# Network Reference Architecture
# Technical Report MTR-004
# Release 2.0

Contribution Reference Number: MWIF 2001.053.3

**NOTICE: Please review this Draft Technical Report for any undisclosed intellectual property (including but not limited to trademarks, copyrights, patents or any similar, registered or other allowable intellectual property rights, published or unpublished, anticipated or actual, presently existing or potentially arising in the future, in any country). If you have any undisclosed intellectual property that either will or may be infringed by the implementation of this Draft Technical Report, you must disclose this fact to the Board of Directors of MWIF immediately. If you fail to make such a disclosure, and the Draft Standard is adopted, you must grant all Members of MWIF a nonexclusive worldwide license to use this intellectual property on fair, reasonable and nondiscriminatory terms. Please direct any questions to the Board of Directors.**

# Mobile Wireless Internet Forum

| | |
|---|---|
| **Contribution Reference Number:** | MWIF 2001.053.3 |
| **Last Saved:** | 6/13/2002 1:03 PM |
| **Working Group:** | Architecture |
| **Title:** | MWIF Network Reference Architecture |
| **Source:** | MWIF Architecture Working Group |
| **Editor** | Mick Wilson |

**IPR Acknowledgement:**

Attention is called to the possibility that use or implementation of this MWIF Technical Report may require use of subject matter covered by intellectual property rights owned by parties who have not authorized such use. By publication of this Technical Report, no position is taken by MWIF or its Members with respect to the infringement, enforceability, existence or validity of any intellectual property rights in connection therewith, nor does any warranty, express or implied, arise by reason of the publication by MWIF of this Technical Report. Moreover, the MWIF shall not have any responsibility whatsoever for determining the existence of IPR for which a license may be required for the use or implementation of an MWIF Technical Report, or for conducting inquiries into the legal validity or scope of such IPR that is brought to its attention. This Technical Report is offered on an “as is” basis. MWIF and its members specifically disclaim all express warranties and implied warranties, including warranties of merchantability, fitness for a particular purpose and non-infringement.

**Status:** Revision 2

**Abstract:**

This document describes the MWIF Network Reference Architecture in terms of a model and the definitions of the Network Functional Entities and the interconnecting Reference Points.

**For addition information contact:**

Mobile Wireless Internet Forum
39355 California Street, Suite 307
Fremont, CA 94538
+1 (510) 608-5930
+1 (510) 608-5917 (fax)
info@mwif.org
www.mwif.org

## Table of Contents

# 1 INTRODUCTION

This document defines the MWIF Network Reference Architecture. It provides a model of the Network Reference Architecture (NRA) and defines the Network Functional Entities and the interconnecting Reference Points.

## 1.1 Objectives of the MWIF Technical Report

The objective of the Network Reference Architecture is to define the distribution of functions into Network Functional Entities and to define the Reference Points that interconnect individual Network Functional Entities. A Network Functional Entity contains logical functions. A physical implementation may consist of one or more Network Functional Entities. Reference Points are physical interfaces when the interconnected Network Functional Entities are on separate physical implementations.

## 1.2 Definitions

This document employs the following terminology:

- Must, Shall, or Mandatory — the item is an absolute requirement of the Technical Report (TR).
- Should — the item is highly desirable.
- May or Optional — the item is not compulsory, and may be followed or ignored according to the needs of the implementers.

## 1.3 Overview of the Technical Report

This report describes a network reference architecture as a set of Network Functional Entities interconnected by Reference Points.

This document has the following organization:

Section 1: Introduction

Section 2: References

Section 3: Nomenclature: Abbreviations and Definitions

Section 4: MWIF Network Reference Architecture Diagram

Section 5: Descriptions of Network Functional Entities

Section 6: Descriptions of Reference Points

Section 7: Data Dictionary

Section 8: Document History

Appendix A: Message Sequence Charts

## 1.4 MWIF Technical Report Release Plan

It is the objective of the MWIF to provide timely industry direction for mobile wireless internet. In order to accomplish this, the MWIF will periodically release Technical Reports. The period in which Technical Reports will be released will be frequent enough to meet the objective of timely industry direction.

This Technical Report is the fourth in a series intended to specify the MWIF architecture. At the time of release of this report, the following MWIF Technical Reports are scheduled:

| | |
|---|---|
| MTR-001 | MWIF Architectural Principles |
| MTR-002 | MWIF Architecture Requirements |
| MTR-003 | MWIF Layered Functional Architecture |
| MTR-004 | MWIF Network Reference Architecture |
| MTR-005 | MWIF Gap Analysis |
| MTR-006 | MWIF IP Transport in the RAN |
| MTR-007 | MWIF IP Radio Control / Bearer in the RAN |

## 1.5 Release Plan for This Document

| | |
|---|---|
| MTR-004 Release 1.0 | Initial provisional release. |
| MTR-004 Release 2.0 | Refinement release to include additional requirements and to clarify issues and items for further study. |
| MTR-004 Release 3.0 | To address the following outstanding issues: |

- Security including firewall control.
- Interworking with legacy systems
- OAM&P
- Accounting including "Real Time aspects"
- Service Architecture

# 2 REFERENCES

[AAA] IETF Authentication-Authorization-Accounting: Protocol Evaluation, www.ietf.org/internet-drafts/draft-ietf-aaa-proto-eval-00.txt, work in progress.

[ANSI-41] TIA/EIA-41 Cellular Intersystem Operations

[ANSI-TCAP] ANSI Transaction Control Application Part, T1.114-1988.

[COPS] IETF RFC 2748, COPS (Common Open Policy Service) Protocol.

[DIAMETER] IETF "DIAMETER Base Protocol" draft-calhoun-diameter-16.txt, work in progress.

[DiffServ] IETF RFC 2475, An Architecture for Differentiated Services

[DS0] ITU G.703, Digital Service Zero (56 or 64 kbps circuit)

[G.711] ITU G.711, Pulse Code Modulation (PCM) of Voice Frequencies

[GSM-MAP] 3GPP TS 29.002, V3.4.0, Mobile Application Part (MAP) Specification

[IP] IETF RFC 2460, Internet Protocol, Version 6 (Ipv6).

[ITU-TCAP] ITU Transaction Control Application Part.

[LDAP] IETF RFC 2251, Lightweight Directory Access Protocol (v3).

[LFA] MWIF MTR-003 Layered Functional Architecture

[MEGACO] IETF draft-ietf-megaco-protocol-08.txt, work in progress.

[MGCP] IETF RFC 2705, Media Gateway Control Protocol.

[MPLS] IETF Multiprotocol Label Switching www.ietf.org/internet-drafts/draft-ietf-mpls-framework-05.txt, work in progress.

[MTP2] Message Transport Protocol Layer 2 (usually some national variation of *ITU Q.701 – Q.710*).

[MTP3] Message Transport Protocol Layer 3 (usually some national variation *ITU Q.701 – Q.710*).

[RADIUS] IETF draft-ietf-radius-radius-v2-06.txt, work in progress.

[RSVP] IETF RFC 2205, Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification Framework Architecture for Signaling Transport

[RTCP] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Applications

[RTP] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Applications

[RTSP] IETF RFC 2326, Real Time Streaming Protocol (RTSP).

[SCCP] Signaling Connection Control Part (usually some national variation of *ITU Q.711 – Q.714*).

[SCTP] IETF RFC 2719, Framework Architecture for Signaling Transport.

[SIP] IETF RFC 2543, Session Initiation Protocol.

[SLP] IETF RFC 2165, Service Location Protocol (SLP).

[TCP] IETF RFC 793, Transmission Control Protocol (TCP).

[UDP] IETF RFC 768, User Datagram Protocol (UDP).

# 3 Nomenclature

## 3.1 Abbreviations

| | |
|---|---|
| 3GPP | Third Generation Partnership Project |
| 3GPP2 | Third Generation Partnership Project 2 |
| AG | Access Gateway |
| AN | Access Network |
| API | Applications Programming Interface |
| ATG | Access Transport Gateway |
| CN | Core Network |
| CSM | Communication Session Manager |
| D-Channel | ISDN delta channel 16 or 64 kbps |
| DNS | Directory Name Service |
| DTMF | Dual Tone Multi-Frequency |
| EIA | Electronics Industry Association |
| FTP | File Transfer Protocol |
| GLM | Geographic Location Manager |
| GNS | Global Name Server |
| GSM | Global System for Mobility |
| HMM | Home Mobility Manager |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| MA | Mobile Attendant |
| MAP | Mobile Application Part (e.g., TIA/EIA-41 MAP or GSM MAP) |
| MG | Media Gateway |
| MGC | Media Gateway Controller |
| MRC | Multimedia Resource Controller |
| MRF | Multimedia Resource Function |
| MWIF | Mobile Wireless Internet Forum |
| OAM&P | Operations, Administration, Maintenance, and Provisioning |
| OMG | Object Management Group |
| PSTN | Pubic Switched Telephone Network |
| QoS | Quality of Service |
| RAN | Radio Access Network |

| | |
|---|---|
| SIP | Session Initiation Protocol |
| TIA | Telecommunications Industry Association |
| UIM | User Identity Module |
| UMTS | Universal Mobile Telecommunications System |
| URL | Universal Resource Locator |
| UTRAN | UMTS Terrestrial Radio Access Network |
| VPN | Virtual Private Network |

## 3.2 Definitions

**administrative domain:** Within the Internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same administrative domain.

**Border router:** 1) a router that connects two or more IP routing domains and use Border Gateway Protocol (BGP) to communicate with other border routers. 2) a demarcation point for an IP routing domain or Autonomous System.

**Border gateway:** an entity that connects two administrative domains hiding the details of internal administration of each domain from the other. It performs the necessary firewall functions to protect the entities and users within a domain.

**CSM sessions**: voice calls or multimedia sessions that are controlled via interaction with the Communication Session Manager (e.g., SIP session).

**Edge router:** an entity that is the first or last hop for any packets within a logical domain (e.g., a Diff-Serv domain, a MPLS domain) that provides traffic conditions or shaping, packet admission control, and packet marking and remarking.

**Firewall:** a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized users from accessing private networks, especially intranets, connected to the public Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**Non-CSM sessions:** sessions that are not controlled by the Communication Session Manager (e.g., FTP transactions).

**QoS request:** a request for specific attributes of quality (e.g., bandwidth, nominal throughput, maximum throughput, maximum allowable jitter, maximum allowable packet loss, maximum allowable error rate, maximum allowable retransmission rate, maximum allowable delay).

**Subscriber:** is a unit of billing that may comprise one or more terminals and one or more users. Each subscriber has a unique identifier.

# 4 MWIF NETWORK REFERENCE ARCHITECTURE DIAGRAM

The following diagram depicts the MWIF Network Reference Architecture:

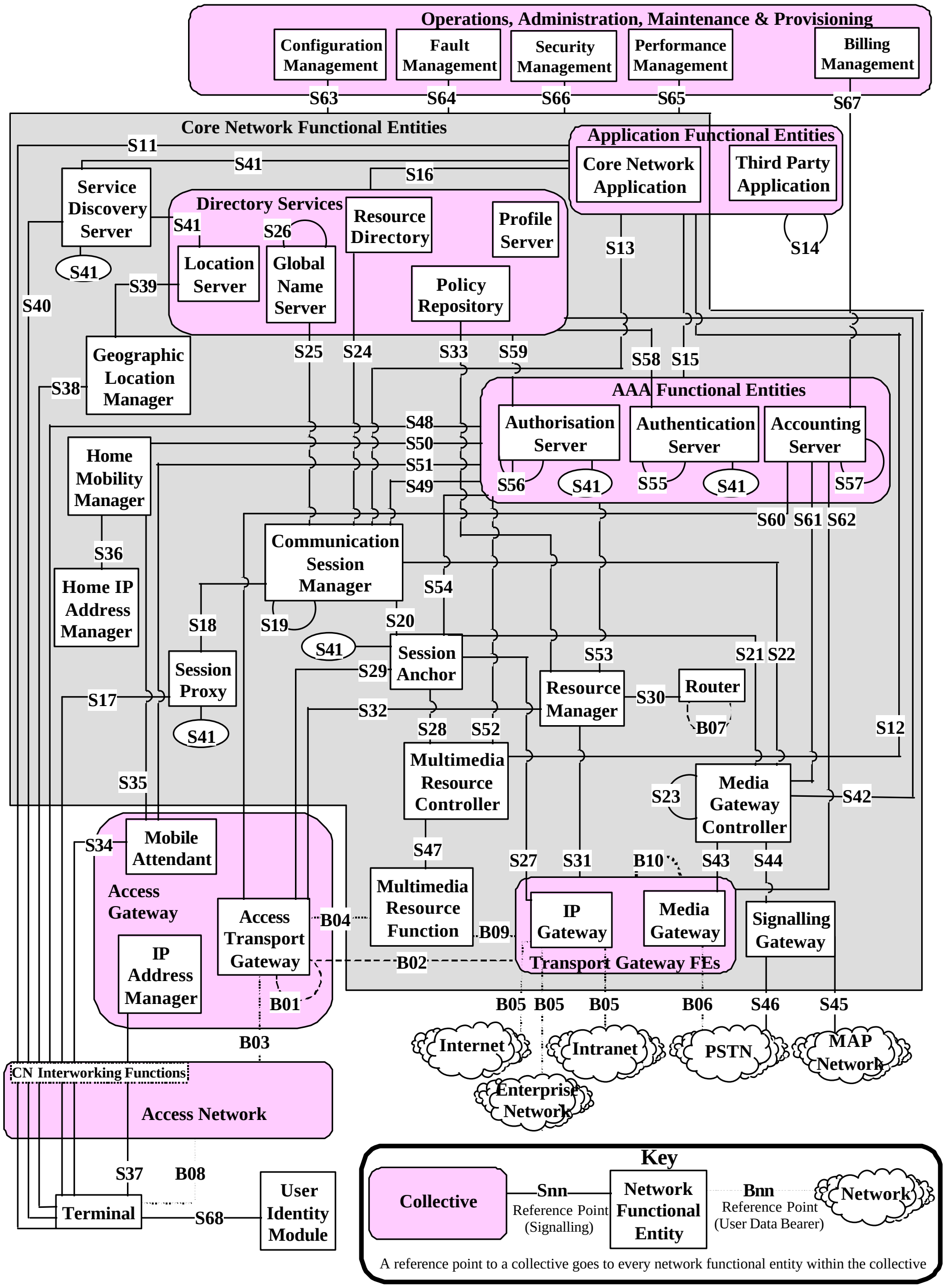


Figure 1. MWIF Network Reference Architecture Model

# 5 Network Functional Entities

This section describes the Network Functional Entities comprising the MWIF Network Reference Architecture.

## 5.1 AAA Functional Entities

The AAA Functional Entities is a collective containing the functions associated with:

- Authentication
- Authorisation
- Accounting

## 5.2 Access Gateway (AG)

The Access Gateway is a collective that interfaces an access network to the core network. It contains the functional entities:

- Access Transport Gateway
- IP Address Manager
- Mobile Attendant

## 5.3 Access Transport Gateway (ATG)

The Access Transport Gateway interfaces the access network transport and the core network transport.

The Access Transport Gateway:

- Receives a QoS request from the UE via the Access Network and propagates QoS request to the Resource Manager in the core network.
- Receives a QoS request from the core network, authorizes the request with the Resource Manager in the core network and forwards the QoS request to the Access Network using mechanisms appropriate to that Access Network. This may include conversion between different QoS mechanisms and policies.
- Admits IP flows to and from the Access Network based on QoS.
- Admits IP flows to and from the Access Network based on emergency service requirements.
- Enforces QoS on IP flows, which may include policing, packet marking, packet forwarding, priority queuing, and packet discarding i.e. serves as the QoS Policy Enforcement point for control and bearer streams between the Access Network and the Core Network.
- Tracks QoS usage on a per flow basis and forwards as needed to the Accounting Server.
- Provides firewall functionality as required.
- Interacts with other Access Transport Gateways to manage tunnels to support real time handover. In addition supports the duplication of user traffic and transfer over the inter AG tunnels.

**Reference Points:**

**B01:** Access Transport Gateway—Access Transport Gateway

**B02:** Access Transport Gateway—Transport Gateway Functional Entities

**B03:** Access Transport Gateway—Access Network

**B04:** Access Transport Gateway—Multimedia Resource Function

**S29:** Session Anchor—Access Transport Gateway

**S32:** Resource Manager—Access Transport Gateway

**S60:** Access Transport Gateway—Accounting Server

## 5.4 Access Network

The underlying structure of Access Network is technology dependent and beyond the scope of this document.

An Access Network:

- Allows terminals to attach or detach.
- Provides micro mobility management functionality.
- Relays signaling traffic between the Access Gateway and Terminals.
- Provides geographic location information for the Geographic Location Manager.
- Manages its own resources (e.g., radio resources, IP QoS).
- Interworks Terminal bearer streams (B08) and the access transport gateway bearer streams (B03). This may be a pass through.
- May use Core Network support for authentication, authorization and accounting.
- May provide interworking functions for interconnection to the CN Functional Entities
- May support legacy terminals.
- Measures the performance of access network specific technology. (For further study.)

**Reference Points:**

**B03:** Access Transport Gateway—Access Network

**B08:** Terminal—Access Network

**S48:** Access Network—AAA Functional Entities

## 5.5 Accounting Server

The Accounting Server keeps track of the services, QoS, and multimedia resources requested and used by individual subscribers.

The Accounting Server:

- Records session details (e.g., requesting party, requested services, actual services used, date and time of requests, duration of usage, QoS used, terminal used).
- Records mobility (e.g., administrative domain location, date and time of attach, date and time of detach).

- Collects session details from various sources (e.g., Communication Session Manager, Resource Manager, Home Mobility Manager, and other Accounting Servers).
- Allows session details to be retrieved for further processing.
- Provides accounting information to downstream OAM&P functions (e.g. Billing Management).
- Records accounting information in real-time. (For further study.)
- Records location sensitive accounting information. (For further study.)

**Reference Points:**

**S15:** Application Functional Entity—Accounting Server

**S49:** Communication Session Manager—Accounting Server

**S50:** Home Mobility Manager—Accounting Server

**S51:** Mobile Attendant—Accounting Server

**S52**: MRC—Accounting Server

**S53:** Resource Manager—Accounting Server

**S54**: Session Anchor—Accounting Server

**S57:** Accounting Server—Accounting Server

**S60:** Access Transport Gateway—Accounting Server

**S61:** Media Gateway Controller—Accounting Server

**S62:** Transport Gateway Functional Entities—Accounting Server

**S48:** Access Network—Accounting Server

**S67:** Accounting Server—Billing Management

## 5.6 Application Functional Entity

An Application Functional Entity is a collective that contains entities that store and execute functions for subscribers. The AFE resides within either the network operator's administrative domain or an external administrative domain such as a service provider or business enterprise. It accesses network capabilities to provide end user services. This collective contains the following functional entities:

- Core Network Applications
- Third Party Applications

## 5.7 Authentication Server

The Authentication Server verifies the identity of a requesting entity.

The Authentication Server:

- Verifies any entity's identity for network access, QoS request, multimedia resource request, or service request.
- Verifies a subscriber's identity as requested by the Mobile Attendant.

- Provides identity credentials for entities (e.g., authentication keys) requesting network verification.
- Maintains security association and performs authentication interaction with peer entities in other Administrative Domains to support inter-administrative domain authentication.
- Verifies a session user’s identity for the Communication Session Manager.
- Verifies the identity of an application user for an Application Functional Entity.
- Interacts with other Authentication Servers in other administrative domains to verify an entity’s identity.
- Updates the identity of the serving administrative domain of the mobile subscriber and Terminal in the Location Server.

**Reference Points:**

**S15:** Application Functional Entity—Authentication Server

**S41:** Service Discovery Server—Authentication Server

**S48:** Access Network—Authentication Server

**S49:** Communication Session Manager—Authentication Server

**S50:** Home Mobility Manager—Authentication Server

**S51:** Mobile Attendant—Authentication Server

**S52**: MRC— Authentication Server

**S53:** Resource Manager—Authentication Server

**S54**: Session Anchor— Authentication Server

**S55:** Authentication Server—Authentication Server

**S58:** Authentication Server— Directory Services Functional Entity

## 5.8 Authorization Server

The Authorization Server verifies that the one or more services, the QoS, or the multimedia resources requested by a subscriber are allowed based on the services subscribed and policies of the service provider. The policies of a service provider may be based on any number of factors including, but not limited to, time-of-day, day-of-year, day-of-week, location of subscriber, type of access, other services already in use, availability of the service, and the credit worthiness of the subscriber. Authorization may be granted for a limited time, QoS usage, administrative domain, or geographic area. To avoid authorization requests for periods of time, the requestor may be instructed to refrain from sending the same authentication request for a specified period.

The Authorization Server:

- Verifies that requested services are allowed.
- Applies user or network specific restrictions on the use of services.
- Provides a descriptor to identify applications or services to be invoked.
- Retrieves and applies policy rules from Policy Repository.
- Retrieves additional information from Directory Services as directed by the policy rules (e.g. Subscriber Profile, location information).

- Makes an authorization decision based upon the policy rules.
- Interacts with other Authorization Servers in other administrative domains to obtain authorization for roaming subscribers.
- Correlates user requested Qos with the authorised usage of resources for an application e.g SIP session. Inclusion of this in the Profile is for further study.

**Reference Points:**

**S15:** Application Functional Entity—Authorization Server

**S41:** Authorization Server— Service Discovery Server

**S48:** Access Network— Authorization Server

**S49:** Communication Session Manager—Authorization Server

**S50:** Home Mobility Manager—Authorization Server

**S51:** Mobile Attendant—Authorization Server

**S52**: MRC— Authorization Server

**S53:** Resource Manager—Authorization Server

**S54**: Session Anchor— Authorization Server

**S56:** Authorization Server—Authorization Server

**S59:** Authorization Server—Directory Services Functional Entity

## 5.9 Billing Management

Billing Management is responsible for collection, storage, and processing of all necessary data for billing network services and applications.

Billing Management:

- Prepares subscriber bills.
- Performs net settlement for usage between service providers, access providers, transit providers, and application providers.
- Collects, stores and processes all necessary data for billing according to service provider pricing and tariffing policies.

**Reference Points:**

**S67:** Accounting Server—Billing Management

## 5.10 Communication Session Manager

The Communication Session Manager (CSM) provides the controls for all sessions for a given subscriber.

The Communication Session Manager:

- Invokes address resolution to support session setup.
- Requests authentication of the Session Proxy.
- Manages the state of voice calls.

- Manages the state of multimedia sessions for a given service user.
- Controls basic voice calls.
- Requests the application of tones and announcements.
- Invokes service logic in an Application Functional Entity as directed by a Service Descriptor (a script or pointer to a particular Application Functional Entity).
- Requests and enforces the authentication of subscriber identity with the Authentication Server.
- Requests and enforces the authorization of service requests with the Authorization Server.
- Requests the Session Anchor to allocate, modify and de-allocate the multimedia resources needed to support a call or session.
- May interact with another Communication Session Manager as a peer.
- May interact with a Media Gateway Controller as a peer for calls or sessions involving a party interconnected by the PSTN.
- May redirect session setup requests to a peer Communication Session Manager of a called party..
- Uses Directory Services to determine the specific CSM associated with a called party in the current network using the called party's identification (e.g. a termination).
- Directs session setup requests to the user's CSM (e.g. a termination).
- Provides the Accounting Server with session details (e.g., session participant identifiers, agreed sessions description, encoding method, time of session start, duration).

**Reference Points:**

**S13:** Application Functional Entity— Communication Session Manager

**S18:** Session Proxy—Communication Session Manager

**S19:** Communication Session Manager— Communication Session Manager

**S20:** Communication Session Manager— Session Anchor

**S22:** Media Gateway Controller— Communication Session Manager

**S24:** Communication Session Manager—Resource Directory

**S25:** Communication Session Manager—Global Name Server

**S49:** Communication Session Manager—AAA Functional Entities

## 5.11 Configuration Management

Configuration Management is responsible for managing network resources, and maintaining an accurate record of their existence, usage, and status.

Configuration Management:

- Manages information about provisioned network resources, their configuration and status.
- Provides administration of a subscriber's profile, including authorized features and service levels.
- Provides methods to create, access, and modify subscriber, terminal and service objects in the Subscriber Profile by the service provider and subscriber.
- Provides methods to create, access, modify, and manage policies in the Policy Repository.

**Reference Points:**

**S63:** Configuration Management—Core Network Functional Entities

## 5.12 Core Network Application

The Core Network Application stores and executes functions for subscribers. One of the mandatory CN applications will be an Emergency Services application.

The Core Network Application:

- May be invoked by specific service triggers or event notifications from various network functional entities (e.g., Communication Session Manager, Location Server, or other Core Network Applications).
- May be invoked directly by a Terminal e.g. using HTTP, SIP for the emergency service application.
- Determines a sequence of actions to be performed, QoS requirements, and multimedia services to be used for a particular application request and returns this information to the requestor.
- Provides services independent of network point of attachment and terminal, subject to the limitations of the network point of attachment and terminal.
- May invoke services on other Core Network Applications or Third Party Applications.
- Manages service interactions (e.g., determining service precedence or parallelism).
- May provide application programming interfaces (APIs) to Third Party Applications.
- May request authorization from Authorization Server for specific QoS, multimedia services, or service requests.
- May request application specific policies from the Policy Repository.
- May request serving location or geographic position information from Location Server.
- May request or update subscriber profile information in the Profile Server.
- Registers itself with a Service Discovery Server.
- May manipulate multimedia resources
- May request the Authentication Server to authenticate a Core Network Application.
- Provides credentials for authentication.
- The Emergency service application will provide local call or session control.
- Local call or session control to meet other requirements e.g. for calls to activate service subscriptions, when the home network Communication Session Manager is not accessible, to satisfy regulatory requirements, and to satisfy business relationships are for further study.

**Reference Points:**

**S11:** Terminal—Core Network Application

**S12:** Core Network Application—Multimedia Resource Controller

**S13:** Core Network Application—Communication Session Manager

**S14:** Core Network Application—Application Functional Entity

**S15:** Core Network Application—AAA Functional Entity

**S16:** Core Network Application—Directory Service Functional Entity

**S41:** Core Network Application—Service Discovery Server

## 5.13 Core Network Functional Entities

The Core Network Functional Entities is a collective comprising all of the functional entities in the core network. Each element provides a common functionality to external system (e.g., OAM&P systems), although each is tailored for the specific network functional entity. The core network elements include:

- Accounting Server
- Authentication Server
- Authorization Server
- Communication Session Manager (CSM)
- Core Network Application
- Geographic Location Manager (GLM)
- Global Name Server (GNS)
- Home IP Address Manager
- Home Mobility Manager (HMM)
- IP Gateway
- Location Server
- Media Gateway (MG)
- Media Gateway Controller (MGC)
- Multimedia Resource Controller (MRC)
- Multimedia Resource Function (MRF)
- Policy Repository
- Profile Server
- Resource Directory
- Resource Manager
- Routers
- Service Discovery Server
- Session Anchor
- Session Proxy
- Signaling Gateway

Each Core Network Functional Entity, in addition to its inherent functions:

- Generates statistics of resource usage (for OAM&P).
- Generates failure event history (for OAM&P).

**Reference Points:**

**S63:** Configuration Management—Core Network Functional Entities

**S64:** Fault Management—Core Network Functional Entities

**S65:** Entities Performance Management— Core Network Functional

**S66:** Security Management—Core Network Functional Entities

## 5.14 Core Network (CN) Interworking Entities

A core network interworking entity provides any adaptation required in an access network to enable interworking to the MWIF core network functional entities.

## 5.15 Directory Services

Directory Services is a collective containing the processing and necessary data to external entities to provide the following:

- Global Name Server.
- Location Server.
- Policy Repository.
- Profile Server.
- Resource Directory

## 5.16 Enterprise Network

An enterprise network is a private IP-based network operated by a third party.

**Reference Points:**

**B05:** IP Gateway—Intranet, Internet, and Enterprise Networks

## 5.17 Fault Management

Fault Management is responsible for detection, isolation and recovery of the network from failures.

Fault Management:

- Detects faults and errors in individual network functional entities.
- Collects information about individual faults and errors detected.
- Manages the detected faults and errors to isolate the fault.
- Detects the abatement of the fault and error condition.

**Reference Points:**

**S64:** Fault Management—Core Network Functional Entities

## 5.18 Geographic Location Manager (GLM)

The Geographic Location Manager provides the geographic location of a terminal.

The Geographic Location Manager:

- Accepts terminal geographic location information, as it becomes available.
- Requests up to date terminal geographic location information when necessary.
- Updates the Location Server with terminal geographic location information.

**Reference Points:**

**S38:** Terminal—Geographic Location Manager

**S39:** Geographic Location Manager— Location Server

## 5.19 Global Name Server (GNS)

The Global Name Server provides address mapping services including IP infrastructure functions such as DNS.

The Global Name Server:

- Maps between the following subscriber identifiers for a specific subscriber:
  - Subscriber URL.
  - E.164 telephone number
  - IP address
  - Subscriber Identity (e.g., E.212 number)
- Maps URLs to Application Functional Entities.
- Maps E.164 telephone numbers to IP addresses or to URLs.
- Interacts with other Global Name Servers to resolve identities from other networks.
- May map domain names to IP addresses.

**Reference Points:**

**S16:** Core Network Application—Global Name Server

**S25:** Communication Session Manager—Global Name Server

**S26:** Global Name Server—Global Name Server

**S42:** MGC—Global Name Server

**S58:** Authentication Server—Global Name Server

**S59:** Authorization Server—Global Name Server

## 5.20 Home IP Address Manager

The Home IP Address Manager supports dynamic allocation of IP addresses to terminals e.g. to support VPNs (for further study).

The Home IP Address Manager:

- Manages IP address allocation status.

- Allocates and de-allocates IP addresses.
- Accepts and handles allocation or de-allocation requests from the Home Mobility Manager.

**Reference Points:**

**S36:** Home Mobility Manager—Home IP Address Manager

## 5.21 Home Mobility Manager (HMM)

The Home Mobility Manager supports the movement of a terminal across Administrative Domain boundaries (i.e., inter-AD terminal mobility) as well as across Access Gateway boundaries (i.e., macro terminal mobility). It supports terminal registration in the home network. The Home Mobility Manager acts as a proxy for the terminal by routing traffic bound for a terminal to the current location of the terminal.

The Home Mobility Manager:

- Supports IP level (i.e., network layer) mobility management by providing the Mobile IP Home Agent functionality.
- Updates the currently assigned Subscriber care-of address.
- Interacts with peer Mobile Attendants in the serving network for registration updates.

**Reference Points:**

**S35:** Mobile Attendant—Home Mobility Manager

**S36:** Home Mobility Manager—Home IP Address Manager

**S50:** Home Mobility Manager—AAA Functional Entities

## 5.22 Intranet

An intranet is a private IP-based network operated by a service provider.

**Reference Points:**

**B05:** IP Gateway—Intranet, Internet, and Enterprise Networks

## 5.23 Internet

The Internet is the global public IP-based network.

**Reference Points:**

**B05:** IP Gateway—Intranet, Internet, and Enterprise Networks

## 5.24 IP Gateway

The IP Gateway provides controlled access between the core network and other IP networks, such as the Internet, intranets or enterprise networks.

The IP Gateway:

- Applies QoS policy.
- Provides firewall functionality as required.

- Handles bearer traffic to and from another IP Gateway, an Access Transport Gateway, a Media Gateway or a Multimedia Resource Function.

**Reference Points:**

**B02:** Access Transport Gateway—IP Gateway

**B05:** IP Gateway—Intranet, Internet, or Enterprise

**B09:** IP Gateway—Media Resource Function

**B10:** IP Gateway—Transport Gateway Functional Entity

**S27:** Session Anchor—IP Gateway

**S31:** Resource Manager— IP Gateway

**S62:** IP Gateway—Accounting Server

## 5.25 IP Address Manager

IP Address Manager controls network level address assignment and recovery of addresses within the address space of the network domain.

The IP Address Manager:

- Manages IP address allocation status.
- Allocates and de-allocates IP addresses.
- Accepts and handles allocation or de-allocation requests from the Terminal.

**Reference Points:**

**S37:** Terminal—IP Address Manager

## 5.26 Location Server

The Location Server stores all dynamic information associated with subscriber/terminal and service mobility. Location information will include both network location and geographic position.

The Location Server:

- Stores the location of individual mobile subscribers.
- Stores the location of individual terminals.
- Maintains knowledge of the terminal's geographic position (e.g., latitude, longitude, and altitude).
- Requests authorization of requestor to satisfy privacy policy and regulatory issues. (For further study.)
- Makes the location of a terminal available to authorized requestors (including Application Functional Entities and Authorization Servers).
- Makes the geographic position (latitude, longitude and altitude) available to authorized requestors (including Application Functional Entities and Authorization Servers).
- Notifies authorized requestors of terminal entry and exit from defined areas or domains either for specific subscribers or for all subscribers.
- Requests and accepts geographic position information from the Geographic Location Manager.

**Reference Points:**

**S16:** Core Network Application—Location Server

**S39:** Geographic Location Manager—Location Server

**S41:** Service Discovery Server— Location Server

**S42:** MGC— Location Server

**S58:** Authentication Server— Location Server

**S59:** Authorization Server— Location Server

## 5.27 MAP (Mobile Application Part) Network

A MAP network is a signaling network using either TIA/EIA-41 or GSM MAP signaling to support mobility functions for circuit-mode wireless service providers.

For further study.

**Reference Points:**

**S45:** Signaling Gateway—MAP Network

## 5.28 Media Gateway (MG)

A Media Gateway interconnects the core network to the PSTN or to circuit terminations.

A Media Gateway:

- Enforces QoS policies for volume, delay, and delay variance.
- Provides firewall functionality as required.
- Interacts with a Media Gateway Controller.
- Handles bearer traffic to and from another Media Gateway, an Access Transport Gateway, an IP Gateway or a Multimedia Resource Function.
- Translates between media formats (e.g., transcoding) as required.

**Reference Points:**

**B02:** Access Transport Gateway—Media Gateway

**B06:** Media Gateway—PSTN

**B09:** Media Gateway—Media Resource Function

**B10:** Media Gateway—Transport Gateway Functional Entities

**S31:** Resource Manager—Media Gateway

**S43:** Media Gateway Controller—Media Gateway

**S62:** Media Gateway—Accounting Server

## 5.29 Media Gateway Controller (MGC)

A Media Gateway Controller controls the bearer paths through a Media Gateway.

A Media Gateway Controller:

- Interacts with the Communication Session Manager as a peer.
- Interacts with the Media Gateways to activate and deactivate firewalls.
- Interacts with another Media Gateway Controller as a peer for a call with two parties each interconnected by the PSTN.
- Controls a Media Gateway.
- Interacts with the Signaling Gateway to send and receive signaling (e.g., ISUP) to control circuit mode calls on the PSTN.
- Converts application level protocol messages (e.g., ISUP messages to and from IP session control messages).
- Interacts with the Signaling Gateway to send and receive PSTN queries (e.g., 800-translation queries, Line Information Database (LIDB) queries, and Local Number Portability queries) to the PSTN.
- Interacts with a Session Anchor for the allocation of media resources functions for the support of IP sessions.

**Reference Points:**

**S21:** Session Anchor—Media Gateway Controller

**S23:** Media Gateway Controller—Media Gateway Controller

**S42:** Media Gateway Controller— Directory Service FEs

**S43:** Media Gateway Controller—Media Gateway

**S44:** Media Gateway Controller—Signaling Gateway

**S61:** Media Gateway Controller—Accounting Server

## 5.30 Mobile Attendant (MA)

The Mobile Attendant is responsible for supporting initial and subsequent Mobile IP registrations from the terminal. The initial registration is carried via AAA to the Home Mobility Manager. Registration updates may go directly to the Home Mobility Manager. The Mobile Attendant assists in handover for inter-Administrative and intra-Administrative core domain and macro terminal mobility. The Mobile Attendant is a component of the Access Gateway.

The Mobile Attendant:

- Supports IP level (i.e., network layer) mobility management by providing the Mobile IP Foreign Attendant functionality.
- Assigns the care-of address for a terminal or validates a terminal's selected care-of address with the Access Network domain.
- Requests subscriber authentication upon receiving registration requests from the terminal and propagates corresponding registration responses.
- May request subscriber authentication upon receiving registration update requests from the terminal and propagates corresponding registration response.
- May maintain subscriber authentication and authorization information in order to forward registration update requests directly to the Home Mobility Manager.
- Initiates handover (handoff) control for the macro terminal mobility and the inter-administrative domain terminal mobility upon receiving a handover (handoff) request.

**Reference Points:**

**S34:** Terminal—Mobile Attendant

**S35:** Mobile Attendant—Home Mobility Manager

**S51:** Mobile Attendant —AAA Functional Entities

## 5.31 Multimedia Resource Controller (MRC)

A Multimedia Resources Controller controls the multimedia resources available in a Multimedia Resource Function.

A Multimedia Resource Controller:

- Manages a Multimedia Resource Function.
- Controls multimedia resources in response to Session Anchor requests.
- Controls multimedia resources in response to Application Functional Entity requests.

**Reference Points:**

**S12:** Application Functional Entity—Multimedia Resource Controller

**S28:** Session Anchor—Multimedia Resource Controller

**S47:** Multimedia Resource Controller—Multimedia Resource Function

**S52:** Multimedia Resource Controller — AAA FEs

## 5.32 Multimedia Resource Function (MRF)

A Multimedia Resource Function provides resources for the manipulation of the bearer path.

A Multimedia Resource Function:

- Interacts with a Multimedia Resource Controller.
- Provides notification of detected DTMF digit(s).

- Generates DTMF tones.
- Generates tones.
- Plays announcements.
- May accept descriptor of tones (e.g., tones in the precise tone plan[1] and cadences as in: apply high tone for 500 ms, apply idle tone for 500 ms, repeat forever) that it can generate.
- May accept URL of tones or announcements that it can download.
- May accept streaming tones or announcements.
- Provides audio conference bridging services, including necessary transcoding.
- Provides other transport-related services (e.g., swap of audio between two call waiting parties).
- Handles bearer traffic to and from itself, an Access Transport Gateway, an IP Gateway or a Media Resource Function.

**Reference Points:**

**B04:** Access Transport Gateway—Media Resource Function

**B09:** Multimedia Resource Function—Transport Gateway Functional Elements

**S47:** Multimedia Resource Controller—Multimedia Resource Function

## 5.33 Operations, Administration, Maintenance, and Provisioning

Operations, Administration, Maintenance, and Provisioning (OAM&P) is a collective containing:

1. Configuration Management
2. Fault Management
3. Performance Management
4. Security Management
5. Billing Management

## 5.34 Performance Management

Performance Management comprises all functions (e.g., monitoring, etc.) necessary to ensure QoS and efficient use of resources in the network.

Performance Management provides means of (For further study.):

- Performance quality assurance to set and assess the network QoS policies,
- Perfomance monitoring for event correlation and filtering, and threshold crossing alerts,
- Performance management control to set, assess, and update the network traffic management policies, and
- Performance analysis to
  - Make recommendations on performance improvement, traffic forecasting for network expansion

[1] The precise tone plan is defined in the LSSGR and in Notes for the InterLATA Network.

- Obtain customer service and traffic summary
- Traffic exception and capacity analysis, and network performance characterization.

**Reference Points:**

**S65:** Core Network Functional Entities—Performance Management

## 5.35 Policy Repository

The Policy Repository provides the policy rules for subscriber policy usage, expected QoS, valid times and routes. The Policy Repository allows for separation of policy rules from policy enforcement (e.g. QoS management, packet counting and packet queuing). The Policy Repository is a policy repository and does not make policy decisions or provide policy enforcement. The Policy Repository also provides policy rules for the applications serving a user.

Some of the information that might be checked by policy rules is:

- Subscriber authentication status,
- Subscriber authorization status,
- Business-to-business service level agreements,
- Time-of-day,
- Day-of-week,
- Day-of-year,
- Dynamic overload controls,
- Current resource utilization,
- Current resource utilization by subscriber's class,
- Amount of resource requested,
- Maximum amount of resource allowed by subscription,
- Security Information, and,
- QoS Information (e.g., bandwidth, nominal throughput, maximum throughput, maximum allowable jitter, maximum allowable packet loss, maximum allowable error rate, maximum allowable retransmission rate, maximum allowable delay).

The Policy Repository:

- Is a repository of policy rules.
- Provides the rules for data and multimedia policy usage.
- Accessed by the Authorization Server, Core Network Application, and Resource Manager.

**Reference Points:**

**S16:** Core Network Application—Policy Repository

**S33:** Resource Manager—Policy Repository

**S58:** Authentication Server—Policy Repository

**S59:** Authorization Server—Policy Repository

## 5.36 Profile Server

The profile server is a repository of subscriber, service, and terminal objects. An object is a container of attributes. Each subscriber has a subscriber object to define the basic service authorizations, one or more terminal objects to define the capabilities of various terminals that the subscriber normally uses and one or more service objects defining the services available to a subscriber. These objects may be stored in distributed locations, but the objects are all accessed by a common data base schema.

- Stores subscriber objects containing subscriber identity, subscriber name, service preferences, terminal-to-service associations and transport authorization (toll, international, etc.). Stores terminal objects containing bearer capabilities (e.g., voice packets, data rates), terminal capabilities (e.g., authentication type, call processing, specific tone generation, alerting options, notification options), teleservice capabilities (e.g., voice for different vocoders or codecs, data, short message services).
- Stores service objects containing the location and service specific attributes (e.g., service authorization, service data (service activations, service registrations, etc.)) for each particular service.
- Stores location objects containing location descriptions, authorizations, allowed terminal objects, and allowed services. (For further study.)
- Stores associations of triggering events and applications to be invoked.
- Accessed by the Authorization Server and Core Network Application.

**Reference Points:**

**S16:** Core Network Application— Profile Server

**S58:** Authentication Server— Profile Server

**S59:** Authorization Server — Profile Server

## 5.37 Public Switched Telephone Network (PSTN)

The PSTN is a circuit switched network controlled by ISUP. This includes the fixed networks and the circuit-switched portion of wireless service provider networks (e.g., Public Land Mobile Networks).

**Reference Points:**

**B06:** Media Gateway—PSTN

**S46:** Signaling Gateway—PSTN

## 5.38 Resource Directory

The Resource Directory contains information on the available resources e.g. Media Gateways, to support communication sessions.

**Reference Points:**

**S24:** Communication Session Manager—Resource Directory

**S42:** Media Gateway Controller—Resource Directory

## 5.39 Resource Manager

The Resource Manager manages the overall quality of service (QoS) provided by the core network.

The Resource Manager:

- Provides QoS admission control in support of both CSM and non-CSM sessions.
- Provides QoS (bandwidth) broker functionality.
- Manages the status of core network managed QoS.
- May access the Policy Repository to retrieve network-wide QoS policies
- Coordinates with other network functional entities that track QoS requests and usage for the purpose of core network resource management (e.g., Authorisation Servers, Accounting Servers).
- Accepts QoS requests from the Access Transport Gateway to provide resources for both CSM and non-CSM sessions.
- Requests user level authorization for the requested resources. (Involvement in this correlation is further study.)
- Interacts with transport resources (Gateways, Routers) to coordinate QoS. The mechanism used is an operator choice.
- Interacts with transport resources (Gateways, Routers) to control firewalls (for further study).

**Reference Points:**

**S30:** Resource Manager—Router

**S31:** Resource Manager—Transport Gateway Functional Entity

**S32:** Resource Manager—Access Transport Gateway

**S33:** Resource Manager— Policy Repository

**S53:** Resource Manager—Accounting Server

## 5.40 Routers

Routers are used to route packets between other network functional entities. Routers are part of the core network, but the bearer paths to the routers are not shown for clarity.

Routers:

- [May Interact with Resource Manager depending on the QoS mechanisms used (operator choice)]
- Enforce the QoS allocations given by the Resource Manager.

**Reference Points:**

**B07:** Router—Router

**S30:** Resource Manager—Router

## 5.41 Security Management

Security Management is responsible for maintaining the network security infrastructure (e.g., passwords, security credentials).

**Reference Points:**

**S66:** Security Management—Core Network Functional Entities

## 5.42 Service Discovery Server

The Service Discovery Server enables discovery of network services.

The Service Discovery Server:

- Provides accessing terminal and applications with information such as the address, attributes and supported interfaces of servers.
- Provides service registration through receipt of service address information, server attributes, supported interfaces, etc., from servers (e.g., Session Proxy, Session Anchor, Authentication Server, Authorization Server, and Application Functional Entities).
- Application Functional Entities

**Reference Points:**

**S40:** Terminal— Service Discovery Server

**S41:** Service Discovery Server—Core Network Functional Entities

## 5.43 Session Anchor

The Session Anchor serves as a system agent for allocation of media resources relative to a given session.

The Session Anchor:

- Requests authentication of the requestor (e.g., the Communication Session Manager).
- Validates trust relationships including mutual authentication.
- The session anchor may provide a level of indirection or hiding for a set of MGCs in which case the Session Anchor is responsible for selection of Media Gateway Controller (MGC).
- Accepts requests to control core multimedia resources (e.g., announcement servers, tone collectors) and forwards those requests to Multimedia Resource Controller.
- Interacts with the Access and IP Gateways to activate and deactivate firewalls (for further study).
- De-allocates MRF resources

Deactivates firewalls when mobile loses authorization.

**Reference Points:**

**S20:** Communication Session Manager—Session Anchor

**S21:** Session Anchor—Media Gateway Controller

**S27:** Session Anchor—IP Gateway

**S28:** Session Anchor—Multimedia Resource Controller

**S29:** Session Anchor—Access Transport Gateway

**S41:** Session Anchor—Service Discovery Server

**S54:** Session Anchor—AAA FEs

## 5.44 Session Proxy

Session Proxy serves as a proxy for all CSM requests to and from the terminal in the anchor system (i.e., the system serving the subscriber when the session was initiated) and forwards those service requests to a Communication Session Manager in the subscriber's home network. Session Proxy plays no role in initial terminal registrations. Session Proxy's role in application level registrations (e.g. SIP) is for further study. The Session Proxy may be stateful.

The Session Proxy:

- Determines the address (IP or URL) associated with the Communication Session Manager for a subscriber. (For further study.)
- Requests authentication of the Communication Session Manager.
- Accepts CSM session requests from a Terminal and forwards them to the Communication Session Manager.
- Generates anchor system session accounting records. (For further study)

**Reference Points:**

**S17:** Terminal—Session Proxy

**S18:** Session Proxy—Communication Session Manager

**S41:** Session Proxy—Service Discovery Server

## 5.45 Signaling Gateway

A Signaling Gateway interconnects the core network to a legacy signaling (e.g., SS7, out-band) networks.

A Signaling Gateway:

- Applies throughput control and firewall policies.
- Interworks transport protocols as required (e.g., core network IP-based signaling transport to external signaling networks).
- Provides firewall functionality as required.
- Interworks MAP signaling protocols (as a Roaming Gateway). (For further study.)

**Reference Points:**

**S44:** Media Gateway Controller—Signaling Gateway

**S45:** Signaling Gateway—MAP Network

**S46:** Signaling Gateway—PSTN

## 5.46 Terminal

A Terminal is a device that allows a subscriber or user to access the network to use communication services.

A Terminal:

- Terminates bearer streams.
- Provides conversion of bearer streams to make them useful to the user (e.g., display text messages, provide audio, provide video or multimedia displays, provide data interfaces to other end user devices).
- Controls sessions.

**Reference Points:**

**B08:** Terminal—Access Network

**S11:** Terminal—Application FEs

**S17:** Session Proxy—Terminal

**S34:** Terminal—Mobile Attendant

**S37:** Terminal—IP Address Manager

**S38:** Terminal—Geographic Location Manager

**S40:** Terminal— Service Discovery Server

**S68:** Terminal—User Identity Module

## 5.47 Third Party Application

The Third Party Application is outside the MWIF Core and is provided by an external application provider. The Third Party Application stores and executes functions for subscribers. Access by a Third Party Application to resources in the transport and control layer shall be subject to authentication of the Core Network Application and authorization that the access is allowed.

A Third Party Application:

- May provide credentials for authentication.
- May be invoked by specific service triggers or event notifications from various network functional entities (e.g., Communication Session Manager, Location Server, Core Network Applications, or other Third party applications).
- May be invoked directly by a Terminal.
- Determines a sequence of actions to be performed, QoS requirements and multimedia services to be used for a particular application request and returns this information to the requestor.
- May invoke other Third Party Applications.
- Provides services independent of network point of attachment and terminal, subject to the limitations of the network point of attachment and terminal.
- Manages service interactions (e.g., determining service precedence or parallelism).
- May provide application programming interfaces (APIs) to other Third Party Applications.

- May request authorization from Authorization Server for specific QoS, multimedia services, or service requests. (For further study.)
- May request authorization from the Authorization Server for the capability to access (i.e., either read status of or exert control over) resources in the control or transport layers.
- May request authentication from the Authentication Server.
- May request policies from Policy Repository. (For further study.)
- May request serving location or geographic position information from Location Server.
- May request or update subscriber profile information in the Profile Server. (For further study.)
- Registers itself with a Service Discovery Server. (For further study.)
- May manipulate multimedia resources. (For further study.)

**Reference Points:**

**S11:** Terminal—Third Party Application

**S12:** Third Party Application—Multimedia Resource Controller

**S13:** Third Party Application—Communication Session Manager

**S14:** Third Party Application—Third Party Application

**S15:** Third Party Application—AAA Functional Entity

**S16:** Third Party Application—Directory Service Functional Entity

**S41:** Third Party Application—Service Discovery Server

## 5.48 Transport Gateway Functional Entities

This is a collective of the functional entities that provide IP bearer transport and interconnectivity with external bearer networks. These are:

- Access Transport Gateways
- IP Gateways.
- Media Gateways

## 5.49 User Identity Module (UIM)

A User Identity Module contains information to identify the subscriber and to verify the subscriber's identity. It may contain personal information, such as speed calling lists, for the subscriber. The UIM may or may not be removable at the option of the terminal design.

**Reference Points:**

**S68:** Terminal—User Identity Module

# 6 Reference Points

A reference point exists between two network functional entities that exchange information. Each reference point is described as:

- A short description.
- A list of abstract messages with a set of abstract parameters enclosed in parenthesis "( )" and optional abstract parameters enclosed in braces "[ ]". The abstract messages and parameter are meant to convey requirements for information transfer and not necessarily specify a protocol. Messages may have a directional symbol "→" or ←" before the message name to indicate the direction of the message. This is the only direction for uni-directional interfaces and the direction of request and response in bi-directional reference points where either end can initiate a request.
- Note: The messages in Section 6 are subject to further study.
- A list of proposed protocols stacks. One or more protocol stacks are proposed which may be used to carry the messaging for a particular reference point as a set of protocols separated by slashes "/" (e.g., "TCP/IP/any" means TCP is carried by IP over any media).
- Note: The proposed protocol stacks in Section 6 are subject to further study.

## 6.1 B01 Access Transport Gateway—Access Transport Gateway

This reference point carries signaling and bearer information between Access Transport Gateways to provide the management of tunnels and the transport of user data to support real time handover.

**Messages:**

Qos and firewall control (For further study).

**Proposed protocol stacks:**

any/IP/any

## 6.2 B02 Access Transport Gateway - Transport Gateway FE

This is a generic core bearer path reference point providing specific reference points between an Access Transport Gateway and an IP Transport Gateway Functional Elements (IP Gateway or Media Gateway). Interfaces are supported between:

- An Access Transport Gateway and an IP Gateway. The Access Transport Gateway has edge router functions and the IP gateway has border gateway router functions. Both of them are routers in the Core IP Network. Therefore, the interfaces between these two types of routers are the same as in large-scale service provider IP network.
- An Access Transport Gateway (ATG) and a Media Gateway (MG). This is a transport interface for handling the bearer channels established by signaling between the Communication Session Manager and the Media Gateway Controller. It is assumed that the ATG and the MG communicate over the core IP network. This interface includes the methods for framing real-time multimedia stream samples for transmission over UDP. Such application-level framing should provide the necessary information on the type of media being transmitted, provides information to detect lost packets, provides information to order media samples at the destination, and provides information to compensate network-generated jitter when playing out streams to play out streams at the destination.

**Messages:**

Not applicable.

**Proposed protocol stacks:**

any/IP/any

## 6.3 B03 Access Transport Gateway—Access Network

This reference point carries signaling and bearer information between an Access Transport Gateway and the Access Network.

**Messages:**

Issue for WG4

**Proposed protocol stacks:**

Issue for WG4

## 6.4 B04 Multimedia Resource Function—Access Transport Gateway

This reference point supports bearer paths between a Media Resource Function and the Access Transport Gateway.

**Messages:**

Not applicable.

**Proposed protocol stacks:**

any/IP/any

## 6.5 B05 IP Gateway—Intranet, Internet, and Enterprise Networks

The Core Network operates as a private IP network (Intranet) and it interfaces with other service provider's intranets and possibly with the public Internet. Therefore it has functions of border router and also of security firewall.

**Messages:**

Not applicable.

**Proposed protocol stacks:**

any/IP/any.

## 6.6 B06 Media Gateway—PSTN

This reference point includes the traditional time-division multiplexed trunks used in the Public Switched Telephone Network (PSTN).

**Messages:**

Not applicable.

**Proposed protocol stacks:**

Voice bearer: G.711/DS0.

Data bearer: any/IP/DS0.

## 6.7 B07 Router—Router

This reference point supports inter-router protocols. This main intent of this reference point in MWIF is to identify QoS support and not to covers all the protocol options over this reference point:

**Messages:**

Not applicable.

**Proposed protocol stacks:**

RSVP/IP/any

MPLS/IP/any

Diffserv/IP/any

Standard routing configuration protocols

## 6.8 B08 Terminal—Access Network

This reference point is dependent upon the technology of the Access Network and is technology specific.

**Messages**:

Dependent upon the technology of the Access Network.

**Proposed protocol stacks:**

Dependent upon the technology of the Access Network.

## 6.9 B09 Media Resource Function— Transport Gateway Functional Entity

This reference point supports bearer paths between a Media Resource Function and the Core Network Transport Gateways.

**Messages:**

Not applicable

**Proposed protocol stacks:**

any/IP/any

## 6.10 B10 Transport Gateway FE—Transport Gateway FE

This is a generic core bearer path reference point providing specific reference points between IP Transport Gateway Functional Elements (IP Gateways and Media Gateways). Interfaces are supported between:

- Two IP Gateways. This is an interface between two border routers in the Core IP Network. The interfaces are router-to-router interfaces as exist in large-scale IP service provider networks.
- An IP Gateway and a Media Gateway. The IP Gateway (Border Router) and the Media Gateway (Edge Router) see each other as routers in the Core IP Network. The interfaces are router-to-router interfaces as exist in large-scale IP service provider networks.
- Two Media Gateways. This is an interface between two edge routers in the Core IP Network. The interfaces are router-to-router interfaces.

**Messages:**

Not applicable.

**Proposed protocol stacks:**

any/IP/any

## 6.11 S11 Terminal—Application Functional Entity

The reference point allows a Terminal to request execution of a function of an Application FE.

**Messages:**

Application specific

**Proposed protocol stacks:**

any/IP/any

## 6.12 S12 Application Functional Entity—Multimedia Resource Controller

This reference point enables an Application Functional Entity to request a Multimedia Resource Controller (MRC) to execute functions and respond with the results.

**Messages:**

→**Request-MRC-Function** (Request ID, Service Name, Input Parameter List)

←**Response-MRC-Function** (Request ID, Output Parameter List)

**Proposed protocol stacks:**

Multiple protocols shall be supported at this reference point:

SIP/TCP/IP/any.

SIP/UDP/IP/any.

RTSP/UDP/IP/any

## 6.13 S13 Application Functional Entity—Communication Session Manager

The reference point allows a Communication Session Manager to request execution of a function of an Application FE. This interface enables a Communication Session Manager to reliably send requests invoking functions in remote servers. In addition Application FEs may request the use of service control functions from a CSM e.g. to support an emergency service application.

**Messages:**

For further study

**Proposed protocol stacks:**

SIP/IP/any

Any RPC mechanism/IP/any

API Sets (ffs)

## 6.14 S14 Application Functional Entity—Application Functional Entity

An Application FE uses this reference point to request functions of another Application FE. This covers:

- Core Network Applications to Core Network Applications
- Core Network Applications to Third Party Applications
- Third Party Applications to Third Party Applications

**Messages:**

Application specific

**Proposed protocol stacks:**

API Sets

any/IP/any

## 6.15 S15 Application Functional Entities—AAA Functional Entities

The reference point allows an Application Functional Entity to:

- Request the Authentication Server to verify the identification of an entity.
- Request the Authorization Server to approve the use of network QoS or a multimedia resource for a given subscriber.
- Report chargeable service usage to an Accounting Server.

**Messages:**

→**Request-Authentication** (Request ID, Subscriber ID, [Terminal ID])

←**Response-Authentication** (Request ID, Authentication Result)

→**Request-Authorization** (Request ID, [Requestor ID,] Subscriber ID, Session Descriptor)

←**Response-Authorization** (Request ID, Authorization Descriptor)

→**Notify-Accounting** ([Session ID,] Source Subscriber ID, Destination Subscriber ID, Authorization Descriptor, Session Descriptor, Billing Descriptor)

This message must be sent at the completion of a session or potentially chargeable resource usage, upon the occurrence of a singular event that is potentially chargeable, or upon the occurrence of a potentially chargeable threshold event (e.g., a long session, packet usage event). The message may be sent at the at the start of a session or use of a chargeable resource or when resource usage changes,

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.16 S16 Application Functional Entity—Directory Service Functional Entity

This reference point allows an Application Functional Entity to request:

- A translation from a Global Name Sever.

- The location of a terminal or subscriber from a Location Server.
- Policy information from a Policy Repository.
- A subscriber's profiles from a Profile Server.

**Messages:**

→**Request-Name-Translation** (Request ID, Translation Description)

←**Name-Translation-Response** (Request ID, Translation Result)

→**Request-Location** (Request ID, Subscriber ID, Location Information)

←**Response-Location** (Request ID, Location Information)

→**Request-Policy** (Request ID, Subscriber ID, Policy)

←**Response-Policy** (Request ID, Policy)

→**Request-Profile** (Request ID, Subscriber ID, Subscriber Profile)

←**Response-Profile** (Request ID, Subscriber Profile)

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

DNS/IP/any (for GNS).

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

SLoP (for location Service)

## 6.17 S17 Terminal—Session Proxy

This reference point carries session control signaling between a Terminal and the Session Proxy.

**Messages:**

**Request-Session-Setup** (Destination-ID, Source-ID, Session-ID, Source Session Descriptor)

This message requests the establishment of a session. This message contains identifiers for the source and destination subscribers and contains a descriptor with information about the session source entity. This information includes session media type, supported encoding methods, IP address, RTP port number, and QoS requirements.

**Response-Session-Setup** (Session ID, Response Type, Destination Session Descriptor)

Response message corresponding to a previous Request-Session-Setup. It contains the reply type which can be one of the following: the call was accepted, the request is being processed, the request was denied, the destination party is busy, the destination is being alerted (ringing), the destination requests to forward the call, and the destination accepted the session. This message also contains a descriptor with information about the session destination entity with the same type of contents as the source descriptor. There can be multiple session set up replies for a given session. For example a first reply indicates the request is being processed, a second reply indicates the destination is being alerted, and finally the last reply contains acceptance of the session pl us the destination's descriptor.

**Confirm-Session-Setup** (Session ID)

Message from the calling party indicating it has received the Request-Session-Setup Message from the called party. Reception of this message by the called party completes a session set up transaction and the called party can start transmitting data to the calling party.

**Request-Session-Modify** (Session ID, Source Session Descriptor)

This command may be sent by either the source or destination party to request a session change. The session change is described in the included Session Descriptor. Such changes include QoS requirements, encoding method, IP address, and RTP port number.

**Response-Session-Modify** (Session ID, Destination Session Descriptor, Reply Type)

This is a reply to a Request-Session-Modify. The Reply Type parameter indicates whether the request was accepted, denied, or is in progress. The returned Destination Session Descriptor contains corresponding session changes at the destination side.

**Confirm-Session-Modify-Confirm** (Session ID

Equivalent to Confirm-Session-Setup, but used in session modification transactions.

**End-Session** (Session ID)

Command sent by any of the parties in a session and indicates the sending party is releasing the session.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.18 S18 Session Proxy—Communication Session Manager

This reference point is for session control between a Communication Session Manager and a Session Proxy. The Session Proxy acts as a signaling relay (proxy) between a terminal and its corresponding Communication Session Manager. (For further study.)

**Messages:**

Similar to S17.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.19 S19 Communication Session Manager—Communication Session Manager

This reference point is for exchanging session controls between two Communication Session Managers with each Communication Session Manager controlling a half-call.

**Messages:**

Similar to S17.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP +SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.20 S20 Communication Session Manager— Session Anchor

This reference point carries home system requests for serving system functions between a Communication Session Manager and a Session Anchor.

**Messages:**

Similar to S17.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.21 S21 Session Anchor—Media Gateway Controller

This reference point carries serving system requests to the Media Gateway Controller.

**Messages:**

Similar to S17.

**Proposed protocol stacks:**

To update the session

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

To indicate MG reachability

TRIP/IP/any

## 6.22 S22 Multimedia Gateway Controller—Communication Session Manager

This reference point carries session requests for serving system functions between a Multimedia Gateway Controller and a Communication Session Manager.

**Messages:**

Similar to S17.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.23 S23 Media Gateway Controller—Media Gate way Controller

This reference point is for exchanging session control between two Media Gateway Controllers each controlling a PSTN connection.

**Messages:**

Similar to S17.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.24 S24 Communication Session Manager to Resource Directory

This reference point enables the CSM to locate resources required to support a session.

**Messages:**

→for further study

**Proposed protocol stacks:**

→ LDAP/TCP/IP/any.

## 6.25 S25 Communication Session Manager—Global Name Server

This reference point allows a Communication Session Manager to request a translation from a Global Name Sever.

**Messages:**

→**Request-Name-Translation** (Request ID, Translation Description)

←**Name-Translation-Response** (Request ID, Translation Result)

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

DNS/TCP/IP/any

## 6.26 S26 Global Name Server—Global Name Server

This reference point allows a Global Name Server to request a translation from another Global Name Sever.

**Messages:**

Similar to S25.

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

DNS/TCP/IP/any

## 6.27 S27 Session Anchor—IP Gateway

This reference point carries the firewall support controls for sessions to the IP Gateway. (For further study.)

**Messages:**

For further study.

**Proposed protocol stacks:**

MIDCOM/IP/any.

For further study.

## 6.28 S28 Session Anchor—Multimedia Resource Controller

This reference point carries serving system requests to the Multimedia Resource Controller.

**Messages:**

Same as S12.

**Proposed protocol stacks:**

SIP+SDP/TCP/IP/any.

SIP+SDP /UDP/IP/any.

SIP+SDP /SCTP/IP/any.

## 6.29 S29 Session Anchor—Access Transport Gateway

This reference point carries the firewall support controls for sessions to the Access Transport Gateway (For further study.).

**Messages:**

Similar to S27.

**Proposed protocol stacks:**

MIDCOM/IP/any.

For further study.

## 6.30 S30 Resource Manager—Router

This interface applies to handling QoS mechanisms that require propagation of state information on the routers in the path of a session's media flow. In RSVP such mechanism can only be accesses via the end (edge) routers. In MPLS it is done through a special "label distribution protocol". In DiffServ control is also performed at the edges by marking packets. Depending on the type of QoS method used the protocol is going to vary and the number and type (edge, vs. core) or routers is a going to vary.

**Messages:**

→**Request-Allocate-QoS-Resources** (Request ID, Session ID, QoS Descriptor)

This message requests the allocation of resources necessary to handle the QoS requirements of a session.

←**Response-Allocate-QoS-Resources** (Request ID, Result)

This message contains the result of a corresponding request. The Result parameter indicates whether the QoS requirements were granted or not and also what resources are used. This information may also be necessary for accounting purposes.

→**Request-Release-QoS-Resources** (Request ID, Session ID)

This message requests the release of the resources corresponding to a specified session.

←**Response-Release-QoS-Resources** (Request ID, Result)

**Proposed protocol stacks:**

COPS/TCP/IP/any

## 6.31 S31 Resource Manager—Transport Gateway Functional Entity

This reference point is used by the IP Transport Functional Entities to request allocation and de-allocation of QoS resources for data sessions.  Possibly firewall control.

**Messages:**

Similar to S30

**Proposed protocol stacks:**

COPS/TCP/IP/any

## 6.32 S32 Resource Manager—Access Transport Gateway

This reference point is used by the Access Transport Gateway to request allocation and de-allocation of QoS resources for data sessions.

**Messages:**

Similar to S30

**Proposed protocol stacks:**

COPS/TCP/IP/any

## 6.33 S33 Resource Manager—Policy Repository

This reference point allows the Resource Manager to retrieve policies from the Policy Repository.

**Messages:**

→**Request-Policy** (Request ID, Subscriber ID, Policy)

←**Response-Policy** (Request ID, Policy)

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

## 6.34 S34 Terminal—Mobile Attendant

A Terminal uses this reference point to request registration of itself with a Mobile Attendant.

**Messages:**

→**Request-Terminal-Registration** (Request ID, [Subscriber ID,] Terminal ID, Terminal Address, Registration Descriptor)

←**Response-Terminal-Registration** (Request ID, Registration Result)

**Proposed protocol stacks:**

MIPv6/IP/any

## 6.35 S35 Mobile Attendant—Home Mobility Manager

The reference point supports proxying, so messages arriving at a Mobile Attendant can be relayed to another Home Mobility Manager. Some of these messages are assumed to be encapsulated in AAA messages.

**Messages:**

→**Request-Terminal-Registration** (Request ID, [Subscriber ID,] Terminal ID, Terminal Address, Registration Descriptor)

←**Response-Terminal-Registration** (Request ID, Registration Result)

**Proposed protocol stacks:**

MIPv6/IP/any

## 6.36 S36 Home Mobility Manager— Home IP Address Manager

This reference point is used by the Home Mobility Manager to support dynamic allocation of IP addresses to terminals e.g. to support VPNs (for further study)

**Messages:**

→**Request-IP-Address** (Request ID, [Subscriber ID], Terminal ID)

←**Response-IP-Address** (Request ID, IP Address)

**Proposed protocol stacks:**

DHCP/IP/any

DHCP options and extensions for further study

## 6.37 S37 Terminal—IP Address Manager

The Terminal uses this reference point to request the assignment of an IP address.

**Messages:**

→**Request-IP-Address** (Request ID, [Subscriber ID], Terminal ID)

←**Response-IP-Address** (Request ID, IP Address, Session Proxy Address, SDS Address)

**Proposed protocol stacks:**

DHCP/IP/any

DHCP options and extensions for further study

## 6.38 S38 Terminal—Geographic Location Manager

This interface is used by a Geographic Location Manager to request geographic location information from an Access Network or from a terminal and by an Access Network or Terminal to send geographic information to a Geographic Location Manager.

**Messages:**

→**Request-Geographic-Location** (Request ID, Terminal ID)

Message requests geographic location information for a specified terminal.

←**Response-Geographic-Location** (Request ID, Geographic Location)

Message carries requested geographic location information.

→**Request-Geographic-Location-Notification** (Terminal ID, Notification Rules)

Message requests notifications of geographic location for a specified terminal.

←**Notification-Geographic-Location** (Terminal ID, Geographic Location)

Notification message contains updated information on a specified terminal.

**Proposed protocol stacks:**

Various IETF protocols supporting request-response transactions as well as notifications

LDAP/TCP/IP/any.

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any

SLoP

## 6.39 S39 Geographic Location Manager— Location Server

This reference point is used by a Geographic Location Manager to update the terminal geographic information data stored in a Location Server.

**Messages:**

→**UpdateLocation** (Request ID, Subscriber ID, Location Information)

←**Response-Update Location** (Request ID)

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any

SLoP

## 6.40 S40 Terminal—Service Discovery Server

A Terminal uses this reference point to request service address information from a Service Discovery Server.

**Messages:**

→**Request-Service-Location** (Request ID, Service Descriptor)

←**Response-Service-Location** (Request ID, Service Address)

**Proposed protocol stacks:**

SLP/IP/any

DHCP/IP/any

DNS/IP/any

## 6.41 S41 Core Network FE— Service Discovery Server

This reference point allows a Core Network Functional Entity to register itself with a Service Discovery Server and to request service address information from a Service Discovery Server. In particular the following Core Network Functional Entities are expected to require registration to a discovery service:

- Session Proxy
- Session Anchor
- Authentication Server
- Authorisation Server
- Core Network Application
- Location Server

**Messages:**

→**Request-Service-Registration** ()

→**Response-Service-Registration** ()

→**Request-Service-Location** (Request ID, Service Descriptor)

←**Response-Service-Location** (Request ID, Service Address)

**Proposed protocol stacks:**

SLP/any

DHCP/any

DNS/IP/any

## 6.42 S42 Media Gateway Controller to Directory Service FEs

This reference point enables the Media Gateway Controller to access information contained within the Directory Services to support functions such as incoming call routing and registration of multimedia resources.

**Messages:**

ffs

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

TRIP/SCTP/IP/any.

TRIP/TCP/IP/any.

## 6.43 S43 Media Gateway Controller—Media Gateway

This reference point is used by the Media Gateway Controller to control the operation of an associated Media Gateway (MG).

**Messages:**

→**Establish-Connection** (Local Port Descriptor, Remote Port Descriptor)

This message requests a connection be set up between an RTP port in Media Gateway and a remote RTP port (in another Media Gateway or IP device). A connection is an association between ports in two separate Media Gateways.

→**Modify-Connection** (Connection ID, Local Port Descriptor, Remote Port Descriptor)

This message requests the modification of an existing connection. This command is used to update the Remote Port Descriptor information with the IP address, RTP port number, and codec information for the remote port. This information is usually unavailable when an originating Media Gateway creates a new connection. Such parameters are obtai ned later when the MGC receives information about the terminating side port.

→**End-Connection** (Connection ID)

This message requests the specified connection be ended.

→**Establish-Binding** (Local Port Descriptor, Local Port Descriptor)

This message requests the binding between two or more Media Gateway ports. A binding is an association between ports in the same Media Gateway. For a common point-to-point, IP to PSTN call it binds an RTP port on the IP side of the Media Gateway with a TDM port on the PSTN side o f the Media Gateway. A binding with multiple ports performs multi-point bridging functions.

→**Add-Port** (Binding ID, Local Port Descriptor)

This message requests a port added to a specified binding. This is required for handling of multi-point calls.

→**Remove-Port** (Binding ID, Local Port Descriptor)

This message requests a port be removed from specified binding.

→**Move-Port** (From Binding ID, Destination Binding ID, Local Port Descriptor)

This message requests a port be moved to another binding (Destination Binding ID). This function is used to support services such as call waiting, where each call has its own binding.

→**Notification-Request** (Request ID, Local Port Descriptor, Event List)

This message requests notification when the Media Gateway observes the occurrence of events specified in Event List at the specified port. In trunking gateways it is used to detect reception of in-band tones such as used in fax communication or DTMF tones used for certain services. For user line gateways it is used to detect user interface events such as on-hook, flash-hook, and hang-up.

←**Notification** (Request ID, Observed Events)

This message contains the notification of observed events on a port and corresponding to a previous notification request identified by Request ID.

**Proposed protocol stacks:**

MEGACO/UDP/IP/any.

MEGACO/TCP/IP/any.

## 6.44 S44 Media Gateway Controller—Signaling Gateway

This reference point handles the transport of PSTN signaling protocols over IP networks. The PSTN protocols that must be supported are the application and user parts of SS7, including ISUP and TCAP. This interface is a transport protocol over IP with equal or above performance and security characteristics as existing PSTN signaling transport protocols.

**Messages:**

For further study.

**Proposed protocol stacks:**

These are transport stacks to carry ISUP and/or TCAP

SUA/SCTP/IP/any.

M3UA/ SCTP/IP/any

## 6.45 S45 Signaling Gateway—MAP Network

This reference point carries Mobile Application Part (MAP) signaling to support interconnection to legacy (IS-41 and GSM) mobile networks. The network entity that is capable of composing and reacting to MAP signaling is for further study.

**Messages**:

For further study.

**Proposed protocol stacks:**

These are transport stacks to carry ANSI-41/ANSI-TCAP, GSM-MAP/ANSI-TCAP or GSM-MAP/ITU-TCAP

SCCP/MTP3/MTP2/DS0.

## 6.46 S46 Signaling Gateway—PSTN

This reference point carries PSTN ISUP and TCAP signaling from the PSTN to the Signaling gateway.

**Messages:**

For further study.

**Proposed protocol stacks:**

These are transport stacks to carry ISUP and/or TCAP

SCCP/MTP3/MTP2/DS0.

## 6.47 S47 Multimedia Resource Controller—Multimedia Resource Function

This reference point allows a Multimedia Resource Controller (MRC) to control a Multimedia Resource Function.

**Messages:**

Similar to S43.

**Proposed protocol stacks:**

MEGACO/UDP/IP/any.

MEGACO/TCP/IP/any.

RTSP/UDP/IP/any.

## 6.48 S48 Access Network to AAA Functional Entity

This reference point enables an access network the use of AAA functionality within the Core Network.

**Messages:**

→**Request-Authentication** (Request ID, Subscriber ID, [Terminal ID])

←**Response-Authentication** (Request ID, Authentication Result)

→**Request-Authorization** (Request ID, [Requestor ID,] Subscriber ID)

←**Response-Authorization** (Request ID, Authorization Descriptor)

→**Notify-Accounting** (Source Subscriber ID, , Authorization Descriptor, Billing Descriptor)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.49 S49 Communication Session Manager—AAA Functional Entity

The reference point allows a Communication Session Manager to:

- Request the Authentication Server to verify the identification of an entity.
- Request the Authorization Server to approve the use of network QoS or a multimedia resource for a given subscriber.
- Report chargeable events and usage to an Accounting Server.

**Messages:**

Similar to S48.

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.50 S50 Home Mobility Manager—AAA Functional Entities

The reference point allows a Home Mobility Manager to:

- Request the Authentication Server to verify the identification of an entity.
- Request the Authorization Server to approve the use of a visited core network.
- Report chargeable mobility events to an Accounting Server.

**Messages:**

Similar to S48

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.51 S51 Mobile Attendant— AAA Functional Entities

The reference point allows a Mobile Attendant to access the functions provide by the AAA Functional Elements.

In particular it enables the MA to:

- Request the Authentication Server to verify the identification of an entity.
- Request the Authorization Server to approve the use of a visited core network.
- Report chargeable mobility events to an Accounting Server (for further study).

**Messages:**

→**Request-Authentication** (Request ID, Subscriber ID, [Terminal ID], Registration Request)

←**Response-Authentication** (Request ID, Authentication Result, Registration Response)

→**Request-Authorization** (Request ID, [Requestor ID,] Subscriber ID)

←**Response-Authorization** (Request ID, Authorization Descriptor)

→**Notify-Accounting** (Source Subscriber ID, , Authorization Descriptor, Billing Descriptor)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.52 S52 Media Resource Controller to AAA Functional Entity

This reference point enables the Media Resource Controller the use of AAA functionality.

**Messages:**

→**Request-Authentication** (Request ID, Subscriber ID, [Terminal ID])

←**Response-Authentication** (Request ID, Authentication Result)

→**Request-Authorization** (Request ID, [Requestor ID,] Subscriber ID)

←**Response-Authorization** (Request ID, Authorization Descriptor)

→**Notify-Accounting** (Source Subscriber ID, , Authorization Descriptor, Billing Descriptor)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.53 S53 Resource Manager—AAA Functional Entities

The reference point allows a Resource Manage to:

- Request the Authentication Server to verify the identification of a subscriber, a terminal, or both. Such request is necessary when an Access Transport Gateway has asked the Resource Manager to allocate QoS resources for a data session.
- Request the Authorization Server to approve the use of network QoS for a given subscriber.
- Report chargeable events and usage to an Accounting Server.

**Messages:**

Similar to S48

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.54 S54 Session Anchor to AAA Functional Entity

This reference point enables the Session Anchor the use of AAA functionality to authenticate a requester for resources in a network and to authorize the use of those resources.

**Messages:**

→**Request-Authentication** (Request ID, Subscriber ID, [Terminal ID])

←**Response-Authentication** (Request ID, Authentication Result)

→**Request-Authorization** (Request ID, [Requestor ID,] Subscriber ID)

←**Response-Authorization** (Request ID, Authorization Descriptor)

→**Notify-Accounting** (Source Subscriber ID, , Authorization Descriptor, Billing Descriptor)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.55 S55 Authentication Server—Authentication Server

The reference point allows an Authentication Server to request another Authentication Server to verify the i dentification of an entity.

**Messages:**

→**Request-Authentication** (Request ID, Subscriber ID, [Terminal ID], [MobileIP message])

←**Response-Authentication** (Request ID, Authentication Result)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

Extension to diameter for the format of authentication is ffs

## 6.56 S56 Authorization Server—Authorization Server

The reference point allows an Authorization Server to request another Authorization Server to approve the use of network QoS or a multimedia resource for a given subscriber.

**Messages:**

→**Request-Authorization** (Request ID, [Requestor ID,] Subscriber ID, Session Descriptor)

←**Response-Authorization** (Request ID, Authorization Descriptor)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

The format of the session descriptor needs to be defined (SDP?)

## 6.57 S57 Accounting Server—Accounting Server

The interface supports proxying, so messages arriving at an Accounting Server can be relayed to another Accounting Server.

**Messages:**

→**Notify-Accounting** ([Session ID,] Source Subscriber ID, Destination Subscriber ID, Authorization Descriptor, Session Descriptor, Accounting Record)

This message must be sent at the completion of a session or potentially chargeable resource usage, upon the occurrence of a singular event that is potentially chargeable, or upon the occurrence of a potentially chargeable threshold event (e.g., a long session, packet usage event). The message may be sent at the at the start of a session or use of a chargeable resource or when resource usage changes,

←**Set-Accounting Event** (Event Description)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any

Diameter/TCP/IP/any

Format of accounting records for further study

## 6.58 S58 Authentication Server— Directory Service Functional Entity

This reference point allows an Authentication Server to request:

- A translation from a Global Name Server.
- The location of a terminal or subscriber from a Location Server.
- Policy information from a Policy Repository.
- A subscriber's profiles from a Profile Server.

**Messages:**

→**Request-Name-Translation** (Request ID, Translation Description)

←**Name-Translation-Response** (Request ID, Translation Result)

→**Request-Location** (Request ID, Subscriber ID, Location Information)

←**Response-Location** (Request ID, Location Information)

→**Request-Policy** (Request ID, Subscriber ID, Policy)

←**Response-Policy** (Request ID, Policy)

→**Request-Profile** (Request ID, Subscriber ID)

←**Response-Profile** (Request ID, Subscriber Profile)

→**Update-Profile** (Request ID, Subscriber ID, Subscriber Profile)

←**Update-Profile Ack** (Request ID, Subscriber Profile)

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

DNS/IP/any (for GNS).

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

SLoP (for location Service)

## 6.59 S59 Authorization Server— Directory Service Functional Entity

This reference point allows an Authorization Server to request:

- A translation from a Global Name Server.
- The location of a terminal or subscriber from an Location Server.
- Policy information from a Policy Repository.
- A subscriber's profiles from a Profile Server.

**Messages:**

Similar to S58

**Proposed protocol stacks:**

LDAP/TCP/IP/any.

DNS/IP/any (for GNS).

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

SLoP (for location Service)

## 6.60 S60 Access Transport Gateway—Accounting Server:

The reference point allows an Access Transport Gateway to report chargeable usage to an Accounting Server.

**Messages:**

→**Notify-Accounting** ([Session ID,] Source Subscriber ID, Destination Subscriber ID, Authorization Descriptor, Session Descriptor, Accounting Record)

This message must be sent at the completion of a session or potentially chargeable resource usage, upon the occurrence of a singular event that is potentially chargeable, or upon the occurrence of a potentially chargeable threshold event (e.g., a long session, packet usage event). The message may be sent at the at the start of a session or use of a chargeable resource or when resource usage changes,

←**Set-Accounting Event** (Event Description)

**Proposed protocol stacks:**

Diameter/SCTP/IP/any

Diameter/TCP/IP/any

Format of accounting records for further study

## 6.61 S61 Media Gateway Controller—Accounting Server

The reference point allows a Media Gateway Controller to report chargeable session events and usage to an Accounting Server.

**Messages:**

Similar to S60.

**Proposed protocol stacks:**

Diameter/SCTP/IP/any

Diameter/TCP/IP/any

Format of accounting records for further study

## 6.62 S62 Transport Functional Entity—Accounting Server

The reference point allows IP Transport Gateways (an IP Gateway or Media Gateway) to report chargeable usage to an Accounting Server.

**Messages:**

For further study.

→**Notify-Accounting** ([Session ID,] Source Subscriber ID, Destination Subscriber ID, Authorization Descriptor, Session Descriptor, Billing Descriptor)

This message must be sent at the completion of a session or potentially chargeable resource usage, upon the occurrence of a singular event that is potentially chargeable, or upon the occurrence of a potentially chargeable threshold event (e.g., a long session, packet usage event). The message may be sent at the at the start of a session or use of a chargeable resource or when resource usage changes,

**Proposed protocol stacks:**

Diameter/SCTP/IP/any.

Diameter/TCP/IP/any.

## 6.63 S63 Configuration Management—Core Network Functional Entities

This reference point allows Configuration Management to maintain the configuration database of each core network functional entity.

**Messages:**

For further study.

**Proposed protocol stacks:**

SNMPv3

## 6.64 S64 Fault Management—Core Network Functional Entities

This reference point allows each core network functional entity to report faults.

**Messages:**

For further study.

**Proposed protocol stacks:**

SNMPv3

## 6.65 S65 Performance Management—Core Network Functional Entities

This reference point allows core network functional entities to report performance data to Performance management.

**Messages:**

For further study.

**Proposed protocol stacks:**

SNMPv3/IP/any

RMON/IP/any

## 6.66 S66 Security Management—Core Network Functional Entities

This reference point allows Security Management to control the security functions of each core network element.

**Messages:**

For further study.

**Proposed protocol stacks:**

For further study.

## 6.67 S67 Accounting Server—Billing Management

The reference point allows an Accounting server to report chargeable events and usage to Billing Management. This is likely to be driven by operator specific implementations.

**Messages:**

For further study

**Proposed protocol stacks:**

SNMPv3 - a possible option.

## 6.68 S68 Terminal—User Identity Module

This reference point allows a terminal to use an User Identity Module.

**Messages:**

Outside the scope of the NRA

**Proposed protocol stacks:**

Outside the scope of the NRA

# 7. DATA DICTIONARY

This section provides a definition of the abstract parameters used in this document.

- **Authentication Result:** a set parameters that comprise the result of an authentication request.
- **Authorization Descriptor:** a set of parameters that comprise the result of the operations performed by the Authorization Server. These include indication of whether the request was approved or not, list of attributes approved (such as QoS), and, possibly, a descriptor indicating how to handle authorized services.
- **Billing Descriptor:** a set of parameter that describe billing considerations (e.g., prepaid charging, calling party pays, called party pays, collect, third party billing) for the current reported event.
- **Binding ID:** identifier for a binding within a Media Gateway.
- **Connection ID:** identifier for a connection within a Media Gateway. A connection is an association between two ports in two separate Media Gateways. A Connection ID has scope only within one Media Gateway. Each Media Gateway at the ends of a connection assigns their own Connection ID to a given connection.
- **Destination ID:** the identifier for the party with which the source party wants to establish a communications session.
- **Destination Binding ID:** a destination in a move port operation.
- **Destination Subscriber ID:** Identifier for the party with which the source party wishes to establish a communications session.
- **Event List:** a list of events that a Media Gateway is to monitor.
- **From Binding ID:** a source binding in a Move-Port operation.
- **Geographic Location:** latitude, longitude, altitude, and resolution.
- **Input Parameter List:** contains the parameters required by the remote function.
- **IP Address:** an address of a network functional entity in an IP-based network.
- **Local Port Descriptor:** the characteristics of the local port in a Media Gateway or similar device.
- **Location Information:** This parameter indicates the subscriber location including, but not limited to, geographic location, administrative domain, subnet address, etc.
- **Location Result:** information about the location of a subscriber or terminal.
- **Observed Events:** a list of the events observed in a Media Gateway.
- **Output Parameter List:** contains the parameters returned by the remote function.
- **Policy**: a set of instructions defining what to do in a particular situation for a given subscriber.
- **Port Descriptor**: a set of parameters that contains all the information about a port including: name, port type, IP address, RTP port number, media type, encoding type, QoS requirements, other. A Port Descriptor both identifies a port and contains its characteristics. Ports are sources or sinks of data. Ports may be of various types including IP/RTP, TDM trunks, analogue lines, etc.
- **QoS Description:** the characteristics of a QoS request (e.g., maximum bandwidth, nominal throughput, maximum throughput, maximum allowable delay, and maximum allowable jitter, maximum allowable packet loss, maximum allowable error rate, maximum allowable retransmission rate).

- **QoS Result:** the QoS characteristics allowe d. See QoS Description.
- **Registration Descriptor:** a set of parameters that describe a particular registration including a type (e.g., initial, power-on, power-off, periodic, change of administrative domain, change of location area (technology dependent)), bcation (e.g., administrative domain, service provider identification).
- **Registration Result:** The results (success or failure) of a registration attempt.
- **Remote Port Descriptor:** the characteristics of a remote port in a Media Gateway or similar device.
- **Request ID:** an identifier used to bind request and response messages in one transaction.
- **Requestor ID:** a set of parameters that identify (and perhaps authenticate) a requestor.
- **Response Type:** a parameter indicates the type of reply message sent in response to either a Session-Setup-Request or Session-Modify-Request. Possible types of reply are: the call was accepted, the request is being processed, the request was denied, the destination party is busy, the destination is being alerted (ringing), the destination request to forward the call, and the destination accepted the session
- **Service Address:** the IP address of a requested service.
- **Service Name:** the name of the function to be invoked in the Core Network Application.
- **Session Descriptor:** a set of parameters describing the characteristics of a session on a specific endpoint of such session (e.g., date, time, destination party identifier, media type, and QoS requirements). A point-to-point call has a descriptor for the source or originating side of the session and descriptor for the destination side of the session.
- **Session ID:** a globally unique identifier used to correlate events corresponding to the same session (e.g., by an accounting server and its client servers to correlate accounting events for a given sessio n).
- **Source ID:** the identifier of the party that attempts to establish a communication session.
- **Source Session Descriptor:** the characteristics of a session as required by the source of the session.
- **Source Subscriber ID:** an identifier for the party that issues a Session-Setup-Request.
- **Subscriber ID:** a set of parameters that uniquely identify a particular subscriber.
- **Subscriber Profile:** a set parameters that describes the unique identity, services, and rights of a subscriber. It may also include the subscriber's Terminal ID(s).
- **Terminal Address:** the IP address of a terminal.
- **Terminal ID:** a set of parameters that uniquely identify a terminal.
- **Translation Description:** a set of parameters that indicate the type and inputs for translation.
- **Translation Result:** a set of parameters that indicate the result of a translation.

## Document History

| Date | Version | Comment |
|---|---|---|
| June 27, 2000 | Draft 1 | Initial draft format |
| June 30, 2000 | Draft 2 | Second draft based on San Diego lockdown session |
| July 20, 2000 | Draft 3 | Roll in of more details |
| July 21, 2000 | Draft 4 | Polishing |
| July 31, 2000 | Draft 5 | Include changes agreed to in Toronto Architecture meeting and more polishing |
| August 9,2000 | Draft 0.6 | Incorporate Architecture Working Group comments. |
| September 22,2000 | Draft 0.7 | Incorporate Technical Committee comments, ballot version |
| October 20, 2000 | Draft 1.1 | Incorporate agreements from MWIF TC#7 Berlin to create version 2 |
| November 12, 2000 | Draft 1.2 | Incorporated comments from audio conference |
| December 15, 2000 | Draft 1.3 | Incorporate agreements from MWIF Architecture Lockdown New Orleans |
| January 29 2001 | Draft 1.4 | Incorporate agreements from MWIF TC#8 Sydney |
| February 12 2001 | Draft 1.5 | Incorporated comments from audio conference 7/2/01 |

# 8. Annex A: Message Sequence Charts

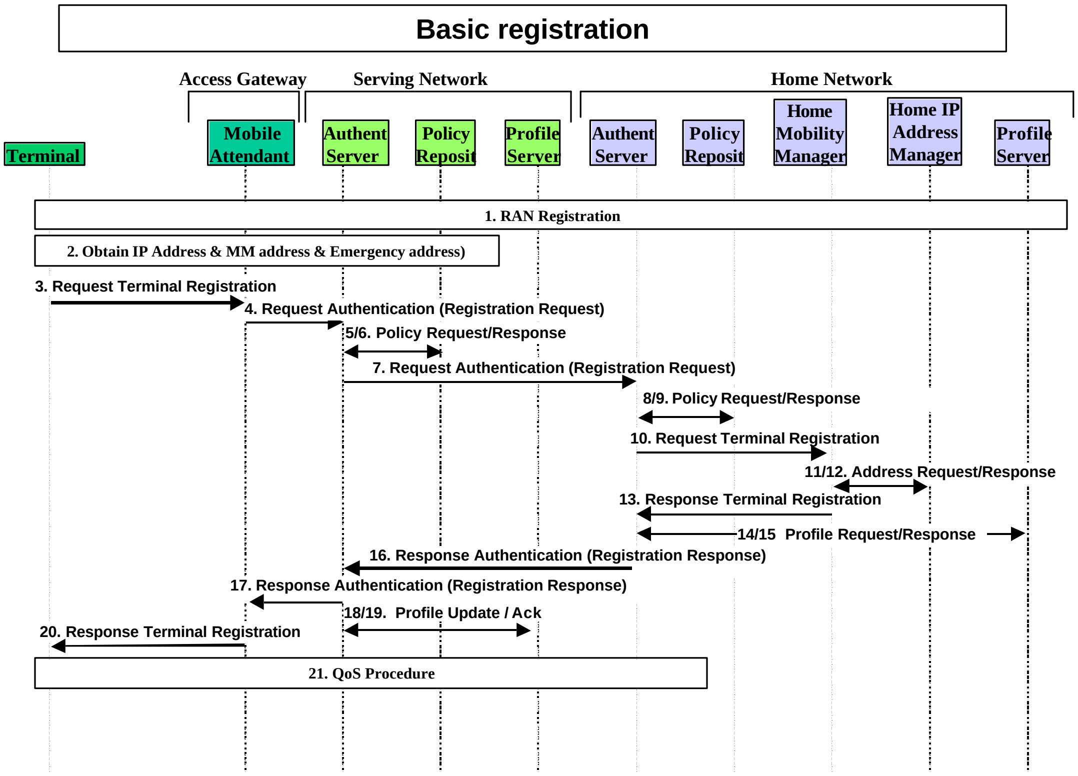
The following Message  Sequence Charts as example scenarios supported by the MWIF Architecture:

- Basic Registration
- Handover
- Mobile Originated SIP based Call
- Mobile Terminated SIP based Call
- Mobile to PSTN Call
- PSTN to Mobile Call
- Mobile Originated, Non CSM, QoS based communication
- Best Effort
- Emergency Call

# A1: Basic Initial Registration

## Scenario Description

## Information Flow


Basic registration
Access Gateway
Serving Network
Home Network
Terminal
Mobile Attendant
Authent Server
Policy Reposit
Profile Server
Authent Server
Policy Reposit
Home Mobility Manager
Home IP Address Manager
Profile Server
1. RAN Registration
2. Obtain IP Address & MM address & Emergency address)
3. Request Terminal Registration
4. Request Authentication (Registration Request)
5/6. Policy Request/Response
7. Request Authentication (Registration Request)
8/9. Policy Request/Response
10. Request Terminal Registration
11/12. Address Request/Response
13. Response Terminal Registration
14/15 Profile Request/Response
16. Response Authentication (Registration Response)
17. Response Authentication (Registration Response)
18/19. Profile Update / Ack
20. Response Terminal Registration
21. QoS Procedure

## Description of Messages:

1. Access technology specific registration, including Authentication and Authorisation to use access network resources. Detailed message flow not shown.
2. Obtain an Ipv6 address (a Care of Address - CoA) to use in the Access Network. Also obtain other addresses necessary for the terminal to contact elements in the Core Network e.g. Session Proxy, Service Discovery Server, Mobile Attendant. Detailed message flow not shown.
3. Ipv6 Mobile IP Registration Request, including information necessary for address management, authentication, and authorisation. In this message, the terminal registers itself with the Mobile Attendant, and assumes the Mobile Attendant will register the Terminal in the home network.
4. AAA registration and Mobile IP registration to local AAA server.
5. If necessary, the local Authentication Server fetches policy information needed to make the local policy decisions necessary for local authentication and authorisation of the current Terminal. Note that this policy information may be cached and messages 5 and 6 not needed.
6. Return policy data.

7. Forward the Mobile IP and AAA request to the home network. There is a trust relationship between the visited AAA server and the home AAA server. The Mobile IP registration message is encapsulated in the AAA message.
8. The home Authentication server fetches any necessary policy information from the Policy Repository.
9. Return policy information.
10. Pass the Mobile IP registration information to the Home Mobility Manager. This includes the currently assigned Care of Address for the Terminal (or possibly the address of the Mobile Attendant).
11. Address Request – obtain a new address from home network (e.g. possibly to support VPN)
12. Address Response
13. Mobile Registration response.
14. Profile Request
15. Profile Response.
16. Home AAA replies to the visited AAA with a response from the original registration request. This response includes any default profile information, including the authorisation for any default bandwidth.
17. Visited AAA replies to Mobile Attendant. Terminal is now registered in the home network and IP packets may be sent from the home network the Terminal.
18. If message 16 includes a default profile for the Terminal, then send it to the Profile Server so it can be locally cached.
19. Response from caching message.
20. Final Mobile IP registration message back to the Terminal
21. Allocate local network resources for any default profile. Details of this sequence are not shown, but should be similar to the QoS procedure in flow 8.7 has been cached in the visited network.

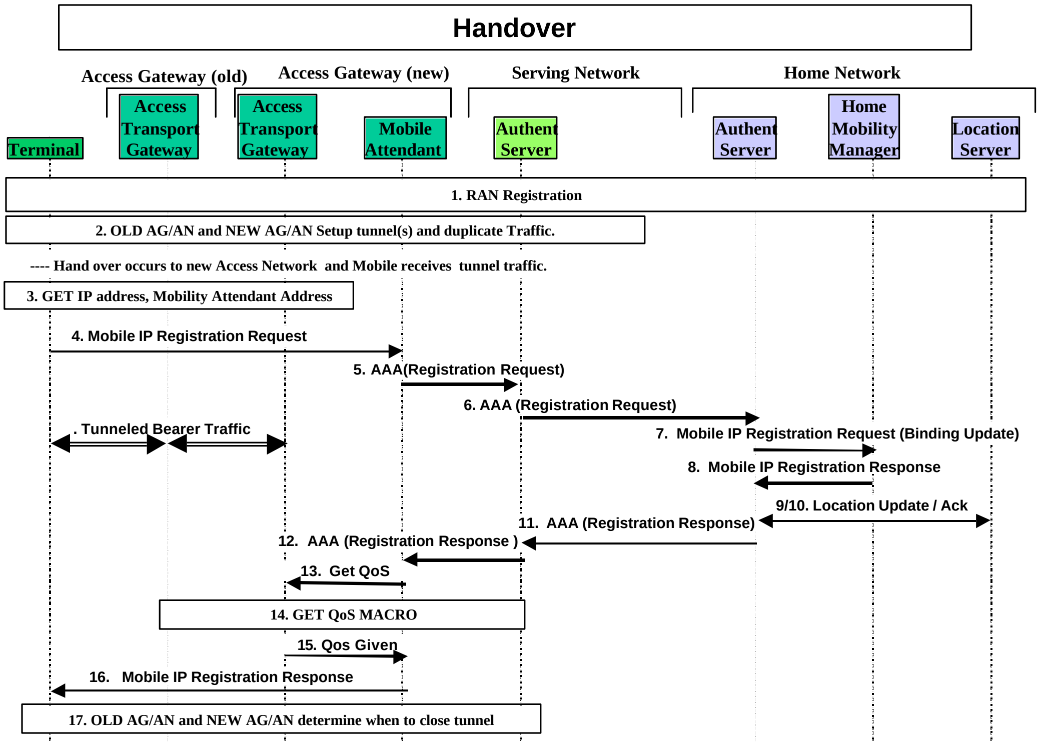
# A.2: Handover

## Scenario Description

It is assumed that the policy information has been cached in the Authentication Server, therefore no messages are shown to fetch or update policy and profile information.

It is assumed that there is active traffic between the MS and corresponding hosts.

## Information Flow


Handover
Access Gateway (old)
Access Gateway (new)
Serving Network
Home Network
Terminal
Access Transport Gateway
Access Transport Gateway
Mobile Attendant
Authent Server
Authent Server
Home Mobility Manager
Location Server
1. RAN Registration
2. OLD AG/AN and NEW AG/AN Setup tunnel(s) and duplicate Traffic.
---- Hand over occurs to new Access Network and Mobile receives tunnel traffic.
3. GET IP address, Mobility Attendant Address
4. Mobile IP Registration Request
5. AAA(Registration Request)
6. AAA (Registration Request)
. Tunneled Bearer Traffic
7. Mobile IP Registration Request (Binding Update)
8. Mobile IP Registration Response
9/10. Location Update / Ack
11. AAA (Registration Response)
12. AAA (Registration Response )
13. Get QoS
14. GET QoS MACRO
15. Qos Given
16. Mobile IP Registration Response
17. OLD AG/AN and NEW AG/AN determine when to close tunnel

## Description of Messages:

Under the assumption that there is active traffic between the Terminal and corresponding hosts, then until the new contact address for the Terminal has been passed back to every corresponding host, there can be traffic arriving at the old Access Transport Gateway/Mobile Attendant that should be sent to the Terminal. This flow shows this interaction in the “Tunnelled Bearer Traffic” messages between messages 6 and 7. Unlike the other messages, this tunnelling will continue between the time the Terminal hands off to the new Access Network and the time that the Corresponding Host receives an update of the current contact address of the Terminal.

1. Access technology specific registration, including Authentication and Authorisation to use access network resources. Detailed message flow not shown.

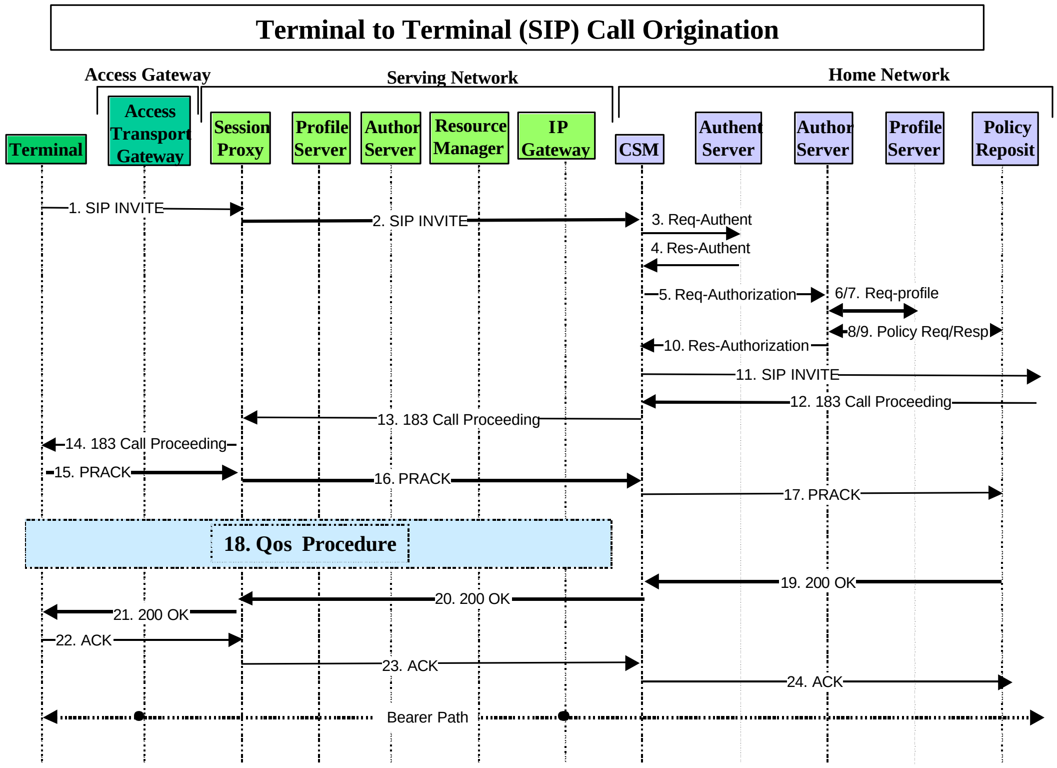
2. Old and New Access Transport Gateways perform any access technology messaging. This is assumed to include setting up tunnels between the two gateways to carry real time traffic during the handover.
3. Obtain an Ipv6 address (a Care of Address, CoA) to use in the Access Network. Also obtain other addresses necessary for the MS to contact elements in the Core Network. Detailed message flow not shown.
4. Ipv6 Mobile IP Registration Request, including information necessary for address management, authentication, and authorisation. In this message, the Terminal registers itself with the Mobility Attendant, and assumes the Mobile Attendant will register the Terminal in the home network.
5. AAA registration and Mobile IP registration to local AAA server.
6. Forward the Mobile IP and AAA request to the home network. There is a trust relationship between the visited AAA server and the home AAA server. The Mobile IP registration message is encapsulated in the AAA message.
7. Pass the Mobile IP registration information to the Home Mobility Manager. This includes the currently assigned Care of Address for the Terminal (possibly the address of the Mobile Attendant).
8. Response from the Home Mobility Manager. This Mobile IP Registration Response will be included in the AAA response back to the visited network.
9. Location Update. Update any information necessary in the location server.
10. Location Update Response.
11. Home AAA replies to the visited AAA with a response from the original registration request. This response includes any default profile information, including the authorisation for any default bandwidth.
12. Visited AAA replies to Mobile Attendant. Terminal is now registered in the home network and IP packets may be sent from the home network the Terminal.
13. Mobile Attendant requests the Access Transport Gateway to set up bandwidth in the new network to satisfy the QoS requirements of every active context in the terminals current profile.
14. Allocate local network resources for any default profile. Details of this sequence are not shown, but should be similar to flow 8.8 where the QoS authorisation (returned in message 16) has been cached in the visited network.
15. Access Transport Gateway replies indicating the success of setting up network bandwidth needed to satisfy the current profile.
16. Final Mobile IP registration message back to the Terminal
17. Tunneling of traffic continues until no longer necessary. These messages are access network specific.

Issue: Not shown are binding update messages between the Terminal and corresponding hosts. These need to be added to this flow.

# A.3: Mobile Originated SIP based Call

## Scenario Description

## Information Flow



## Description of Messages

1. The terminal requests for a session set-up sending a SIP INVITE to the Session Proxy containing the destination address (*e.g.*, URL or E.164 number) as well as a session description in the body of the SIP INVITE.
2. The Session Proxy forwards the set up request to the CSM in the home network of the originating user.
3. The home CSM request for user authentication.
4. The Authentication server returns the authentication results.
5. The home CSM requests for the authorization of this session.
6. The Authorization Server sends a request to the Profile Server to retrieve the user profile.
7. The Profile Server returns the user's profile.
8. The Authorization Server checks the Policy Repository for the given subscriber and requested services.
9. The relevant policies are retrieved and returned to the Authorization Server.

10. Authorization server makes a decision on the request and sends appropriate response to a CSM in the home network for the destination terminal.

*Note, if the authorization fails the home CSM returns an appropriate failure status code (e.g. 606) to the Terminal via the Session Proxy to inform it about the set up request failure.*

11. The CSM forwards the SIP INVITE to the Destination CSM.
12. The Destination sends a 183 Call Proceeding message to the home CSM
13. The home CSM forwards the 183 Call Proceeding message to the Session Proxy.
14. The Session Proxy forwards the 183 Call Proceeding to the Terminal.
15. The terminal sends a PRACK to the Session Proxy.
16. The Session Proxy forwards the PRACK to the home CSM.
17. The home CSM forwards the PRACK to the destination.
18. The Terminal initiates the QoS procedure towards the IP Gateway in the Serving Network.
19. The Destination sends a 200 OK message to the home CSM
20. The home CSM forwards the 200 OK message to the Session Proxy.
21. The Session Proxy forwards the 200 OK to the Terminal.
22. The Terminal sends a confirmation (SIP ACK) to the Session Proxy to confirm the reception of the session set-up request.
23. The Session Proxy forwards the SIP ACK to the home CSM.
24. The home CSM forwards the SIP ACK to the destination.
25. An end to end bearer path is available via the Access Transport Gateway and and IP Gateway in the Serving Network.

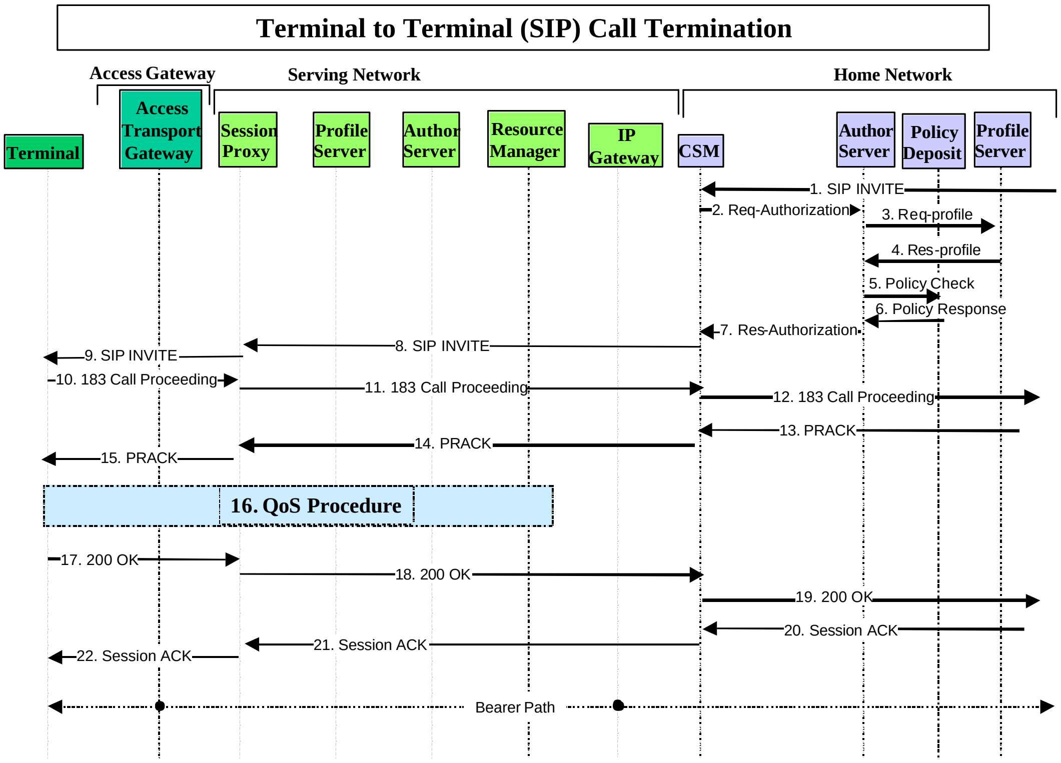
# A.4: Mobile Terminated SIP based Call

## Scenario Description

- The Terminal is roaming in a Serving Network and is the called-party of the scenario.
- The flow details, such as intermediate acknowledgements, call progression messages, etc., are omitted from this flow. This flow is intended to demonstrate the role performed by each network entity.

## Information Flow

The Mobile Terminated SIP message flow is shown below:



## Flow Description

1. The remote endpoint sends a request for a session ([SIP] INVITE ) message to the CSM of the Terminal's home network. This CSM might not be the one that is allocated for the destination user. In this case the CSM would forward the SIP INVITE to the appropriate CSM (determined through a Directory Service look-up).
2. The CSM examines the *To:* field and forwards the [SIP] INVITE message to the appropriate Authorisation Server.
3. The Authorisation Server examines the *To*: field and requests the subscribe r profile data from the appropriate Profile Server.
4. The Profile Server returns the relevant subscriber data for the call termination.

5. The Authorisation Server checks Policy for the given subscriber and the requested service (the call termination).

6. The policy answer is returned to the Authorisation Server.

7. The Authorisation Response is returned to the CSM.
*Note: Steps 2-7 could be considered a registration-time function. The CSM could obtain the profile directly and assert control based on the subscriber profile, either directly or through Core Network Applications.*

8. The CSM forwards the [SIP] INVITE message to the Session Proxy. The CSM adds its address in the Record Route field.

9. The Session Proxy forwards the [SIP] INVITE message to the Terminal.

10. The Terminal sends a 183 Call Proceeding message to the Session Proxy

11. The Session Proxy forwards the 183 Call Proceeding message to the CSM in the Home Network.

12. The CSM forwards the 183 Call Proceeding to the origination.

13. A PRACK is received by the CSM from the origination.

14. The CSM forwards the PRACK to the Session Proxy.

15. The Session Proxy forwards the PRACK to the Terminal.

16. The Terminal executes the QoS procedures to establish bearer path network resources through the IP Gateway in the Serving Network using the procedure described in section 8.7.
*Note: the dialogue between the Session Proxy/CSM establishment of required resources is described in detail in the relevant IETF documents, and is not detailed here.*

17. The Terminal sends the result of the session set-up request ([SIP] 200 OK ) to the Session Proxy.

18. The Session Proxy forwards the [SIP] 200 OK message to the CSM.

19. The CSM forwards the [SIP] 200 OK message to the remote end point.

20. The remote end point acknowledges the session by sending a [SIP] ACK toward the CSM.

21. The CSM forwards the [SIP] ACK to the Session Proxy.

22. The Session Proxy forwards the [SIP] ACK to the Terminal.

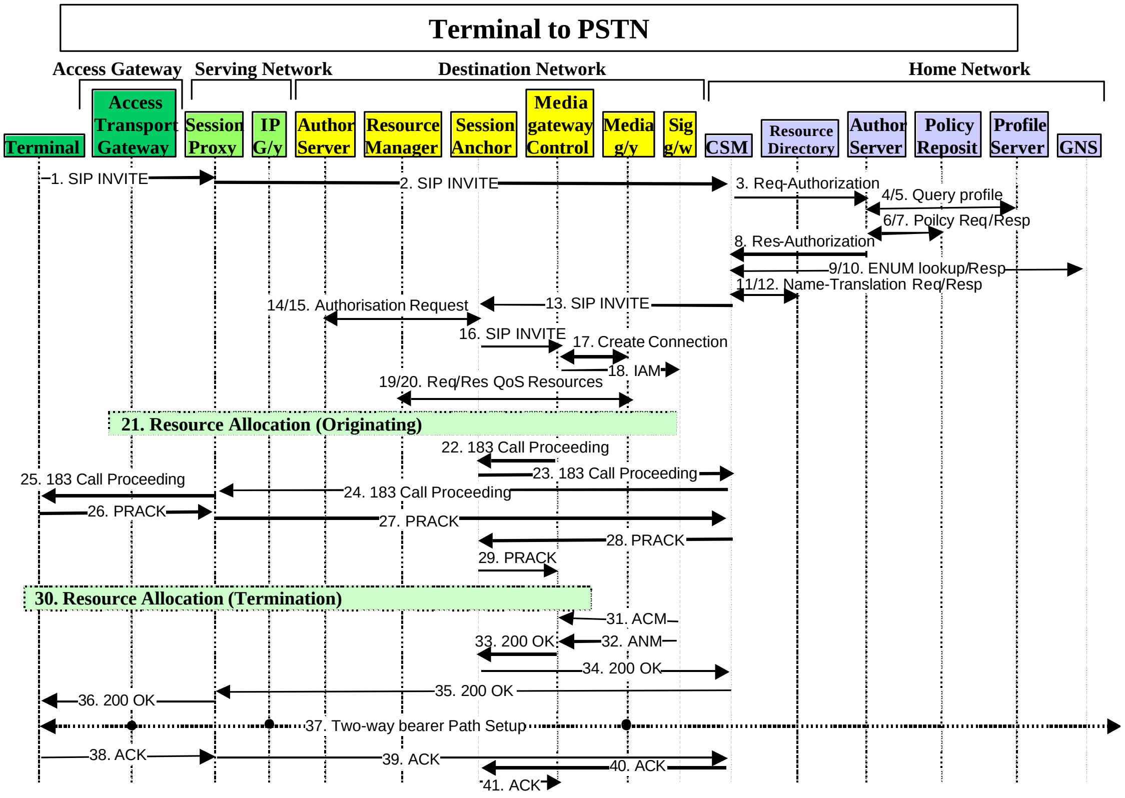
23. Two-way communications occurs between the Terminal and the remote end point via the Access Transport Gateway and an IP Gateway in the Serving Network.

# A.5: Mobile to PSTN Call

## Scenario

A Terminal user whilst roaming places a call to a user in a PSTN station. The media gateway selected for connection to the PSTN is in a different service provider network to both the serving and home service networks.

## Information Flow



## Description of Messages

1. The Terminal sends a SIP Invite with To header containing an E.164 phone number with the following format: To: CallerName <sip: To: +1-617 233-3476@telcodest.com>; user=phone. The Invite is sent to the MS's Session Proxy. The domain name of the home service provider is telcoorig.com
2. The Session Proxy forwards the Invite to the home CSM. Note that the home CSM is received in the Request-URI of the Invite and was sent to the terminal during initial SIP Registration.
3. The home CSM sends a Request for authorization to its corresponding authorization server
4. The authorization server sends a request for the profile to the Profile Server
5. The Pro file Server returns the user's profile.

6. The Authorization Server checks the Policy Repository for the given subscriber and requested services.
7. The relevant policies are retrieved and returned to the Authorization Server.
8. The Authorization Server returns an authorization approval to the CSM. (Note, the authorization may involve determining that the destination is in the PSTN).
9. The CSM sends an ENUM request to the GNS.
10. The GNS sends an ENUM response to the CSM indicating a failure to find the destination.
11. The CSM sends a TRIP translation request to the Resource Directory, where given the destination E.164 number the TRIP location server will provide the IP address of the best entity that can handle this call to the PSTN.
12. For this scenario the TRIP Location server returns the IP address of the session Anchor at a destination service provider, which is different from both the originating and the home network
13. The home CSM forwards the SIP Invite to the Session Anchor at the destination network.
14. The Session Anchor requests an authorization to handle this call.
15. The authorization server returns an authorization to proceed with the call.
16. The Session Anchor selects a media gateway controller to (MGC) handle this call (this may require use of local TRIB) and forwards the SIP Invite to the MGC.
17. The MGC selects a media gateway and sends a Create Connection request to the media gateway
18. The MGC sends an IAM ISUP message to the PSTN via the Signaling gateway, to set up the PSTN portion of the call
19. The MG sends a request for QoS resources to the Resource Manager
20. The Resource Manager returns the request approval
21. The MG performs the necessary procedures for resource allocation in the destination network.
22. The MGC sends a SIP 183 progress message to the session anchor.
23. The Session Anchor relays the SIP 183 back to the CSM in the Home Network for the originating terminal..
24. The CSM relays the SIP 183 back to the Session Proxy in the in the Serving Network.
25. The Session Proxy forwards the SIP 183 to the originating terminal.
26. Once the 183 progress arrives in the Terminal, a two-way bearer path (this path may not have QoS yet, only best effort) is available between the Terminal and the MG, and a one way bearer path is available between the PSTN and the MG. The terminal responds with a PRACK to the Session Proxy in the Serving Network. *The processing for resource allocation in the serving network should be identical to that as for 8.3 (Mobile Originated SIP).*
27. The Session Proxy relays the PRACK back to the CSM for the terminal in the Home Network.
28. The CSM in turn relays the PRACK onto the Session Anchor in the destination network.
29. The Session Anchor sends the PRACK to the MGC.
30. The Terminal initiates the QoS procedure to allocate resources to the IP Gateway in the Serving network.
31. The PSTN returns an ACM message to the MGC via a Signalling Gateway.
32. The PSTN returns ANM message indicating that the destination user answered the call

33. The MGC sends a SIP 200 OK message indicating that the call has been accepted, this message is relayed all the way back to the Terminal, going through the Session Anchor, CSM, and Session Proxy

34. 200 OK

35. 200 OK

36. 200 OK arrives in the Terminal

37. A two way bearer path is available via the Access Transport Gateway, an IP Gateway in the Serving Network, an IP Gateway in the Destination Network (not shown) and the Media Gateway in the Destination Network.

38. The Terminal responds with a SIP ACK to the Session Proxy.

39. The Session Proxy relays the SIP ACK back to the CSM for the terminal in the Home Network.

40. The CSM in turn relays the SIP ACK onto the Session Anchor in the destination network.

41. The Session Anchor sends the SIP ACK to the MGC.

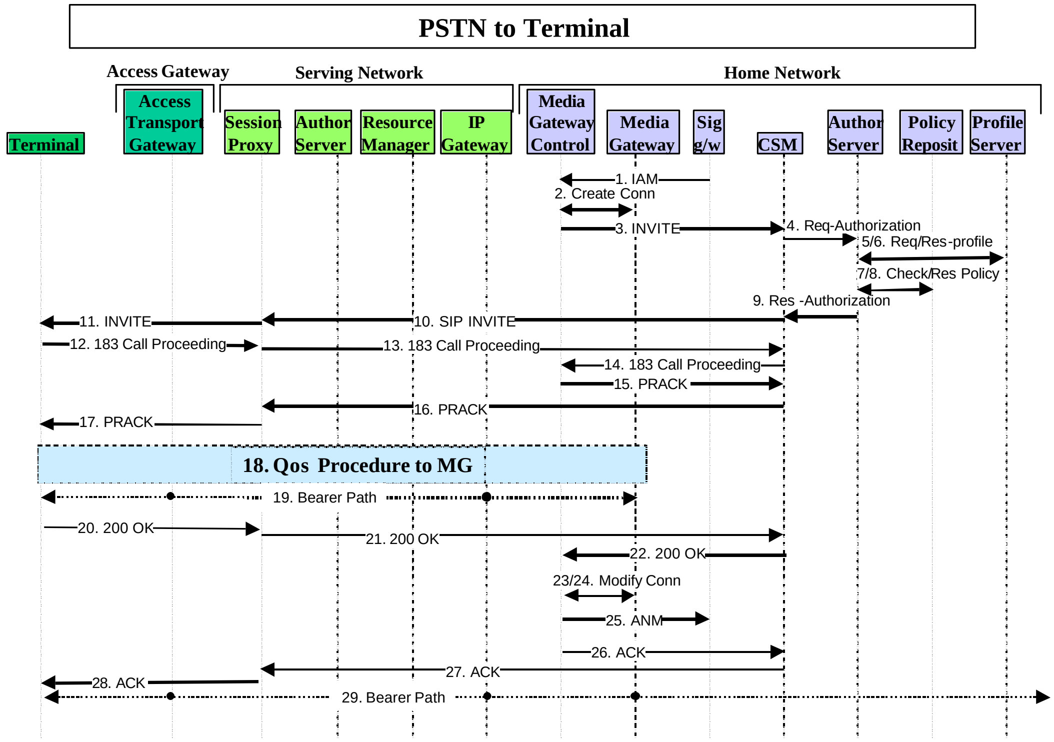
# A.6: PSTN to Mobile Call

## Scenario

## Assumptions

- The destination terminal behaves the same irrespective of whether the call was originated from the PSTN or from another SIP phone.
- At this stage this flow is developed to a level of detail consistent with the SIP to SIP flows. Interim terminal states such as alerting, trying etc are not included here.
- The destination terminal initiates the QoS procedure as in the SIP case except that in this case the target is a Media Gateway rather than an IP Gateway.
- In the case shown below the bearer path is routed through a Media Gateway in the home network. The MGC and MG could also be located in the Serving Network - assuming there is a mechanism to route the IAM (and drop back any PSTN resources) to the Serving Network. Which functional entity takes this decision? Possibly the MGC could interrogate the Profile Server before sending the INVITE to the CSM and forward the IAM towards a MGC in the Serving Network for a roaming subscriber if this is supported.

## Information Flow



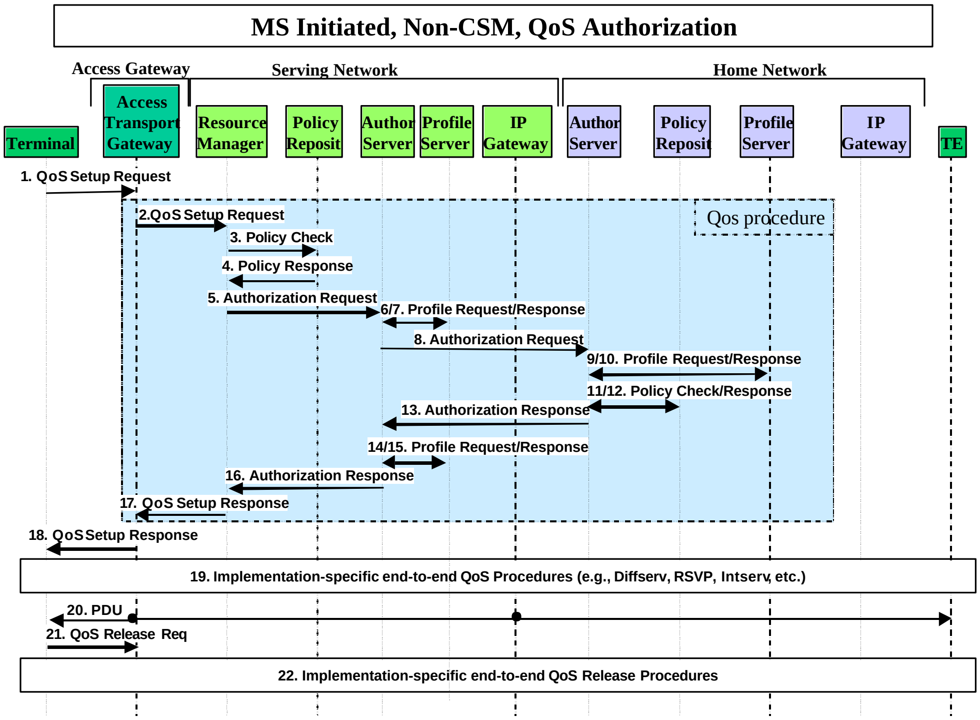
### Details of Messages

1. The Signalling Gateway receives an incoming IAM from the PSTN over a SS7 network and forwards the IAM using appropriate IP Transport to it's Media Gateway Controller.
2. The MGC establishes a connection in the Media Gateway.
3. The MGC forwards a SIP INVITE message to a CSM for the terminating subscriber. This may be via another CSM that determines the actual CSM allocated to the user.
4. Flows 4 to 13 are the same as for the SIP to SIP call termination flow (see 8.4 flows 2 to 1).
14. The CSM forwards the 183 Call Proceeding message to the MGC.
15. The MGC responds with a PRACK message back to the terminal via the CSM in the home network and Session Anchor in the Serving Network.
16. The PRACK message is relayed towards the terminal.
17. The PRACK message is relayed to the terminal.
18. The Terminal initiates the QoS procedure towards the Media Gateway.
19. A bearer path is established between the Terminal and the Media Gateway.
20. The Terminal sends the result of the session set-up request ([SIP] 200 OK ) to the Session Proxy.
21. The Session Proxy forwards the [SIP] 200 OK message to the CSM.
22. The CSM forwards the [SIP] 200 OK message to the MGC.
23. The MGC requests any modifications required to the Media gateway resources (ffs).
24. The MGC forwards the [SIP] 200 OK message to the MGC.
25. The MGC initiates a ANM messages to the originator and sends using appropriate IP transport to the Signalling Gateway where it is transferred to a SS7 network.
26. The MGC initiates the [SIP] ACK to the CSM.
27. The CSM forwards the [SIP] ACK to the Session Proxy.
28. The Session Proxy forwards the [SIP] ACK to the MS. Two-way communications occurs between the Terminal and the remote end point.
29. A bearer path is established end to end via the Access Gateway, and IP Gateway in the Serving Network, an IP Gateway in the Home Network (not shown) and a Media Gateway in the Home Network.

# A.7: Mobile Originated, Non CSM, QoS based communication

## Scenario

## Information Flow



## Message Descriptions

1. There are several mechanisms to initiate the QoS Setup. The mechanism shown in this particular flow is based on the Terminal initiating the QoS Setup.
2. Upon receipt of the QoS Setup message, the Access Transport Gateway forwards the QoS Setup message to the Resource Manager in the Serving network.
3. Upon receipt of the QoS Setup, the Resource Manager initiates a Policy Check with the Policy Repository in the Serving network to check network to network policies.
4. Upon receipt of the Policy Check, the Policy Repository returns the network policies in the Policy Response message sent to the Resource Manager.
5. Upon receipt of the Policy Response and associated data, the Resource Manager validates that there are network resources available to support the QoS. The Resource Manager then initiates the Authorization of the QoS request by sending an Authorization Request to the Authorization Server in the visited/serving network.
6. Upon receipt of the Authorization Request, the serving Authorization Server sends a Profile Request to the serving Profile Server to determine if there is a locally available profile for the Terminal (obtained by a previous QoS procedure).

7. The Profile Server returns the profile information if available. For this scenario, the information is not locally available, thus the Authorization Server needs to interface with the Home network to obtain the profile.

8. Upon receipt of the response from the serving Profile Server indicating that a local profile is not available, the visited Authorization Server forwards the request to the Home Authorization Server for authorization by the Home Service provider.

9. Upon receipt of the Authorization request, the Home Authorization Server sends a Profile Request to the Profile Server to obtain the terminal's profile.

10. The Profile Server returns the terminal's QoS profile to the Home Authorization Server.

11. Upon receipt of the Profile from the Profile Server, the Authorization Server sends a request to the Policy Repository to obtain the policy rules for the specific QoS in the terminal's profile.

12. Using the QoS profile and the requested QoS received in the Authorization Request message, the Authorization server applies the policy rules to determine if the requested QoS is allowed. Upon successful authorization, the Authorization Server may update the terminal's profile to reflect the currently requested QoS if the profile had not been updated during the initial access of the profile (steps 9/10).

13. The Home Authorization Server sends an Authorization response to the visited Authorization Server including the subscribed QoS profile and an indication of the success/failure of the QoS request.

14. Upon receipt of the Authorization response, the serving Authorization Server sends a Profile Request to the serving Profile Server with the subscribed and decided QoS.

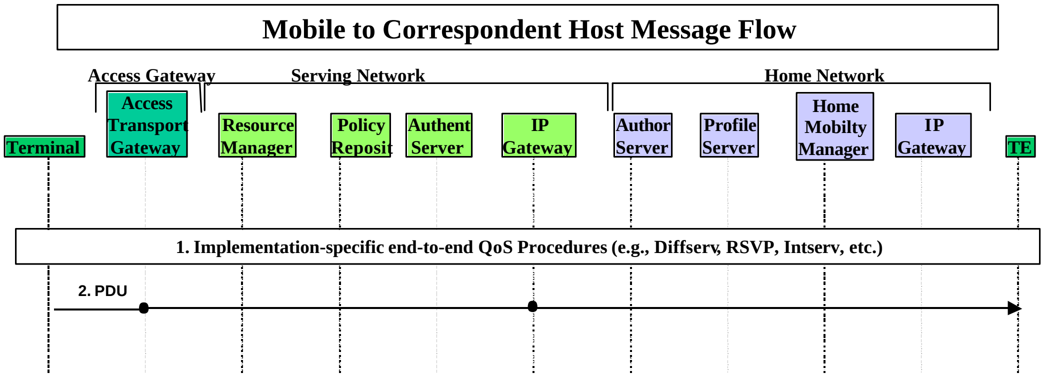
15. The serving Profile Server updates the subscribed and decided QoS for the terminal's session and sends a Profile Response to the serving Authorization Server.

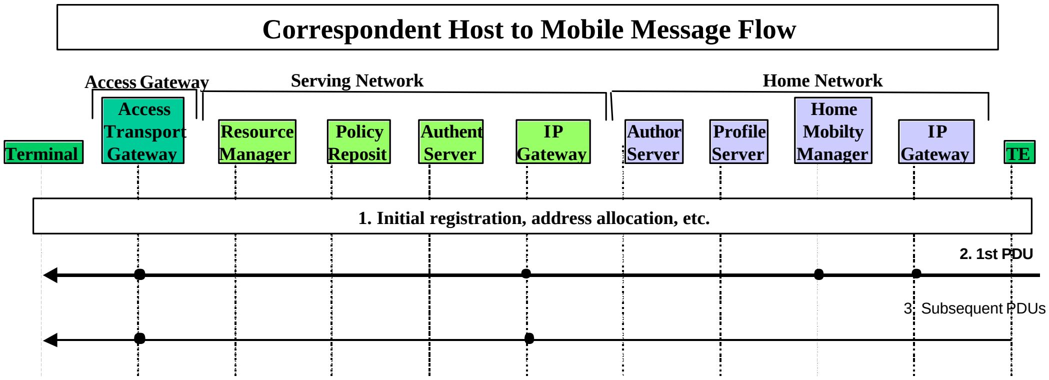
16. Upon receipt of the Profile Response, the serving Authorization Server send an Authorization Response (indicating success/failure, decided QoS of the initial Authorization Request) to the Resource Manager.

## A.8: Best Effort

### Scenario

### Information Flow





### Description of Messages

## A.9: Emergency Call

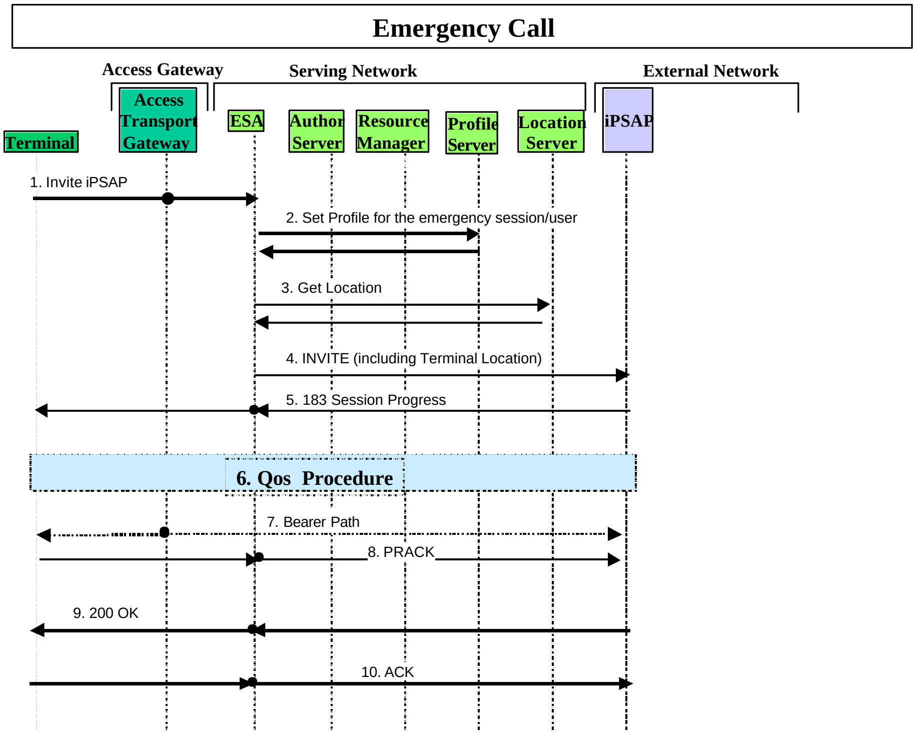
### Scenario

The main problem for the support of emergency calls (e-911) is not the basic SIP call control, but is the ability to process calls for non-authenticated terminals. The emergency call support must balance the ability to support emergency calls with the desire to protect the network from theft of services. This is performed by having the firewall functionality in the Access Transport Gateway support the limited transport of signals between any terminal and an Emergency Services Application. This ESA accepts SIP invites for emergency calls, validates that the address is indeed the address of a Public Services Answering Point. PSAP (or iPSAP, Internet PSAP), and acts as the CSM (or proxies control to another CSM) for the terminal to support the emergency call(s).

### Assumptions

- The terminal does not have to be registered, authenticate, nor even contain a valid SIM.
- The access network specific functions to permit traffic for an emergency call are not shown here.
- The terminal generates a site local Ipv6 address
    - Site local address should be unique and is composed of IpV6 Site Local prefix + link address
    - It would be best if there was a defined way for any terminal to have a 64-bit unique number for its link address.
    - Generating a 64 bit random number is probably sufficient since the probablity of generating one that is already in use is very small.
- There is a defined IpV6 site local multicast address defined for emergency services (could be an anycast address if anycast is really implemented)
- The Access Transport Gateway firewall functionality has a predefined “pinhole” that will pass IP traffic from a MS’s site local address to the Emergency Services Multicast Address.
- There is a specific Core Network Application, the Emergency Services Application (ESA) which responds to the Emergency Services Multicast Address and processes Emergency calls.

## Information Flow



## Details of Messages

1. Terminal generates a site local IP address and sends an invite to emergency address multicast address
   Firewall in Access Transport Gateway passes invite to core network (based on emergency multicast address)
2. Emergency Server Application
   - reads invite from multicast address
   - validates “to” is an emergency service
   - Sets up local profile to permit subsequent resource allocation
3. “Obtains Geographic address of terminal
4. Sends Invite to emergency service (iPSAP)
5. “183 progress” message with iPSAP addressing information returned.
6. Terminal performs “normal” QoS operations.
   Note that the local profile server has been filled in to permit the resources necessary for the call (see step 2).
7. Bearer Path now exists – can send RTP packets for the emergency call
8. Terminal returns PRAC to iPSAP
9. IPSAP returns OK

10. Terminal returns ACKs

**Revision History**

| **Date** | **Version** | **Comment** |
|---|---|---|
| 27th April 2001 | Draft 1.7 | Approved by the membership via ballot. |
| 15th May 2001 | Draft 1.7 | Ratified by the MWIF Board of Directors. |