and Overload Control", more specifically congestion control.

6.32.2 General

Sometimes the congestion is triggered only by part of MTC devices controlled by one APN or one MTC group. For example, parts of MTC devices belonging to an APN concurrently attach to the network and cause the congestion for the network node. At the same time the other MTC devices with the same APN that already have PDP context and are in IDLE state attempt Service Request to the network, and their requests will be rejected.

Additionally, the different signalling request indicates the different application's appeal. For example, Attach request with Follow-on indicator may mean a MTC device wants to initiate data transfer immediately, which is more important than the one without Follow-on indicator. If undistinguished signalling rejection by the network node is executed on the congestion time, any MTC device requests can not survive. In fact the congestion may be also released while keeping some important requests unaffected.

Two alternatives to accomplish the solution of rejecting connection requests based on signalling types can be considered.

1) The network node count numbers of different kinds of signalling requests around the congestion time. The O&M periodic counting data created in the nearest time to the congestion occurrence can be used. The network nodes reject one or more signalling requests with the largest amount and extend the scope of rejection until the congestion disappears.

Editor's note: It is out of the specification scope how to get the O&M statistic data for the signalling requests.

2) The operator or MTC users provide the configuration for the priority of different kinds of signalling requests. The network nodes reject one or more signalling requests with the lowest importance firstly and extend the scope of rejection until the congestion disappears.

The both alternatives could be used together for congestion control. How many kinds of signalling requests shall be selected once time to the rejection list can be decided by the operator's configuration.

The mechanism of back-off time to the MTC Device as described in the clause 6.22 is also applicable for this solution. This solution could be used together with other basic solutions for congestion control, e.g. solution .6.22 Rejecting connection request per APN or MTC group.

6.32.3 Impacts on existing nodes or functionality

Additional impacts on CN nodes (SGSN, GGSN, MME, S-GW, P-GW)

- Rejecting a connection request with a particular type
- Counting numbers of different kinds of signalling requests in the statistics period nearest to the time of congestion occurrence.

6.32.4 Evaluation

Benefits

On the congestion time part kinds of signalling request can still be handled normally.

Drawbacks

Rejecting part kinds of signalling request at the beginning and extending the signalling scope of rejection gradually may not resolve the congestion in a short time.

6.33 Solution – UE behaviour changes

6.33.1 Problem Solved / Gains Provided

5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices".

6.33.2 General

The scenarios outlined in clause 5.14 highlight some areas where the UE internal behaviour would benefit from small but important changes:

a) the ability to remotely configure a device as, a "low value M2M" device. Typically this could be done via OMA DM.

b) modification (increase) of the minimum value of the timer for the background PLMN search, e.g. to greater than one hour, for a "low value M2M" device. This UE internal value would over-rule any smaller value contained on the (U)SIM.

   It is FFS whether this modification applies to just the background search for a more preferred VPLMN, or, to the background search for both VPLMN and HPLMN.

c) for ALL M2M devices, modification of the behaviour following receipt of 'fatal' MM/GMM/EMM cause values such as "IMSI unknown in HLR", "illegal ME" and "persistent" cause values such as "PLMN not allowed". These cause values could be wrongly sent "in panic" by an overloaded (V)PLMN, or, in a denial of service attack by a (mobile) false base station. Following receipt of these cause values, a site visit to all M2M devices is untenable, however, so is immediate re-accessing by the device. Some new middle ground is needed (e.g. retry at a randomly selected time between 24 and 48 hours later).

   It is FFS whether the behaviour following receipt of "PLMN not allowed" needs modification or not.

d) For a "low value M2M" device, always use IMSI when Attaching to a new network, or, performing an RA update into a different PLMN that is not an ePLMN. This decreases UE-network signalling in a potentially heavily loaded network.

   It is FFS whether this solution is applicable to EUTRAN.

e) In the CS domain, at power on in a new location area, perform a location update with LU type=Attach rather than "normal".

f) Modification of "low value M2M" device behaviour following repeatedly unsuccessful MM/GMM/EMM procedures so that the device does NOT move to competing network(s) and inflict them with similar levels of signalling (over)load.

6.33.3 Impacts on existing nodes or functionality

The above features are internal to the M2M device (and/or application on the M2M device).

6.33.4 Evaluation

These features seem useful to be developed in more detail (e.g. by CT 1) and specified as part of 3GPP release 10.

6.34 Solution – M2M device indication to network

6.34.1 Problem Solved / Gains Provided

5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices".

6.34.2 General

By providing the network with indications that the UE is a "low priority" M2M device, the network is able to more easily protect itself against overload, and/or to detect that an increase in load is being caused by M2M devices.

Clause 5.14 highlighted the utility of M2M device indicators in the following signalling:

a) in the GSM Channel Request message, and UTRAN and E-UTRAN RRC Connection Establishment messages;

b) in the IDNNS signalling at Attach and RA update from a non-equivalent PLMN;

NOTE: From the stage 2 design point of view, there is no harm in always sending this M2M indicator in the IDNNS. It is left to stage 3 to decide whether to do this simplification.

c) in the NAS signalling to the MME/SGSN/MSC.

6.34.3 Impacts on existing nodes or functionality

For the Channel Request message (and its equivalents), the RAN will probably need to broadcast its support/non-support for the new code points.

For b, c the signalling should be able to be added in a backwards compatible manner.

6.34.4 Evaluation

These indicators appear useful to specify in 3GPP Release 10.

6.35 Solution - Overload control within an MTC access grant time interval

6.35.1 Problems solved / Gains provided

See Clause 5.9 "Key Issue –Time Controlled" and Clause 5.12 "Key Issue – Signalling Congestion Control".

6.35.2 General

The network may suffer from a dramatic increase in its load at the beginning of the MTC access grant time interval due to the simultaneous signalling actions (e.g., simultaneous attachment operations) of many MTC devices. The main idea of the solution presented here is to let SGSN/MME restrict the number of its attached MTC devices in such a manner that the total number of attached UEs (including both MTC and non-MTC devices) is always under, or, at most, fluctuates slightly around, a pre-defined upper bound during the MTC access grant time interval.

Developed to restrict MTC device accesses only, this solution recommends that each MTC device carry an MTC indication with which the network can distinguish MTC devices from normal human-to-human (H2H) devices. Also,

we suggest that the MTC devices remain detached if they are not expected to have any mobile terminated communications.

To implement this method, the network operator needs to set an upper bound of the number of attached UEs. This upper bound is supposed to be the maximum number of attached UEs while keeping the network in a normal working condition. It can be determined according to the network equipment capability and the operating experience.

As the load increases or decreases, the allowed number of UE sessions may have to be adjusted, as a number that is too high will ensure congestion, while a number that is too low will ensure underutilization.

A series of discrete time points (e.g., with a spacing of 1 second) are selected within the MTC access grant time interval as the time instants at which the MTC devices are allowed to request attachment. At other times, the network shall reject the MTC attachment requests and tell each of those MTC devices to resend the request at an aforementioned time point.

At each of the time points described above, the SGSN/MME checks the number of attached non-MTC UEs, the margin between this number and the aforementioned upper bound is regarded as the maximum number of MTC devices allowed to attach at this moment. If the number of currently attached MTC devices is less than that maximum number, the SGSN/MME accepts the attach requests from MTC devices until the number of attached MTC devices reaches the maximum number, otherwise the attach requests are rejected. While rejecting an attach request, the SGSN/MME selects a subsequent MTC attachment time point and tells the MTC device to resend the attach request at that specific time point.

The algorithm is first-come-first-serve. Any device that requests access after the maximum number have been allowed access, will be given a deferral. It is therefore anticipated that devices will attempt to access the network as soon as possible (at the beginning of the Grant Time Interval). Further, it is possible that devices may get deferrals repeatedly, and there is no bound to the number of deferrals that may occur.

The SGSN/MME must select a subsequent MTC attach time such that the MTC Device can complete its minimum Access Duration.

After completing the communication tasks in the MTC access grant time interval, the MTC devices shall get detached (either by themselves or by the network) from the SGSN/MME so that other MTC devices can have chances to successfully attach to the network.

Editor's note: It is FFS how surcharging instead of detaching can be supported by this solution.

6.35.3 Impacts on existing nodes or functionality

Impacts on the SGSN/MME:

- With the MTC indication carried by each MTC device, the SGSN/MME needs to be able to distinguish MTC devices from normal H2H devices.
- The SGSN/MME needs to store the discrete time points at which the MTC devices are allowed to request attachment, and reject MTC attach requests except at those time points. While rejecting an attach request, the SGSN/MME needs to select a subsequent MTC attachment time point and inform the MTC device.
- The SGSN/MME needs to count the numbers of both MTC and non-MTC devices separately. At the time points when MTC devices are allowed to request attachment, the SGSN/MME needs to calculate the maximum number of MTC devices allowed to attach at this moment, and decide how many more MTC attach requests it can accept.
- The SGSN/MME must take into account the Grant Time Interval, Forbidden Time Interval and Access Duration policy that applies to the subscription corresponding to the MTC Device when it calculates the deferred access time point. The MTC Device must be able to fulfil its Access Duration within a Grant Time Interval.

Impacts on the MTC device:

- Each MTC device needs to carry an MTC indication.
- MTC devices need to remain detached if they are not expected to have any mobile terminated communications.
- When its attach request is rejected, the MTC device needs to resend the request at the time point provided by the SGSN/MME in the rejection message.

- After completing the communication tasks, the MTC device needs to get detached (either by themselves or by the network) from the SGSN/MME.

6.35.4 Evaluation

6.36 Solution - Time controlled feature via Operator and MTC User Business Agreements

6.36.1 Problem Solved / Gains Provided

See clause 5.9 "Key Issue – Time Controlled".

6.36.2 General

The outline of the solution is as follows:

- The operator informs the MTC user about preferred time-window for MTC devices to communicate with the network. This is performed as part of business agreement between the operator and the MTC User.

- The MTC device informs the MTC Server about its current location and PLMN via application layer.

NOTE: Finer granularity than PLMN may be needed if the time-window is based on geographical location within the PLMN, e.g. for a PLMN covering a large geographical area

- The MTC user via the MTC Server informs the MTC device about the appropriate time window to communicate with the network via application layer.

- The charging for MTC communication may be set such that the communication has higher charges if these occur outside of the preferred time-window.

- The Operator keeps track, via regular OAM, about the time when the communication with MTC device occurs. The operator provides this information, e.g. as part of bill, to the MTC User. The MTC user takes appropriate action if certain MTC devices are communicating outside of the desired time-window. The operator may also take appropriate action, based on analyzing the call-records, e.g. cancel MTC devices subscription.

- Based on traffic pattern, the operator may modify the preferred time-window for MTC device communication and provide this information to the MTC User. The MTC user updates the new time-window of communication to MTC device via application layer.

6.36.3 Impacts on existing nodes or functionality

None

6.36.4 Evaluation

The over-the-top solution exists independent to 3GPP standardization.

This solution cannot enforce time control policy as defined by TS 22.368 [2], clause 7.2.2. It would be possible to configure a surcharging policy using PCC.

Dynamic local criteria, e.g. current load on network beyond perhaps 'time zone information', especially from the VPLMN, cannot be taken into account by in a real-time manner, as it is based upon subscription and roaming agreements.

This solution is based on application control. If the same MTC Device uses more than one application, all applications will need to be controlled in a coordinated manner.

6.37 Solution - Simple Subscription Control

6.37.1 Problem Solved / Gains Provided

This solution answers the requirements of 5.7 "Key Issue - MTC Subscriptions."

6.37.2 General

Solution 1) "Do Nothing"

It is possible that there will be no MTC Features in release 10. If this is the case, it would suffice that the lack of any MTC subscription elements indicates that no MTC Features are subscribed.

Solution 2) "Simple Solution"

The MTC Subscription identifies subscribed MTC Features (as an IE or as IEs) in the HSS.

It is assumed for this release of this specification that all subscribed MTC Features may be considered by the network to be 'essential' and mandatory. If an MTC Device or visited network does not support one or more subscribed MTC Features, the MME/SGSN may inform the MTC Device and the MTC Device detaches.

To determine whether a subscribed MTC Feature is activated:

- The Network may determine if a given MTC Device supports a given MTC Feature through implementation dependent evaluation of the IMEI. For example, the operator may maintain a database of MTC Devices types based upon the IMEI.
- Further, it may be assumed that a subscribed MTC Feature is supported by the MTC Device. If this is not the case, the MTC Device will fail to operate
- If either the network or the MTC Device (e.g. based on IMEI or due to missing but expected parameters during the attach request) does not support a subscribed MTC Feature, the MME/SGSN may reject the MTC Device when it attempts to attach. The MME/SGSN includes information regarding the unsupported MTC Feature in the rejection cause.

An indication of capabilities from the MTC Device is unnecessary to define in a general way. For each MTC Feature, such interaction between the MTC Device and the network may be defined (as has been done for other features, e.g. SR VCC capability, etc.).

If the MME/SGSN is pre-Rel-10 and accepts the MTC devices without any notification about the MTC features, and the device expects such an indication for the feature, the MTC device performs detach procedure.

6.37.3 Impacts on existing nodes or functionality

Solution 1)

None

Solution 2)

The HSS must support an IE (or IEs) representing MTC Features included in the MTC subscription.

The MME/SGSN determine whether an MTC Device supports the subscribed set of MTC Features on the basis of the IMEI the device capabilities (e.g. by means of a database) or by checking whether expected IEs are present.

The MME/SGSN knows (due to local policy) whether a given MTC Feature is supported by the network.

The MME/SGSN may reject MTC Devices attempting to attach using a new rejection code.

6.37.4 Evaluation

Solution 1 is preferable if no MTC Feature is standardized in release 10. This solution has no impact on the standard and will not complicate future MTC Feature control mechanisms.

Solution 2 is preferable if MTC Features are standardized in release 10. A simple approach is taken in which the minimum semantics are assumed in order to support the architecture requirements expressed by the Key Issue.

6.38 Solution – Device identifier used over MTC_{SP}

6.38.1 Problems solved / Gains provided

See
clause 5.8 "Key Issue –MTC Device Trigger",
clause 5.13 "Key Issue - MTC Identifiers",
clause 5.10 "Key Issue - MTC Monitoring",
clause 5.11 "Key Issue - Decoupling MTC Server from 3GPP Architecture".

6.38.2 General

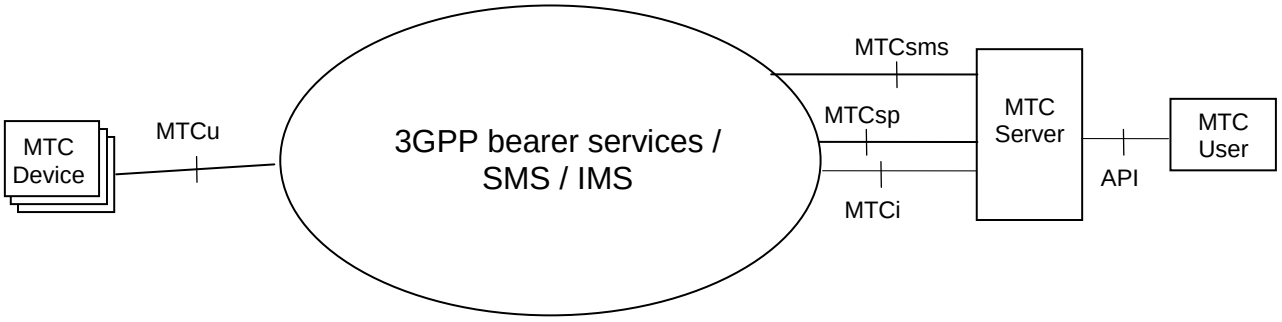


Figure 6.38.2-1: 3GPP Architecture for Machine-Type Communication

The reference points are listed as below:

MTCu: It provides MTC Devices access to 3GPP network for the transport of user plane and control plane traffic. MTCu interface could be based on Uu, Um, Ww and LTE-Uu interface.

MTCi: It is the reference point that MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP bearer services/IMS. MTCi could be based on Gi, Sgi, and Wi interface.

MTCsp: It is the reference point the MTC Server uses for signalling with the 3GPP network.

MTCsms: It is the reference point MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP SMS.

Editor's note: It is ffs if MTCsms exists as a separate reference point or whether MTCsp is used for 3GPP SMS as well.

In the general case the MTC Server is located outside the operator domain. In the special case when the MTC Server is located in the operator domain, the MTC_{SP} and the MTC_i becomes internal in the operator network. In a deployment there may simultaneously be MTC Server located inside the operator domain and MTC Servers located outside the operator domain. There might be one or several functional entities in the mobile operator network that terminate the MTC_{SP} reference point. In the text below these entities(s) are simply referred to as "Service Centre configured for MTC". The MTC Server and the MTC User may either be separate entities or co-located.

Guiding requirements for a device identifier to be used instead of MSISDN at signalling between the MTC Server and the mobile operator network are:

- The identifier must be globally unique since some MTC service providers operate worldwide.
- The allocation of the new identifier should be efficient.
- The identifier shall also be usable towards other access networks such as 3GPP2, etc.
- The new identifier shall support certain functions in the operator domain:
  - Enable routing of signalling, that is, discovering which MTC Server or service provider the MTC device belongs to and its signalling shall be routed to

- Enable charging and billing. One device (and the charging data produced from its activities) shall easily be traced back to the service provider it belongs to. Optionally also which user at the service provider it belongs to.

- Selective congestion control or enabling/disabling e.g. per MTC User and per Service Provider.

- Migration aspects when changing from MSISDN to the new identifier should be considered.

- Other.

The details for a device identifier used in MTCSP protocols should be specified in stage 3 (already established protocols such as HTTP RESTful may be candidates for a MTCSP protocol). However in the SA2 requirements of a device identifier, there may also be requirements such as what information it contains (see example below).

In this example below the "Service Provider ID" is a domain name that belongs to the MTC service provider. The "topdomain" would ensure that the "Service Provider ID" becomes internationally unique. The "topdomain" would be a FQDN in itself such as ".com", ".se", ".co.uk", ".operator.com", etc. The "User ID" should identify a subscriber within the service provider domain, for example an enterprise or even a person using MTC services. There would be a unique "Device ID" part for each MTC device a user has (at least unique within the user domain). The "Device ID" may for example be a serial number of the hardware running the "application part" of the MTC device (i.e. not the IMEI) or any other number used by the MTC user to distinguish the MTC device. All these different parts together constitute the full device identifier, as used over a MTCSP interface. In the reminder of this document, the term "International Service provider Subscription Identifier" (abbreviated to ISSI) is used for a device identifier used over the MTCSP interface and meeting the requirements listed above.

Editor's note: The name for the device identifier "International Service provider Subscription Identifier" (ISSI) is tentative and may change.

a) **FQDN:** deviceid.userid.serviceprovideriid.topdomain.

b) **Dedicated 3GPP URN:**
urn:issi:deviceid.userid.serviceprovideriid.topdom

Figure 6.38.2-2: Examples of different URI style formats of a device identifier (ISSI)

An advantage with an URI style format of a device identifier is that this can be considered mainstream internet technology and that the administration and allocation of the different identifier parts, e.g. the Service Provider ID part, does already exist as part of the normal domain name administration. A slight disadvantage could be that if the different identifiers parts are domain names, such as the "serviceprovideriid.topdomain", care needs to be taken so that clashes with other usages of the same domain name is avoided.

Another advantage of a URI style format for the device identifier is that it allows much more flexibility in the subdivision of the addressing space than an identifier based on a number. However, this advantage would disappear if a constraint to only use URI derived from numbers (such as sip+33612345678@domain.topdomain) would be introduced.

Alternative a) above using a FQDN for identifying a device should work but there is an implicit assumption of the content/structure of the domain name that needs to be specified.

Alternative b) using a Uniform Resource Name (URN) is probably more correct way to use a URI when the intention is to specify an identity. By using a new specific Namespace ID in the URN such as "ISSI" in the example, the syntactic interpretation of the Namespace Specific String would be defined. There may be other already registered Namespace ID's that can be used more or less according to 3GPP requirements.

Alternative c) using a SIP URI is also a possibility. The syntax associated with SIP URI's should be possible to use for what 3GPP requires of a device identifier, but when following it strictly the SIP protocol is also expected for a SIP URI which may not be the case for the MTCSP interface.

NOTE: Depending on what type of URI is selected as device identifier, there might be assumptions on what protocol is used over the MTCsp.

6.38.3 Impacts on existing nodes or functionality

Impact on GPRS/EPS architecture:

- A new termination point for the MTCSP reference point in the operator network.

Impacts on the HSS/HLR:

- Storage of a new parameter (ISSI) in the subscription information. Making ISSI searchable to be able to find a specific subscriber profile based on an ISSI.
- A new or modified existing protocol is specified for the reference point between the HSS/HLR and a Service Centre configured for MTC. It is FFS how the Service Centre configured for MTC can find the HLR/HSS when there are multiple HLR/HSS.

Editor's note: The place where to store the ISSI is still subject for discussion. Hence the HSS/HLR impacts may change.

6.38.4 Evaluation

6.39 Solution - Triggering MTC devices via HSS and NAS signalling

6.39.1 Problem Solved / Gains Provided

See clause 5.8, "Key Issue – MTC Device Trigger" and clause 5.13 "Key issue - MTC Identifiers".

6.39.2 General

6.39.2.1 Overview

A network application server (e.g. Device Management Server) that needs to trigger a connection request from a UE informs the HSS/HLR about this need by providing "UE application trigger request" information defined in clause 6.40.2

Each of the UE targeted by the network application server request is then notified about that request via signalling exchange through the serving MME/SGSN, during the next NAS signalling exchange with the UE if there is no on-going signalling connection between the UE and MME/SGSN, or immediately if there is an on-going signalling connection with the UE or if this is an urgent request.

Upon reception of this "UE application trigger request" information, the UE application is triggered and contacts the network application server.

6.39.2.2 Detailed solution

The procedure is illustrated in figure 6.39.2-1 and works as follows:

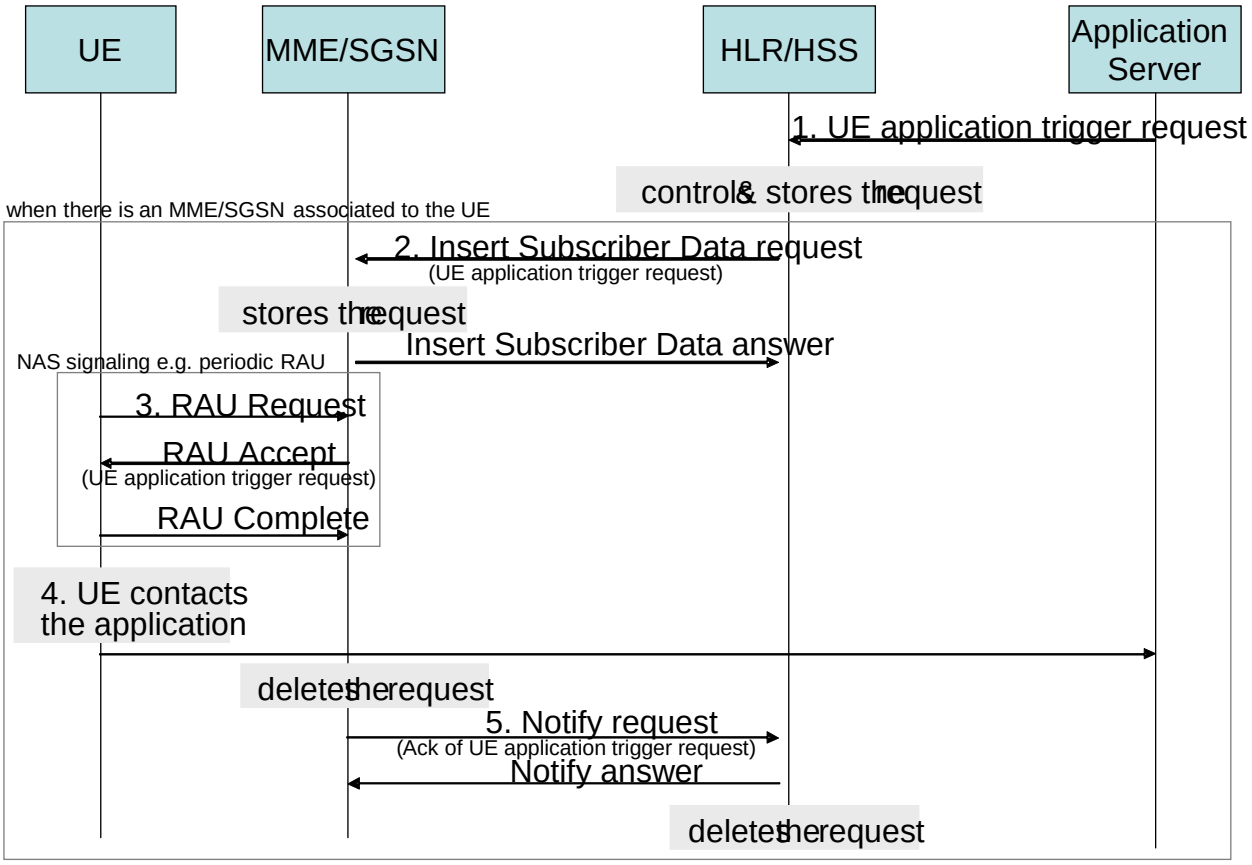


Figure 6.39.2-1: Triggering MTC devices via HSS and NAS signalling

1) Each time a network application server wants to contact a UE, it informs the HSS/HLR about this need by providing "UE application trigger request" information.

   The interface between an external application and the HSS/HLR needs to be secured. Limitation may be enforced to avoid simultaneous storage of too many "UE application trigger request" in the network.

   The HSS/HLR (or a gateway between the application and the network):

   a) validates the request from the application (e.g. checking the application rights to issue such requests, enforcing application throttling , etc.);

   b) translates the identity of the target UE received from the application into a network identity of the UE (e.g. corresponding to the IMSI of the target UE);

   c) stores this request in its database record associated with the target UE;

   d) determines the MME/SGSN that currently serves the target UE or waits for such a MME/SGSN to be allocated to the UE (i.e. waits for a subsequent Update Location from an MME/SGSN for that user).

2) The HSS/HLR notifies/updates the serving MME/SGSN with this "UE application trigger request" information, immediately if the UE is already served by a SGSN/MME, or when the SGSN/MME changes, otherwise when the UE registers to the network.

   The "UE application trigger request" may be sent within the MAP (Gr) or Diameter (S6a/S6d) Insert Subscriber Data operation. The MME/SGSN stores this request in its database record associated with the UE and returns an Insert Subscriber Data answer.

   If more than one serving nodes are registered with the HSS (e.g., both the MME and the SGSN are registered with the HSS), the HSS sends "UE application trigger request" to each registered serving node.

3) The serving MME/SGSN transfers the "UE application trigger request" information to the UE upon the next NAS signalling exchange with the UE:

a) RAU / TAU procedure:

- the RAU/TAU Accept message may carry the "UE application trigger request" notification;

- the TAU/RAU Complete message acknowledges the correct UE reception of the "UE application trigger request" notification. The UE has to send a TAU/RAU Complete message as if a new GUTI or a new P-TMSI had been assigned.

b) Attach procedure:

- the Attach Accept message may carry the "UE application trigger request" notification;

- the Attach Complete message acknowledges the correct UE reception of the "UE application trigger request" notification. The UE has to send an Attach Complete message as if a new GUTI or a new P-TMSI had been assigned.

c) a dedicated Notification procedure (with a UE acknowledgment) which takes place immediately if there is an on-going signalling connection with the UE when the MME/SGSN receives the request from the HSS/HLR.

This may be implemented as follows:

- for LTE access: the Network and UE initiated Generic transport of NAS messages procedures (see TS 24.301 [17] clauses 5.6.4.3 and 5.6.4.2) may be used to carry the "UE application trigger request" notification to the UE and its acknowledgment by the UE. I.e. using the DOWNLINK GENERIC NAS TRANSPORT message and the UPLINK GENERIC NAS TRANSPORT message with a Generic message container type IE set to a specific value for the transfer of "UE application trigger request" and with the Generic message container IE containing the "UE application trigger request" information.

- For 2G/3G access, a similar mechanism may be defined or an existing GMM message may be extended to carry the UE application trigger request, e.g. GMM Information message (see TS 24.008 [16] clause 9.4.19).

4) Upon reception of this "UE application trigger request" information, the UE

a) acknowledges the reception of this information via NAS signalling to the MME/SGSN;

b) checks that this is not a duplicate request (using the request counter). If this is a duplicate step 4) stops here. Otherwise, the UE application is triggered;

c) establish the relevant PDN connection / PDP context using the existing EPC/GPRS procedures, if it is not already established;

d) triggers the UE application which then contacts the network application server in the network. The addressing information to contact the application server in the network may be known in advance on the UE or may have been communicated in the "UE application trigger request" notification.

5) Upon receipt of the acknowledgement from the UE:

a) the MME/SGSN removes the UE application trigger request information from its database record associated with the UE and notifies the HLR/HSS that the UE has received the "UE application trigger request" by sending a Diameter Notification message or a MAP Update GPRS Location message.

b) When the HSS/HLR receives the acknowledgement from either the MME or the SGSN about a UE, the HSS/HLR removes this request in its database record associated with this UE.

The HSS/HLR does not need to wait for the acknowledgement from both MME and SGSN to remove the request. This means that an UE may receive twice (once via MME, once via SGSN) such a notification. If so, the UE can detect a duplicated request via the request counter, discards the repeated request and returns a positive acknowledgement to the sending node. Another alternative would be for the HSS/HLR to remove an obsolete UE application trigger request from a MME/SGSN.

An application may cancel an UE application trigger request using its application Id and the request counter.

If an MME/SGSN fails and loses the information about not yet transferred "UE application trigger request" notifications, this is not an issue as the HSS/HLR sends to an MME/SGSN that starts serving an UE all "UE application trigger request" notification information it has in its database record associated with this UE.

An urgency request parameter may also be associated with the "UE application trigger request" notification. If the request is urgent, the UE is notified as soon as possible i.e. the serving MME/SGSN pages the UE as soon as it receives the "UE application trigger request" information from the HSS/HLR. Otherwise the UE is notified only the next time it exchanges signalling with the MME/SGSN.

If an "UE application trigger request" indicates an expiration time and the timer is about to expire, and there is no ongoing NAS signalling exchange with the UE, the SGSN/MME pages the UE to deliver the "UE application trigger request" a configurable times before the expiry of the expiration time.

6.39.3 Impacts on existing nodes or functionality

HLR/HSS provides interface to application server for receiving trigger requests and to report trigger results. HLR/HSS stores UE application trigger requests, transfers them to the each serving MME/SGSN and erase them upon getting the acknowledgement from either of the serving MME or SGSN entities that they have been successfully delivered to the UEs. The signaling cost of this procedure on HSS/HLR should be equivalent to the cost of a triggering based on terminating SMS.

MME/S4-SGSN stores UE application trigger requests, transfers them via NAS signalling to the UE and erase them upon getting the acknowledgement that they have been successfully delivered to the UEs.

UEs receive and acknowledge UE application trigger requests via NAS signalling and trigger the corresponding application.

6.39.4 Evaluation

6.40 Solution - Information sent to trigger a UE used for MTC

6.40.1 Problem solved

This solution describes the information to be provided by a network application server (e.g. Device Management Server) that needs to trigger a connection request from a UE. See clause 5.8, "Key Issue - MTC Device Trigger".

6.40.2 Required Functionality

A network application server (e.g. Device Management Server) that needs to trigger a connection request from a UE provides "UE application trigger request" information containing e.g.:

- the identity of the target UE;
- the identity of the application;
- a request counter associated to this request allowing to detect duplicated requests, to correlate requests with their acknowledgement and to allow the application to cancel a request;
- optionally the IP@ (or FQDN) and/or TCP (or UDP) port of the server/application that the UE has to contact;
- optionally an urgency request indication;
- optionally a validity timer (allowing to remove storage of the UE application is triggered when it is no more needed);
- optionally application specific information (of limited size).

Editor's note: It is FFS whether other parameters such as provided within a SMS based trigger are needed.

6.41 Solution - Triggering of attached MTC Devices by reusing Network Requested PDP Context Activation procedure

6.41.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger".

6.41.2 General

This solution proposes to trigger the attached MTC Devices by reusing Network-Requested PDP Context Activation procedures. This solution supports the scenario where an MTC Device has a subscribed static IP address and the scenario where only dynamic IP address assignment for MTC Devices is supported. The MTC Device can obtain IP address dynamically during the subsequent PDP context activation procedure in case there is no subscribed static IP address.

The MTC Server initiates DNS query to retrieve the IP address for the MTC Device if it is not available in the MTC Server. The DNS Server can be standalone or the front-end of the AAA Server. The DNS Server lookup the entry based on the query input (i.e. a FQDN, which includes the device identifier) provided by the MTC Server. If there is a valid record in the DNS Server, the DNS Server returns IP address to the MTC Server (e.g. a PDP context or PDN connection has been established) directly, otherwise, it requires the AAA Server to trigger the MTC Device to establish PDP context or PDN connection firstly.

Editor's note: The device identifier format, e.g. FQDN is FFS.

NOTE 1: For E-UTRAN access, a default PDN connection is established during Attach procedure, so the DNS Server can return the IP address directly.

NOTE 2: The AAA Server and DNS Server can be deployed as standalone physical entities or as functional entities collocated in a Device Trigger Gateway (DT-GW; refer to Figure 6.45.2-1).

There are two alternatives for the AAA Server to trigger the MTC Device.

Alternative 1:

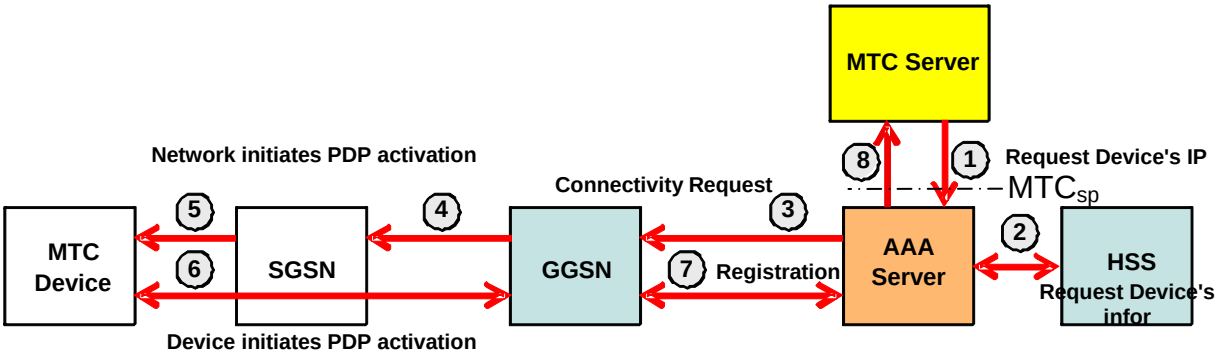


Figure 6.41.2-1: Illustration of alternative 1

The AAA Server selects the HLR/HSS based on the IMSI, which is derived from the device identifier (i.e. the IMSI is included in the device identifier) or mapped from the device identifier based on local configuration, and sends an information request (IMSI) message to the HLR/HSS. The HLR/HSS returns the serving SGSN address for the MTC Device.

The APN can be provided by the MTC Server (e.g. included in the FQDN for DNS query), or derived from, e.g. the FQDN according to local configuration.

The AAA Server selects a GGSN based on e.g. APN, and initiates Network-Requested PDP Context Activation procedure as specified in TS 23.060 [21], with the exception as follows:

1) In step 3 of above figure, the AAA Server sends a Connectivity Request message (IMSI, APN, SGSN address) to the selected GGSN.

2) In step 4 of above figure, the GGSN sends PDU Notification Request (IMSI, APN, PDP address) message to the SGSN. The PDP address is set to zero or the static IP address configured in the GGSN.

3) In step 7 of above figure, the GGSN registers the MTC Device to the DNS Server via AAA Server as specified in TS 29.061 [4], with providing the device identifier, APN and the IP address (i.e. the subscribed static IP address or the dynamically allocated IP address during the PDP context activation procedure in step 6), which are provided by the MTC Device in PCO IE.

NOTE 3: For IPv6 it is assumed that the MTC Device relies on DHCPv6 for stateful address allocation, or uses the solution described in clause 6.49.

NOTE 4: Alternative 1 can be combined with the solution described in 6.50 to avoid the use of stateful address allocation.

Alternative 2:

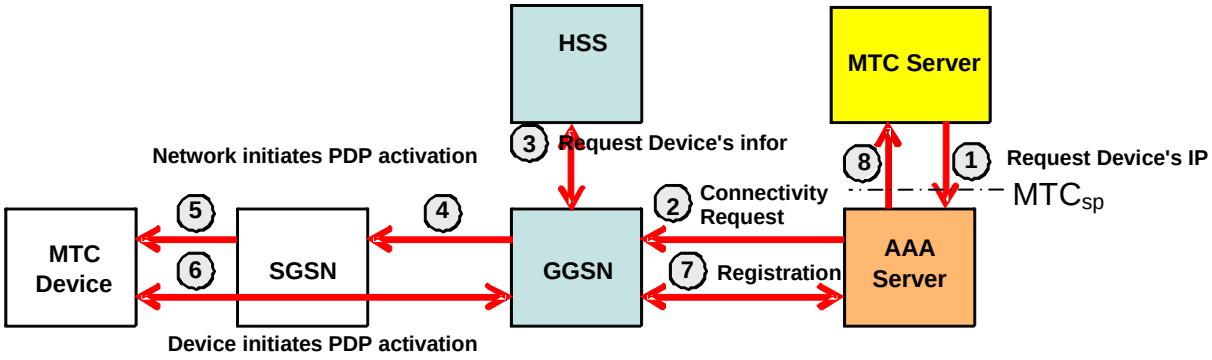


Figure 6.41.2-2: Illustration of alternative 2

The AAA Server selects a GGSN based on e.g. APN which is provided by the MTC Server (e.g. included in the FQDN for DNS query), or derived from, e.g. the FQDN according to local configuration, and then initiates Network-Requested PDP Context Activation procedure as specified in TS 23.060 [21], with the exception as follows:

1) In step 2 of above figure, the AAA Server sends a Connectivity Request message (IMSI, APN) to the selected GGSN. The IMSI is derived from the device identifier (i.e. the IMSI is included in the device identifier) or mapped from the device identifier based on local configuration.

2) In step 3 of above figure, the GGSN sends MAP_SEND_ROUTING_INFO_FOR_GPRS Service (IMSI) message to the HLR/HSS. The HLR/HSS address is derived from the IMSI. The HLR/HSS returns the serving SGSN address.

3) In step 4 of above figure, the GGSN sends PDU Notification Request (IMSI, APN, PDP address) message to the SGSN. The PDP address is set to zero or the static IP address configured in the GGSN.

4) In step 5 of above figure, the SGSN sends a Request PDP Context Activation (APN, PDP address) message to the MTC Device.

5) In step 7 of above figure, the GGSN registers the MTC Device to the DNS Server via AAA Server as specified in TS 29.061 [4], with providing the device identifier, APN and the IP address (i.e. the subscribed static IP address or the dynamically allocated IP address during the PDP context activation procedure in step 6), which are provided by the MTC Device in PCO IE.

NOTE 5: For IPv6 it is assumed that the MTC Device relies on DHCPv6 for stateful address allocation, or uses the solution described in clause 6.49.

NOTE 6: Alternative 2 can be combined with the solution described in 6.50 to avoid the use of stateful address allocation.

Afterwards, the DNS Server returns the IP address of the MTC Device to the MTC Server, so that the MTC Server can transmit packet data to the MTC Device.

Editor's note: The alternative with using dynamic address allocation needs to solve issues addressed in TR 23.976. The solution with using static IP address allocation needs to detail how static address allocation is performed as it has been removed from TS 23.060 [21] and TS 23.401 [5].

6.41.3 Impacts on existing nodes or functionality

Impacts on the Network-Requested PDP Context Activation procedure:

- It is triggered by a signalling over Gi interface instead of a PDU;

- It needs to support dynamical IP address allocation;
- In alternative 1, the GGSN does not communicate with HLR/HSS via Gc interface.

6.41.4 Evaluation

6.42 Solution - Triggering of attached MTC Device via Pre rel-11 SMS

6.42.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger". The solution focuses on the scenario that MTC devices receive trigger indication in attached state w/o PDP/PDN connection.

6.42.2 General

The MTC server sends indication to MTC Devices via SMS and make MTC Devices initially establish data communication with the MTC server. The short message should contain MTC Server address and required triggering information.

6.42.3 Impacts on existing nodes or functionality

None.

6.42.4 Evaluation

Benefits:

- No impact for existing network.

Drawbacks:

- The subscription of MTC Device must associate with a MSISDN.
- CS network is involved in case the short message is only supported by the CS domain and/or LTE access is deployed.

6.43 Solution - Triggering of attached MTC Device via intermediate node

6.43.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger". The solution focuses on the scenario that MTC devices receive trigger indication in attached state.

6.43.2 General

This solution re-uses the intermediate node introduced by MTC Monitoring solution specified in clause 6.25. MTC Server may first register its desired events with IMSI or device ID. Towards the triggering purpose, the monitoring event should include CN node-level location change (e.g. SGSN/MME change) of the MTC device and it might be configured in SGSN/MME by operators or inserted into SGSN/MME along with the subscription. SGSN/MME shall report location changes to the intermediate node once the new MTC device enters into or the already camping MTC device changes location. Upon the location report, the intermediate node shall store the SGSN/MME address associated with the IMSI or device ID and then push registered location information to the related MTC server. Above procedures shall follow monitoring mechanism covered in clause 6.25.

When the MTC user wants to trigger an attached MTC Device which can be located, the MTC Server sends notification message with the IMSI or device ID and the MTC Server address to the intermediate node, which thus forwards the message to the SGSN/MME that sends location update message last time. SGSN/MME might use the existing or new NAS message to initiate data communication between the MTC device and MTC server.

In case of no PDP context, the MTC device activates a PDP context after receiving trigger indication. Or SGSN may initiate PDP context activation directly.

Editor's note: How SGSN initiates a PDP based on the notification from the intermediate node is FFS. The MTC server can also trigger the MTC device without register location monitoring service if all related MTC device are monitored with location by default. Since the MTC Server does not know whether the MTC device is attached before triggering, the triggering might not success.

The intermediate node shall keep the SGSN/MME address per IMSI or device ID in this solution.

Editor's note: Whether there are changes to the roaming architecture and message flow are FFS.

6.43.3 Impacts on existing nodes or functionality

CN nodes:

- Event reporting function through the intermediate node specified in clause 6.25 shall be supported by SGSN/MME, HLR/HSS.
- A new network entity may be introduced and new interfaces are introduced.

Editor's note: Whether there are additional impacts in roaming scenario is FFS.

6.43.4 Evaluation

Benefits:

- MSISDN is not mandatory for this solution.
- It is applicable for PS only network.

Drawbacks:

- The new network entity and new interfaces add complexity of the system.
- SGSN/MME need report location changes to the intermediate node.

6.44 Solution – Device Triggering reuse of MT SMS

6.44.1 Problems solved / Gains provided

See clause 5.7 "Key Issue -MTC Device Trigger".

6.44.2 General

The solution described and evaluated below addresses the Key issue "MTC Device Triggering" and allows an MTC server to trigger registered devices (i.e. IMSI attached or GPRS attached) without a PDP connection to establish a connection making communication with the MTC server possible.

The MTC-IWF (e.g. potentially collocated with SMS-SC) would use a standardized protocol over the MTCsp interface point. The Service Centre resides at the edge of the operators' network (see figure 6.44.2-1). The MTC Server could request the Service Centre to deliver a device trigger over the MTCsp.

The role of the MTC-IWF (clause 6.45 Solution- Device trigger gateway solution) is to hide the details of the triggering mechanism in the operator' domain and provide the MTC Server a generalized interface for it to make a device triggering request.

The functionality includes:

- Support for a function for MTC device triggering and acknowledgement over the MTCsp reference point between the MTC server and the MTC-IWF.
- May be collocated with the SMS-SC

- May operate in PS domain only or it may operate in both PS and CS domain. In the latter case it may do the triggering through the MSC
- Reuse of a existing SMS infrastructure and protocols
- Reuse of existing functionality in the terminal to trigger the application (i.e. no terminal impact).
- Mapping the validity time in MTCsp to the Validity Period for SMS delivery.

A first solution can allow the MTC Server to request a Device Trigger using the new external identifier (see clause 6.38 Solution - Device identifier used over MTCsp). This new external identifier could be mapped by the MTC-IWF to the MSISDN and allow for delivery of device trigger using the existing MT SMS functionality. This approach allows reuse of the SMS nodes with no system impact.

A later evolution could be a MSISDN-less mode of operation allowing SMS-GMSC to interrogate the HLR using the new identifier for retrieval of the corresponding IMSI and routing information. In conjunction with updates allowing for a MSISDN-less mode (e.g. SMS interfaces and nodes would be impacted) the MT SMS would be delivered using the IMSI.

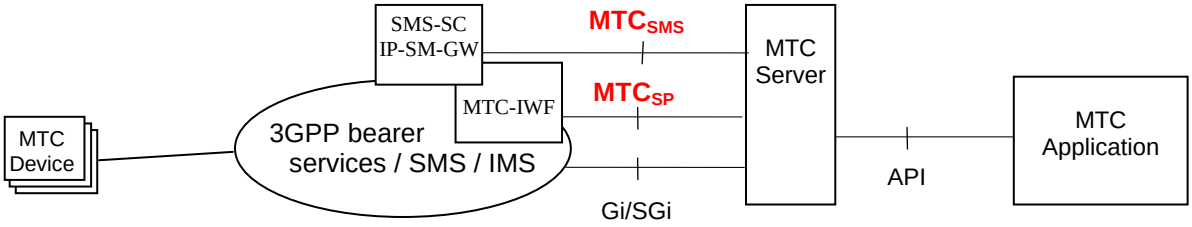


Figure 6.44.2-1: MTC-IWF at edge of Mobile Operator Domain

NOTE: If MTC server uses MTCsms to send an SMS for triggering, then similar principles applies as if MTC-IWF forwards the trigger towards SMS entities. Whether MTCsms is enhanced e.g. to support non-E.164 MSISDNs is out of scope.

From TS 23.040 [6] clause 4.1 the follow entities are in the provision of SMS.

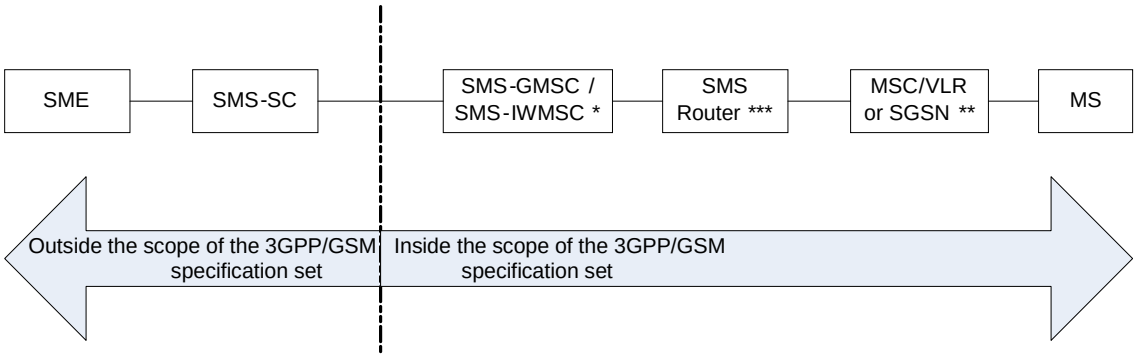


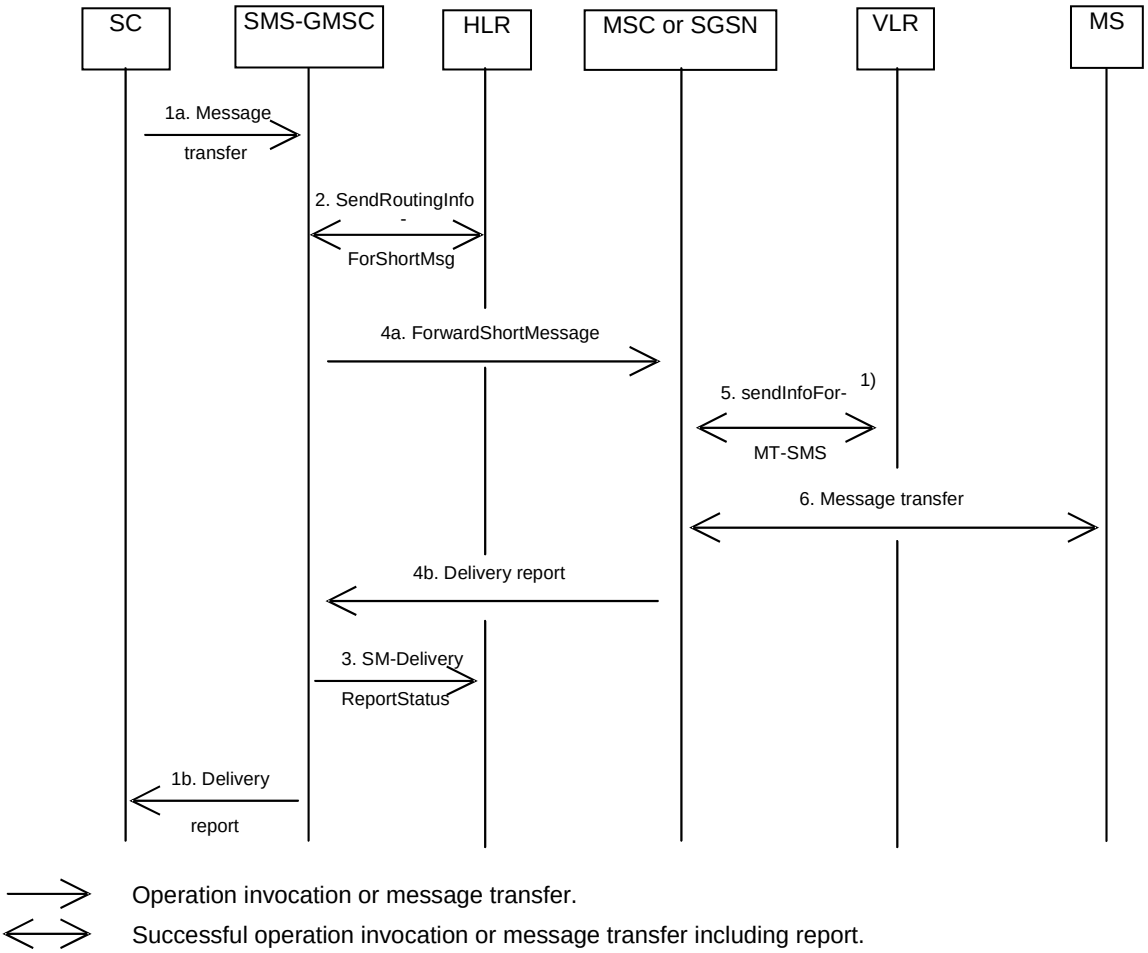
Figure 6.44.2-2 Entities involved in the provision of short message

The MTC-IWF takes the role of the SME (Short Message Entity). The MTC-IWF may be co-located with the SMS-SC. As per TS 23.040 [6] the Service Centre may be integrated with the SMS GMSC/SMS IWMSC.

Steps for the MTC Server to request a device trigger include:

- The MTC-IWF would receive the Device Trigger Request over the MTCsp interface point. The Device Trigger request may use the new external identifier as per Solution - Device Identifier used over MTCsp (clause 6.38) or using private numbering plans as detailed below.
- When the MTC-IWF decides to trigger via the SMS SC, the SMS Service Centre receives the device identifier and initiates a message transfer that eventually results in a MT SMS that triggers the MS to establish a PDP connection.

- The SM TP SUBMIT DELIVERY message needs to carry an indication when the MT-SMS carries device triggering information.
- The SM TP User Data may contain further details for the MTC device on what PDP connection to establish if this is not implicit for the MTC application. The format of this information can be application specific. An example would be to use SMS application port addressing with an URL embedded in the payload similar as once defined for WAP Push and nowadays used for MMS triggering).
- Mechanisms similar to Authentication and security headers as for USIM download could be contained in the TP-User_Data to ensure that an authorized MTC servers has triggered the MTC device.
- The existing flow as per clause 10 of TS 23.040 [6] would be triggered by the Service Centre without impacts (i.e. for the MSISDN case) to the SMS interfaces and involved nodes. The Service Centre sends the short message to the SMS GMSC. The SMS GMSC interrogates the HLR to retrieve routing information necessary to forward the short message, and then sends the message to the relevant MSC or SGSN, transiting other networks if necessary. The MSC or SGSN then sends the short message to the MS.
- The MTC Server receives Device Trigger Report from the Service Centre.



NOTE 1: This operation is not used by the SGSN.

Figure 6.44.2-3: Successful short message transfer attempt via the MSC or the SGSN

A further evolution of the MT SMS device trigger mechanism could be considered for a MSISDN-less mode of operation on the SMS provisioned interfaces.

The MAP message the SMS-GMSC uses to interrogate the HLR to retrieve routing information necessary to forward the short message currently carries the MSISDN. The HLR uses the MSISDN to retrieve the IMSI as well as other necessary information (e.g. Network Node Number/GPRS Node indicator) to which to forward the short message.

The MSIDSN usage for MT SMS would have to be replaced by a new device identifier. Two possibilities include:

- The MTC-IWF could maintain a mapping of the Device Identifier to the IMSI by interrogating the HLR. The intent would be to use the IMSI instead of the MSISDN in the MAP message possibly introducing a new IMSI IE. The HLR would subsequently be interrogated by the SMS-GMSC use the received IMSI as the index to retrieve the subscriber record containing the routing information. This approach requires 2 interrogations and is not efficient (unless the MTC-IWF also receives the routing information to be forwarded to the SC and used by the SMS-GMSC).

- Alternately, and more efficiently, the device identifier used on the MTCsp interface could be stored in the subscription information and would be propagated to the SC and used by the SMS-GMSC to interrogate the HLR which would return the IMSI and routing information based on the new device identifier.

- Either option requires introduction of new Device Identifier IE to replace the MSISDN in the existing MAP message (i.e. SendRoutingInfoForShortMsg).

NOTE 2: Typically the MSISDN (e.g. using MNC, MCC) and/or IMSI number series is used to determine which HLR to interrogate. If a solution is pursued such that the Service Centre does not map the new device identifier to an existing 3GPP Identifier (i.e. MSISDN, IMSI) an alternate means to determine which HLR to interrogate would be required and be FFS.

MAP services that may be influenced by a new identifier to replace the MSISDN include: MAP-SEND-ROUTING-INFO-FOR-SM , MAP-REPORT-SM-DELIVERY-STATUS , MAP-ALERT-SERVICE-CENTRE and MAP-INFORM-SERVICE-CENTRE. Correspondingly the following nodes that use these services would be influenced: HLR, SMS-GMSC, SMS-IWMSC, SMS-Router and IP-SM-GW.

Originator and destination address as defined in TS 23.040 [6] are qualified with "Type of number" (TON) and "Numbering plan identification" (NPI). This fields allow to define a private numbering plan other then E.164 MSISDN type number. Such a private numbering plan could be used as External Identifier for identifying UEs used for MTC that have to be reachable only from the operator domain to which they are subscribed. An advantage of such an Operator Specific External Identifier would be that existing SME SMS-SC protocols can be used on the MTCsp interface as established protocols typically expose the TON and NPI fields.

Editor's note: Whether the structure of the private numbering plan and the exact use of TON and NPI has to be specified by 3GPP or whether this is Operator specific is FFS.

6.44.3 Impacts on existing nodes or functionality

6.44.3.1 Impacts for MT-SMS device trigger - MSISDN based

In the case of a solution using MT SMS and the existing MSISDN based SMS interfaces it is expected that the entities and interfaces (i.e. interfaces 1 thru 5 of figure ZA below) are not impacted.

Impact on GPRS/EPS architecture:

- None, a SMS Service Center receiving triggers for MTC is identical to a SMS-SC as currently defined in the GPRS/EPS architecture.

Impact on the SMS-SC:

- May be impacted for solution that co-locates the MTC-IWF with the SMS-SC.

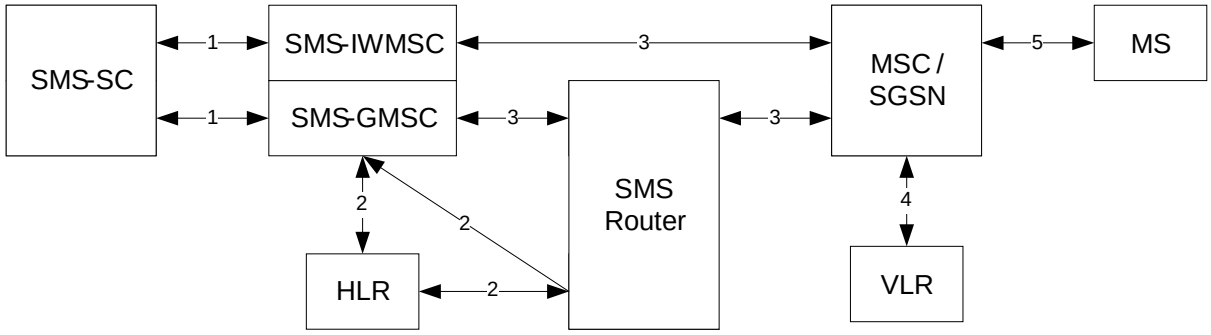
Introduction of a new protocol over the MTCsp interface point between MTC Server and the MTC-IWF. Depending on the external identifier format selected it will even be possible to use established protocols defined between SME and SMS-SC.

The Device Trigger Request could contain new device identifier (e.g. URI based or SMS-SC private address scheme) that the Service Centre will map to an existing 3GPP identifier (i.e. MSISDN) thereby eliminating impacts to interfaces 2-5 in figure 6.44.3-1 below.

6.44.3.2 Impacts for MT-SMS and MSISDN-less based

Impacts include the above along with SMS entities and related interface to allow MT-SMS based on IMSI

The main network structure from TS 23.040 [6] illustrated in figure 6.44.3-1 below highlights potential scope of impacts.



NOTE 1: Reference point 4 is not used for SMS transfer via the SGSN.
NOTE 2: The SMS Router is an optional entity that may be present in the MT case only. If it is not present, reference point 3 extends from the SMS-GMSC directly to the MSC/SGSN.

Figure 6.44.3-1: Main network structure and reference pts

MSISDN usage in existing messages on interfaces 1-5 would have to allow for an equivalent MSISDN-less mode. MSISDN usage primarily appears in operation in interface pts 1, 2, 3(SMS Router) and 4. On interface 5 IMSI appears to be use and may not be impacted by an MSISDN-less mode of operation.

HLR:

- The interrogation to the HLR to retrieve routing information, interface 2, would be based on new device identifier. HLR would store and access information based on this new device identifier.
- Handle updated MAP messages:
  - MAP-SEND-ROUTING-INFO-FOR-SM
  - MAP-REPORT-SM-DELIVERY-STATUS
  - MAP-INFORM-SERVICE-CENTRE
  - MAP-ALERT-SERVICE-CENTRE

NOTE 3: The HLR is already capable of retrieving routing information based on IMSI for applications other than SMS.

SMS-GMSC

- Interrogation of the HLR to retrieve routing information will be based on the new device identifier
- Handle updated MAP messages:
  - MAP-SEND-ROUTING-INFO-FOR-SM
  - MAP-REPORT-SM-DELIVERY-STATUS
  - MAP-INFORM-SERVICE-CENTRE

SMS-IWMSC

- Handle updated MAP message: MAP-ALERT-SERVICE-CENTRE

SMS-Router

- Handle updated MAP messages:
  - MAP-SEND-ROUTING-INFO-FOR-SM
  - MAP-INFORM-SERVICE-CENTRE

IP-SM-GW

- Handle updated MAP messages:

- MAP-SEND-ROUTING-INFO-FOR-SM
- MAP-REPORT-SM-DELIVERY-STATUS

Other non SMS functionality may be affected by the absence MSISDN in the subscriber record. For example charging records generated by the SGSN may be populated with the MSISDN. See Annex A for further MSISDN dependencies and impacts for supporting MSISDN-less subscriptions which is a prerequisite for MSISDN-less/MT-SMS functionality.

Further MAP messages are impacted in case SMS is enhanced for MSISDN-less subscriptions for the general case i.e. not only for MT-SMS used for online triggering.

6.44.3.3 Properties of the solution

This solution for MSISDN-less MT-SMS device triggering implies that:

a) The MTC-IWF shall behave as a Short Message Entity towards the SMS Service Centre;

b) The MTCsms interface pt shall maximize reuse of existing SME (MTC-IWF) SMS Service Centre protocols. SMPP is a main target for support.;

c) A decision needs to be taken whether the MTCsms interface shall be brought into 3GPP or whether to continue having it outside the 3GPP specification (as per existing TS 23.040 [6] support) and be referenced using existing TS 23.039, to identify updated de-facto standards(s);

d) For MTCsms: usage of other numbering plan than "ISDN/telephone numbering plan (E.164/E.163)" between the SME and SMS service centre may be considered if that minimize system impacts;

e) Necessary MAP (TS 29.002 [18]) updates for MSISDN-less MT-SMS may require techniques (e.g. use of dummy MSISDN, MSISDN Alert values) to populate mandatory fields allowing introduction of new identifier information elements in a manner that minimizes system impacts;

NOTE: Similar way to extend MAP will be required to introduce MSISDN-less support for PS only subscriptions in general;

f) Consideration to exclude CAMEL support for MSISDN-less MT-SMS if not deemed essential for Rel-11 device triggering; and

g) Deployment of MSISDN-less MT-SMS is dependent on and requires general MSISDN-less subscription system support, or shared/dummy MSISDNs used by multiple subscriptions.

6.44.4 Evaluation

This solution minimizes system impacts by building on and extending the existing SMS functionality.

Benefits for both solutions include:

- Allows for use of new Device identifier within the MTC Server Provider domain
- Provides over a standardized interface the means for the MTC Server to trigger a device to establish a connection and to start to communicate with the MTC Server.
- The MTCsp interface can be a stable interface to the MTC Server, while allowing device triggering methods internal in the PLMN to evolve (e.g. MT SMS - MSISDN-less, or even new non-SMS triggering techniques).
- Can be used as a first phase in a migration towards a more optimized triggering solution. The interface towards the MTC Server is stable regardless what triggering method is used internally in the PLMN.
- Well established protocols for SME SMS-SC can be re-used on the on the MTCsms interface.
- Also addresses "Key issues" for small data transmission.

Drawbacks for both solutions include:

- SMS infrastructure and interface impacts.

MT-SMS - MSISDN based

Benefits

- MTC-IWF that performs MTCsp device id mapping to MSISDN allows for complete re-use of MT-SMS and associated infrastructure with no impacts to the SMS nodes and interfaces.
- Address part of the "Key Issue - MTC Identifiers" by using non E164 numbering plans.

MT-SMS– MSISDN-less

Benefits

- Re-uses existing SMS infrastructure (though with impacts).
- Address part of the "Key Issue - MTC Identifiers" whereby PS-Only MT SMS can be delivered without MSISDN.

6.45 Solution – Device trigger gateway solution

6.45.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger",

clause 5.3 "Key Issue - IP Addressing",

clause 5.11 "Key Issue - Decoupling MTC Server from 3GPP Architecture" and

clause 5.13 "Key Issue - MTC Identifiers".

6.45.2 General

This solution shows how the key issue MTC Device Trigger can be solved with a control plane Device Trigger Gateway (DT-GW) function in the HPLMN that is flexible enough to transparently, from MTC Server/Application perspective, utilize different 3GPP services available within a particular PLMN for delivery of device trigger information from the 3GPP system to the UE while providing a single protocol for submission of the device trigger request from the MTC Server to the 3GPP system. The set of device trigger delivery services described in this solution are only for example purposes in order to show how the DT-GW solution can support any device trigger delivery service supported by the HPLMN.

A DT-GW function could be implemented as a standalone physical entity or a functional entity. At least one DT-GW function is deployed in a HPLMN that supports the MTC device trigger feature. The DT-GW function is deployed on the boundary between the HPLMN and the public Internet, Intranet or ISP.

To align this solution with the architectural reference model for MTC, described in clause 4.3, the DT-GW function is implemented as a functional entity within the MTC-IWF, thus simply further referred to as the Device Trigger (DT) function. The device trigger request is submitted by the MTC Server to the HPLMN of the subscribed device over the MTCsp reference point.

6.45.3 Submission of device trigger request from MTC Server to HPLMN

At any given point of time, there is at least one reachable MTC-IWF with DT function capability assigned for each subscribed MS/UE. The MTC-IWF terminates the MTCsp reference point which is used for submission of a device trigger request from an authorized MTC Server.

The authorized MTC Server determines the IP address/ports for submitting device trigger request to a particular UE used for MTC over MTCsp through either local configuration in the MTC Server or DNS resolution as described in clause 6.46.4. Once the IP address/ports of the assigned MTC-IWF are known, the MTC Server submits a device trigger request to the assigned MTC-IWF encapsulated in an IP packet.

When a trigger indication is received from a submitting node, the DT function first authorizes the received request, making sure it originated from a trusted MTC Server and is targeted for a device for which the MTC Server is authorized to trigger. The set of authorized MTC Servers for device triggering of a particular UE used for MTC could be configured in the assigned MTC-IWF or in the subscription data for the UE in the HSS/HLR.

6.45.4 HPLMN internal handling of device triggers

The next step is for the DT function to determine the device trigger delivery service and route to utilize for delivery of the device trigger to the UE used for MTC. This decision can be based on the one or more of the following criteria:

- current reachability information of the UE; and/or;
- the possible device trigger delivery services supported by the HPLMN and, when roaming, VPLMN; and/or
- the UE's device trigger delivery service capabilities; and/or
- any MNO device trigger delivery policies; and/or
- information received from the MTC Server.

The HLR/HSS is interrogated to gather UE reachability information. The relational identity (e.g. MCC, MNC) of the HLR/HSS to interrogate can be abstracted or derived from the external identifier included in the device trigger request (e.g. as is done today based on MSISDN). The external identifier could be a hostname device identity or a 3GPP/EPS-level subscription identity (e.g. MSISDN or ICCID). After which, the DT function then interrogates the determined HLR/HSS using the C and/or Sh interface.

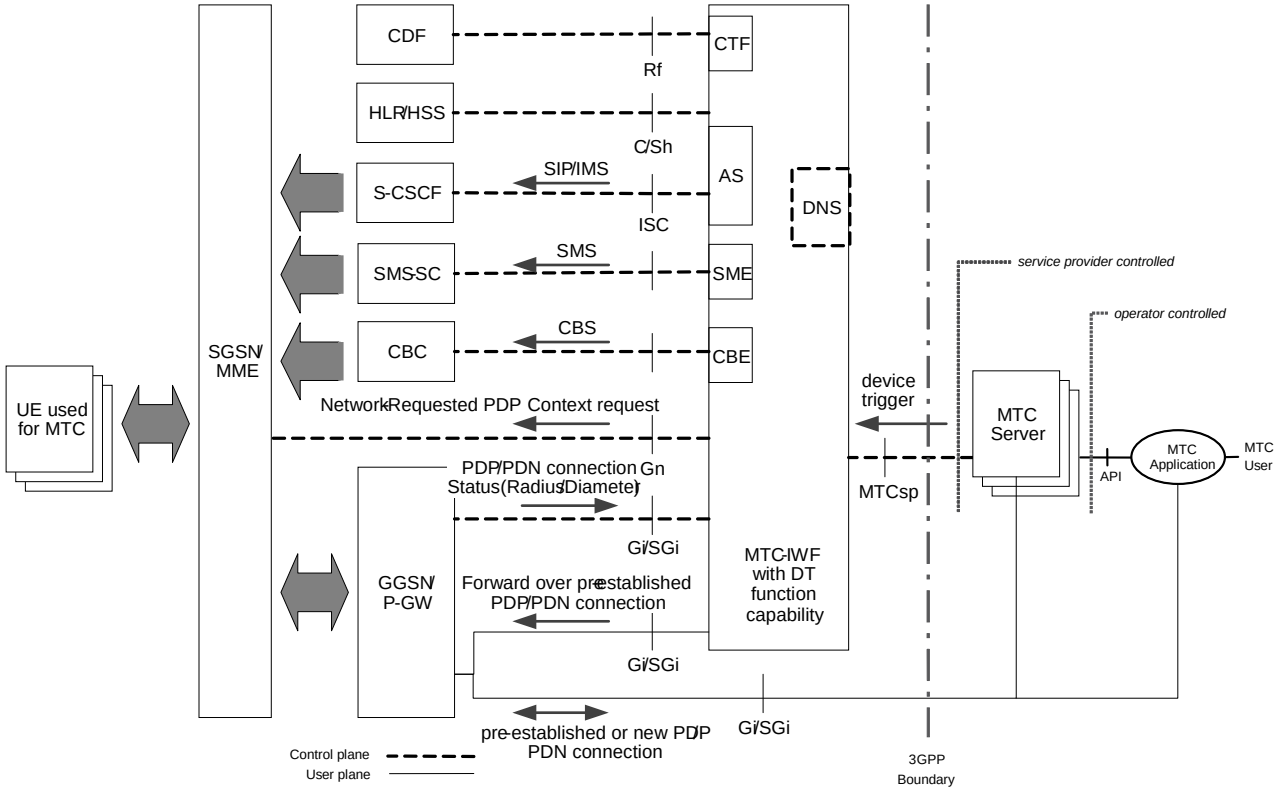


Figure 6.45.4-1: MTC device trigger function architecture with examples of possible DT delivery services

The interrogated HLR/HSS returns the latest reachability information available in the HLR/HSS for the specified UE. Additionally, the HLR/HSS could return the device trigger delivery service capabilities of the UE.

Separately, for each UE with an assigned MTC-IWF, GGSN/P-GW reports the status of PDP/PDN connections (i.e. PDP/PDN connection establishment/disconnection and IP address changes) to the assigned MTC-IWF using the Radius/Diameter interface (as described in clause 16 of TS 29.061 [4]).

MNO device trigger delivery policy information could be configured as part of the subscription data in the HLR/HSS, the MTC-IWF.

The DT function uses the gathered reachability, capabilities and MNO policy information to determine the most efficient and effective service and route to use for forwarding delivery of the device trigger indication to be delivered to the UE used for MTC.

To support the charging of device triggering, the DT function includes a CTF (Charging Trigger Function) in order to generate charging events based on the triggering indications sent by the MTC Server. To support this, an Rf reference point is defined between the MTC-IWF and the CDF entity.

To support the SMS based trigger, the DT function includes a SME (Short Message Entity) function in order to generate SMS trigger requests based on the triggering indications sent by the MTC Server. The SME uses validity time in MTCsp for mapping to the Validity Period in SMS delivery.

6.45.5 Delivery of device trigger from HPLMN to UE

The device trigger delivery services described in this clause are for example purposes only in order to show how the DT-GW solution can support any device trigger delivery service supported by the HPLMN. Some possible examples of device trigger delivery services that could be supported are shown in Figure 6.45.4-1, for which the DT function reformats, as needed, and forwards the trigger indication to the appropriate:

a) GGSN/P-GW for delivery over an already established PDP context / PDN connection;

b) GGSN for delivery over a newly established PDP context (via a Network-Requested PDP Context Activation Procedure initiated by the DT function e.g. as described in clause 6.41);

c) S-CSCF for delivery over SIP/IMS service;

d) SMS-SC for delivery over SMS; or

e) CBC for broadcast delivery over CBS (assumes location information available in trigger indication request or from other source in order to limit the broadcast area).

When a routable PDP context / PDN connection is pre-established in the UE used for MTC (as described in bullet a) or is newly established (as described in bullet b), the DT function utilizes this connection to deliver the device trigger to the UE using IP-based communications.

The deployment of these trigger delivery services could be done in a phased approach without impacting the MTC Server implementation which will be largely transparent to the delivery service mechanism selected by the DT function.

6.45.6 DT functionality

The DT functionality includes the following:

- submission over MTCsp of a device trigger indication messages into the PLMN request from an MTC Server to the assigned MTC-IWF of a targeted UE used for MTC;

NOTE: It should be possible for an MTC Server to resolve by DNS the MTC-IWF for a specific UE used for MTC.

- authorization that the device trigger request is from a trusted MTC Server;

- authorization that the UE used for MTC addressed in a device trigger request is from a MTC Server that is authorized to trigger the addressed UE used for MTC;

- determination of HLR/HSS to interrogate for the availability of the UE used for MTC based on the external identifier included in the device trigger request;

- selection of the device trigger delivery service and route to use for delivery of the device trigger to the UE used for MTC (e.g. based on collected reachability information , UE's device trigger delivery service capabilities and network operator policy);

- reformatting, as needed, of the device trigger information to match the format required for the selected delivery service;

- forwarding of trigger information from the DT function to the selected delivery service entity for delivery to the UE used for MTC;

- generation of accounting messages at the CTF; and

- Appropriate e.g. error handling, error logging and/or error notification when trigger indication is determined to be invalid or unauthorized.

The UE used for MTC must be capable of receiving, interpreting and providing a trigger indication to the appropriate MTC application on the UE, if the trigger content is application specific.

6.45.7 Information flows

MTC-IWF receives a Device Trigger request from the MTC server, interrogates the HSS to obtain UE IMSI and serving SGSN/MME information etc., if not available locally and delivers trigger information to the next serving node involved in the delivery of the trigger request.

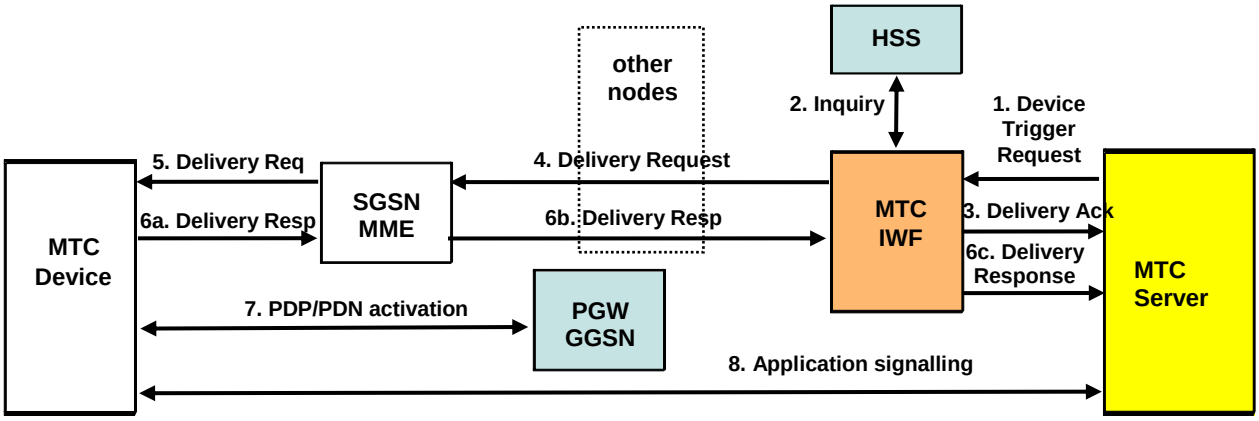


Figure 6.45.7-1: Device Trigger Flow

1. The MTC Server wants to communicate with the MTC device, but has no sufficient information for being able to send data packets to the MTC device or identified a need to recover or test IP connectivity, e.g. as the device is not responding anymore. The MTC server submits a Device Trigger Request providing the external device identifier and optionally a validity period or need for recovery of the IP connectivity.

2. The MTC-IWF authorises the trigger request. The IWF interrogates the HSS with the external device identifier to derive the IMSI and any additional information needed for trigger delivery.

3. The MTC-IWF may return trigger Deliver Ack to the MTC server confirming the submission of trigger request. In case of failure, a failure cause may be included to indicate the reason of failure e.g., network congested or overloaded, MTC-IWF can not find UE routing information from HSS, UE is unreachable, etc.

4. The MTC-IWF selects the trigger delivery method and forwards the delivery request to the next node involved in the delivery.

   For the trigger delivered over T5a/T5b, if any APN is provided and known and no bearer exists for that APN the SGSN/MME may perform APN related load control, i.e. decides whether to deliver the request to the device.

5. The SGSN/MME delivers the device trigger to the MTC device using Delivery Request message. For the trigger delivered over T5a/T5b, the delivery of Delivery Request may be upon the next NAS signalling exchange with the UE as indicated in clause 6.39 step 3.

6. The success or failure of delivery of trigger Delivery Request is acknowledged to the MTC server via Delivery Response message with appropriate cause value.

   For successful delivery of the device trigger, the MTC device acknowledges the Delivery Request using Delivery Response message with a success cause value to the MTC server via SGSN/MME and MTC-IWF (steps 6a, 6b and 6c). For the trigger delivered over T5, the Delivery Response message may be different NAS messages.

7. The MTC device activates the PDP/PDN connection if necessary.

8. The application on the MTC device communicates with the MTC server, e.g. it registers with the application server.

Editor's note: The handling of the validity period needs to be described.

6.45.8 Impacts on existing nodes or functionality

Impact to the Core Network:

- Deployment of the DT function;
- New instances of pre-defined reference points (e.g. C, Sh, ISC, Gn, Gi/SGi) to connect the DT function in the MTC-IWF to HLR/HSS, the GGSN/P-GWs and the actual trigger delivery services (e.g, SMSC, CBS, S-CSCF, GGSN/PGW, etc.).
- Storage of the assigned MTC-IWF of a particular UE used MTC and possibly the UE's device trigger delivery service capabilities;
- HLR/HSS, MTC-IWF or UE to store addresses of authorized MTC servers for device triggering of a particular MTC device;
- HLR/HSS or MTC-IWF to store network operator policy information used for device trigger delivery service and route.

6.45.9 Evaluation

Benefits:

- Remove the burden of determining the type of trigger delivery service to invoke and support from MTC Server implementation;
- Allow for many different sets of trigger delivery services to be utilized across MNOs without impacting MTC Server on the device trigger request submission functionality (i.e. delivery to UE transparent from submission to HPLMN);
- Allows for secure authorization and delivery of device triggers from authorized MTC Servers;
- Supports both MSISDN-based and MSISDN-less subscriptions (with phased rollout approach and/or simultaneously support).

Drawbacks:

- Requires new device trigger information to be stored in HLR/HSS;
- Requires new DT function in the HPLMN;
- Requires new instances of pre-defined reference points for reachability determination;

6.46 Solution - Address resolution via MTC-IWF

6.46.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue - IP Addressing" , clause 5.8 "Key Issue - MTC Device Trigger" and clause 5.13 "Key Issue - MTC Identifiers".

6.46.2 General

This solution solves two similar requirements:

- How to determine the routable IP address(es) of a UE used for MTC for initiating UP MT communications (as required in clause 5.3.2); and;
- How to determine the MTCsp reference point terminating in the assigned MTC-IWF of a UE used for MTC to initiate CP device triggering (required in clause 5.8.2).

Similar to the solution in clauses 6.1 and 6.38, UEs used for MTC that need to be reachable for data plane mobile terminated communications are assigned an external identifier that can be structured as a static unique hostname (e.g. a FQDN, NAI, dedicated 3GPP URN or URI).

Distinct from the solutions in clause 6.1 and 6.38, the hostname of the device is used to perform a DNS query for the address of the MTCsp reference point terminating in the assigned MTC-IWF. This address is then used either to request the assigned MTC-IWF for the routable IP address(es) to use for initiating data plane mobile terminated communications, as described further in clause 6.43.3, or to request the assigned MTC-IWF to e.g. perform control plane device triggering, as described further in clause 6.43.4.

When a message related to a particular UE used for MTC is sent over MTCsp, the device external identifier included in the message could be a hostname or just the standalone 3GPP/EPS-level external subscription identity of the UE (e.g. MSISDN, ICCID). In either case, this solution can simultaneously support both MSISDN-based and MSISDN-less subscriptions. However, to allow for a phased rollout of MTC features, initially this solution may only support subscriptions with an assigned MSISDN.

As the assigned MTC-IWF for a particular UE used for MTC will rarely change, if at all, the MTC Server will infrequently need to perform the DNS query to resolve the assigned MTC-IWF address. This approach significantly reduces the number of DNS query procedures to be performed relative to if a DNS query were to be performed each time a MTC Server needed to determine the current reachable IP addresses of a particular UE used for MTC. Additionally, this approach significantly reduces the number of DNS updates that must be performed relative to if a DNS update were to be performed each time a PDN connection was established or disconnected for a UE used for MTC (aka dynamic DNS).

6.46.3 UP MT communications UE current IP address resolution

When the routable UP IP address of the target UE is unknown, the sample call flow scenario depicted in Figure 6.46.3-1 illustrates how UP MT communication can be achieved through the use of the hostname device identity lookup of the IP address of the assigned MTC-IWF.

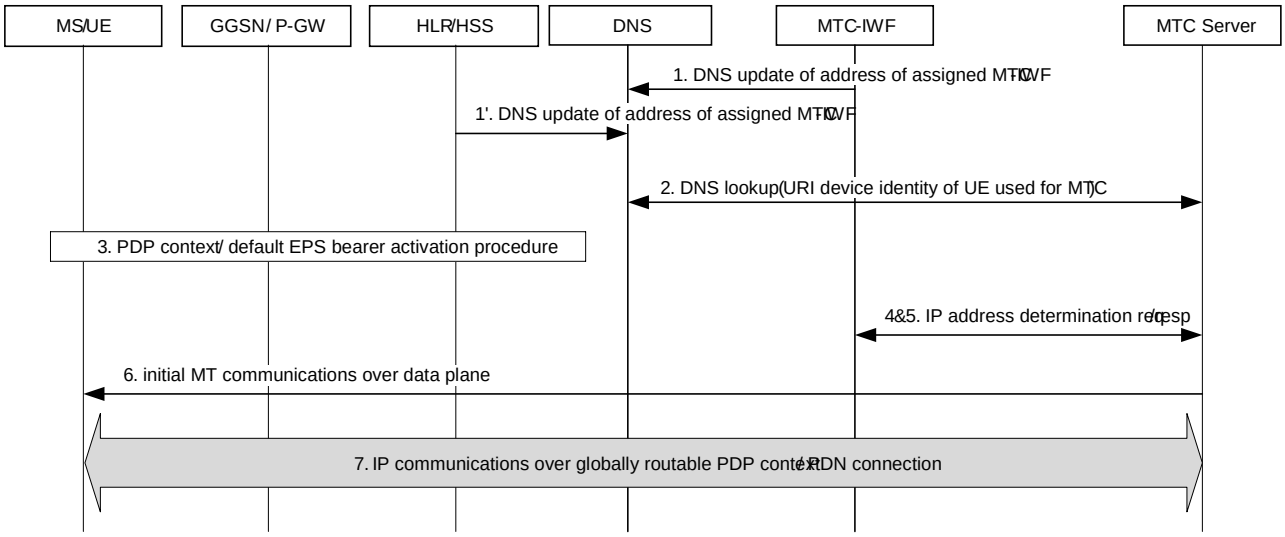


Figure 6.46.3-1: Call flow scenario for UP MT communications UE current IP address resolution

1. Initially, e.g. when the UE used for MTC subscription is provisioned or changed, a MTC-IWF of the HPLMN is assigned as part of the subscription data stored in the HSS/HLR. Afterwards, the MTC-IWF performs a DNS update to the DNS authoritative server that stores the association between the hostname of the UE and the assigned MTC-IWF address.

1'. Alternatively, the HSS/HLR could perform the DNS update to the DNS server.

2. At some point thereafter, the MTC Server performs a DNS query for the hostname of the UE in order to determine the address of the assigned MTC-IWF. The MTC Server may then store the assigned MTC-IWF address for later use while assuming the assigned MTC-IWF will largely not be changed for the UE.

3. At some point thereafter, a PDP/PDN connection is initiated and established for the UE that is reachable by the MTC Server.

4. At some point thereafter, the MTC Server needs to initiate MT communicate with the UE but does not know the routable IP address(es); thus will send an IP address determination query to the assigned MTC-IWF over MTCsp.

5. The assigned MTC-IWF returns an IP address determination response with the routable IP address(es) and, possibly, the SRC/DST ports to use for MT communications with the UE.

6. The MTC Server initiates the MT communications.

6.46.4 CP device triggering assigned MTC-IWF address resolution

When the MTCsp reference point for submitting a CP device trigger to a target UE is unknown, the sample call flow scenario depicted in Figure 6.46.4-1 illustrates how CP device triggering can be achieved through the use of the hostname device identity lookup of the IP address of the assigned MTC-IWF.

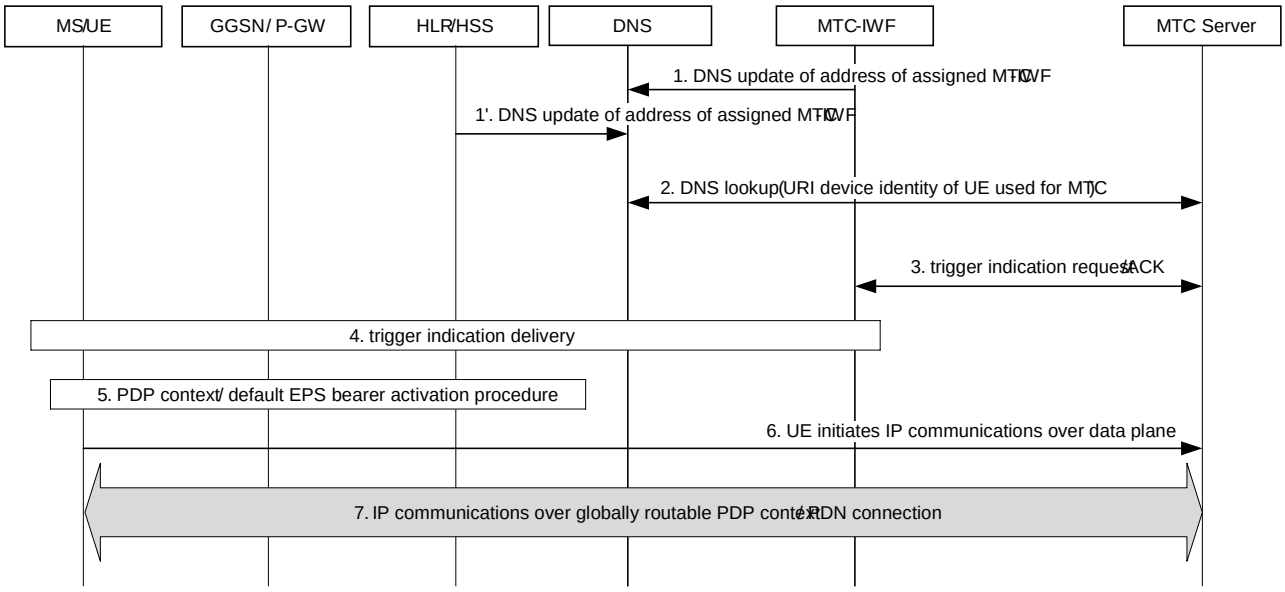


Figure 6.46.4-1: Call flow scenario for CP device triggering assigned MTC-IWF address resolution

1-2. Same as steps 1-2 illustrated in figure 6.46.3-1.

3. At some point thereafter, the MTC Server needs to send a device trigger indication to the UE used for MTC; thus sending it to the assigned MTC-IWF over MTCsp.

4. The network delivers the device trigger indication to the UE.

5. A PDP/PDN connection is initiated and established for the UE that is reachable by the MTC Server.

6. The UE initiates data plane communications with the requesting entity (e.g. MTC Server).

7. IP communications continues.

6.46.5 Impacts on existing nodes or functionality

Impacts on CN nodes:

- DT function solution specified in clause 6.45 shall be supported by the Core Network;

- a network interface between authoritative DNS server and DT-GW is required to perform DNS updates when the assigned DT-GW for a UE used for MTC is initially assigned or changed.

6.46.4 Evaluation

Benefits:

- DNS update and DNS query frequency drastically less vs. requiring a DNS update/query each time a PDN connection is established/disconnected or the IP address of the device changes;

- As assigned MTC-IWF will rarely change, if at all, there is little risk of "middlemen" ISPs ignoring the TTL for a DNS record containing the association of the hostname of the UE used for MTC and the assigned MTC-IWF address;
- For security, DNS updates of the authoritative DNS server can be limited to only originating from within the HPLMN;
- Supports both MSISDN-based and MSISDN-less subscriptions (with phased rollout approach and/or simultaneously).

Drawbacks:

- Dependency on MTC-IWF deployment in HPLMN.

6.47 Solution – UE without unique MSISDN using ICCID

6.47.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue – MTC Device Trigger", see clause 5.13 "Key Issue – MTC Identifiers".

6.47.2 General

A unique Integrated Circuit Card ID (ICCID), defined by ITU-T Recommendation E.118 [7], is stored today in every UICC. The ICCID may be used by a mobile network, MTC Server, MTC Application and/or MTC user as a unique external identifier for PS only devices that do not specifically require an MSISDN (i.e. no Circuit-Switched support).

The ICCID is a 20-digit number comprised of a variable length (maximum 7-digits) Issue Identification Number (IIN), a variable length (11 to 14 digits) Individual account identification number and a check digit. It is stored in the UICC Elementary File, EFICCID and efficiently encoded in BCD format (1-nibble per digit) as described in ETSI TS 102.221 [8].

An ICCID with the minimum sized Individual account identification number (11-digits) provides ~$10^{\wedge 11}$ or 100B unique identifiers per IIN. This amount per issuer (e.g. per MNO) would appear to be more than adequate to provide a new unique subscription identifier for the expected onslaught of new M2M devices.

Similar to the MSISDN, the composition of the ICCID contains enough routeing information that can be used to identify the HSS/HLR of the MS/UE. The IIN is composed of a Country code field (analogous to the CC in the MSISDN or MCC in the IMSI) and an Issue identifier number field (analogous to the NDC in the MSISDN or the MNC in the IMSI). If further routeing information is required, it could be contained in the first few digits of the Individual account identification number field.

When a hostname based external identifier (e.g. FQDN, NAI, URI or 3GPP specific URN) is defined for a UE, the ICCID can be included as part of the hostname (e.g. FQDN: mtc.ICCID.pub.3gppnetworks.org or ICCID.userid.serviceproviderid.topdomain) in order to associate the hostname with a particular UE used for MTC.

If flexibility for 1-to-1 mapping between the external subscription identifier and IMSI are required (i.e. multiple unique external subscription identifiers per IMSI) then the ICCID could be used as a base for a set of multiple unique IDs associated with a particular IMSI.

The impacted network entities (e.g. MTC-IWF, HLR/HSS) and interface protocols are enhanced to support the above functionality so that a UE subscription can be identified by its ICCID and mapped to the internal identifier of the UE.

6.47.3 Impacts on existing nodes or functionality

6.47.4 Evaluation

Benefits:

- provides a pre-existing unique ID that is generated and available today at the device;
- could be a base for unique IDs when multiple subscription identifiers per IMSI are required;
- plethora (~100B) of unique IDs per Issue Identification Number;

- efficiently encoded.

Drawbacks:

- if (U)SIM needs to be swapped to change network operator subscription, ICCID will not be portable to new network operator;

- if (U)SIM is permanently coupled to ME, when subscription needs to be swapped to a different UE/MS, ICCID will not be portable to new device and MNO cannot use ICCID as a permanent identifier for the subscription;

Editor's note: It is FFS if subscription identifier portability is required for PS only subscriptions without MSISDN.

- the granularity for the ICCID is per MT and there could be multiple TEs per MT;

- similar to MSISDN, ICCID identifier of a UE/MS is easily ascertainable (e.g. sometimes printed on inside device).

6.48 Solution - Transfer data via SMS for MTC Devices sharing one MSISDN

6.48.1 Problem Solved / Gains Provided

See clause 5.2 "Key Issue - MTC Devices communicating with one or more MTC Servers." and 5.13 "Key Issue - MTC Identifiers"

6.48.2 General

For the lack of MSISDN, MTC Devices belonging to the same MTC Subscriber could share one MSISDN for the purpose of transferring data via SMS. For these MTC Devices, a static unique "MTC Device ID" (e.g. an FQDN identifier or a private number specific to the MTC device or subscription such as IMSI) needs to be assigned and the association between the "MTC Device ID" and the IMSI is stored in HLR/HSS, in case the "MTC Device ID" is not the IMSI, and optionally in the VAS AS. The static "MTC Device ID" can be configured into the MTC Device via OMA DM or SIM OTA or be statically configured as part of the subscription info. Privacy of "MTC Device ID" has to be protected if the "MTC Device ID" is configured in the MTC Device.

NOTE 1: Using the IMSI as "MTC Device ID" (i.e. as an External identifier) implies that the MTC Server may have to be under operator control or have trust relationship with the operator.

Editor's note: How the coupling between the common MSISDN and a static unique "MTC Device ID" can support number portability requirements, if needed, is FFS.

For MO communication of MTC devices sharing one MSISDN via SMS (i.e. the SMS is sent from the MTC Device to the MTC Server), the MTC Device shall insert the "MTC Device ID" into the SMS. The MTC Server identifies the MTC Device by the "MTC Device ID" contained in the SMS.

Alternatively, the "MTC Device ID" is inserted by the MSC/SGSN in the MAP-MO-FORWARD-SHORT-MESSAGE similar to how it works with the MSISDN in current specifications.

For MT communication of MTC devices sharing one MSISDN via SMS (i.e. the SMS is sent from the MTC Server to the MTC Device), the following procedures are performed:

- The MTC Server sends a SMS with the "MTC Device ID" in the header or the body of the SMS and the DA (destination address) of the SMS is set to the common MSISDN of the target MTC Device. And the SMS is routed to the VAS AS serving the MTC Devices identified by the common MSISDN.

- The VAS AS acts as an SMS GMSC to interrogate the HLR/HSS with the "MTC Device ID" which is obtained from the SMS directly. Or, if the VAS AS has stored the mapping information between the IMSI and the "MTC Device ID" of the MTC Device, the VAS AS interrogates the HLR/HSS with the IMSI of the MTC Device if the "MTC Device ID" is not the IMSI, based on the "MTC Device ID" in the SMS.

- The VAS AS delivers the SMS to the MTC Device according to the routing info returned from the HLR/HSS.

- The MTC Device verifies the "MTC Device ID" in the message upon receiving the SMS.

Alternatively, in case having stored the internal association between "MTC Device ID" and the IMSI, if the "MTC Device ID" is not the IMSI, VAS AS can submit to the SMS Center a new SMS as specified in TS 23.142 [9] with the DA of the SMS set to the IMSI of the MTC Device. After receiving the SMS submitted by the VAS AS, SMS GMSC interrogates the HLR/HSS with the IMSI. With the returned routing information from HLR/HSS, SMS GMSC delivers the SMS to the MTC Devices according to the IMSI and the routing info as specified in TS 23.040 [6].

Another alternative method is that the SMS GMSC interrogates the HLR/HSS with the "MTC Device ID" which is obtained from the SMS and delivers the SMS according to the IMSI and the routing info returned from HLR/HSS as specified in TS 23.040 [6] when receiving the SMS from the MTC Server. No VAS AS is involved in this alternative.

Editor's note: The use of the shared MSISDN in the delivery of SMSs needs to be further developed.

6.48.3 Impacts on existing nodes or functionality

This solution is dependent on 6.2 Solution - Transfer data via SMS. See also clause 6.2.3.

6.48.4 Evaluation

Drawbacks:

- Including the "MTC Device ID" inside the SMS would decrease the effective payload size and increase overhead. Some "MTC device ID" proposed in this TR may exceed the size of SMS, e.g. an URI. Concatenated SMSs can be used in order to transfer the data and contain the "MTC device ID". The "MTC Device ID" when provided by the UE will need to be linked to the subscription so that it can be trusted.
- Modifications to the MSC/SGSN are required if the "MTC Device ID" is asserted by the MSC/SGSN. Modifications to the protocol are also required if the "MTC Device ID" cannot be carried in the TS 23.040 [6] TP-OA field.
- For MT communication of MTC devices sharing one MSISDN modifications will be required to SMS-GMSC and HSS if the "MTC Device ID" cannot be carried in the TP-DA field.
- The MSC/SGSN may have problems with large numbers of devices sharing the same MSISDN.
- Impacts on the OCS if a large number of devices are sharing the same MSISDN.

6.49 Solution - UE configured to build its IPv6 address with the provided interface identifier

6.49.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue - IP addressing".

6.49.2 General

According to TS 23.401 [5] and TS 23.060 [21], the GGSN/P-GW shall provide an interface identifier to the UE to use it as a link-local address in order to avoid any collision with the link-local address of the GGSN/P-GW. This interface identifier may also be used by the UE to build its global IPv6 address.

For functions requiring the full IP address knowledge in the network, it is proposed in this solution that the UE uses the interface identifier assigned by the GGSN/P-GW to construct its global IPv6 address. Thus, the MTC device will append its interface identifier (64 bits) to the prefix (64 bits) received in the Router Advertisement. For security reasons, it is assumed that the GGSN/P-GW is in charge of providing a well randomized interface identifier.

Consequently, the GGSN/P-GW knows the full IPv6 address used by the MTC device and solutions listed in clauses 6.1 and 6.41 can be realised without any need for a stateful address configuration.

To support this solution, a "UE configured to build its IPv6 address with the provided interface identifier" is introduced. Such UE shall indicate to the GGSN/P-GW that it will use the interface identifier to construct its global IPv6 address. In addition, MTC device should keep the global address configured and avoid changing its interface ID.

6.50 Solution - Use of FQDN Identifier with Dynamic DNS Update

6.50.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue - IP addressing" and clause 5.2 "Key Issue - MTC Devices communicating with one or more MTC Servers".

6.50.2 General

This solution addresses some aspects of IP addressing related to MT communications initiated by the MTC server. It is based on the FQDN Identifier solution described in clause 6.1 and proposes to use dynamic DNS updates initiated by the UE instead of a network entity. In case of stateless IPv6 addressing, this overcomes the problem of the network ignoring the global IPv6 address used by the MTC device. In this case, DNS updates are performed after the UE configures its IPv6 address via stateless IPv6 address autoconfiguration and when the UE changes its IPv6 address. Hosts with a IPv6 stack that frequently change their address for privacy reasons can use Dynamic DNS Updates (RFC 2136) to allow the authoritative DNS to keep the association between FQDN and the current IP address up to date. This solution is also applicable to IPv4 addressing.

Editor's note: Huge numbers of UEs that frequently signal a change of IP address may create an untenable load on the network. Therefore, the use of IPv6 privacy extensions, and if used the frequency at which the UE may be allowed to change its IP address, is FFS.

Consequently, the call flow depicted in clause 6.1 becomes:

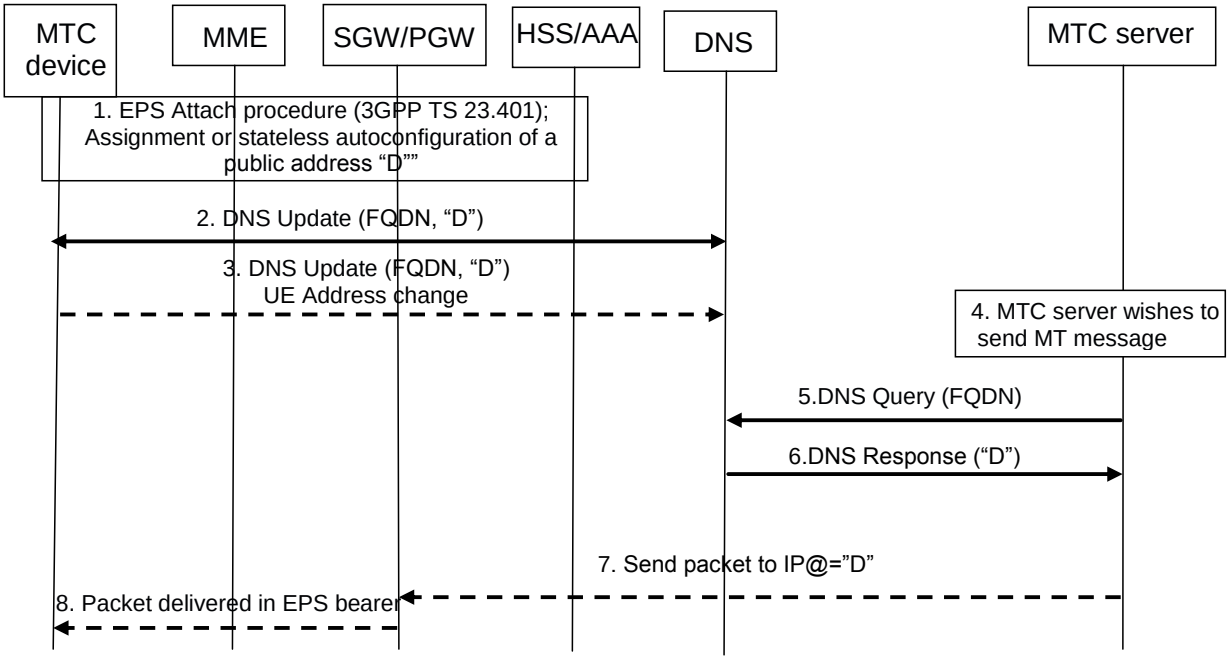


Figure 6.50.2-1: Call flow for MT communication with MTC device using Dynamic DNS Updates

1. MTC device performs the EPS Attach procedure as described in TS 23.401 [5]. As part of the EPS Attach procedure, a public IP address is assigned or Stateless IPv6 address autoconfiguration is accomplished, resulting in the MTC device being configured with a public IP address, referred to here shortly as "D", and information about the authoritative DNS is sent in PCO.

2, 3. MTC device stores the association between the FQDN and "D" in the authoritative DNS server. The MTC device performs DNS Updates whenever it changes its interface ID.

Editor's note: Huge numbers of UE that frequently signal a change of IP address may create an untenable load on the network. Therefore, the use of IPv6 privacy extensions, and if used the frequency at which the UE may be allowed to change its IP address, is FFS.

4. At some point the MTC server wishes to send a Mobile terminated (MT) message to the MTC device whose unique identifier is FQDN.
5. MTC server sends a DNS query to the authoritative DNS server.
6. The authoritative DNS sends "D" to the MTC server.
7. MTC server sets the Destination IP address in the packet it wishes to send to the MTC device to "D".
8. The PGW serving the MTC device delivers the packet to the MTC device using an appropriate EPS bearer.

NOTE 1: Security measures shall be taken in order to avoid attacks on the DNS from a rogue/misbehaving MTC device.

Editor's note: If the MTC device has multiple PDN connections, it is FFS which IP address the MTC Server selects for sending packets to the MTC device.

Editor's note: Scalability of this solution is FFS.

6.51 Solution- MT Communication with MTCsp/MTCsms signalling

6.51.1 Problem Solved/ Gains Provided

See clause 5.3 "Key Issue - IP Addressing".

6.51.2 General

This solution is based on using MTC Device Trigger from MTC Server in order to have the MTC device initiate an IP communication with the MTC server. The first outbound IP packet from the UE creates a mapping in the NAT device between the private IP address of the UE and a (public IP address, port number) couple. When the MTC server receives this IP packet, it knows the public IP address and port number allocated by the NAT to the UE.

This procedure is depicted in the figure below:

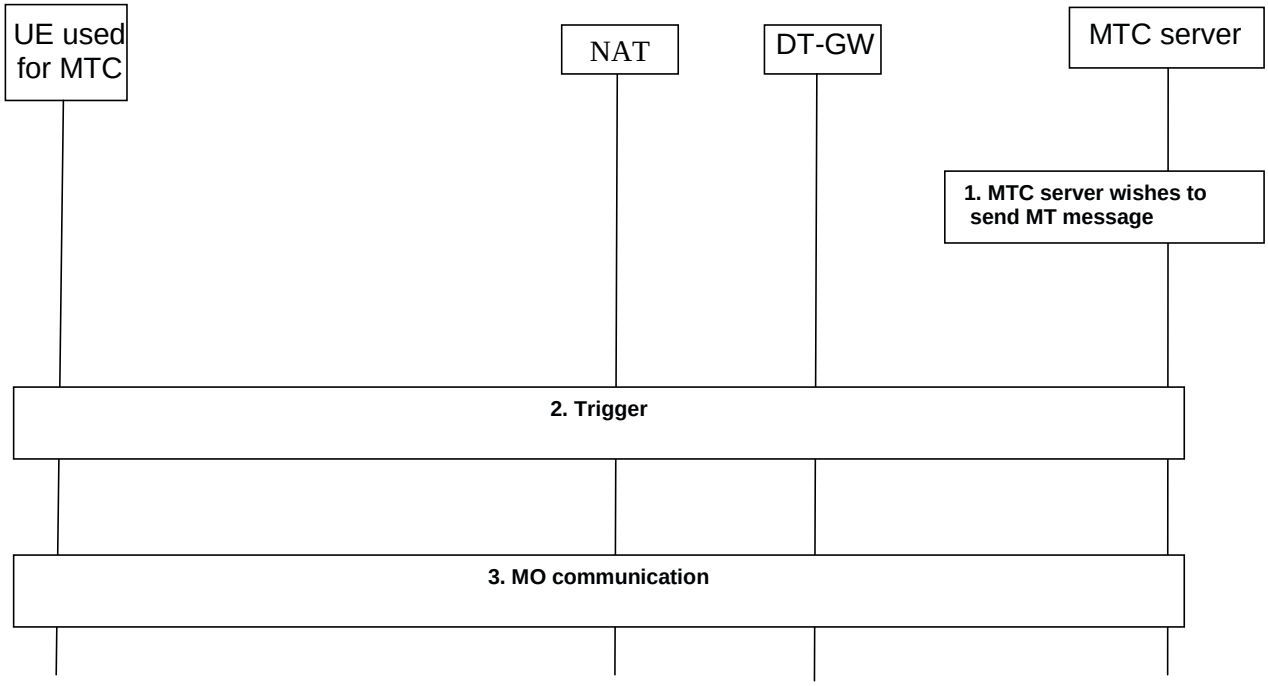


Figure 6.51.2-1: MT communication with MTCsp signalling

1. The MTC server wishes to send a Mobile Terminated packet to the UE used for MTC and the MTC server doesn't know the IP address of the UE used for MTC.

2. The MTC server sends a trigger indication over the MTCsp reference point to DT-GW (also called MTC IWF) or using MTCsms. Which trigger solution to use is agnostic for this solution, but the trigger needs to include the IP address (or FQDN) and port of the application that the UE has to contact.

NOTE 1: The trigger delivery service selected by the DT-GW is outside of the scope of this solution. The trigger delivery service is mainly described in clause 6.45, but can be also a part of other solutions.

3. Once the UE used for MTC is notified by the network, it initiates a communication to the MTC server by sending a trigger response; the first outbound packet creates a mapping from a port number on the NAT, which forwards the IP packet with a mapped public IP address and a port number that distinguishes the UE used for MTC within the private addressing space. The MTC server sends the MT packet to the targeted UE used for MTC within this communication.

NOTE 2: In order to recognize which UE used for MTC sent the IP packet containing the trigger response, the UE used for MTC should include its Device Identifier, which may be different from the one used over MTCsp/MTCsms. Alternatively, another mechanism could be specified to solve this need.

NOTE 3: If there are several applications running on the UE used for MTC, then the trigger needs to support multiple applications (e.g. see clauses 6.40 and 6.45)

6.51.3 Impacts on existing nodes or functionality

This solution reuses the Device Trigger Gateway solution described in clause 6.45. The only additional impact is on the MTC Server, to behave as described above.

6.51.4 Evaluation

Benefits for this solution include:

- No configuration of NAT is required.
- An external port on NAT is open only when there is a need for communication; this avoids the UE used for MTC to receive IP packets from non legitimate sources.
- Keep-alive messages are avoided when there is no traffic exchanged between the UE used for MTC and the MTC Server.

Drawbacks of this solution include:

- the solution relies on a trigger response message between the UE used for MTC and the MTC Server for delivery of the device ID;
- the solution relies on a separate channel to deliver a 'Push' stimulus.

6.52 Solution - Transfer of device trigger or data via optimised SMS

6.52.1 Problem Solved / Gains Provided

See clauses 5.4 "Key Issue - Online Small Data Transfer" and 5.8 "MTC Device Trigger".

6.52.2 General

6.52.2.1 Overview

Various mechanisms for addressing the MTC 'small data transmission' topic have been proposed in contributions to SA WG2. Typically they proposed message flows with some similarities to SMS, but, propose new interfaces and slightly different functionality. The use of such new functionality poses some challenges for rolling out the feature in roaming situations.

In order to allow a proper evaluation and identification of the best solution, this solution takes an alternative approach by looking at what optimisations can be made to the existing SMS mechanisms.

There are 6 components to the optimisations:

i) For UMTS-PS; UMTS-CS; GSM-CS; 2G-GPRS; and SMS over SGs in LTE; removal of the CP protocol layer.

ii) For LTE, SMS over SGs enhancements that give greater flexibility in the deployment of the MSC functionality.

iii) Extension of ii) to support stateless SMS-IWF.

iv) Evolution of the signalling interfaces between MME and HSS/SMSC.

v) For LTE, use of the pre-established NAS security context to transfer the SMS PDUs as NAS signalling without establishment of all the radio bearers or RRC security context.

vi) For delivery of Device Trigger information to UE over E-UTRAN using NAS signalling, an additional optimisation related to bullet point v) above is described.

Each component can be deployed independently. The capability to deploy these sub-features independently is anticipated to ease rollout and deployment issues, especially for roaming situations, and, where the MTC-subscriber needs coverage from more than one RAT.

Editor's note: Need to address how this solution can support subscription and operator policy on data size.

Editor's note: The small data upper limit needs to be specified for this solution.

Editor's note: The frequency of small data transmissions that can be supported with this solution needs to be described.

Editor's note: Whether or not mobility management needs to be supported during small data transmission needs to be specified (or the solution needs to provide retransmissions).

6.52.2.2 Removal of CP protocol layer

The 'real SMS' is sent in an RP-DATA message. Successful delivery of the SM to the SMSC (for Mobile Originated SMS) and to the mobile (for Mobile Terminated SMS) leads to the transmission of an RP-ACK message.

On all of the radio and network interfaces (LTE, 3G, 2G-PS, 2G-CS), a relatively reliable concatenation of layer 2 data links are used to transport the RP messages. Following successful radio transfer at layer 2, message loss is rareand can be covered by application layer retransmission at SMSC or mobile.

However, the RP messages are always encapsulated in CP-DATA messages and each CP-DATA message generates a CP-ACK message. The CP layer messages appear unnecessary, and, e.g. if a CP-ACK is lost, the CP layer can cause added delay. The CP layer also causes radio interface inefficiency.

Given the local nature of the CP protocols (they run between 'edge CN node' and the mobile) they could be removed independently on any RAT/domain.

The use/no-use of the CP protocol layer can be negotiated between the mobile and the 'edge CN node' at Attach/TAU/RAU/LAU and is then applicable within that TA, RA or LA.

NOTE 1: The "removal" of the CP protocol layer does not necessarily imply removal from the protocol stack. Instead, the "removal" can be effectively achieved by enhancing the state machines in the UE and in the network (refer to the normative Annex B: "SDL description of the CM layer" in TS 24.011), so that the CP-ACK is rarely sent. Moreover, for MO SMS the CP retransmission timer in the UE (TC1M) needs to be properly configured to account for the round-trip delay of the RP-PDU (from the network edge to the SMS-SC and backwards).

Removal of the CP layer would save one or two messages on the radio interface for MO SMS and MT SMS.

NOTE 2: For MO SMS the UE may need to indicate to the network that it has no more messages for sending, so that the network's signalling connection release procedure does not overtake the 'low priority' RP-ACK. In current specifications the network releases the signalling connection upon receipt of CP-ACK.

6.52.2.3 Flexible deployment of MSC functionality for SMS over SGs

In LTE, SMS is currently supported by both "SMS using IMS" and "SMS over SGs". In some deployment scenarios, the use of "SMS over IMS" can be regarded as rather heavyweight for low end M2M applications.

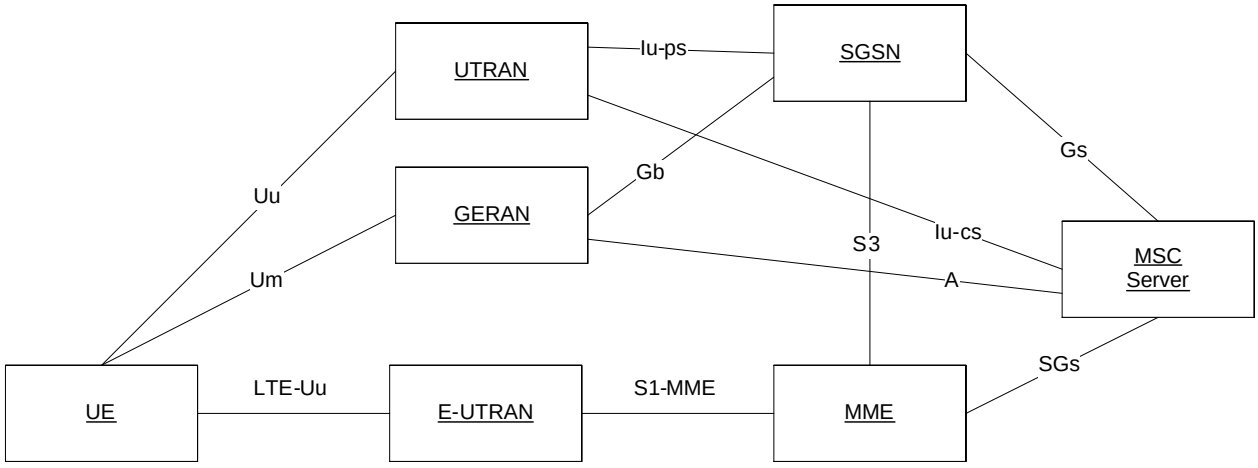


Figure 6.52.2.3-1: CS Fallback architecture (from TS 23.272 [23])

Figure 6.52.2.3-1 shows the current CS-Fallback architecture, the MSC/VLR function can become a standalone SMSoSGs function. The resulting architecture is shown below in Figure 6.52.2.3-2.

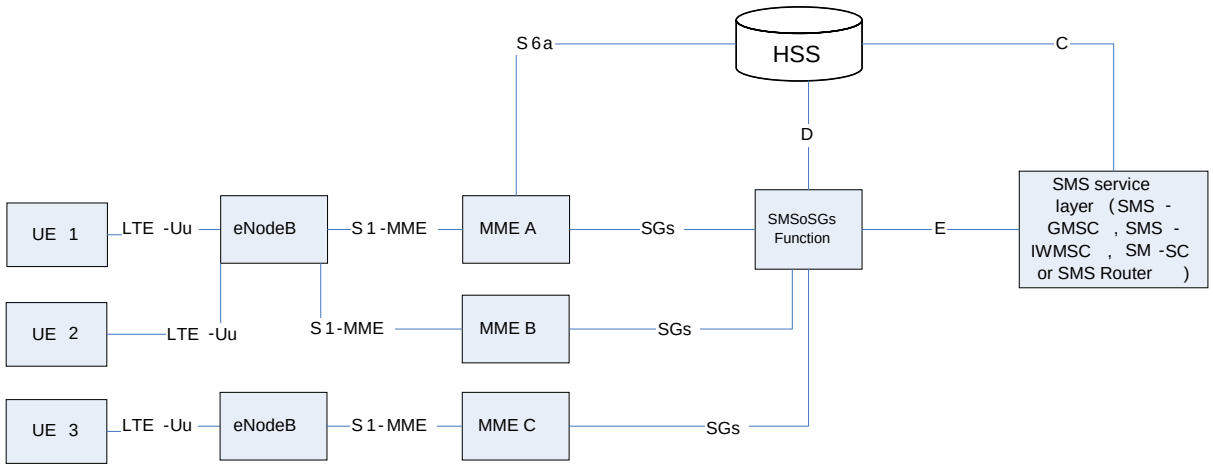


Figure 6.52.2.3-2: New architecture of MME and SMSoSGS Function, showing that multiple MMEs can be connected to one SMSoSGs Function

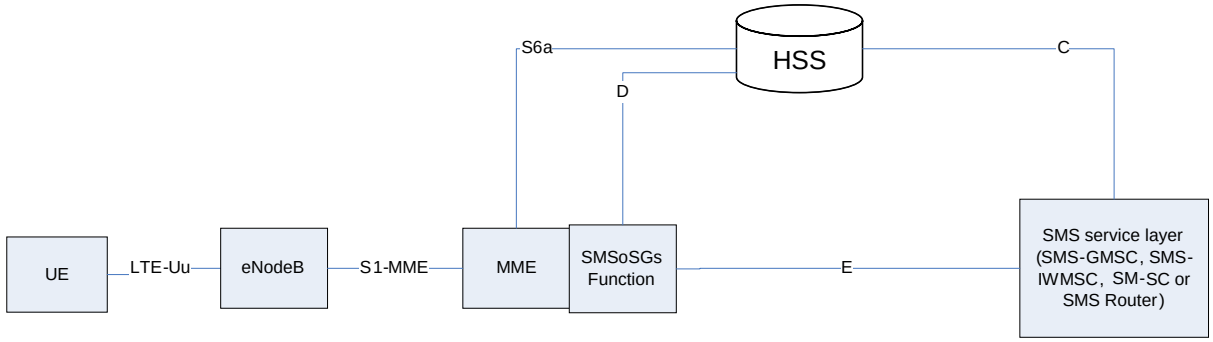


Figure 6.52.2.3-3: MME and integrated SGs SMSoSGs Function

NOTE: The architectures shown in Figures 6.52.2.3-2 and 6.52.2.3-3 could also be used by CSFB devices, but, Fall Back will entail an MSC change.

These architectures permit an LTE operator to use SMS over SGs without substantial investments in CS domain infrastructure. Upgrades to the HSS or SMSC are not required.

6.52.2.4 Stateless SMS IWF

The handling of SMS in CS Fall Back today requires the MSC/VLR to have 'CS domain' Mobility Management functionality and to maintain long term storage of the MSISDN that corresponds to the mobile's IMSI.

SA WG2 document, S2-095320 described how, by the addition of the MSISDN to certain SGs interface messages, the MSC/VLR function can become a simple interworking function that does not require long term storage of the IMSI-MSISDN relationship. The resulting architecture is shown below in Figure 6.52.2.4-1.

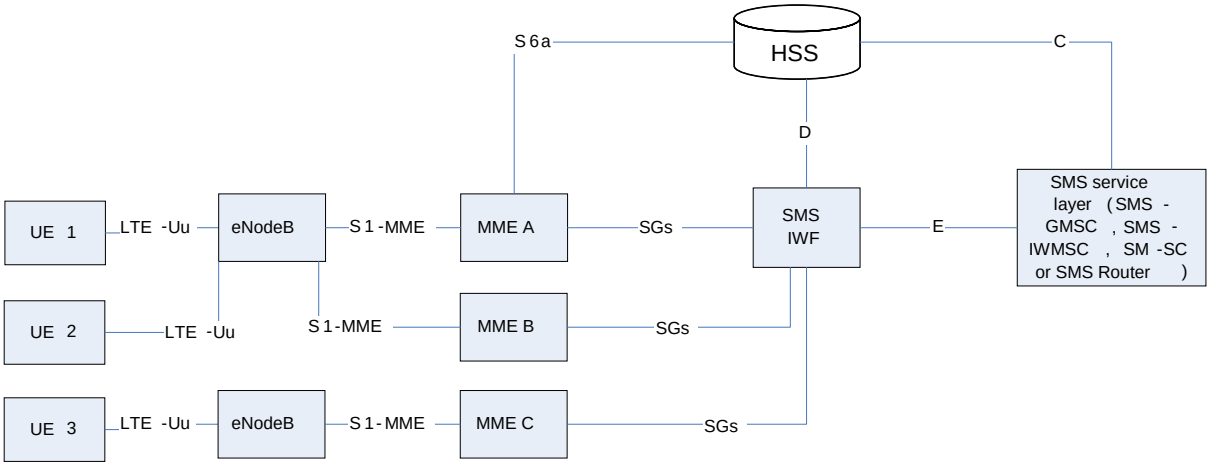


Figure 6.52.2.4-1: New architecture of MME and SMS IWF, showing that multiple MMEs can be connected to one SMS IWF

When using the architecture in Figure 6.52.2.4-1, the 'source address' of the SMS IWF (used in Registration messages to the HSS) depends upon the MME in which the UE is registered, e.g. as shown in Table 6.52.2.4-1 below. The HSS stores these different SS7 Global Title addresses as if they were the "real MSC/VLR address" and gives them to the SMSC in the SendRoutingInformation for Short Message Response. The SMSC then uses that SS7 GT to send the Short Message to the SMS IWF. The SMS IWF uses the addressed SS7 GT to identify the correct MME.

Table 6.52.2.4-1: Mapping table of MME name to SS7 GT stored in SMS IWF

MME	MME name/IP address	Assigned SS7 GT
A	192.168.1.4	447700900111
B	aaa-1.internal.operator.com	447700900112
C	10.34.78.67	447700900113

A further reduction in the number of nodes can be achieved if the SMS IWF is co-located with the MME (see Figure 6.52.2.4-2 below). This would mean that the MME would have to support the MAP D and E interfaces, however, as many vendors offer combined MME/SGSN platforms, this is not necessarily a huge problem.

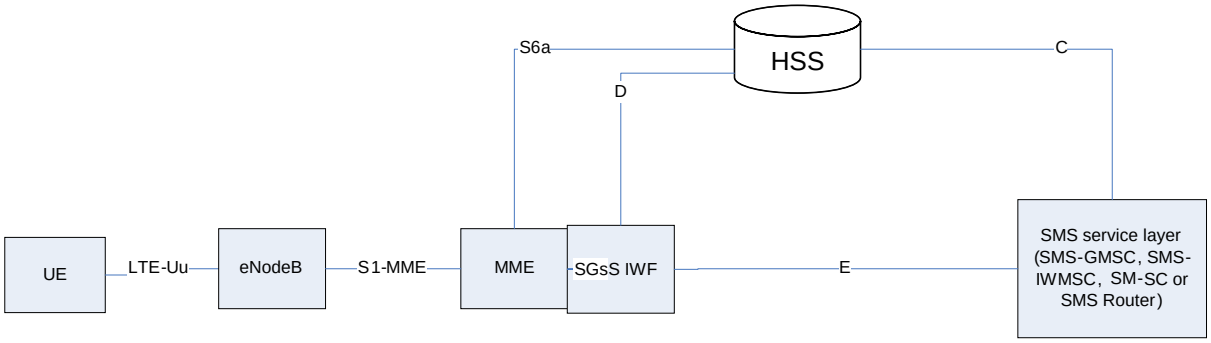


Figure 6.52.2.4-2: MME and integrated SGs SMS IWF

NOTE: The architectures shown in Figures 6.52.2.4-1 and 6.52.2.4-2 can be used by CSFB devices, but, Fall Back will entail an MSC change.

These architectures permit an LTE operator to use SMS over SGs without substantial investments in CS domain infrastructure. Upgrades to the HSS or SMSC are not required.

6.52.2.5 Evolution of the signalling interfaces between MME and HSS/SMSC

In the architectures shown in clauses 6.52.2.3 and 6.52.2.4, movement of the mobile inter a new MME area results in the HSS receiving mobility related signalling on both S6a and D interfaces. In the case of successful uptake of LTE M2M using SMS for small data transmission, this 'double update' may represent a significant load/inefficiency.

For the case of an "SMS over SGs Function/IWF" being integrated in the MME, to prepare for such a situation, it would be logical to consider extending the S6a functionality to incorporate the CS domain update (for SMS only). This can be done on a "per MME-HSS pair" basis.

Similarly, if load or cost reasons were to warrant it, the "MME/SMS over SGs Function/IWF" to SMSC interface could be upgraded from its current MAP protocol form to an appropriate IETF based interface. Again this can be done on a "per MME-SMSC pair" basis.

6.52.2.6 Use of pre-established NAS security context to transfer the SMS PDUs as NAS signalling without establishing RRC security

In LTE, the current SMS over SGs procedures require the use of the Service Request procedure. This entails the download of the RRC security context to the eNB and the establishment of the radio bearers. If all that is intended is the transfer of one SMS-like data packet, these procedures lead to a substantial increase in radio resource utilisation.

In 2G GPRS, these procedures are avoided as 2G-PS is relatively connectionless, and, the user plane and signalling messages are encrypted at the SGSN, not in the RAN.

The MME has encryption functionality for the NAS signalling and thus the transfer of the RRC security context to the eNB does not seem strictly necessary. Note that when performing a TAU from Idle mode, the RRC security context and radio bearers are not established.

The following bullets describe more optimised radio interface message sequences for SMS over SGs. They are most suited for (and are described here for) the case when the CP layer has been removed, but, they can still function if the CP layer is retained.

MO LTE procedure for SMS over SGs:

a) The mobile performs a combined Attach/TAU, typically, for "SMS-only" and returns to RRC-idle.

   During the Attach and TAU procedures, the UE and MME exchange information on their (and in the case of a real, separate, MSC, the MSC's) ability to support optimised SMS procedures.

b) The UE's NAS requests the UE's AS to establish an RRC connection "for a Tracking Area Update" (sending the S-TMSI in the RRC Connection Request). However, the NAS PDU is a new form of initial layer 3 message that includes the RP-DATA in an encrypted IE. This NAS PDU is sent in the NAS container in the RRC Connection Setup Complete message. The unencrypted part of this new initial layer 3 message in the NAS PDU carries the "KSI and sequence number" IE and the MME uses this, and the S-TMSI, to identify the security context to decrypt the RP-DATA.

NOTE 1: During the Attach procedure, the RRC Connection Setup Complete message typically carries a NAS PDU of around 80 bytes (for an SRVCC mobile), so, the radio's Layer 1 and 2 mechanisms are probably not harmed by an RP-DATA payload of up to 160 bytes.

The size of this NAS PDU means that it is worth setting the RRC establishment cause to "mo-Signalling' rather than "mo-Data".

NOTE 2: the "mo-Signalling" cause value, potentially coupled with the receipt of the S-TMSI in the RRC Connection Request, can be used by the eNB to detect that a short lived signalling procedure is in progress. Hence it is unlikely that the MME will download the security context to the eNB. Without the security context, handover cannot be performed. Thus radio resources can be saved if the eNB does not configure the UE to perform measurement reporting.

If the UE's application knows that it needs to send multiple or concatenated SMSs, then the UE sets a (new) flag in the NAS PDU to inform the MME of this fact. The UE's application could also indicate the number of SMSs that need to be sent.

c) The eNB forwards the encrypted RP DATA to the MME in the S1AP Initial UE message.

d) The MME decrypts the RP-DATA, and the MME (or SGs SMS IWF) adds the UE's identity information (e.g. MSISDN received from the HSS in step a) and forwards the Short Message to the SMSC.

e) The SMSC stores the SM and returns an RP-ACK to the MME.

f) The MME forwards the RP-ACK in an encrypted NAS PDU to the eNB in an S1 Downlink NAS Transport message.

An additional, optional, IE is added to the S1 Downlink NAS Transport message that allows the MME to request the eNB to release the RRC connection. (The MME does not use this indication if the UE indicated that multiple SMSs needed to be transferred in step b).

NOTE 3: this situation is similar to the completion of a (periodic) TAU. i.e. the MME has not sent the Initial UE Context message to the eNB and so the eNB cannot perform any commands on the UE that require RRC level security (in particular clause 5.3.1.1 of TS 36.331 specifies that Handover cannot be performed in this state).

g) The eNB sends the RP-ACK to the UE and releases the RRC Connection. The small size of the RP-ACK means that it is possible for the eNB to include it as a NAS PDU within the RRC Connection Release message itself.

Facets of the above procedure:

- This MO SMS transfer only uses 4 RRC messages (plus the Hybrid ARQ frames and the 2 messages that precede the RRC Connection Request).
- The CP Layer messages are not used.

MT SMS

This uses similar concepts to MO SMS, but it requires 2 more RRC messages.

a) The MME and UE have negotiated (at Attach/TAU) that the CP layer need not be used.

b) Paging leads to the establishment of the RRC Connection. The addition of a "SMS flag" to the radio interface (and S1 interface) paging messages allows the UE to change the RRC establishment cause from "mt-access" to "mo-signalling" (or to a new cause value of "mt-signalling"). In turn, this RRC establishment cause allows the eNB to optimise its resource allocation and to not configure the UE for measurement reporting).

The Service Request sent as the paging response by the UE carries the "KSI and sequence number" IE. The MME uses this, and the S-TMSI, to encrypt the RP-DATA sent in step c below.

c) The MME then sends the RP-DATA in an encrypted IE in a NAS PDU in an S1 Downlink NAS Transport message and the eNB sends the NAS PDU onto the UE.

d) The UE sends the RP-ACK in an encrypted IE in a NAS PDU in an UL Information Transfer message and the eNB forwards the NAS PDU to the MME.

The UE adds a new optional IE to the UL Information Transfer to request the eNB to release the RRC connection.

e) The eNB releases the RRC Connection.

6.52.2.7 Transfer of Device Trigger as MT SMS or NAS payload without U-plane bearer establishment in E-UTRAN

For the transmission of the Device Trigger contained in the MT SMS the establishment of U-plane bearers is not necessarily needed. Depending on the triggered MTC application, the UE used for MTC may either not require the establishment of U-plane bearers, or not the immediate establishment of U-plane bearers.

NOTE 1: In the following exemplary cases the establishment of the U-plane bearers is not needed: 1) the UE used for MTC may reply to the MTC server using MO SMS; 2) the UE used for MTC may first need some time to gather information and then the IP-based communication to the MTC server is initiated (e.g. 1 minute later).

The solution proposed in this clause is an alternative to the one proposed in clause 6.52.2.6 above. The main difference results from the UE behaviour after receiving the Device Trigger message. Namely, the eNB/MME may not immediately initiate the NAS/RRC connection release after the delivery of the Device Trigger (e.g. MT SMS) to the UE. During the Device Trigger processing in the UE, the UE determines if uplink data shall be immediately sent to the MTC server. Further, the uplink data may result in either:

1) establishment/activation of EPS bearers for IP/based MO communication or

2) the transmission of MO SMS to the MTC Server.

If the UE needs to transmit an MO SMS, the UE reuses the existing NAS MM connection to the MME. If the UE needs to set up the U-plane bearers, the UE sends a corresponding EPS Bearer Activation message to the MME.

If the UE determines that the uplink data will be transmitted later (i.e. MO communication will be established later), the UE indicates to the MME that the NAS signalling connection is not anymore needed. The latter helps the network to shorten the radio resource occupation.

As an alternative to solution from clause 6.52.2.6, the MME may establish the Access Stratum (AS) security for the Signalling Radio Bearers. For this reason, the MME establishes only the UE AS-security context at the eNB for the RRC connection (i.e. the MME doesn't include the E-RAB context in the S1-AP Initial Context Setup request message to the eNB). The main reasons for the establishment of the AS-security are:

1) The support of mobility; and

2) The ability of the UE to reliably activate the U-plane bearers if needed.

NOTE 2: Some further alternative signalling and/or indications during the Paging and Service Request procedure are possible compared to the MT SMS solution from clause 6.52.2.6. If the UE has no data to send via the U-plane when responding to the Paging message with "SMS flag", then the UE can send a new or an existing initial NAS message, e.g. TAU request without an active flag, to the MME. This message only triggers the establishment of the NAS signalling connection. After the reception of the Device Trigger, in the reply from the UE to the MME (e.g. SMS Relay protocol PDUs, RPDUs), the UE indicates further actions to the MME such as keeping or releasing the NAS signalling connection. This helps the network to shorten the radio resource occupation.

Editor's note: The evaluation of the benefits and drawbacks has to be done when the evaluation for the whole clause 6.52 will be provided.

6.52.3 Impacts on existing nodes or functionality

a) Extensive use of SMS for transmission of small data puts additional load on control plane nodes (e.g., MME, SGSN, MSC Server, SMS-GMSC, SMS-IWMSC, SMS-SC) in order to transport user data.

6.52.4 Evaluation

6.53 Solution - Small Data Transfer (E-UTRAN): Use of pre-established NAS security context to transfer the IP packet as NAS signalling without establishing RRC security

6.53.1 Problem Solved / Gains Provided

See clauses 5.4 "Key Issue – Small Data Transfer".

6.53.2 General

NOTE: This is a development of the concept in clause 6.52.2.6 "Use of pre-established NAS security context to transfer the SMS PDUs as NAS signalling without establishing RRC security".

In LTE, the current data transfer procedures require the use of the Service Request procedure. This entails the download of the RRC security context to the eNB and the establishment of the radio bearers. If all that is intended is the transfer

of one, possibly small, IP data packet, and perhaps its response, these procedures lead to a substantial increase in radio resource utilisation.

In 2G GPRS, these procedures are avoided as 2G-PS is relatively connectionless, and, the user plane and signalling messages are encrypted at the SGSN, not in the RAN.

If the MME is using encryption functionality for the NAS signalling the transfer of the RRC security context to the eNB does not seem strictly necessary. Note that when performing a TAU from Idle mode, the RRC security context and radio bearers are not established.

Figure 6.53-1, below, illustrates the architecture for this 'small data' feature.

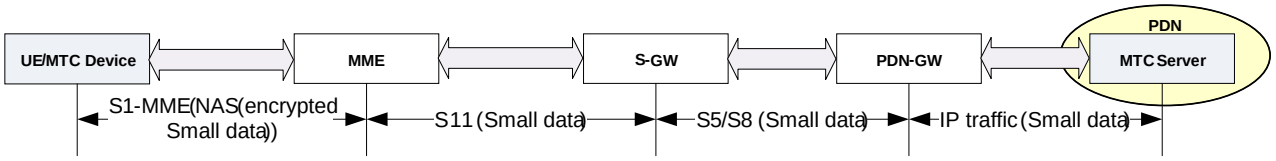


Figure 6.53-1: E2E data paths for small data transmission

The following bullets describe more optimised radio interface message sequences for the transfer of one IP packet (and its response).

LTE procedure for single MO IP packet (and response):

a) The mobile performs Attach activating a PDN connection or TAU (with an already active PDN a connection).

   During the Attach and TAU procedures, the UE and MME exchange information on their ability to support the "small data" procedures. The MME also obtains information (e.g. from the HSS) about the likelihood that this UE will predominately use (or not use) the small data transfer feature.

   As a result, the MME might perform UTRAN-MOCN style MME redirection procedures to cause the UE to register on an MME optimised for MTC Small Data Transfers.

   The finally selected MME instructs the UE to use encryption of NAS signalling messages.

   The finally selected MME performs S-GW and P-GW selection taking into account the UE's likelihood to perform small data transfers.

   The UE returns to RRC Idle mode.

b) When the UE's application knows that it needs to send just one IP packet (and that this uplink IP packet should not trigger multiple downlink IP packets), the UE's application requests NAS to request the UE's AS to establish an RRC connection "for a Tracking Area Update" (sending the S-TMSI in the RRC Connection Request). However, the NAS PDU is a new form of initial layer 3 message that includes the IP packet and its EPS Bearer ID in an encrypted IE. This NAS PDU is sent in the NAS container in the RRC Connection Setup Complete message. The unencrypted part of this new initial layer 3 message in the NAS PDU carries the "KSI and sequence number" IE and the MME uses this, and the S-TMSI, to identify the security context to decrypt the IP packet and EPS Bearer ID.

NOTE 1: RRC has not placed any significant size constraint on the NAS PDU payload. Hence RRC is believed to be able to support a 1500 byte IP packet within the NAS PDU. Any loss of radio efficiency needs to be determined, but, it is believed that power control features would work correctly, and, that low end devices would not deploy advanced/multi antenna features that need the download of the UE Radio Capabilities IE from the MME to the eNB.

The size of this NAS PDU means that it is worth setting the RRC establishment cause to "mo-Signalling' rather than "mo-Data".

NOTE 2: The "mo-Signalling" cause value, potentially coupled with the receipt of the S-TMSI in the RRC Connection Request, can be used by the eNB to detect that a short lived signalling procedure is in progress. Hence it is unlikely that the MME will download the security context to the eNB. Without the security context, handover cannot be performed. Thus radio resources can be saved if the eNB does not configure the UE to perform measurement reporting.

If the UE's application knows that it needs to transfer more than one uplink and one downlink IP packet, then it should (shall) use the normal service request procedure.

NOTE 3: It could be considered to use this procedure to transfer more than one (pair) of IP packets. This may be possible (e.g. it is not dissimilar to TAU procedures where several NAS messages can be exchanged without downloading the UE Radio Capabilities to the eNB), however this would have a larger RAN performance impact.

NOTE 4: How to ensure that the application correctly uses the Service Request procedure and does not abuse this 'Small Data' NAS procedure is an open issue. However the MME's ability to release the connection provides a control point. An additional possibility is for the NAS signalling in the Attach/TAU procedure to carry a TFT, or some other 'rule', to the UE which the UE uses to restrict the traffic that can use the 'Small Data' procedure.

c) The eNB forwards the encrypted IP packet to the MME in the S1AP Initial UE message.

d) The MME decrypts the IP packet.

Using the EPS Bearer ID, the MME retrieves the IP address and TEID of that bearer, forms the GTP-U packet and sends it to the S-GW.

e) The S-GW sends the packet to the P-GW and the P-GW forwards the IP packet on to the SGi interface.

f) The MME uses knowledge of the subscriber to determine whether to proceed with the full UE triggered Service Request procedure, or, to immediately release the RRC connection, or to wait for some time (e.g. to see if a downlink IP packet causes the S-GW to send a Downlink Data notification to the MME).

g) (If the MME has not proceeded with the full UE triggered Service Request procedure,) when a (response) IP packet arrives in the S-GW, the S-GW appends the IP packet to the Downlink Data Notification and sends it to the MME. The S-GW also buffers the IP packet.

h) If the MME has retained the RRC connection, then the MME can append the EPS Bearer ID to the downlink IP packet, encrypt them and send them in a downlink NAS PDU to the UE. Knowledge of the subscriber type would permit the MME to request the eNB to release the RRC connection in conjunction with the eNB's delivery of the NAS PDU/IP response packet.

i) The Downlink Data Notification Ack sent by the MME to the SGW is extended to inform the SGW that the packet has been delivered (or, that the normal Network Initiated Service Request procedure has been triggered).

j) If the S-GW has not received a Downlink Data Notification Ack indicating that the normal Network Initiated Service Request procedure has been triggered, when a second downlink IP packet arrives in the S-GW, the S-GW sends a new Downlink Data Notification with that IP packet appended to the S-GW. If the S-GW receives multiple IP packets, the S-GW can use the Downlink Data Notification to request the MME to perform the normal Network Initiated Service Request procedure.

Facets of the above procedure:

- This IP packet pair transfer only uses 4 RRC messages (plus the Hybrid ARQ frames and the 2 messages that precede the RRC Connection Request).

LTE procedure for single MT IP packet delivery

This uses similar concepts to the MO case described above.

a) The MME and UE have (at Attach/TAU) performed similar negotiations to those for the MO case, NAS encryption is activated and a PDN connection has been activated.

b) when an IP packet arrives in the S-GW, the S-GW buffers the IP packet, appends it to the Downlink Data Notification and sends it to the MME. The S-GW monitors whether subsequent packets have arrived for the delivery to the UE and whether the total size of these packets is greater than the value configured by the operator's policy or subscription. If this is the case the S-GW sends the Downlink Data Notification to request the establishment of the S1 bearer(s).

c) The MME pages. The addition of a "Small data flag" to the radio interface (and S1 interface) paging messages allows the UE to change the RRC establishment cause from " mt-access" to "mo-signalling" (or to a new cause

value of "mt-signalling"). In turn, this RRC establishment cause allows the eNB to optimise its resource allocation and to not configure the UE for measurement reporting).

The MME uses knowledge of the subscriber to decide whether to include the "Small Data Flag", and, whether to not fully proceed with the subsequent Service Request procedure.

The Service Request sent as the paging response by the UE carries the "KSI and sequence number" IE. The MME uses this, and the S-TMSI, to encrypt the IP packet sent in step d below.

d) The MME then sends the IP packet and EPS Bearer ID in an encrypted IE in a NAS PDU in an S1 Downlink NAS Transport message and the eNB sends the NAS PDU onto the UE.

e) Typically the UE sends an IP packet as an acknowledgement. This IP packet, along with the EPS Bearer ID, is sent in an encrypted IE in a NAS PDU in an UL Information Transfer message. The eNB forwards the NAS PDU to the MME. The MME decrypts the IE, adds the GTP header and forwards it to the S-GW.

The UE adds a new optional IE to the UL Information Transfer to request the eNB to release the RRC connection.

f) The eNB releases the RRC Connection.

6.53.3 Impacts on existing nodes or functionality

6.53.4 Evaluation

Typical IP flow scenarios (e.g. when TCP transport is used) require multiple round trips.

6.54 Solution - NAT Traversal using controlled NAT

6.54.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue - Ipv4 Addressing" and clause 5.8 "Key Issue - MTC Device Trigger".

6.54.2 General

This alternative is intended to give a NAT traversal option that could be implemented without requiring normative impacts on existing 3GPP entities. This is one option of how this could be implemented, and other variants exist today on the market.

This alternative is similar in nature to clause 6.18 "Solution - MT Communication with NATTT", but with the difference that there is no need to setup a tunnel between the NAT and MTC Server (or MTC application). This solution addresses the scenario where the MTC Server/Application impact needs to be minimized, but where similar principles for DNS based lookup is considered beneficial. In general, it is assumed that the UE applications are using a few ports and that these ports are either known or possible to learn from application layer signalling. When the UE has received the (private) IP address from the PGW, the PLMN NAT at Gi is configured to map the configured port values to public IP ports. The values of the ports at the public side of the NAT are automatically configured in the DNS.

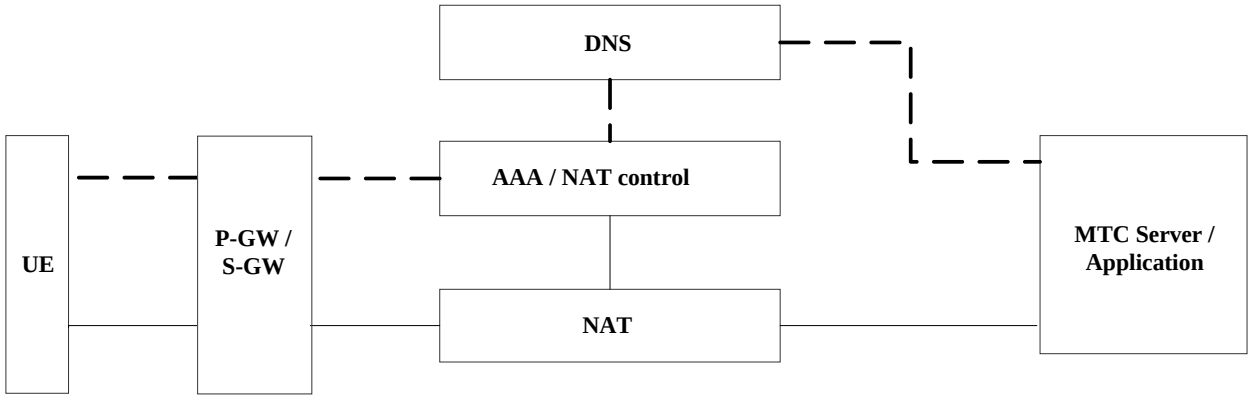


Figure 6.54-1: Overall outline of NAT solution

NOTE: The AAA/NAT control function is considered out of 3GPP standardization scope.

In this alternative, the following will take place:

- The UE is attached to the network, and the AAA/NAT Control function is updated with the user context, including IP address.
- Based on configuration or user profile data, the NAT is setup with a number of bindings for the communication between the UE and MTC Server. This could be done in similar fashion as for the Micro port forwarding in clause 6.19. The AAA/NAT Control function will be the responsible to perform this. It is expected, that only a limited set of ports may be required to be kept in the NAT, for a specific standard set of services.
- The AAA / NAT Control function updates the DNS with IP address for the UE, including the ports to which it can be reached for the specific advertised services.
- The MTC Server will be able at anytime perform a DNS query according to normal DNS lookup procedures, and retrieve correct IP address (and port) for the device (and service on the device) it wish to contact.

6.54.3 Impacts on existing nodes or functionality

Under the assumption that M2M dedicated APNs are used with Radius forwarding performed by PGW, existing functions would not be impacted.

6.54.4 Evaluation

Benefits:

- No impact on existing Core Network nodes and UE;
- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a "push" stimulus;
- Works also for device-to-device communication;
- No impact on MTC Server/MTC-IWF.

Disadvantages:

- Using DDNS for exposing the IP address may case problem due to the applications and SP ignoring the TTL of the DNS bindings.
- Not efficient for short lived PDN connections, unless same IP address re-used for the UE.
- For local breakout, a large number of trusted interfaces would be required to update the DNS.
- The solution is limited to one (or pre-defined number) of port number(s).
- The solution is limited to the number of port bindings per IP address.

6.55 Solution - NAT Traversal using Non-Managed-NAT

6.55.1 Problem Solved/ Gains Provided

See clause 5.3 "Key Issue - IP Addressing".

6.55.2 General

In order to support communications between the MTC Server and the UE used for MTC that are located in different IPv4 address spaces, Network Address Translator (NAT) is deployed at the address space boundary. Such NAT could be a managed-NAT or a non-managed-NAT.

The solution described in clause 6.19: 'MT Communications with Micro Port Forwarding' is an example of the managed-NAT solution shown. The proposal in this clause provides the architectural framework for a non-managed-NAT solution for MTC.

NOTE 1: NAT Traversal proposal illustrated here applies to the Indirect and Hybrid communication models in clause 4.2. The solution assumes that UE used for MTC initiates communications for Direct communication model. NAT traversal is not an issue if the UE used for MTC initiates communications.

NOTE 2: Market requirements and Use Case for non-Managed NATs is FFS.

6.55.3 Non-Managed-NAT for MTC

Architectural overview of non-managed-NAT traversal solution for 3GPP MTC is illustrated in Figure 6.55.3-1. Bindings in non-managed-NATs are not controlled by the network. Bindings in the non-managed-NAT are created when the MTC Server wants to initiate communications with the UE used for MTC.

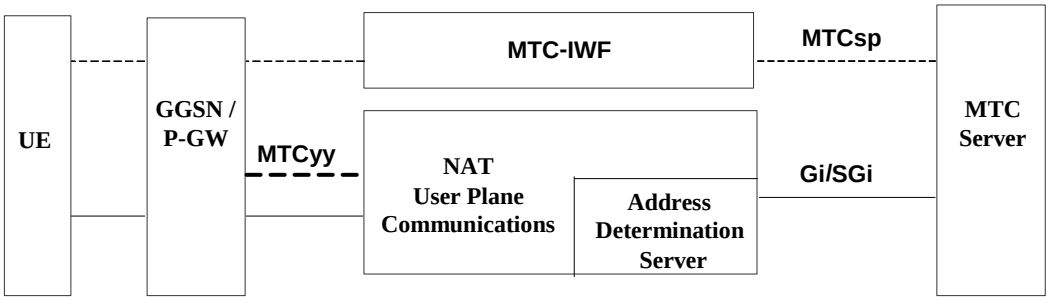


Figure 6.55.3-1: Non-Managed NAT with Address Determination Server

1. Once PDP/PDN connection is established for a UE used for MTC, the IP address is made available to the MTC-IWF.

2. When the MTC Server queries the MTC-IWF for UE's public IP address and port information (transport address), the MTC-IWF initiates Address Translation Request/Reply procedure with the GGSN/P-GW by passing the assigned IPv4 Address and Port information (based on the Application ID/Port information received in the trigger request from the MTC Server) to the GGSN/P-GW. The GGSN/P-GW emulates the UE by sending address determination packets through the NAT to an Address Determination Server over the MTCyy interface. The Address Determination Server is used to discover the public side of the transport address assigned to the UE.

3. The UE emulation IP packets include the address assigned to the UE and the expected port to be used. Such IP packets create bindings for the UE at the NAT. The UE emulation IP packets conform to the protocol defined in RFC 5389 (STUN) or RFC 5766 (TURN), depending on the type of the non-managed-NAT.

4. The STUN/TURN packets are intercepted by the Address Determination Server (STUN Server/Turn Relay) on the public side of the NAT. The Address Determination Server returns the public side of the IP Address and port information (transport address) for the UE to the GGSN/P-GW. The GGSN/P-GW intercepts the public AP Address/Port information, which is passed to the MTC Server via the MTC-IWF.

5. With such information about the public transport address for the UE, the MTC Server initiates user plane communications with the UE used from MTC.

Depending on the nature of the non-managed-NATs (EIM or non-EIM type), the UP traffic flows directly from the public side of the NAT or via the Address Determination Server.

- For EIM type NAT, UP traffic flows from the public side of the NAT over Gi/SGi interface.
- For non-EIM type NAT, UP traffic flows through the Address Determination Server (TURN Relay) over Gi/SGi interface.

NAT bindings are kept alive by virtue of the flow of UP traffic. Additionally, some traffic monitoring capability at the GGSN/P-GW or the MTC-IWF can keep the bindings alive via appropriate keep alive STUN/TURN signalling.

6.55.3 Impacts on existing nodes or functionality

Impact on MTC-IWF:

- Perform address translate procedure with the GGSN/P-GW.

Impact on GGSN/P-GW:

- STUN/TURN user agent function at the GGSN/P-GW.

6.55.4 Evaluation

Benefits:

- Low impact on existing Core Network nodes.
- The solution is based on known IETF protocols.
- No complex configuration of 'forwarding-rules' at the MTC device and/or in the Core Network entities.
- No impact on subscription data.

Drawbacks:

- New Address Determination Server entity (STUN/TURN server) in the Core Network.
- STUN/TURN user agent function at the GGSN/P-GW.
- Public IP Address/Port pairs per public IP address limited to 65,536 (2^16).
- Control plane communications needed between the GGSN/P-GW and the MTC-IWF.
- The solution assumes that UE used for MTC initiates communications for Direct communication model.

6.56 Solution – SMS Transfer by SGSN for PS-only

6.56.1 Problem Solved / Gains Provided

"PS-Only Support".

6.56.2 General

For 2G/3G the SGSN already supports SMS transfer in PS domain, which doesn't rely on a CS registration of the UE. For GERAN/UTRAN, the PS only MTC Device only registers in PS domain. SMS transfer is via the SGSN without involving MSC/VLR. MM protocols and state machines may need to be updated to reject any potential CS registration attempt without affecting PS services or SMS provision via E-UTRAN.

The MME registers a device that initiates combined Attach/TAU procedure with an SGSN instead of an MSC/VLR. Comparable to 6.52.2.3/4 or other solutions that deploy a reduced SGs-MSC-function just for SMS the approach of SGs with an SGSN provides only SMS services. CSFB devices may also be registered via SGs with the SGSN so that the MME is not modified and a CS fallback will fail. Or, the MME is enhanced to select an SGSN instead of an MSC/VLR based on the "SMS only" indication. In the latter case SMS for PS-only device is provided by the SGSN without any CS registration in the network. And CSFB devices are registered with an MSC for receiving CS services.

For E-UTRAN-only devices and/or subscriptions this approach requires only PS subscription data. For multi-RAT capable devices and PS only subscriptions the MM protocols and state machines may need to be updated to reject any potential CS registration attempt without affecting 2G/3G PS services or SMS provision via E-UTRAN. If a CS subscription is required, e.g. to handle LTE capable multi-RAT UEs that cannot be prevented from registering with the MSC via 2G/3G, or if the PLMN doesn't configure SMS transfer via 2G/3G SGSNs, there will be no HSS update signalling caused by RAT-reselection in contrast to solutions that deploy an SGs-MSC-function. When CS registrations are prevented there is only the SGSN registered at HSS for MT SMS. Regardless of the RAT the UE camps on MT-SMS can always be delivered via SGSN. As there is no need for trying the MSC path for MT-SMS there are no unsuccessful delivery attempts, which may occur with an SGs-MSC-function when configuring PS-only for 2G/3G.

As an alternative to cope with devices that require a 2G/3G CS registration the MSC may accept registration requests from the UE without creating an MM context or providing any services to the UE. This assumes that any required SMS services are provided by the SGSN or fail like other MSC provided services when initiated by the UE.

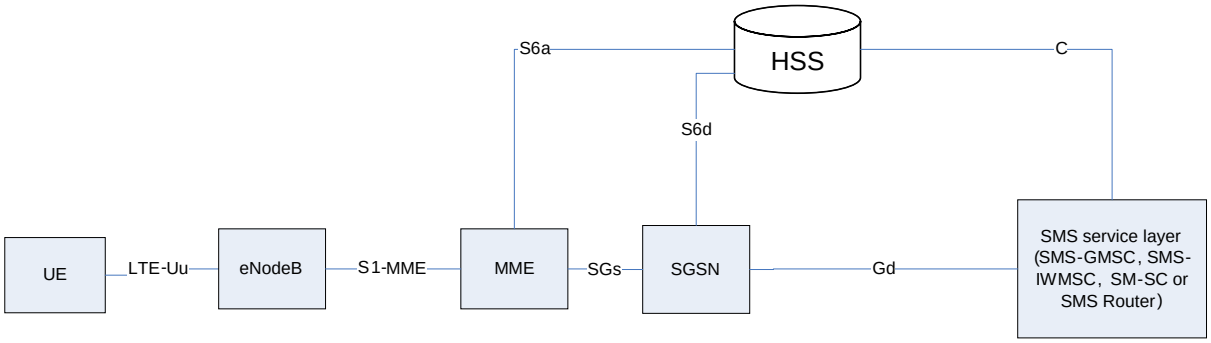


Figure 6.56.2-1: Use of SMS transfer function of SGSN for PS only Device

6.56.3 Impacts on existing nodes or functionality

The SGSN provides SGs functionality for SMS towards MME, like an MSC. Optionally the MME can be enhanced to differentiate "SGs" to an SGSN (for SMS only) and SGs to an MSC (for CSFB). For rejecting CS registrations attempts without affecting any registrations for SMS over SGs the MM NAS signalling may need to be enhanced.

Alternatively the MSC provides functionality to accept CS registrations without providing MSC services for UEs that receive SMS services from the SGSN.

6.56.4 Evaluation

In contrast to solutions with an SGs-MSC-function this approach does not require a CS subscription. With a CS/PS subscription, e.g. when the PLMN prefers transferring SMS by MSC for 2G/3G the multi-RAT UEs will not cause updates for the HSS registered MSC (function), which will happen during every RAT re-selection for alternatives that deploy a dedicated SGs-MSC-function. For PS-only only deployments (SMS transfer by the 2G/3G SGSN) there is only an SGSN registered at HSS for MT-SMS routing.

6.57 Solution - Optimised SMS over SGs architecture

6.57.1 Problem Solved / Gains Provided

See TS 22.368 [2] clause 7.2.24 "Packet Switched (PS) only" and clause 5.8 "Key Issue - MTC Device Trigger".

6.57.2 General

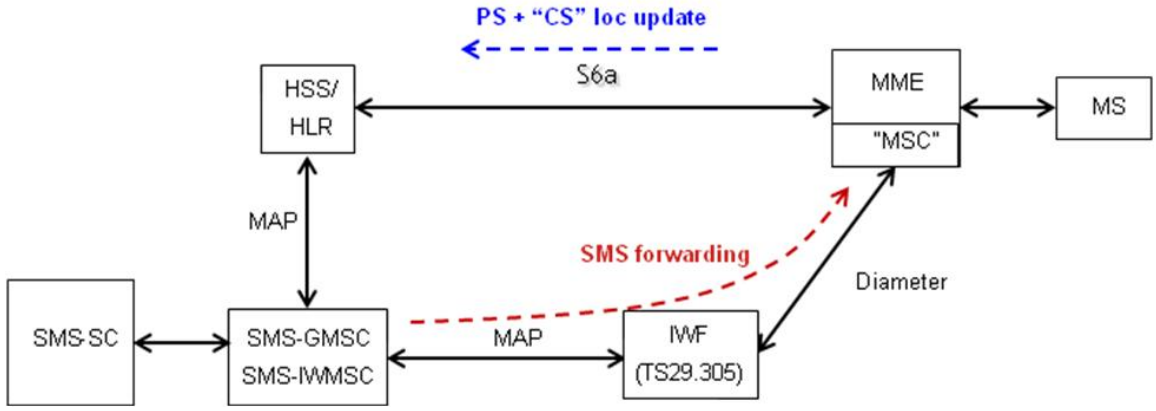


Figure 6.57.2-1: Optimised "SMS over SGs" architecture

Depicted in Figure 6.57.2-1 is an optimised SMS over SGs architecture obtained by merging the MSC Server functionality with the MME. There are no changes to the NAS or AS protocols.

Given that MM signalling in the optimised architecture is performed over the same interface (S6a), the CS and PS location updates are merged into a single procedure.

A MAP-Diameter interworking function (IMF) may be used on the SMS forwarding path in order to avoid the need for MAP interface support on the MME node.

While the architecture still appears to be CS+PS from UE perspective, the "CS domain" in this architecture is completely virtual. The Location Area Identifiers (LAIs) signalled over the radio have no meaning other than identifying the combined MME/MSC node as the destination for mobile terminated SMS.

Editor's note: It is FFS how the HSS/HLR can respond successfully to the piggybacked CS domain MM signalling without having any CS subscription data.

NOTE: An MSISDN parameter is still required on the MAP interface between the SMS-GMSC and the HLR/HSS, but this is addressed by solutions targeting the "MSISDN-less" requirement.

6.57.3 Impacts on existing nodes or functionality

Piggybacking of CS domain mobility management messages over S6a.

Collocation of MSC Server functionality in the MME for handling of SMS-related MAP procedures (possibly interworked via Diameter).

Addition of MAP-Diameter interworking procedures in the TS 29.305 interworking function (IWF) in relation to MAP procedures for SMS.

Editor's note: It is FFS if the MSC Server functionality residing in the MME should register with the HSS as an SGSN, instead of registering as an MSC, This is regardless of the fact that the UE performs combined EPS/IMSI Attach and combined TA/LA Update procedures over the radio.

Editor's note: The impact on the HSS/HLR is FFS.

6.57.4 Evaluation

Benefits:

- Reduces the amount of MM signalling in the Core Network for E-UTRAN devices;
- Allows for PS-only subscription for devices connecting via E-UTRAN;
- There are no changes to the AS or NAS protocols, which is why this architecture can also be used for existing UEs that attach over E-UTRAN as "SMS-only".

Drawbacks:

- The solution as described works only for single-mode E-UTRAN devices.

6.58 Solution – Triggering using Cell Broadcast

6.58.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger", "Key Issue – Low Mobility", "Key Issue - Group Based Optimization"

6.58.2 General

With MTC devices that are attached, if the network has knowledge of the location of the device, a broadcast trigger may be useful to limit the amount of signalling between the CN and the devices, or to trigger communications by means other than via a PDP/PDN connection or SMS.

Clause 6.6.2 describes the use of Cell Broadcast for triggering non-attached devices. This solution can also be used for triggering MTC devices that are attached, whereby triggers may be broadcast by using the Cell Broadcast Service (CBS) as specified in TS 23.041. This solution could be extended for E-UTRAN access, using warning message delivery as specified in TS 23.401 [5]. The existing CBS architecture for GERAN and UTRAN accesses, as well as the warning message approach in E-UTRAN (if extended to support triggering) should be evolved to handle multi-operator shared networks, for example, to allow the independent operation of CBC nodes by the sharing partners.

A mobile network operator may provide an interface to the CBC to third parties, or alternately, the MTC Server may send a trigger containing, for instance, geographic information and trigger information to the MTC-IWF over MTCsp. The MTC-IWF could then act as a CBE to deliver the message to the CBC. The information provided by the MTC Server to the MTC-IWF would include the geographic information on where the broadcast should be done, and the MTC-IWF converts this to cell information for the CBC (or the MTC-IWF could get the serving SGSN/MME from the HLR/HSS and then get the cell information from SGSN/MME.)

In order to limit the number of UEs responding, the message itself could identify the devices to be triggered. In order to allow it, the MTC-IWF would transparently pass the trigger information received from the MTC Server over MTCsp to the CBC.

Device Identification

The Cell Broadcast or Warning Message solution can be used to address MTC devices. For instance, the device's MSISDN, or some other unique paging identifier (UPID) can be used.

Several different options might be considered for directing the cell broadcast messages. One option might be to assign PLMN specific CBS message identifiers to MTC devices that run certain applications. Broadcasting messages in a specific geographic area will trigger devices listening for these message identifiers. The devices to be triggered could be further constrained by using implementation dependent structures within the message itself.

In order to direct the broadcast message in smaller deployments where assignment of separate message identifiers is not practical, a message structure could possibly be used whereby both the type of identifier and the identifier itself are broadcast.

Protocol Aspects

The current message definitions for Cell Broadcast and Warning Message delivery include a Message ID IE (see TS 23.041), which is defined for each different type of service. This IE is sent from the CBC to the UE, and is not acted upon in any of the intervening nodes. As part of the existing protocol, a device that is not interested in a particular Message ID value will simply ignore the message. Hence, already allocated PLMN specific message identifiers can be used, or possibly a new value or values can be allocated for use with MTC device triggering. Only those devices that use this type of triggering, and are programmed to process the specific message identifiers, would have to process messages beyond the message identifier.

Scalability

Indiscriminate use of cell broadcast for triggering could potentially cause a flood of signalling, which could cause problems for both the mobile network operator and the MTC application owner. This should be manageable, but would require limits set by the operator. For instance, the mobile network operator could limit the geography in which the

messages are sent. Also, presuming that this mechanism could be expanded to cover multiple devices with a single broadcast message, agreements between the mobile network operator and the MTC operator could be set such that only a limited number of devices are triggered at a given time. Such agreements in isolation may not be enough and it may also be necessary to consider the context of current and historical network load which can be enforced by the mobile network operator in specific network entities such as the SGSN/MME. The scalability needs to be considered in the context for multi-operator shared networks so that operation of MTC services by the sharing partners are as independent as possible.

Cell broadcast is suitable for triggering individual MTC Devices when triggering is infrequent. When many trigger messages are to be sent, cell broadcast is not likely to be an optimal solution. Hence, this solution should be seen as complementary to other mechanisms for sending triggers where the volume of triggers (product of number and frequency of triggers) exceeds a certain threshold.

Scalability in a Multi-Operator Sharing Scenario

There may be one shared CBC in a multi-operator scenario. For emergency broadcast services, this situation is fine due to the low frequency and limited size of broadcast messages. In commercial services, sharing a CBC brings in the potential for competitive issues related to capacity, fair share of costs, and similar issues.

These concerns can be addressed by recognizing the commercial factors in various ways. One approach is to use the number of instances of sending a broadcast trigger as a basis for sharing costs among the operators sharing the resource. Considering issue 2, with multiple operators using this capability, the likelihood increases that capacity limits might be reached. This can be addressed through providing additional CBCs which can still be shared when deployed geographically (i.e. each CBC covers a reduced geographic area but is still shared by the operators serving that area) or by moving from shared CBCs to individually owned CBCs. It is envisaged that a transition from one shared CBC to multiple non-shared CBCs could include a hybrid arrangement of shared/non-shared CBCs and geographic coverage.

6.58.3 Impacts on existing nodes or functionality

The CBC must be modified to:

- assign the Message ID IE to the value(s) allocated for MTC Device triggering;
- allow independent operation of CBCs by the partners (a maximum of 6) in a multi-operator network, where GERAN, UTRAN, or E-UTRAN radio access networks are shared.

MTC-IWF

- provide conversion of MTC Server provided location (e.g., civic addresses or geographic area) to network location information (e.g., TA/RA/LA);
- Interface to CBC needed.

MME/SGSN

- Possibly add ability to support MTC-IWF location request: MTC-IWF could get the serving SGSN/MME from the HLR/HSS and then get the cell information from SGSN/MME.

MTC devices will need to:

- listen on the appropriate broadcast channel(s) for triggering messages;
- understand the message ID(s) that are to be used by the application;
- understand the device identification mechanisms that might be used to identify the device for triggering;
- perform the appropriate action after being triggered;
- MTC Devices need to have controlled access to avoid network overload.

6.58.4 Evaluation

Benefits

- Provides a base capability for group-based triggering.

Cons:

- For triggering a single device, extra overhead on the device to listen to paging as well as broadcast channel(s).
- The network may need to control access to avoid overload.
- Possible impacts on radio access nodes due to the independent CBC operation by sharing partners in GERAN, UTRAN, and E-UTRAN need further consideration.
- The solution needs to be extended to apply to E-UTRAN.
- Possible complexities due to roaming need to be investigated.
- Charging considerations would have to be investigated (e.g. if application information included), based on size of broadcast.

6.59 Solution – Load/Overload Control via MTC-IWF

6.59.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger".

6.59.2 General

For MTC device triggering, the MTC server can send trigger requests with trigger indication information to the MTC-IWF for further processing to trigger target MTC devices. However due to network congestion the MME/SGSN may not be able to process the trigger requests from the MTC-IWFs or the responses to the trigger requests from the target MTC devices.

The MTC-IWF contains load/overload mechanisms for handling and avoiding overload situations. In addition, under unusual circumstances (e.g. when the load of MME/SGSN exceeds an operator configured threshold or the MME/SGSN performs NAS level congestion control), the MME/SGSN restricts the load of trigger requests that are generating on it by its MTC-IWFs if it is configured to enable the overload restriction. With above considerations, there are two phases that the MTC-IWF performs to restrict the load of trigger requests from the MTC servers as well as to restrict the generated load of trigger requests on the MMEs/SGSNs. The first phase is to conduct load control on MTC servers and the second phase is to conduct overload/congestion control based on the guidance from the MME/SGSNs.

Editor's note: One of the architecture options considered for MTC is that the MTC-IWF delivers triggers through an SMS-SC. The trigger load towards the network in this scenario may rely on existing load control mechanism of an SMS-SC. The interaction between SMS-SC and MTC-IWF load control is FFS.

6.59.3 MTC-IWF Load Control to MTC servers

The use of the load control on MTC-IWF is for handling of signalling load and avoiding signalling overload from the MTC servers sending triggering requests to target UEs which may be for a specific application.

The MTC-IWF should detect the trigger signalling load associated with a particular MTC server, a specific application identifier, etc. The MTC-IWF performs the load control based on criteria such as:

- The ingress/service rate of triggers from a specific MTC server; or
- The aggregate ingress/service rates from all MTC servers; or
- The maximum number of queuing trigger requests from a specific MTC server or all MTC servers for further processing; or
- One or multiple MME/SGSNs indicate congestion to the MTC-IWF; or
- Setting in network management.

The MTC-IWF and MTC servers support the functions to provide load control over the MTCsp interface in the following manners:

- The MTC-IWF provides the rules/instructions to the MTC server to reduce trigger load by sending an appropriate message over MTCsp interface with optional IEs indicating suppression factor, suppression delay or

the suppression subcategories, e.g. an application identifier, a priority type, a specific MTC server, a specific TCP/UDP port, etc., to suppress the triggers sending from one or more MTC servers.

- The MTC-IWF reports the success or failure of the trigger (e.g. due to network congestion) to the MTC server.
- The MTC server follows received rules/instructions received from the MTC-IWF and/or follow the policies of the MTC subscription to control traffic load of the trigger requests.

With load control mechanism at MTC-IWF, it is anticipated that the trigger load generated by each MTC server to the MTC-IWF is handled well. However under certain circumstances, e.g. network congestion on the MME/SGSNs, The MTC-IWF may be overloaded due to slow forwarding rate of the trigger requests to the congested MME/SGSNs (trigger delivery via control plane). In this case, the MTC-IWF needs to conduct overload control which is detailed in the following clause 6.59.4 to adjust load control rules/instructions to the MTC servers, as indicated in clause 6.59.3.

6.59.4 MME/SGSN Overload Control of Trigger Requests to MTC-IWF(s)

To control trigger requests from MTC-IWF that generates trigger loads on the MME/SGSN, the overload control can be achieved by the MME/SGSN invoking the overload control procedure to MTC-IWF over T5b/T5a interface. The MTC-IWF performs the overload control by suppressing trigger requests, e.g. to stop forwarding the stored trigger requests to the next network node, to reject/drop the new arrival trigger requests and send notification message to the MTC server, or to delete the stored trigger request with reporting the trigger failure to the MTC server.

To reflect the amount of trigger load that the MME/SGSN wishes to reduce, the MME/SGSN can sent an appropriate message over T5b/T5a interface with optional IEs indicating the suppression factor, suppression duration, and/or suppressing subcategories, e.g. a specific application identifier, a specific priority type, etc., to reduce the trigger load from the MTC-IWF.

Further, to prevent the network congestion from being exacerbated by UEs that respond to triggers, the network needs to ensure that no UEs is triggered as long as the particular congestion situation remains in the following manners:

- If the MME/SGSN performs General NAS level Mobility Management Congestion Control or APN based Congestion Control, the MME/SGSN shall activate MTC-IWF overload control on trigger loads by sending an appropriate message to the MTC-IWF over T5b/T5a interface with optional IEs indicating suppression factor, suppression delay or the suppression subcategories, e.g. a particular congested APN, an application identifier, a priority type, a specific MTC server, a specific TCP/UDP port, etc. For example, if congested APN information is provided, the MTC-IWF reduces the trigger load of trigger requests for the UE that is targeting at the congested APN (see TS 23.401 [5] ,clause 4.3.7.4.2) by suppressing the trigger requests.

Editor's note: It is FFS how the network node obtains APN information for the trigger requests. The overload control via MTC-IWF for APN based congestion control may not apply for the case when the trigger is sent transparently.

- If the MME/SGSN stores the trigger request for a target UE, the MME/SGSN stops forwarding the trigger request to the UE and restart forwarding the trigger request when the network congestion is resolved and the validity time of the trigger is not expired.
- During an overload situation the MME/SGSN and MTC-IWF should attempt to maintain support for triggering UEs for emergency bearer services or high priority services.

When receiving an appropriate message from the MME/SGSNs, the MTC-IWF can suppress the trigger requests from the MTC servers to reduce trigger load by sending an appropriate message over MTCsp interface as indicated in clause 6.59.3.

The MME/SGSN and MTC-IWF should not suppress trigger requests for emergency services or high priority services due to network congestion.

When the MME/SGSN is recovering, the MME/SGSN can:

- send an appropriate message with optional IEs for suppression triggers, or
- send an appropriate message with new optional IEs that permits more trigger traffic to be carried, or
- resume handling triggers when the suppression delay is expired, to the MTC-IWF.

6.59.5 Impacts on existing nodes or functionality

- MTCsp interface needs to support protocols and messages for signalling suppressing trigger requests between the network node and the MTC server.
- The interface between MTC-IWF and MME/SGSN needs to support protocols and messages for triggers suppression.
- MTC server needs to follow the load control rules sending from the MTC-IWF or configured in the MTC subscription.
- MTC-IWF needs to detect trigger load and support load/overload control mechanisms to the MTC servers, and MME/SGSN.
- MME/SGSN needs to initiate overload control on triggers sending from the MTC-IWF when conducting NAS level congestion control.

6.59.6 Evaluation

Benefits:

- Enable the MTC-IWF to regulate trigger loads by load/overload control to reduce the trigger signalling from the trigger requests received from MTC servers.
- Protect network nodes (e.g. MME/SGSN, MTC-IWF) effectively from network congestions due to massive simultaneous trigger requests from MTC servers.
- Avoid massive individual reject messages responding from a congested network node to the MTC-IWF.

Drawbacks:

- Existing network node (e.g. MME/SGSN) needs to support the load/overload control function for suppressing trigger load from MTC-IWF due to network overload/congestion.

Others:

1) Delivery of device trigger information from 3GPP system to UE:
   - Some information, e.g. validity time, priority type, contained in trigger request message may have impact on the handling of trigger suppression.
2) Submission of device trigger requests from MTC server to 3GPP system:
   - The MTCsp interface supports the protocol for the load control related messages.
   - The MTC server follows the rules/instructions indicated in load/overload control message sending from the MTC-IWF.
   - The MTC-IWF supports load/overload control mechanism based on the detection of criteria or received message sending from the MME/SGSN.
   - The overload control via MTC-IWF for APN based congestion control may not apply for the case when the trigger is sent transparently.
3) 3GPP system internal handling of device triggers:
   - The network node (e.g. MME/SGSN) supports the overload control mechanism based on delivery of device trigger requests in the control plane (e.g. NAS level congestion control).
   - The protocol and the messages of the interface between MME/SGSN and MTC-IWF supports overload control.

6.60 Solution - Device trigger using MT-SMS & direct SGSN/MME delivery

6.60.1 Problem Solved / Gains Provided

Clause 5.8 "Key Issue - MTC Device Trigger",

Clause 5.11 "Key Issue - Decoupling MTC Server from 3GPP Architecture"; and

Clause 5.13 "Key Issue - MTC Identifiers".

6.60.2 General

This solution uses two trigger delivery methods, delivery using MT-SMS, and delivery from the MTC-IWF to the SGSN/MME for delivery to the UE. (It is a scaled down version of clause 6.45).

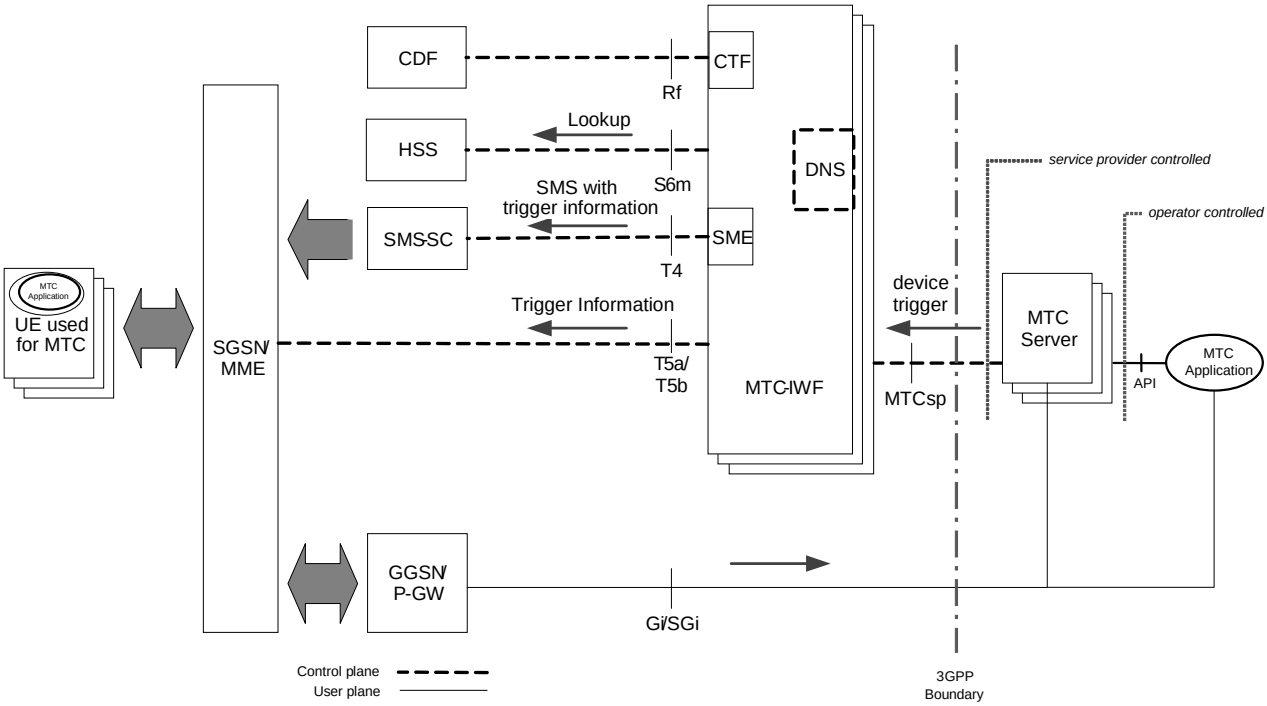


Figure 6.60.2-1: MTC device trigger architecture using MT-SMS delivery or direct MTC-IWF to SGSN/MME delivery

The interrogated HSS returns information related to delivery of the device trigger, such as IMSI and serving SGSN/MME. The trigger information is delivered to the UE using MT-SMS, or delivered from the MTC-IWF to the SGSN/MME for delivery to the UE.

The MTC-IWF is a pure control plane function which delivers the trigger information towards the UE regardless of PDP/PDN connection state. The network confirms the success or failure of delivering the trigger to the UE back to the MTC Server. The trigger information is delivered to the MTC Application in the UE, which may for example start communicating with the MTC Server or MTC Application. For this the user plane connection is established as needed.

Editor's note: The details of the solution are FFS.

6.60.3 Impacts on existing nodes or functionality

Impact to the Core Network:

- Deployment of the MTC IWF;
- New reference points (T4, T5a and T5b) to connect the MTC-IWF to SMSC, to SGSN/MME and to HSS. The T5a and T5b reference points need to be specified as roaming interfaces;

- New instance of pre-defined reference point (Rf) to connect the CDF.

6.60.4 Evaluation

6.61 Solution – Native SMS over NAS for PS-only

6.61.1 Problem Solved / Gains Provided

"PS-Only Support".

6.61.2 General

A PS-only device is a device that avoids using any CS service from a MSC in GERAN/UTRAN and would only use SMS from a MSC in GERAN/UTRAN if the SGSN does not provide support SMS transfer in the serving network. The UE subscribes only to PS domain and SMS services and may not be assigned an MSISDN. As such, if SMS over IP is not used, it can only receive SMS on the PS domain of GERAN/ UTRAN or on the EPS over NAS Signalling. The former is not supported in all networks, the latter has not been defined without a combined registration as in TS 23.272 [23] to achieve SMS delivery over SGs.

In rel-8 the delivery of SMS over NAS in EUTRAN is allowed for UE's that perform a combined registration. The assumption is that these devices can also camp on the CS domain of GERAN/UTRAN when they are out for EUTRAN coverage, to be able to receive SMS in networks not delivering SMS over GPRS. If a UE is only EPS registered, however, it is assumed that the mechanism used for SMS delivery would be SMS over IP. As per statement in clause 6.52.2.3 "Flexible deployment of MSC functionality for SMS over SGs", there is awareness that "In some deployment scenarios, the use of "SMS over IMS" can be regarded as rather heavyweight for low end M2M applications". It may be argued that in an inexpensive MTC device using EUTRA, and maybe also UTRA and GERA, may not need an IMS client for other purposes than SMS, hence it could be something it could be stripped of if SMS could be delivered over NAS.

In order to deliver SMS over NAS without impacting MSC's the UE needs to indicate to the network that it supports Native SMS Capability on E-UTRAN and that it intends to register for that in both EPS Attach and TAU procedures, as in fact from rel-8 an EPS-only registration would not allow for SMS delivery over E-UTRAN (we need a combined registration as in TS 23.272 [23] to achieve that over SGs). The MME also needs to be able to accept or reject the SMS registration at EPS attach time, and indicate whether it support as an alternative SMSoSGs.

An interface needs to be defined between the MME and the SMS-GMSC/SMS-IWMC for SMS delivery (either using existing MAP procedures or equivalent IP based protocols to be defined at stage 3).

The HSS needs to be able to perform SMS routing and SMS waiting list management and interact with the SMS-GMSC/SMS-IWMSC (either using existing MAP procedures or a DIAMETER-based equivalent to be defined at stage 3). The adoption of DIAMETER - based interface may be preferred if we do not want to support legacy protocols in MME and HSS. This is in line with the conclusions b) in clause 7.2.2. However the interface to SGSN may still need to be using the legacy option.

Due to the fact the UE is dual registered on an SGSN and an MME with the HSS, a mechanism is needed to deliver the SMS to the correct serving node in MT-SMS case. One possibility is to update the location of the UE's requiring support of native SMS over EUTRAN and also subscribing to SMS services, when they change RAT, which would have no impact on the delivery interfaces or the SMS-GMSC/IWMSC. This precise "current serving node" information then also may be beneficial for other Mobile terminated services for MTC type devices.

When the PS only UE is in GERAN/UTRAN it may first attempt to register for PS services only. If the UE detects it is not possible to receive SMS from the serving SGSN, then if it is capable of obtaining SMS services from the CS domain it would register on the CS domain also. The CS subscription profile of a PS-only UE would have to be configured only for SMS services and no other CS services.

6.61.3 Impacts on existing nodes or functionality

MME needs to be augmented with Native SMS capability, i.e. an SMS delivery interface with the SMS-GSMS and an updates S6a with SMS delivery capability notification in attach and TAU. The NAS must be capable to transfer SMS and also to receive indication of support of SMS transfer over NAS in EUTRAN from the UE and whether accept it or

reject it. This indication may also need to be provided in TAU's so that when the UE moves from 2G/3G to the EPS the capability is known.

The UE needs to be capable of explicitly registering for native SMS over NAS at EPS attach and to send indication of registration and support to this capability at TAU time (in addition of supporting NAS procedures for SM transfer).

The MME and S4 SGSN shall be capable to detect whether the UE requires SMS delivery on EPS natively, and if so would update the HSS when the UE is changing between EUTRAN and GERAN/UTRAN.

6.61.4 Evaluation

This solution may be superior to SMS over IP in inexpensive devices (see 6.52.2.3 on Flexible deployment of MSC functionality for SMS over SGs).

6.62 Solution - User plane based device Triggering

6.62.1 Problem Solved / Gains Provided

Clause 5.8 "Key Issue - MTC Device Trigger".

6.62.2 High level information flow for Device Triggering using user plane

These solutions assume there is an application on the MTC device listening on a particular TCP/IP port to receive the application triggers.

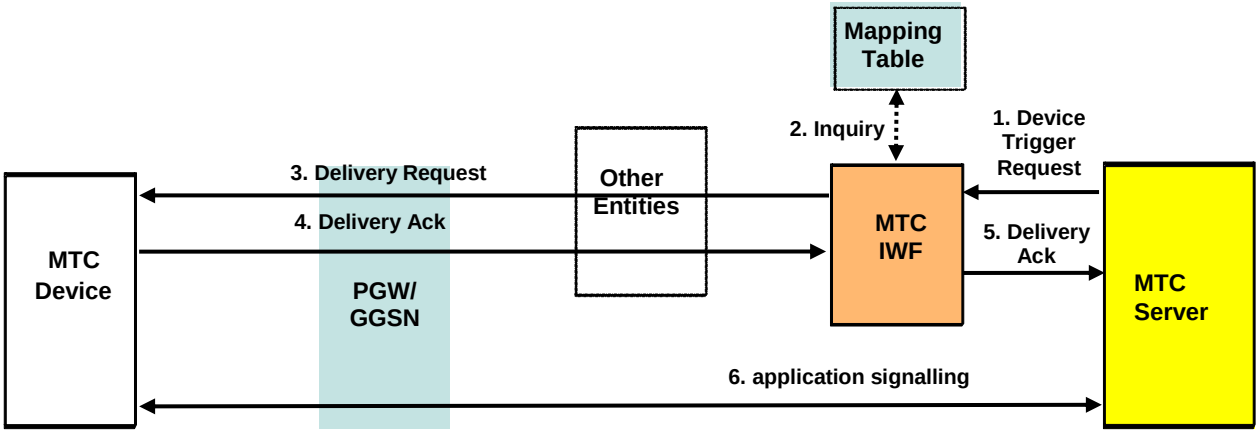


Figure 6.62.2-1:High level information flow for Device Triggering using user plane

1. The MTC server submits a Device Trigger Request providing the external device identifier and optionally a validity period.
2. The MTC-IWF authorises the trigger request. The IWF interrogates the HSS with the external device identifier to derive the IMSI and any additional information needed for trigger delivery.

   The MTC-IWF optionally queries other entities (such as mapping table etc) to obtain the IP address of the MTC Device. If the MTC Device had previously registered its IP address with the MTC-IWF through application layer signalling, the MTC-IWF does not have to query the mapping Table.

   Optionally, the MTC-IWF may also send the trigger to the MTC device over the user plane through other network entities such as IMS.
3. The IWF delivers the trigger request to the MTC device over the user plane. This message is seen as a data packet by the EPC.
4. The MTC UE sends a delivery ack.
5. The delivery or non-delivery is acknowledged to the MTC server.
6. The application on the device communicates with the MTC server.

6.62.3 Proposals for MTC-IWF to determine IP address of MTC device

This clause discusses various alternatives for the MTC-IWF to obtain the IP address of the MTC device.

6.62.3.1 Alternate 1 - Explicit Registration based

In this alternative, the MTC device explicitly registers with the MTC-IWF through application layer signalling.

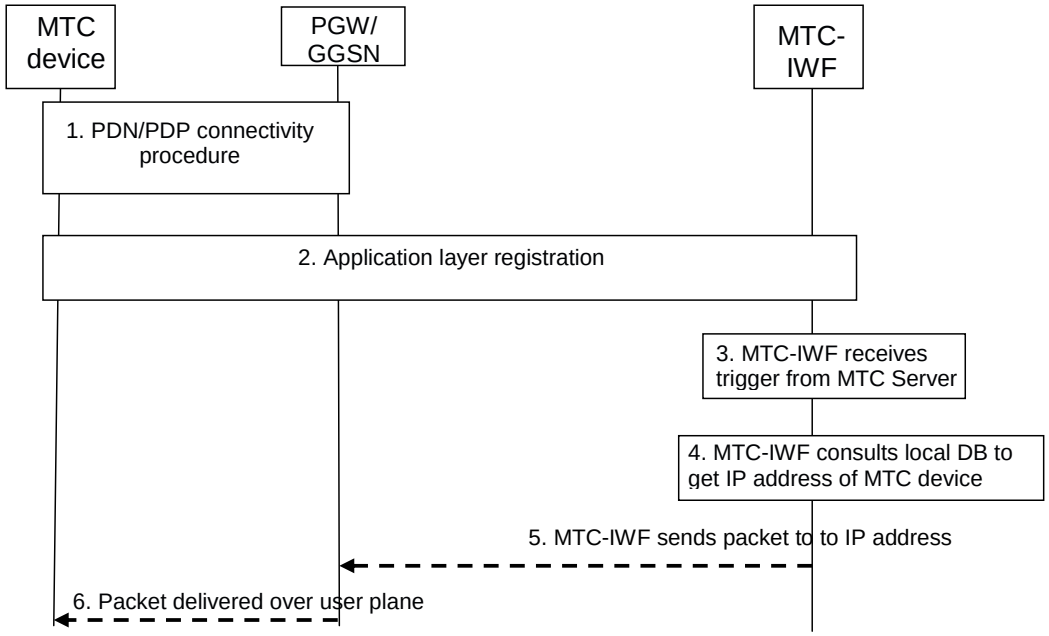


Figure 6.62.3.1-1: Alternate 1 - Explicit Registration based

1. The UE initiates PDN/PDP connectivity procedure as in TS 23.401 [5]/TS 23.060 [21].
2. The application on the MTC device registers its IPv4/IPv6 address with the MTC-IWF.
3. The MTC-IWF receives a trigger over MTCsp from the MTC server.
4. The MTC-IWF queries its local database to obtain the IPv4/IPv6 address of the UE.
5. The MTC-IWF sends the trigger to the MTC device using the IPv4/IPv6 address.
6. The PGW/GGSN delivers the packet to the UE over the user plane bearer.

Evaluation:

- This solution needs to define an application layer signalling message between MTC device and MTC-IWF to transport/register the IP address assigned to the MTC device.
- The MTC device needs to listen on specific port to receive & process the MTC trigger.

6.62.3.2 Alternate 2 - Mapping Table based

This clause discusses possible alternate solutions for the mapping table to be populated by different network entities with the MTC device's IP address.

6.62.3.2.1 MME/HSS based mapping table update

The flow/procedures for this option is specified in clause 6.1.

6.62.3.2.2 PGW/GGSN based mapping table update

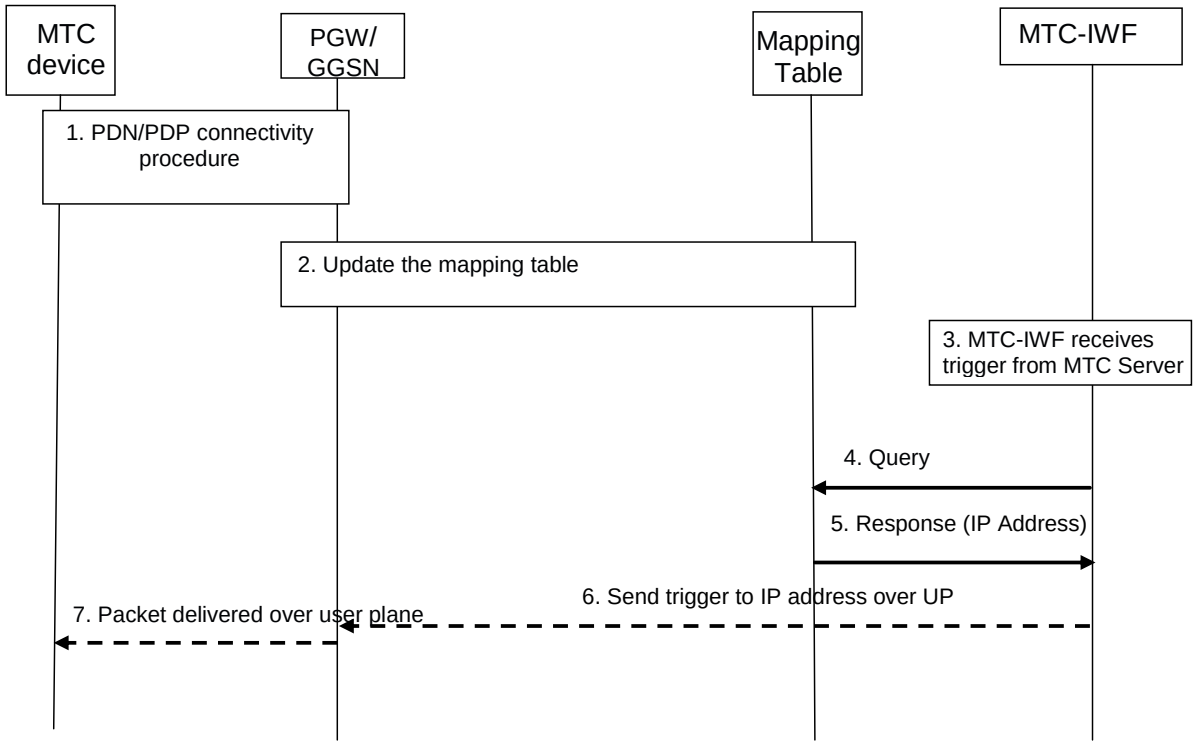


Figure 6.62.3.2.2-1: PGW/GGSN based mapping table update

1. The UE initiates PDN/PDP connectivity procedure as in TS 23.401 [5]/TS 23.060 [21].
2. The PGW/GGSN updates the mapping table with the IP address assigned to the UE.

NOTE 1: In case of the IPv6, the UE is configured to form its global IPv6 address as the concatenation of the IPv6 Prefix and the Interface Identifier provided by PGW/GGSN.

Editor's note: The mechanism/procedures/interfaces for updating the mapping table by the PGW/GGSN is FFS.

Editor's note: The use of DNS server as mapping table is FFS.

3. The MTC-IWF receives a trigger over MTCsp from the MTC server.
4. The MTC-IWF queries the mapping table for the IPv4 and/or IPv6 address that corresponds to the UE's FQDN.
5. The mapping table replies with the IPv4 and/or IPv6 address for the UE.
6. The MTC-IWF sends the trigger to the MTC device using the IPv4/IPv6 address.
7. The PGW/GGSN delivers the packet to the UE over the user plane bearer.

NOTE 2: When the UE detaches, the PGW/GGSN updates the mapping table.

Evaluation:

- This solution requires the PGW/GGSN to update/maintain the mapping table entry related to the MTC device.
- In case of IPv6, the global IPv6 address is constructed using the concatenation of the IPv6 prefix and the Interface ID provided by the PGW/GGSN.

6.62.4 IMS-based trigger delivery over user plane

Trigger can be delivered to UE over IMS using procedures defined in TS 23.204 [15]. There are no further impacts to any specification.

7 Conclusions

Editor's note: This clause is intended to list conclusions that have been agreed during the course of the work item activities.

7.1 Interim conclusions for release 10 specification work

This clause contains the agreed conclusions corresponding to Key Issue 5.12 and 5.14. 3GPP Release 10 specifications should be developed in the following areas:

a) the UE behaviour changes outlined in bullets a, b, c, d and e in clause 6.33;

b) the M2M device indicators outlined in bullets a, b and c in clause 6.34 (some of which are also mentioned in clauses 6.20, 6.23 and 6.26;

c) the non HPLMN (PLMN type) and Low-Priority-device style access class barring functionality outlined in clauses 5.12, 5.14 and 6.28.4;

NOTE: Updates to SA1 specifications such as TS 22.011 may be needed.

'Course grained' (i.e. "Low-Priority-Access" and "PLMN type") MTC access barring triggered via O+M into the RAN, internal RAN functionality, and by signalling from the Core Network is expected to be included in Rel-10. Other options for broadcasting of MTC access barring by RAN (e.g. based on the APN or MTC Group) may be considered for Rel-11.

d) the use of RR(C) connection reject messages with extended Wait Times outlined in clauses 6.23 and 6.26;

e) the use of M2M device specific (long) periodic update timers in MM, GMM and EMM signalling, including signalling from HSS to MSC/SGSN/MME (see clause 6.20);

f) in combination with the use of long, MTC specific PTU/PRU/PLU timers, the specification of signalling that permits the operator to command M2M devices to use Network Mode Of Operation I while keeping existing mobiles in Network Mode of Operation II (see clauses 5.14 and 6.20);

g) the specification of MM/GMM/EMM functionality that can limit load on CN entities of all local PLMNs (e.g. by the transmission of an RA Update ACCEPT message with PRU timer of 20 minutes rather than an RA Update Reject message);

h) the use of NAS-level back-off timer per APN to reject Attach and connectivity establishment requests as outlined in clause 6.22;

i) The use of connectivity establishment request rejection at MME/SGSN and PGW/GGSN as outlined in clause 6.22.

j) The use of the MME/SGSN overload control by DL MTC traffic throttling such as described in clause 6.30;

k) ///list to be completed. ///

7.2 Interim conclusions for release 11 specification work

7.2.1 IP Addressing - Key Issue 5.3

This clause contains the agreed conclusions corresponding to Key Issues 5.3.

3GPP Release 11 specifications should be developed in the following areas:

a) IPv6 as the primary solution for IP addressing of UEs used for MTC.

b) IPv4 based solutions are considered transition solutions and are deprecated. The following IPv4 capable addressing solutions are documented in appropriate informative annexes as described in clause 8.2.

- For all models, when the UE and the network support online device triggering, use the online device triggering to handle NAT traversal.

NOTE 1: The above solution resolves the issue when the UE and the MTC server do not share IPv4 addresses from a common IPv4 address space.

- For indirect and direct model, use of separate APNs (as described in clause 6.29.2), and IPv4 address allocation is performed following procedures already described in 3GPP specifications.

NOTE 2: The scenario where the MTC Server and/or its end-to-end connection to the mobile operator's domain is dependent on IPv4 addressing will be reduced as the migration to IPv6 proceeds. However an IPv6 capable MTC Server (i.e. dual-stack) in an IPv4 public address space can still be a valid scenario for some years. For such scenarios where there is no end-to-end IPv6 connectivity, well known transition mechanisms can be used. This is considered normal network design and should be transparent to 3GPP specifications. Therefore an MTC Server using IPv6 addressing connected to IPv6 UE used for MTC over a public IPv4 address space can be considered as an IPv6 scenario (i.e. scenario A in clause 5.3.1).

7.2.2 MTC Device Triggering - Key Issue 5.8

Editor's note: The conclusions do not imply a decision whether there will be one or multiple triggering methods standardised.

This clause contains the agreed conclusions corresponding to Key Issues 5.8. 3GPP Release 11 specifications should be developed in the following areas:

1) Delivery of device trigger information from 3GPP system to UE:

All device triggering should provide mechanism to ensure authenticity.

The following device trigger delivery mechanisms shall be developed/supported:

A. MT-SMS for the following cases:

   a. For UE subscriptions with an E.164-MSISDN assigned, submitted to SMS-SC of 3GPP system over MTCsms.

      i. This solution is especially applicable for providing triggers via legacy networks, i.e. networks that don't deploy any specific trigger delivery mechanism that might be introduced with Rel-11.

   b. For UE subscriptions with or without an E.164-MSISDN assigned, submitted to MTC-IWF of 3GPP system over MTCsp.

      i. When UE subscription does not have an E.164-MSISDN assigned, the MTC-IWF shall allow the IMSI as the destination address for submission of the MT-SMS to the SMS-SC.

Editor's note: Considerations for alternative to IMSI as the destination address for MTC-IWF submission of the MT-SMS to the SMS-SC is FFS.

   For devices that may camp on E-UTRAN cells, this trigger delivery solution is applicable only when the UE also has a CS domain subscription and the UE and network support SMS using SMSoSGs, as defined in TS 23.272 [23], or the UE and HPLMN are using SMS over IMS.

   UEs should be able to discriminate an MT-SMS carrying device triggering information from any other type of SMS.

Editor's note: It is FFS if MT-SMS procedures will be enhanced in Rel-11 to support MT-SMS to overcome the above limitations.

Editor's note: In order to avoid upgrades to legacy networks a protocol within the SMS body to carry the triggering information identified in clause 6.40 is FFS.

B. Improvements to MT-SMS that:

   a. ensure the SMS can be delivered to a PS-only device with only one HPLMN-VPLMN interaction, as SMS over SGs without improvement would entail an 'MSC' delivery attempt followed by an SGSN delivery attempt;

b. permit the replacement of MAP interfaces with more IETF friendly interfaces (e.g. Diameter); and

c. ensure that the MTC device can verify the authenticity of the trigger.

C. Trigger delivery over T5a/T5b/T5c

a. When serving SGSN/MME/MSC is available, the trigger is sent directly from the MTC-IWF to serving SGSN/MME/MSC over T5a/T5b/T5c.

b. SGSN/MME/MSC delivers the trigger to UE over the NAS.

Editor's note: How trigger is delivered to UE (e.g. using SMS transport or NAS generic container) will be taken during the normative phase of the work.

D. The following solutions related to User plane based trigger delivery:

a. Solutions (e.g., explicit registration, see 6.62.3.1) which do not require enhancements to 3GPP specifications.

NOTE: User plane trigger can be delivered to UE over IMS using procedures defined in TS 23.204 [15]. There are no further impacts to any specifications.

b. The possibility to support other user plane solutions depend on whether mapping between IP address and external id is available as a result of technical specification of the control plane solution.

2) Submission of device trigger requests from MTC server to 3GPP system:

a) The standardised protocol used from the MTC Server to the 3GPP system via reference point MTCsp should support both triggering with unique E.164-MSISDN (for backward compatibility) and without such an MSISDN. The MTCsp is provided by an MTC-IWF. It is transparent for the MTC server how the triggering information is delivered by the 3GPP system to the UE.

b) It shall be possible for an MTC server to resolve the MTC-IWF(s) address(es) for a particular UE, e.g. by DNS

c) The MTC-IWF performs PLMN related control functionality such as MTC server authentication, trigger request authorization and charging, and shields the MTC server from the actual trigger delivery mechanism used in the PLMN.

d) MTCsp shall always be provided by the HPLMN. The MTC-IWF will only accept a device trigger request for a UE whose HPLMN is the operator of the MTC-IWF.

e) The MTC Server uses validity time over MTCsp.

f) The MTC-IWF shall support load control functionality to indicate MTC server over MTCsp interface to limit the load generated on it.

Editor's note: The load control function needs to consider the possible causes to complicate the trigger handling of the MTC server.

3) 3GPP system internal handling of device triggers:

a) The protocols within the PLMN should support an option where the UE can be identified without the use of an E.164-MSISDN. A PLMN may support delivery of MT-SMS submitted with an IMSI as destination address instead of an E.164-MSISDN. However, in order to avoid exposure of IMSI outside of MNO domain, this shall only be allowed for SMEs located in the MNO domain.

b) The 3GPP system shall support MTC-IWF interrogation, when needed, of HLR/HSS to map an external identifier to IMSI and gather information stored in HLR/HSS required for device triggering.

c) The MTC-IWF shall support selection of the trigger delivery mechanism and performs protocol translation if necessary, e.g. to reformat the triggered request to match the selected trigger delivery method, and routes the request towards the relevant network entity.

d) When SMS service is selected as the trigger delivery mechanism, validity time over MTCsp is mapped to Validity Period in SMS delivery.

e) The MME/SGSN/MSC and MTC-IWF shall support overload control functionality to allow the MME/SGSN/MSC to indicate in the rejection or acknowledgement to the MTC-IWF over T5a/T5b/T5c interface to limit the load generated on it.

7.2.3 MTC Identifiers - Key Issue 5.13

This clause contains the agreed conclusions corresponding to Key Issues 5.13. 3GPP Release 11 specifications should be developed in the following areas:

a) IMSI is the internal identifier.

b) The existing 3GPP identifiers are not modified, i.e. there will be neither changes to IMSI/IMEI structure nor other changes to existing 3GPP identifiers.

c) When the MSISDN is not available for CDR generation in the PS domain, the IMSI shall be used for CDR generation purposes. Typically, the external identifier is used for customer billing.

d) Alternative identifier(s) to MSISDN shall be supported on the MTCsp as the external identifier(s).

e) External identifier shall have following components that makes it globally unique:

   a. Domain-Identifier that identifies a domain that is under the control of a Mobile Network Operator (MNO). This is used to find MTC-IWF (i.e. IP address on MTCsp) to be used. Domain-Identifier may have further identification for example to identify MTC-IWF specific for application.

   b. Local-Identifier that is assigned by the mobile network operator. This identifier is used to derive or obtain internal identifier by the network operator. The local identifier shall be unique within this domain. The structure of the Local Identifier is flexible. For Example it may be structured into one or more different parts:

      i. A part optimized to find an entry in MNO database (e.g. subscription context in HLR/HSS to derive Internal Identifier). Few examples are the Subscriber Number part of an E.164 MSISDN (see TS 23.003 [12]) or other scheme specified by the MNO.

      ii. Another part relevant to customer application (e.g. to enable corporate customer to find information in their database). Few examples are serial number, chassis number for car, etc.

f) Multiple external identifiers can map to single internal identifier (i.e. IMSI).

7.2.4 MTC Feature Control - Key Issue 5.7

This clause contains the agreed conclusions corresponding to Key Issues 5.7

a) No solution for MTC Feature Control is standardized for Rel-11.

7.2.5 MTC Feature - Packet Switched only

This clause contains the agreed conclusions for the MTC feature "Packet Switched (PS) only". 3GPP Release 11 specifications should be developed in the following areas:

a) It shall be possible to provide PS services and SMS for a UE via GERAN and UTRAN without involving an MSC. This includes the case where an HSS does not provide subscription data to a GERAN or UTRAN MSC for that UE when both UE and serving PLMN support the feature.

b) Not receiving services from a GERAN or UTRAN MSC due to PS only shall not affect services provided to that UE, which may include that an unsuccessful/rejected registration attempt towards a GERAN/UTRAN MSC shall not result in loosing SMS services provided via another RAT or domain used by the UE.

c) It shall be possible to provide PS services and SMS via E-UTRAN/MME with efficient HSS signalling, which may include an HSS registration procedure that provides subscription data for PS services and SMS together. It should not have adverse effects like increased HSS signalling, e.g. when the UEs reselect between RATs.

d) The PS only feature shall not prevent receiving SMS services when the UE or the visited/serving PLMN don't provide the capabilities required for PS only.

e) There need to be mechanisms to allow the UE to select the appropriate SMS delivery mechanism(s). Whether to adopt existing E-UTRAN access procedures for SMS via NAS signalling (i.e. Combined EPS/IMSI Attach and Combined TA/LA Update) or to use different procedures (e.g. EPS Attach and TA Update with addition of new information elements) is TBD. For 2G/3G access the SGSN and/or MSC registration procedures may be enhanced to inform the UE that it should use only the PS domain for receiving PS and specifically SMS services.

f) The PS only feature shall not affect PS or SMS services and shall work whether the UE has an MSISDN assigned or not.

8 Impacts to normative specifications

Editor's note: This clause is intended to capture the impacts to normative specifications within the responsibility of SA2. It can be used as a placeholder to document agreements until a set of normative CRs can be generated for the selected solutions(s)

8.1 Related to Interim conclusions for release 10 specification work

The changes outlined in bullets a through g in clause 7.1 have minimal impact on SA2's specifications. Probably, some general clause s could be added to TS 23.060 [21] and TS 23.401 [5] to describe the overall problem and solutions.

With the exception of TS 23.122, and a new OMA DM Managed Object, stage 3 work is probably also relatively limited: e.g. a few new code points or information elements are needed in the NAS signalling (TS 24.008 [16] and TS 24.301 [17]); the HSS-MSC/SGSN/MME signalling (TS 29.002 [18] and TS 29.272 [19]); the UE-RAN signalling (TS 36.331, TS 25.331 and TS 44.018); and possibly in the S1/Iu/Gb/A interface Overload messages.

Modified TS 23.122 procedures and the associated UE interactions with multiple local PLMNs probably represents the major complex task ahead in Release 10.

Editor's note: The impact of bullets h, i and j in clause 7.1 still has to be checked.

8.2 Related to Interim conclusions for release 11 specification work

8.2.1 IP addressing

8.2.1.1 Guiding Principles

This clause provides a proposed way forward and guiding principles on how to document IP addressing related aspects in normative Stage 2 specifications.

The guiding principles when to documenting IP addressing solutions are:

A. Focus on most important deployment scenarios as in clause 5.3.1.

B. Maximize the reuse of existing 3GPP standards and minimize the impact on the 3GPP System.

C. Use of IPv6 addressing as the primary solution for IP addressing of UEs used for MTC. IPv4 based addressing is deprecated but not precluded.

8.2.1.2 Documentation approach

It is proposed that IP addressing aspects are documented using the following approach:

- A normative part giving an overview of IPv6 addressing mechanisms.

- An informative annex documenting how existing mechanisms can be used to support IPv4 addressing mechanisms to serve as implementation guideline for transition solutions.

8.2.2 MTC Identifiers

8.2.2.1 Guiding Principles

The guiding principles when documenting identifiers for MTC are:

A. Continued usage of IMSI, i.e. no need to define an Internal Identifier in normative specifications.

B. The External Identifier is required for protocols used across the 3GPP boundary, where MSISDN and IMSI cannot be used (e.g. when MSISDN-less operation is used and security reasons prevent IMSI to be used). These protocols include:

- Protocols used on the Tsp reference point.
- The RADIUS/Diameter protocols used on Gi/SGi reference point.

Editor's note: It is FFS whether and where in CN the External Identifier(s) need to be present to support e.g. Lawful Interception or charging.

8.2.2.2 Documentation approach

MTC Identifiers aspects are documented in SA WG2 specifications using the following approach:

- A normative part giving an overview of External Identifier usage on MTC-IWF based interfaces in TS 23.682 [20].
- Normative parts in TS 23.003 [12], TS 23.060 [21], TS 23.401 [5] and TS 23.682 [20] updating the information storage of relevant key nodes.

Annex A:
Stage 2 PS Dependencies on MSISDN-based Subscriptions

A.1 General Considerations

In order to facilitate the enhancement of the stage 2 architecture to support MSISDN-less subscriptions for PS only devices, this annex attempts to:

a) summarize all the stage 2 PS dependencies on the MSISDN; and

b) analyse the stage 2 impact of supporting MSISDN-less subscriptions for PS only MS/UEs.

A.2 PS stage 2 MSISDN dependencies

A.2.1 General network architecture

1) TS 23.002-a11 (3GPP PLMN network architecture overview):

   a) clause 4.1.1.1.3 - HSS user identification handling includes providing relationship between MSISDN and other appropriate user identities in the PS domain.

2) TS 23.008-920 (organization of subscriber data):

   a) clause 2.1 - specifies MSISDN, basic MSISDN and MSISDN-Alert indicator as permanent UE/MS subscriber data stored in Gn/Gp-SGSN as conditionally appropriate;

   b) clause 3B.1.2 - specifies MSISDN is used for WLAN-IW subscription;

   c) clause 5 - possible to retrieve or store subscriber data for a particular MS/UE from the HSS, 3GPP AAA Server , 3GPP AAA Proxy, WAG, PDG through reference to the MSISDN and IMSI.

3) TS 23.228-a31 (IMS):

   a) clause 4.2.4a - Sh interface supports mechanisms for transfer of user related data stored in the HSS, including the MSISDN.

Editor's note: Additional dependencies are FFS.

A.2.2 GPRS

1) TS 23.060-a20 (GPRS):

   a) MSISDN is stored as part of HLR/HSS GPRS/EPS subscription data (clause 13.1), SGSN MM and PDP/EPS bearer contexts (clause 13.2.3) and GGSN PDP Context (clause 13.3);

   b) clause 9.2.2.1 - SGSN sends MSISDN to GGSN in PDP Context Activation procedure;

   c) clause 9.2.2.1A - SGSN sends MSISDN to S-GW in Create Session Request procedure.

A.2.3 EPS

1) TS 23.401-a21 (EPS):

   a) clause 5.7.1 - The basic MSISDN is optionally stored in the subscription data stored in the HSS;

   b) clauses 5.7.2, 5.7.3 and 5.7.4 - The presence of the basic MSISDN in the MM context and EPS bearer context information stored in the MME, S-GW and P-GW is dictated by its storage in the HSS.

Editor's note: Additional dependencies are FFS.

A.2.4 WLAN

1) TS 23.234-900 (WLAN interworking):

   a) clause F.3.1 - TTG retrieves the IMSI and MSISDN from the AAA server during (Interworking procedure over Gn') Tunnel establishment procedure.

Editor's note: Additional dependencies are FFS.

A.2.5 SMS

Figure A.2.5-1 aims at illustrating the use of MSISDN for SMS communication today. Depicted is a scenario where both the SMS Originator (UE-O) and SMS Recipient (UE-R) are roaming in VPLMN-O and VPLMN-R, respectively, and there is no Home Routeing of SMS.

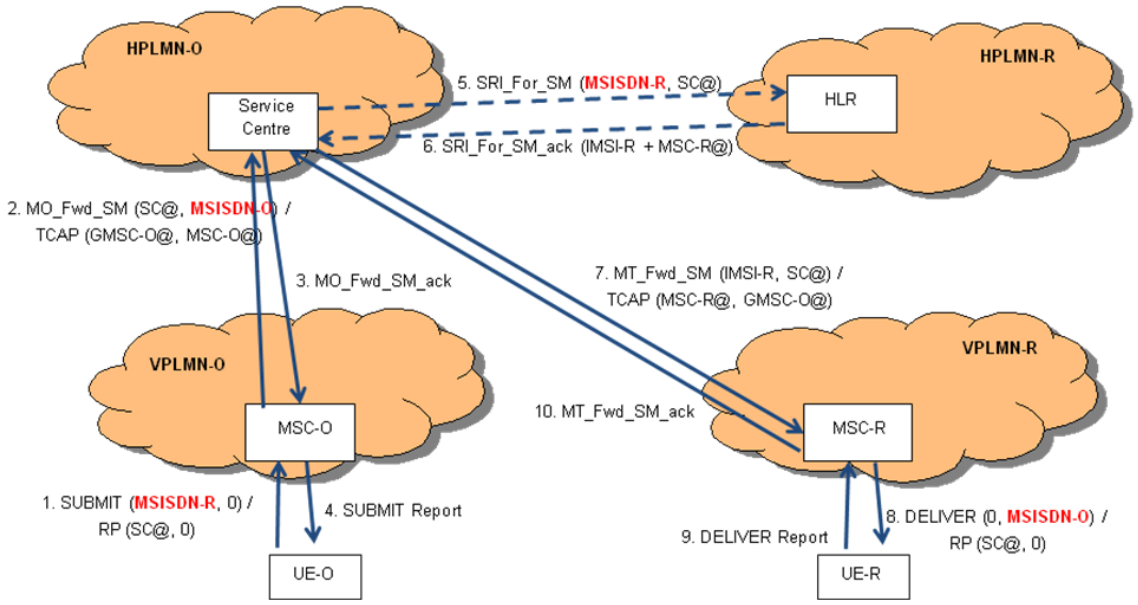


Figure A.2.5-1: Use of MSISDN for SMS communication (no Home Routeing)

1) TS 23.040-920 (SMS)

   a) SM-RL (Short Message Relay Layer) protocol messages can include MSISDN / MSIsdn-Alert in the following messages:

      1) clause 3.2.6 - SMS-GMSC/IP-SM-GW includes MSISDN and conditionally MSIsdn-Alert to set the Message Waiting Data into the HLR or to inform the HLR of successful SM transfer after polling via MAP-REPORT-SM-DELIVERY-STATUS (see TS 29.002 [18] clause 12.3);

      2) clause 9.3.2.4 - conditionally includes the MSIsdn-Alert in RP ERROR => MAP-REPORT-SM-DELIVERY-STATUS (see TS 29.002 [18], clause 12.3) when transfer attempt failed because the MS is not reachable or because the MS memory capacity was exceeded;

      3) clause 9.3.2.1 - RP MO DATA => MAP-MO-FORWARD-SHORT-MESSAGE (see TS 29.002 [18], clause 12.2);

      4) clause 9.3.2.2 - RP-MT-DATA => MAP-MT-FORWARD-SHORT-MESSAGE (see TS 29.002 [18], clause 12.9).

   b) clause 8.1.4 - SMS Router may store the MSISDN against the MT Correlation ID as part of the a routing information retrieval operation;

   c) clause 8.2.1 - MSC/SGSN retrieves MSISDN from VLR/HLR after receiving a short message TPDU from the MS/UE;

d) clauses 9.2.2 and 9.1.2.5 - the Short Message Transfer Layer (SM-TL) protocol allows for MSISDN (E.164) or other types of number-plan-identification. However the address size is limited to 12 octets, which may not be sufficient for some very long identifiers. The MSISDN is used as the address in the following messages:

1) SMS DELIVER (clause 9.2.2.1);

2) SMS SUBMIT (clause 9.2.2.2);

3) SMS STATUS REPORT (clause 9.2.2.3);

4) SMS COMMAND (clause 9.2.2.4).

e) There is no impact on the SS7 TCAP, the addresses used on these layers being node addresses (MSC, GMSC) rather than device addresses.

2) TS 23.204-a20 (SMS over generic 3GPP IP access):

a) clause 5.3.1 - IP-SM-GW acquires and maintains knowledge of the association between the MSISDN, IMSI and the address of the S-CSCF serving of the user;

b) clause 5.3.1 - For SM MT, IP-SM-GW maps the recipient's address from an MSISDN/IMSI to TEL URI format when receiving an SMS for an IP-based UE.

Editor's note: Additional dependencies are FFS.

A.2.6 IMS

1) TS 23.167-b01 (IMS emergency sessions):

a) clause 7.5.1 - PSAP uses the MSISDN (E.164) of the user for call back.

Editor's note: Additional dependencies are FFS.

A.2.7 PCC

1) TS 23.203-b01 (PCC architecture):

a) clauses 6.2.1.1, A.1.3.2.1.1 and A.1.3.2.2.1 - subscriber identity (e.g. IMSI, MSISDN) provided to PCRF as input for PCC decisions;

b) clause A.1.3.2.2.1 - For each PDP context, the PCEF shall accept the MSISDN during bearer establishment and modification and shall use this information in the OCS request/reporting or request for PCC rules.

Editor's note: Additional dependencies are FFS.

A.2.8 LCS

1) TS 23.271-a11 (LCS).

Editor's note: Dependencies are FFS.

A.2.9 SIPTO

1) TS 23.060-a20 (GPRS):

a) Clause 5.3.12.2 and Annex B.1-2 - to support activation of "SIPTO at Iu-ps" function, the SGSN sends MSISDN to target RNC during the:

1) SRNS Relocation procedures (clauses 6.9.2.2.1, 6.9.2.2.2 and 6.9.2.2.3);

2) Service Request Procedures (clauses 6.12.1 and 6.12.2);

3) the intersystem change procedures from A/Gb mode to Iu mode (clauses 6.13.1.2.1 and 6.13.2.2.1);

4) RAB Assignment procedure (clause 12.7.4.1).

Editor's note: Additional dependencies are FFS.

A.2.10 CAMEL

1) TS 23.078-910 (CAMEL Phase 3):

   a) clause 6.6.1.5 - for GPRS interworking for CAMEL, basic MSISDN included in the gprsSSF to gsmSCF Initial DP GPRS IF when a trigger is detected at a DP in the GPRS state model, to request instructions from the gsmSCF:

   b) clause 7.6.1.2 - for MO/MT SMS interworking for CAMEL, MSISDN included as the Called/Calling Party Number in the gprsSSF to gsmSCF Initial DP SMS IF when a trigger is detected at a DP in the SMS state model, to request instructions from the gsmSCF:

   c) clause 7.6.2.1 - for MO/MT SMS interworking for CAMEL, MSISDN may be included as the Calling Party Number in the gsmSCF/gsmSSF or gprsSSF Connect SMS IF to request the gsmSSF/gprsSSF to perform the actions to route the Short Message to a specific destination (for MO SMS) or to deliver the Short Message to the MS (for MT SMS);

   d) clause 9.4.1.1 - for GPRS Mobility Management in CAMEL, basic MSISDN included as GPRS mobile subscriber identity in SGSN to gsmSCF Mobility Management event IF;

   e) clause 10.3.1.1 -for control and interrogation of subscription data by CAMEL, MSISDN or IMSI used as subscription identity in gsmSCF to HLR Any Time Modification Request IF;

   f) clause 10.3.1.2 - for control and interrogation of subscription data by CAMEL, MSISDN and/or IMSI used as subscription identity in gsmSCF to HLR Any Time Subscription Interrogation Request IF;

   g) clause 10.3.2.2 - for control and interrogation of subscription data by CAMEL, MSISDNs used as subscription identity in HLR to gsmSCF Any Time Subscription Interrogation ack IF;

   h) clause 10.3.2.3 - for control and interrogation of subscription data by CAMEL, MSISDN used as subscription identity in HLR to gsmSCF Notify Subscriber Data Change IF;

   i) clause 10.3.3.1 - for control and interrogation of subscription data by CAMEL, MSISDN or IMSI used as subscription identity in IP-SM-GW to HLR Any Time Modification Request IF used to register the IP-SM-GW for a subscriber in the HLR;

   j) clause 11.3.1.1 - for subscriber location and subscriber state information retrieval by CAMEL, MSISDN or IMSI used as subscription identity in gsmSCF to GMLC Any Time Interrogation Request IF used to request information (Mobile Station location) from the GMLC;

   k) clause 11.3.3.1 - for subscriber location and subscriber state information retrieval by CAMEL, MSISDN or IMSI used as subscription identity in gsmSCF to HLR Any Time Interrogation Request IF used to request information (any one or more of subscriber state, subscriber location, IMEI (with software version) and MS classmark information for the requested domain) from the HLR;

Editor's note: Additional dependencies are FFS.

A.2.11 Other services

1) TS 23.066-900 (MNP):

   a) Various - describes several alternatives for the realisation of Mobile Number Portability to retain ones MSISDN.

2) TS 23.141-900 (Presence Service):

   a) clause 6.1.1 - MSISDN can be the contact address attribute of the subscriber.

3) TS 23.246-950 (MBMS):

   a) clauses 8.2 and 10.3 - MSISDN is passed from SGSN to GGSN and GGSN to MB-SC during MBMS Multicast Service Activation to provide the operator with the ability to associate GPRS location information (i.e. serving network identity) with a user.

4) TS 23.240-900 (3GPP GUP):

   a) Annex B - GUP access for the "PLMN specific user information" by the S-CSCF and AS includes the MSISDN;

   b) Annex B - GUP access for the "Authorized and subscribed service information for CS & PS" by the MSC/VLR, GMSC, SGSN, GGSN and MMS server includes the MSISDN.

Editor's note: Additional dependencies are FFS.

A.3 Impact of MSISDN-less subscriptions for PS only MS/UEs

Editor's note: Analysis is FFS.

Annex B:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2010-09	SP-49e	SP-100562	-	-	MCC Update to version 1.0.0 for presentation to TSG SA for information	0.5.1	1.0.0
2012-08	SP-57	SP-120489	-	-	MCC Update to version 2.0.0 for presentation to TSG SA for approval	1.7.0	2.0.0
2012-09	-	-	-	-	MCC Update to version 11.0.0 after TSG SA approval (Rel-11)	2.0.0	11.0.0