TG-NA(00)057

Report from the UMTS Forum

Naming, Addressing & Identification Issues for UMTS

UMTS Forum, December 2000

This report is produced by the UMTS Forum, an association of telecommunications operators, manufacturers and regulatory authorities as well as IT- and media industries interested in broadband mobile multimedia who are active both in Europe and other parts of the world and who share the vision of UMTS. In terms of a technology platform UMTS will move mobile communications forward from where we are today into the Information Society by delivering speech, data, pictures, graphics, video communication and other wideband information direct to people on the move. UMTS is a member of the IMT-2000 family of standards.

Although regulators have participated in the development of this Report, they are not bound by its conclusions.

Editorial remarks are italic bold and will be taken out or added during the final editing process.

This report has been written by the UMTSF TG NA group in which the GSM Association participates by formal agreement:

Chairman Gerd-Hinrich Grotelüschen (Mannesmann Mobilfunk GmbH)

Editors

John Horrocks (DTI), +44 1483 797807, 100441.727@compuserve.com
supported by:
Michael Koch (Siemens), +49 89 7223 3363, michael-j.koch@icn.siemens.de
Jürgen Rauschenbach (DFN and IPv6 Forum), +49 30 8842 9946, jrau@dfn.de

Document history:
Version 0.1, April 2000, Sample of material. Inconsistent in its messages.
Version 0.2, June 2000, Update to version 0.1.
Version 0.3, extensive revision after comments at Heathrow meeting
Version 0.4, revisions after comments at Helsinki meeting
Version 0.5, revisions after comments at Toulouse meeting
Final Draft approved at UMTS Forum General Assembly, Paris, December 2000

Acknowledgements:

- Some text and diagrams used in this report has been copied with permission from a study commissioned by the Netherlands Ministry (DGTP) and undertaken by Ovum Ltd.
- Valuable help has been provided by Anders Roos on behalf of the GSM Association

Copyright © UMTS Forum, 2000. All rights reserved. Reproductions of this publication in part for non-commercial use is allowed if the source is stated. For other use, please contact the UMTS Forum Secretariat, Russell Square House, 10-12 Russell Square, London WC1B 5EE, UK;
Telephone +44 20 7331 2020

References to emerging technologies reflect the situation at the end of Year 2000 and could, in details, be overtaken by further developments. Reasonable care has been taken to assure that the information in this report is accurate. However, no warranty of any kind can be given with regard to this material. The UMTS Forum shall not be liable for any errors contained in the report or for incidental consequential damages in connection with the use of the material.

Table of Contents

Executive Summary

This report is an initial study of the naming, addressing and identification issues that concern UMTS. Because part of UMTS will be based on the core network architecture developed for GPRS, some of its conclusions are also relevant to GPRS.

UMTS is expected to be a very important step in the development of telecommunications because:

- Mobile communications are achieving very high penetration levels and becoming substitutes for fixed telephony services
- UMTS is being designed as a truly multi-service platform
- UMTS will be one of the first "traditional public telecommunications services" to use IP technology in its core network initially as an overlay and ultimately throughout the network. Therefore UMTS is at the forefront of the convergence to IP.

However although there are significant changes and new terminology to be learned by both the mobile telecommunications and the IETF cultures, the fundamental concepts that have already been developed of names and addresses still apply. Failure to apply these fundamental concepts is the cause of some of the concern and confusion that this report seeks to remove.

A General Issues

There does not appear to be adequate information on the relationship between the core networks of the mobile operators and ISPs/Intranets that can be selected by users for access. This is an important area for market development and competition as it affects the creation of a separate competitive layer of service providers on top of the layer of competing network operators.

The report highlights the need for agreements and formal documentation giving technical guidelines about the relationships and connection arrangements between network operators and ISPs/Intranets. It should cover items such as:

1. interconnect guidelines;
2. the implication of interconnect guidelines regarding the allocation of the IP address to the mobile;
3. the identification and development of technical specifications required to implement technical guidelines.

The GSM Association should take responsibility for this work. It is a matter of urgency that standardization in 3GPP receives clear advice on these items. The UMTS Forum may assist with expertise, if required.

B Naming

Each service capability description should specify the form of identification to be used, which may be a name that would be resolved into an address, or just an address. Names offer the benefits of increased user friendliness, a degree of network independence and various degrees of portability.

Third generation mobile technology can support multiple services and hence more than one type of name therefore there is no unique naming solution for UMTS.

The two main naming schemes available for UMTS services are E.164 and Internet names (user@domain) and both schemes will be used for different services. The report provides considerable information about work on these schemes by ITU-T, ETSI and IETF.

The issues covered in the report include:

- The choice of naming scheme

- The allocation of appropriate naming capacity, whether under different number ranges on E.164 or new TLDs
- The support of name to address resolution
- The support of portability
- Selection of ISPs and Intranets
- Future issues

Detailed recommendations are as follows [1]:

Operators should:

1. Check that the GSM Association is willing to continue its role with respect to Access Point Names

2. Ensure that there are published and non-discriminatory principles for the registration of Access Point Names

3. Ensure the support of name (number) portability for E.164 numbers for services similar to those provided on GSM.

4. If practicable build in the capability to support the portability of Internet names in order to ensure compatibility with any future requirements

5. Explore the possibility of using a single E.164 number to be used for telephony, fax and data instead of having separate numbers.

Service providers (ISPs) should:

6. Consider the use of a domain name for individuals that is not explicitly related to their service provider

7. Ensure that their administrative systems and procedures can support name (number) portability for E.164 numbers.

Manufacturers should

8. Consider adherence to ITU-T Recommendation E.161 for the association of alphabetic characters to the numbers of the keypads of UMTS terminals and supplement it with a standard presentation for the "@" symbols.

Regulators should :

9. Consider if any regulation is needed on the portability of E.164 names (numbers) in countries where it is not already required. This would include portability between operators, between operators and service providers and between different service providers and, for called party pays, portability between fixed and mobile services

10. Consider if any regulation is required on the portability of Internet names

11. Consider which numbering ranges in E.164 should be used for services on UMTS (provided that the services/tariffs are similar, there is a good case for using the same ranges as for GSM as this will enable portability between GSM and UMTS)

12. Consider the use of new ranges of E.164 numbers for new emerging services, especially multimedia services under UMTS Release 5.

[1] The recommendations and conclusions on naming and addressing are numbered together in one sequence for ease of reference. This sequence extends through the sections B and C of the Executive Summary.

In addition , further study is needed on the support of packet data-only terminals and the use of E.164 numbers by these terminals as the use of E.164 numbers by these terminals could cause capacity problems in some countries and is not strictly necessary for receiving incoming calls. This could be a substantial potential market.

C Addressing

Addressing issues are covered in some depth. Three types of address are considered:

- IP addresses
- Mobile station roaming numbers
- Routing prefixes for E.164 numbers

The main focus is IP addressing. The issues covered include:

- The support of mobility
- NATs, Firewalls, security and the end-to-end paradigm
- Choice of IP version and migration from IPv4 to IPv6
- Temporary or permanent assignment to the terminal

Areas of IPv6 are identified that are still being investigated.

The following are the main conclusions and recommendations on IP addressing:

13. The protocol and addressing version issues for the SGSNs and internal PLMN core networks are independent from those for the terminals, and connected ISPs or Intranets at least until IP multimedia is introduced. However GGSNs will have to be compatible with:
    - internal network equipment
    - the terminals to which they will assign addresses, both home and visiting terminals
    - SGSNs in other networks to which they support GTP tunnels

14. GPRS/UMTS operators will need global IPv4 addresses for their core network infrastructure because IPv4 is the default protocol at least for Releases 3 & 4.

15. IPv4 address exhaustion is difficult to predict but may be felt in the 2004-2006 timeframe and so network operators should ensure that they obtain adequate public IPv4 address allocations for their core networks

16. A new version of the mobile operators' internal DNS that is compatible with IPv6 and IPv4 (e.g. BIND9.x) will be needed when operators start to use IPv6 in their core networks

17. There is no absolute need for UMTS operators to synchronise the introduction of IPv6 in their internal core networks. However as GGSNs allocate IP addresses to mobiles and establish tunnels with SGSNs in other networks, they will need to know which other networks support IPv6 and therefore they need a system for exchanging information about introduction of IPv6 through dual stack operation. The operators may also wish to set common dates for introducing dual stack to reduce the administrative work so that they can change the arrangements with a whole group of networkes at the same time.

18. The GSM Association should facilitate the introduction of IPv6 by providing mechanisms for operators to exchange information about their plans for introducing IPv6 and the transition tools that they will use

19. The GSM Association should produce a guide and recommended procedure for the introduction of IPv6. Although operators may not need to start migrating to IPv6 immediately, it is important that this work should be undertaken reasonably soon to obtain a deeper understanding of the issues and the time that will be needed for migration.

20. Address assignments to terminals appear to need to be temporary if terminals are to be able to establish PDP Contexts with visited GGSNs. This may conflict with the need for IPv6 to use static assignments for many of the feature advantages of IPv6 to be realised. This area needs further study.

21. The UMTS Forum cannot judge at this time on how well founded concerns about network boundaries are. No forecast can be made on how soon operators will be willing to return to or at least towards the end-to-end paradigm. Further study of these issues especially in relation to migration to IPv6 is needed.

For circuit-switched services, regulators will need to make additional allocations of MSRN numbering space and routing numbers for number portability for operators without GSM networks, but these areas are unlikely to cause any particular problems.

D Other identifiers

D.1 Mobile Network Codes and IMSIs

MNCs may be used by various networks in the future. If substantial growth develops in some countries in the number of:

- Mobile Virtual Network Operators
- Mobility services in fixed networks
- Other networks (e.g. TETRA)

then a shortage of Mobile Network Codes may arise. This situation does not yet appear to be imminent but should be kept under review.

The current system of IMSI allocation is inefficient and may lead to premature exhaustion of existing MNCs. The problem is that IMSIs that cease to be used as a result of customers churning are not recovered and re-used after a period of sterilisation. Therefore the high levels of churn are generating excessive consumption of IMSIs. Operators should investigate a mechanism for recovering and re-using IMSIs.

D.2 IMEIs

The International Mobile Equipment Identifier (IMEI) identifies the mobile terminal. It has been introduced, originally, in relation to the type approval of terminals but is also used for tracking stolen terminals and for fraud prevention. Although type approval is no longer a requirement in large parts of the world, the IMEI has become increasingly important for network operators, regulators, manufactures and users. The industry considers the IMEI an important market requirement therefore the advantages of IMEI and some of its main uses must be retained.

Rules for the assignment and administration of the IMEI have to be reconsidered and adapted to the new regulatory requirement. The implementation of UMTS networks will entail an increasing demand for IMEI numbers. This must be taken into account. In addition, adequate security features must be incorporated.

Manufacturers and operators' are presently jointly reviewing the IMEI scheme and the allocation procedure. This work has started in the "Global IMEI Strategy Forum", a joint initiative of manufacturers and the GSM Association. Agreements on a number of important issues have already been achieved. Other items require further discussion. A change in the format of the IMEI, i.e. a move to hexadecimal notation, has been suggested. This is a very sensitive matter for network operators and deserves careful consideration.

D.3 Issuer Identifier Numbers

These numbers are stored on SIM cards for use with applications supplementary to mobile communications. They are a particularly scarce resource and national regulatory authorities should ensure that national rules for allocation of issuer identifiers according to ITU-T Recommendation E.118 are in place, and that they take account of the limited number available and the increasing importance of identification cards in an emerging M-Commerce environment.

Glossary of terms

3GPP	3rd Generation Partnership Project
APN	Access Point Name
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ASO	Address Supporting Organisation
ccTLD	country code Top Level Domain
CC	Country Code
CLI	Calling line indication
DNS	Domain Name System
DSL	Digital Subscriber Line
DSTM	Dual Stack Transition Mechanism
ENF	European Numbering Forum
ENUM	A working group of IETF developing a method for resolving E.164 numbers into names for Internet resources
ETSI	European Telecommunications Standardisation Institute
GAC	Government Advisory Committee
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Centre
GPRS	GSM Packet Radio System
GSM	Global System for Mobiles
gTLD	Generic Top Level Domain
GTP	GPRS Tunnelling Protocol
HF	Human Factors
HLR	Home Location Register
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation of Assigned Names and Numbers
ICCID	Integrated Circuit(s) Card IDentifier
IEC	International Electrotechnical Commission
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IIN	Issuer Identification Number
IM	IP Multimedia
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Station Identity
IP	Internet Protocol (IPv4: version 4, IPv6: version 6)
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
LIR	Local Internet Registry
MCC	Mobile Country Code
MII	Major Industry Identifier
MNC	Mobile Network Code
MSC	Mobile Switching Centre
MSIN	Mobile Station Identification Number
MSISDN	Mobile Subscriber Integrated Services Digital Network
MSRN	Mobile Station Routing Number
MVNO	Mobile Virtual Network Operator
NAT	Network Address Translator
NMSI	National Mobile Station Identifier
NSI	Network Solutions Inc
NTE	Network Terminal Equipment
OSS	Operation Support System
PDA	Personal Digital Assistant
PDP	Packer Data Protocol

PLMN	Public Land Mobile Network
PSO	Protocol Supporting Organisation
R&TTE	Radio and Telecommunications Terminal Equipment
RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLD	Second Level Domain
TLA	Top Level Aggregate
TLD	Top Level Domain
TWG	Terminals Working Group (GSM Association)
UCI	Universal Communications Identifier
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
VMSC	Visited Mobile Switching Centre
WAP	Wireless Application Protocol

1 Introduction

This Report has been produced jointly by an ad hoc group (TG-NA) consisting of members of the GSM Association, and the UMTS Forum, although it is published by the UMTS Forum. In order to provide adequate coverage of IP issues, TG-NA has co-operated with and welcomed inputs from experts of the IPv6 Forum. The ad hoc group has included manufacturers, operators and regulators.

The purpose of this Report is to assist operators, manufacturers and regulators in their preparations for UMTS by providing a methodical overview and analysis of the various numbering, naming and addressing issues that will occur with the introduction of UMTS. As such this Report is complementary to the standards work in 3GPP, ETSI and ITU and includes issues that are normally outside the scope of standardization.

The first part of the report provides:

- An overview of the migration to UMTS to explain the significance of the different phases described in Releases
- Information on the expected growth of the market to give an indication of the quantities of identifiers, names and addresses that will be involved
- Information on the market structure and how it will differ from that of the current second generation market in terms of players and organisation

This Report considers each area of:

- names
- addresses
- other identifiers

separately, and for each area provides an overview and then identifies the issues and which parties (e.g. operators, manufacturers or regulators) they will primarily affect. The Report does not aim to propose solutions for each issue but rather to increase knowledge and facilitate the development of solutions.

Several annexes are included to provide background on technical aspects and some of the various organisations involved with these issues.

The report is closely related to the work in 3GPP and uses the latest information available from 3GPP. The work in 3GPP on IP Multimedia is at a comparatively early stage and therefore it has not been possible to cover the naming and addressing of IP Multimedia as extensively as will eventually be necessary. In particular there is no coverage of mobility that is supported by methods other than the GTP Protocol that was introduced first for GPRS and is used for the earlier releases of UMTS.

The report does not address explicitly any technologies other than GSM/GPRS/UMTS-3GPP although some of the conclusions may also be valid for other 3G technologies.

2 Overview of Migration to UMTS

Mobile networks are migrating from the circuit switched phase 2 GSM to a multiservice IP based UMTS network. This migration is taking place in the following stages:

- GPRS will provide a core network overlay of IP to the circuit switched phase 2 GSM. The function of GPRS is to provide IP access via pipes (tunnels) from the mobile terminal to an ISP or corporate network at the edge of the mobile networks. The ISPs or corporate networks may be attached to either the visited or home network. GPRS will use the existing radio interface structure so that mobile terminals with GPRS are compatible with mobile terminals without GPRS. The overlay to the core network will have SGSNs and GGSNs which are the IP equivalent of VMSCs and GMSCs respectively. There will not necessarily be a one-one relationship between these switching elements in the two technology domains.

- UMTS Release 99 will introduce the new UMTS radio interface known as UTRAN instead of the GSM radio interface. The basic structure of the core networks will not change much from that of GSM with its overlay of GPRS. The core network will have IP based transport for the IP part and circuit switched transport for the circuit switched part. UMTS also provides a 64kbit/s circuit feature which can be used to carry IP traffic.

- UMTS Release 4 will add some functionality to Release 99 but will not involve substantial changes

- UMTS Release 5 (formerly known as Release 2000 - All IP network) will migrate the core network to a single IP network and add multimedia services based on IP. Release 5 networks shall use the PS domain (UE, UTRAN, SGSN and GGSN) and the IM (IP Multimedia) domain (CSCF, MGW + associated entities) to provide IP multimedia service support, such as voice, video etc. The PS domain shall provide the IP transport in the 3G domain, and the IM domain shall provide the Call (or Session) Control (using SIP - Session Initiation Protocol - an IETF IP based signalling protocol), and media conversion processes. The IM domain shall be connected to the PS (Packet Switched) domain via the GGSN node.

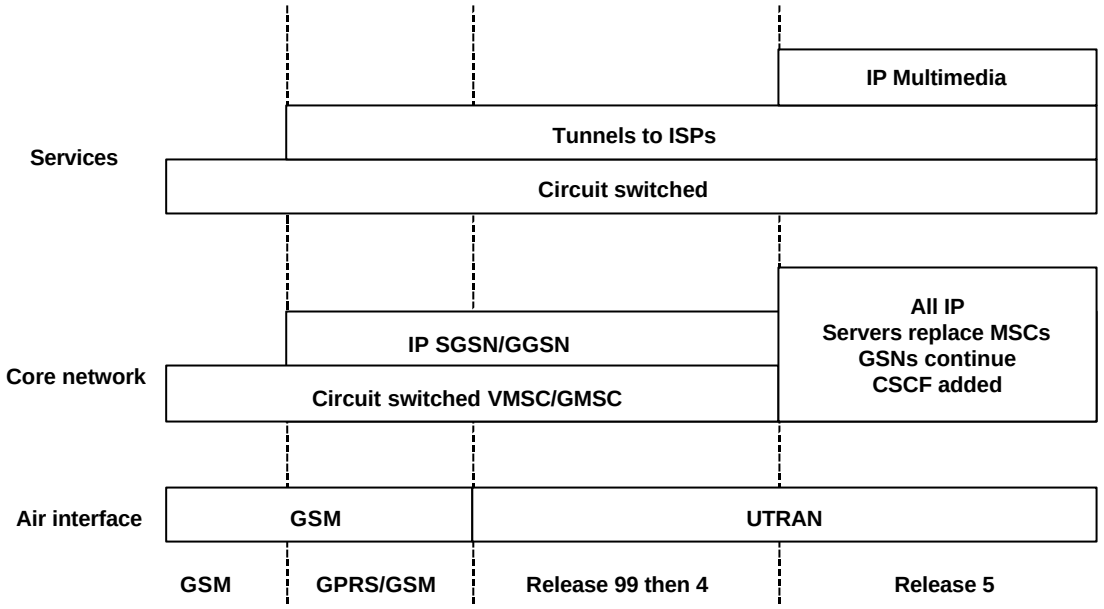
These phases are summarised in Figure 1

Figure 1: Phases of standards development

Phase	Radio interface	Core network	Services
GPRS	GSM	VMSC + GMSC SGSN + GGSN overlay	Circuit switched on GSM Access to ISPs via tunnel
UMTS Release 99	UTRAN	VMSC + GMSC SGSN + GGSN	Circuit switched on GSM Access to ISPs via tunnel
UMTS Release 4	UTRAN	As above	As above
UMTS Release 5	UTRAN	Common IP infrastructure VMSC + GMSC servers and media gateways SGSN + GGSN CSCF	 Circuit switched on GSM Access to ISPs via tunnel Multimedia

and shown diagrammatically in Figure 2.

Figure 2: Diagram of phases of standards development



These diagrams show the developments of the standards. They should not be misunderstood to imply that operators must make abrupt changes in technology, as they are likely to choose to support older technologies in parallel with newer ones until nearly all users have changed to terminals that support the newer technology.

Two of the objectives of Release 5 are that:

- Release 5 shall allow operators to choose to support circuit switched terminals built to Release 99
- Release 5 shall allow IP and circuit switched domains to operate alongside each other so that an operator can use a circuit switched Release 99 domain alongside an IP Release 5 domain

A very important concept in GPRS and UMTS is the tunnel from an SGSN to a GGSN that provides a transparent pipe to through which terminals may access ISPs. This tunnel is established during the PDP context activation by the GPRS Tunnelling Protocol (GTP). During this process the terminal uses the Access Point Name (APN) to identify the ISP with which the terminal is to register. This process is outlined in more detail in Annex C.

3 Market trends

3.1 Growth

The market that will be addressed by UMTS is expected to grow very rapidly. From the fixed network side:

- Traffic from the traditional telecommunications world to Internet Service Providers (ISPs) is growing at a very fast rate (in excess of 30% p.a. in many countries) and is still increasing. Overall Internet and IP based traffic is growing at 400% a year worldwide.

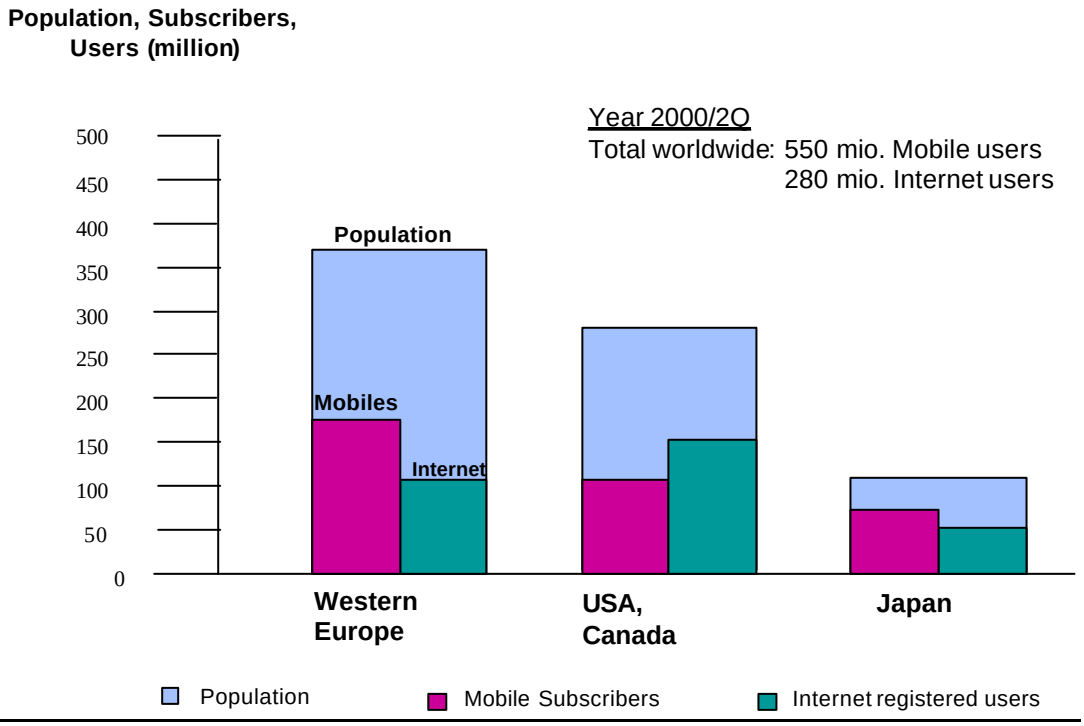
- Investment in cable technologies and DSL will open up a new and dynamic market to businesses, both small and large, and ordinary consumers.

- Web hosting facilities and the introduction of large server farms will also fuel the rapid build out of broadband networks with huge bandwidths. According to some analysts the worldwide Web hosting market will rise from the current figure of $3 billion (E2.9 billion) to $23 billion (E22.3 billion) by 2002.

There is also huge growth in the mobile sector.

Figure 3 shows the current market size.

Figure 3: Current market size

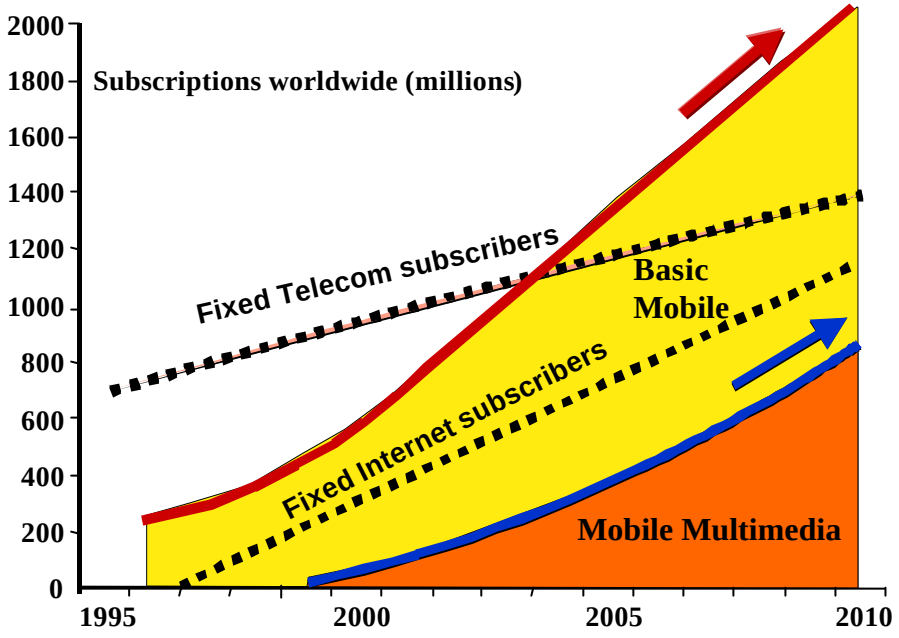


It has been estimated that more than 78% of Internet users also use mobile communications and this is a trend which will only increase with the introduction of 3rd Generation Mobile handsets that bring IP

to the handset. Bluetooth technology will also offer new ways of using mobile devices both for professional and personal use. Merrill Lynch estimates that growth in mobile data is expected to be 70% p.a. in the next 5 years. Data traffic will eclipse voice traffic on wireless networks by 2004. There is also a view that multimedia data will account for up to 60% of total mobile traffic in 2005.

Figure 4 shows some predictions for growth in Internet access from mobiles.

Figure 4: Mobile growth and Internet access capability



Source: UMTS Forum

UMTS will facilitate the integration of traditional mobile communications capabilities with data information capabilities and access to the Internet and Intranets, which will fuel demand. Initiatives like 'Bluetooth' and the rapid introduction of WAP technology, coupled with new types of terminals and digital assistants will serve to increase the demands on the world of naming and addressing.

There are a number of issues that will have an impact on the rate of growth and the technologies that will be used. They include:

- The provision of the “always-on” capability for users
- The quality of service over IP both in terms of communication quality for voice and real-time video, and the end-end delays in setting up and using interactive communications
- The development of new services and e-commerce

The e-commerce and entertainment sectors are already viewed as key markets, but there are also opportunities for business and industrial applications (such as remote learning and electronic publishing) and also domestic applications, where a variety household gadgets will also be controlled across 'the net'.

3.2 Market structure

UMTS is expected to lead to a change in the structure of the mobile market. The greatest growth will be in the areas of:

- Content provision
- Terminal manufacture

- Service provision

This will create a strong incentive for network operators to become service providers and content providers. They will therefore move into the areas currently served by ISPs. This means that they will have to start to handle Internet related naming and addressing and learn about ISP operation. These changes also mean that there will be an increase in the number of players in the mobile market as a whole.

4 Naming

4.1 Introduction

A name is a "combination of characters and is used to identify end users. (Characters may include numbers, letters and symbols)"[2].

An end user is "a logical concept which may refer to a person, a persona (e.g.. work, home etc.), a piece of equipment (e.g.. NTE, phone etc.), an interface, a service (e.g.. Freephone), an application (e.g.. Video on Demand), or a location".

A name is distinct in function from an address, which " identifies the specific termination points of a connection and is used for routing". Addresses are essential for communication as the end points always have to be identified in a way that can be used for routing, but names are not essential. Names are added for some services to make it easier for users to identify the distant end-point or to provide an identification system that is independent of the structure of the networks or the current location of the entity to be communicated with.

There are two common naming schemes:

- E.164 names (numerical strings) defined by ITU-T Recommendation E.164 – The International Public Telecommunication Numbering Plan. This scheme is a mixture of names and addresses. It started primarily as an addressing system but has migrated to become more of a naming system because location and operator portability are functions of names rather than addresses.

- names of the form "user@domain" defined by RFC 1035 - Domain Names - Implementation and Specification

The choice of identification scheme is related to the nature of the service because a service description needs to specify which type of name is used. This is important because:

- users need to know how to identify their correspondents
- the choice of identification system determines the set of potential correspondents that can be reached
- interconnected networks need to have a common method of identifying communicating users

For many services, names are used as the identification system, but some services allow addresses to be used as an alternative to names (e.g. http allows users to identify web sites by IP addresses or domain names), and some services use only addresses.

In the past services and hence name types were related to technology. For example telephony could be provided only on circuit switched technology and Telex had its own naming scheme and own technology. However, third generation mobile technology is designed to support multiple services and there is therefore the possibility of supporting more than one type of name.

4.2 General naming issues

4.2.1 Relationship of names to services and users

Normally each service that uses names specifies a single type of name that is used. However a type of name may be used by several different services. Sometimes these services are distinguished by different ranges as is the case of E.164. Where there is a separate method to identify different services, the same value of a name of the same type may be used for different services. For example a given

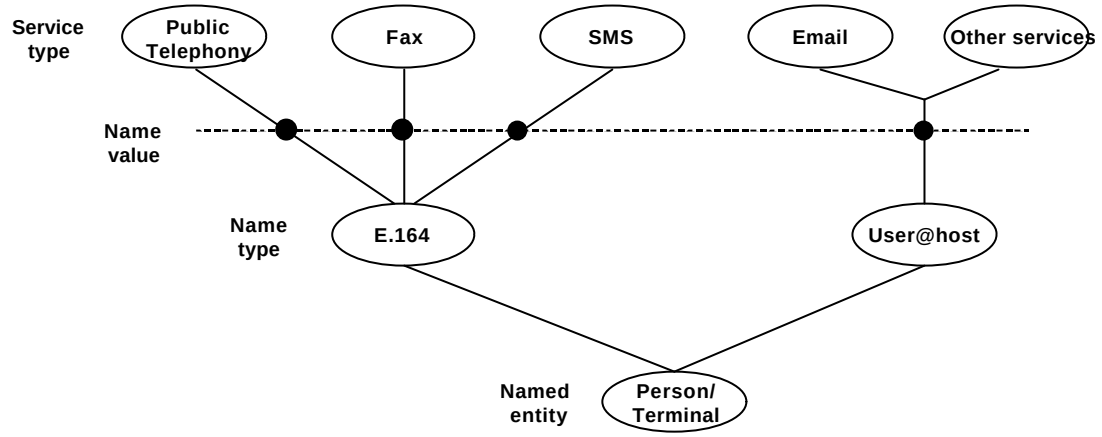
[2] According to ITU-T Recommendation E.191

E.164 number may be shared for both telephony and fax if the terminal can distinguish the services; similarly under Internet naming the same value of user@domain may be used for both email and various SIP based services.

A user may therefore have several names for different services, e.g. GSM users have three different E.164 names for voice fax and data services on GSM. This is not very user friendly because business cards become cluttered up with the different names. A reasonable long term objective could be to work towards having one name per person for private use and perhaps a separate name for business use, however this goal is constrained by the need for compatibility with existing systems.

Figure 5 shows an example of the relationship of named entities to name types and values for different services.

Figure 5: Naming relationships



A single name can also support several different users. Examples are an E.164 name for a telephone service in a house shared by several occupants, or an E.164 name used by a call centre, or an email name used by several people who fulfil the same function in an organisations (e.g. sales@company.com)

One name of the form "user@domain" may be used for several services. Even if these services are supported on different hosts, the SRV record in DNS can be used to point to the IP address of the relevant host. In most cases the host is operated or connected to a single service provider. Despite the SRV capability, a user that wishes to use one service provider for one set of services and another for another set will need different names unless special arrangements are made for DNS to receive different SRVs for the same name from different service providers.

Although the IETF has consistently distinguished names and addresses and introduced the public DNS to support the resolution of names into addresses, IETF does not define services or service capabilities in the way that ETSI and ITU-T do. This means that there is a lack of clarity in relating services defined in 3GPP to work in IETF. This lack of clarity in turn leads to some confusion over the choice of naming schemes for voice in IETF. Currently IETF is assuming the use of SIP as the main protocol for voice services and SIP addresses as the main name, with conversions to E.164 numbers where access from circuit switched networks is needed. This is very different in concept from supporting E.164 as the native naming scheme for telephony on SIP.

4.2.2 Information in names

Although the main function of a name in telecommunications is to provide a unique identification of the end user, considerable additional information may be provided. This additional information may be more or less explicit and may not always be beneficial. Examples are:

- the type of service (e.g. a number range in E.164 dedicated to mobile. This may also indicate the expected tariff level)

- the likely tariff level (e.g. freephone)
- the location (e.g. country code or area code)
- international networks (e.g. shared CC 882 in Rec. E.164)
- the service provider (e.g. the value of “domain” as in john_smith@compuserve.com)

A further form of information is an agreed association from digits to alphabetical characters shown on the keypad of a telephone (defined in ITU-T Recommendation E.161). This form of dialling is used commonly in the USA to support advertising e.g. “dial 1800CALLATT”. The associations used by mobile terminal manufacturers vary slightly and exact conformance to ITU-T Recommendation E.161 is recommended.

The provision of information can limit portability. For example geographic portability is restricted to the area specified by the location information in a name, although there are exceptions such as the use of country identifiers by organisation operating outside the country concerned. Several countries, including some large countries, assign Internet names to organisations outside their boundaries.

In E.164, the number block used does normally indicate the service provider but this information is not recognised by most users and so service provider portability can be supported.

The provision of explicit service provider information that is perceived by the user, such as when the value of "domain" includes the identity of the service provider is not readily compatible with portability between service providers. Names of the form “user@domain” can be portable between service providers without being misleading only if the value of “domain” is not the name of the service provider.

Most companies have their own domain name and the domain name can be hosted either on their own server or on that of an ISP. In contrast a name for an individual such as john_smith@compuserve.com links the user strongly to the service provider Compuserve. In theory such a name could be ported but the continued use of the name "Compuserve" would be misleading as Compuserve would no longer be the ISP. Some countries are starting to provide special domains for individual users who want portability but do not want to have to obtain their own domain name.

4.2.3 Service types supported on IP

Services supported on IP can be categorised roughly as:

- any-to-any
- client-host

Any-to-any services provides communication between end users. Examples are public telephony, facsimile and email. These services may use client-host type relationships in their provisioning (e.g. access to an email server) but the main focus for the user is on communication to another end user and therefore the naming system needs to identify end users uniquely. Any-to-any services typically use E.164 names or Internet names of the form “user@domain”.

Client-host services focus on access to facilities provided by a host, such as access to information on a web page. Client-host services make less use of E.164, although it could be argued that dialling into an information line with a voice or tone response system is a client-host service. In ICANN naming they use just “host” (e.g. web access).

The early releases of UMTS will tend to use IP for client-host services more than for any-to-any services. The IM capability when it is introduced may lead to more any-to-any services.

4.2.4 Backwards compatibility

Since naming determined the set of subscribers that can use a service and the value of any-to-any telecommunications is a very strong function of the number of users, backward compatibility is extremely important. It would be very difficult commercially to launch a new service that is largely an alternative to an existing service with a different naming scheme as users would wish to be able to

reach all the users of the other service. New naming systems can, however, be introduced for wholly new services and this has enabled the name type “user@domain” to be introduced for services such as email..

4.2.5 Human user aspects of names

Where communications are established by humans rather than machines, the human related aspects of names have some importance. This importance is enhanced by the relative under-development of directory services (see Section 4.2.6).

Communications (not just telephone but also data, fax email etc) can be categorized into three types:

A - Regular and frequent any-to-any communications between informal or formal groups (colleagues, family, other activities) for which the main issue is easy establishment

B - Occasional communications to advertisers or major organizations or services (transport, Government, large retailers) where the names needs to be easily memorable.

C - Occasional and largely random communications to other destinations

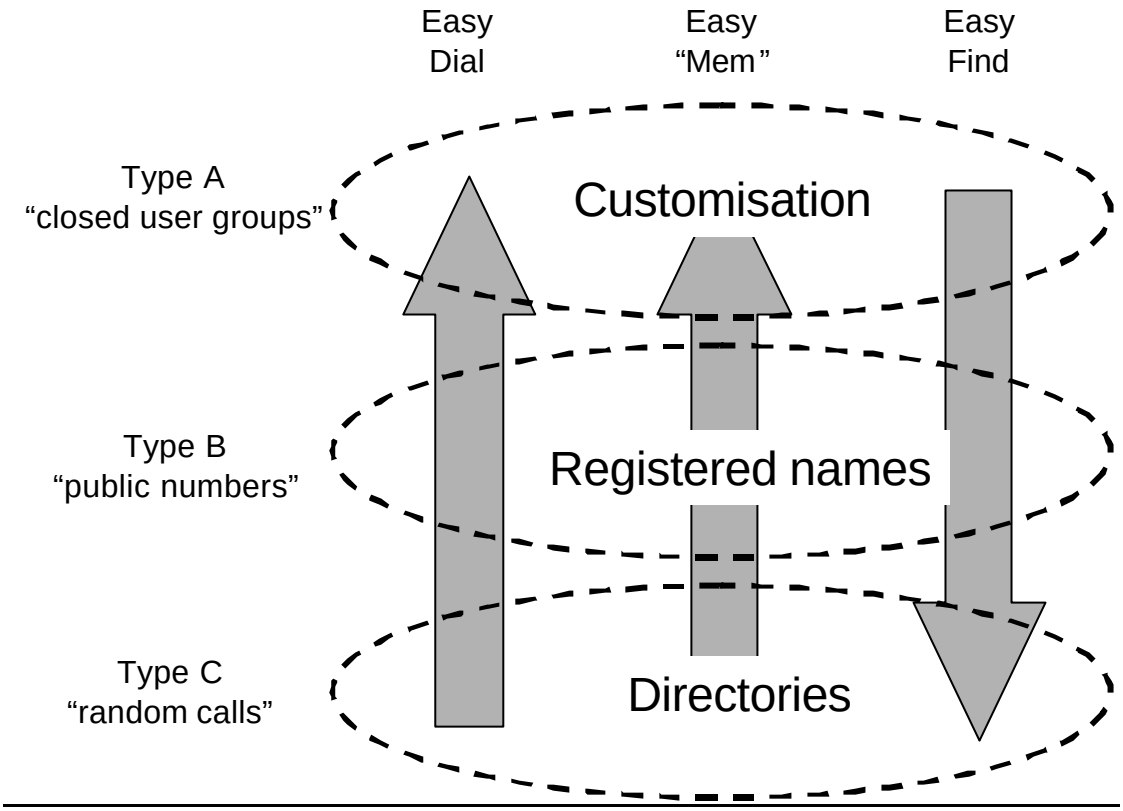
Type A requires the storage of names under customized strings as in personal address books. This requirement can be handled by developments in terminals. It does not require standardisation.

Type B requires human memorability. In E.164 this involves golden numbers or the relationship of a number to a memorable alphabetical string. However the scope for using these associations in E.164 is severely limited because of the problem of duplication especially for individual names. This is not a technical limitation but a limitation intrinsic in the established use of names. ICANN naming provides much more scope but is not without conflict.

Type C requires good directory services or search engines so that terminals can find out the correct number quickly from incomplete searching information when a call is initiated. Terminals should be capable of initiating connections by using the numbers or names obtained without the user having to re-enter (e.g. re-type or re-key) them.

These types are shown in Figure 6

Figure 6: Types of communication



For type A communications, names are being seen and entered less and less by human users due to the growth of:

- capture of caller's names by terminals
- name storage in address book functions in terminals

After the capture of a name a user normally finds the name by using a string that they assign to the name.

Nevertheless memorability is valuable for the period between a name being first presented to a potential caller and the name being entered in a terminal. Readability also helps users to enter names correctly.

User friendliness and memorability are limited because they conflict with uniqueness and so unique user friendly names are in short supply and there is thus a case for registration and careful allocation.

4.2.6 Directory services and search engines

Directory services and search engines enable users to find the formal names that are used by networks from other related information. Search engines are well developed for finding documents on the web but equivalent services for end-end communications are failing to keep pace with the general development of services because of the diversification of service provision and a reluctance by service providers to make available the information needed for these services. The problem is that the information in aggregate discloses the customer base of a service provider, which has great significance in a competitive market.

4.2.7 Related developments

4.2.7.1 ETSI TIPHON

Tiphon is developing a set of standards to support the provision of high quality telephony related services by operators such as the existing public network operators that are concerned with quality, security and call related billing. These operators are expected to migrate from a circuit switched network infrastructure to an IP based infrastructure. They are expected to maintain significant network boundaries and although they will be interconnected to the Internet, they are unlikely to become integrated into the Internet for the foreseeable future.

Tiphon is developing a structured set of standards ranging from service capability descriptions through to protocols and including a general purpose architecture. Tiphon is covering the use of both the H.323 and the SIP protocols and for each will specify a "profile and delta" that defines exactly how the protocol should be used to ensure interoperability in supporting specific services.

One of the main differences between Tiphon and IETF is that Internet is designed to provide stateless end to end connectivity once a session has been initiated. Tiphon is designed to accommodate the option of routing all communications through specific interconnection gateways. This option is expected to be needed in many cases because of:

- call related charging
- quality of service
- lawful interception

The working group that handles numbering within Tiphon has published guidance that E.164 numbers should always be used for public telephony services provided on IP based networks, with an option to use names of the form "user@domain" in addition, but not as an alternative. The use of E.164 numbers is considered to be essential because users of circuit switched telephony services will need to be able to communicate with users of IP based services. The choice of which part of E.164 should be used will depend on the precise characteristics of the telephony service. There was considerable confusion initially because some members of Tiphon advocated the use of a global code for all telephony services on IP but later it was clarified that the numbering arrangements should depend on the service details and not the technology used.

As signalling and media packet streams will need to be routed using IP addresses, Tiphon is currently completing the development of documents that describe a framework for resolving in several stages from an E.164 number to the IP addresses needed for routing. This frame work will encompass several different options from step-by-step routing (similar to that used in circuit switched networks) where each network determines only the IP address of the interconnection gateway to the next network, though to end-to-end routing s uch as is used in the Internet where the originating entity can determine an IP address for the host at the far end.

4.2.7.2 ETSI HF

The Human Factors group of ETSI has recently undertaken some work on the future requirements for naming. They have are proposing a new compound name (Universal Communications Identifier - UCI) consisting of three parts

- A unique numerical identifier related to a person that could be given on business cards and used eventually for service invocation as an alternative to existing naming schemes

- A natural name (e.g. John Smith) that would be presented with the unique numerical identifier as a calling identifier that could be stored in address book functions in terminals

- Information about the named person created and updated by the named person themselves, e.g. street address or keywords that could be used in searches. This information would be used primarily by databases and search engines

If this proposal is implemented, it would be introduced gradually as an overlay and the identifier would be useful for coordinating the contents of special purpose name translation databases. It is too early to consider this proposal as an alternative to E.164 or Internet names for UMTS.

4.2.7.3 ETSI SPAN

ETSI TC SPAN (Services and Protocols for Advanced Networks Group) has a subcommittee (SPAN-2) that deals with naming and addressing and than works closely with ITU SG2. To date it has mainly tracked and commented on the developments in Tiphon, HF and ENUM.

4.2.7.4 ENUM

ENUM is the name of a chartered working group in IETF. It is attracting a great deal of attention in relation to numbering and is supported by several large manufacturers. ENUM is the name given to a set of standards that define a protocol for Telephone Number Resolution.

The function of the ENUM protocol is to map telephone numbers, defined in ITU-T Recommendation E.164, to one or more Internet resources using the existing DNS system. Here a "resource" is an Internet destination that has an associated application protocol such as an email address or a SIP address. ENUM can also support mapping to resources outside the Internet such as fax and mobile numbers. The system is based on telephone numbers because these numbers are widely known and can be input from any telephone keypad.

The main functions of ENUM are to:

- enable calling users or entities to make a selection from the range of services that are available for communicating with a particular person or entity when the calling user knows only their telephone number.
- enable users to access Internet based services and resources from ordinary telephones where they are only able to input digits
- enable users to specify their preferences for receiving incoming communications (e.g. specifying a preference for voicemail messages over live calls or indicating a destination for call forwarding). ENUM will give much improved user control over communications.

In practice, a prime role of ENUM will be to facilitate the migration of traffic from circuit switched networks to the Internet.

When presenting a telephone number to the DNS, the digits are reversed and dots are inserted between each digit. ENUM is designed for users that have exclusive use of an E.164 number. It does not specify how shared E.164 numbers (e.g. a household with one line and E.164 number but several occupants each with their own SIP addresses for Internet telephony).

The issues currently being resolved are:

- What exactly will be the form of the top level part of the name to be resolved by DNS. IETF has proposed .e164.arpa and this proposal is being discussed with ITU-T.

- Which organisations will be registries and run the DNS servers for E.164 numbers. The assumption is that each Government will select the registry for numbers under its own country code but selections have not yet been made yet.

- What control will be exercised over the submission of E.164 numbers and associated information for storage in DNS. The aim is to ensure that only the legitimate user of an E.164 number can submit and alter information and that records are updated when E.164 numbers are ported or cease. This is difficult to achieve especially in countries where there is no national database of subscriber information. The issues are also related to privacy laws that differ from country to country.

The fundamental difference between ENUM and Tiphon is that:

- ENUM is using E.164 numbers that have already been allocated for service on circuit switched networks for directing calls that will be delivered via the Internet (i.e. on a different network). This is the source of the problems of authorisation and authentication.

- Tiphon is working on the support on IP (not necessarily Internet) of services that use E.164 numbers. In Tiphon calls are always delivered to the networks that provide the service associated with the E.164 number, thus the problems of authorisation and authentication do not arise.

Tiphon and UMTS are complementary to ENUM and not conflicting. UMTS users may subscribe to ENUM but that does not affect the use of names in UMTS. UMTS operators and service providers may be reluctant to authenticate their customers' use of E.164 numbers as ENUM may lead to loss of revenue from terminating traffic.

4.2.7.5 ITU-T

Study Group 2 of ITU-T has been tracking developments relating to numbering and naming for voice over IP. It has granted the temporary assignment of part of a global code (+878 878) to TTT Services for a VoIP service that provides personal numbering with full portability at a global level. These trials are expected to start in late 2000.

SG2 has also held a joint workshop with ENUM and is discussing the administrative arrangements concerning the use of E.164 numbers in the DNS system to support ENUM.

The following summarises the main work that is planned or underway within ITU-T:

- Under SG2 Question 1 (Numbering and Addressing), a new project "Global evolution of naming, numbering and addressing" will study the potential evolution of global numbering, naming, and addressing methodologies to accommodate current and anticipated future services, technologies, capabilities, and architectures.

- Under SG2 Question 2 (Routing) a new project "Address translation and routing for mobile and portable terminals" will develop methods for translating between E.164 and IP routing addresses, and the associated routing procedures involved. The scope will include interworking of fixed, wireless, and portable terminals across various technologies, including TDM-, ATM- and IP-based networks. A new recommendation will reflect new technologies, such as IP-based network capabilities, and reflect issues such as tracking the routing address mapping of E.164 numbers and/or names to IP addresses. The intention is to complement existing protocols, including DNS, Recommendation E.174 on UPT, and Recommendations E.212/E.214 on mobile station identity and global title derivation.

- Under SG13's IP Project, Work Area 5 is examining interworking between conventional telecommunication networks and IP-based networks. The project will also work on proposals for a long-term identification scheme to be used by end-user of electronic services in order to identify the recipient(s) of a telecommunication instance (call), regardless of the systems or protocols used

- Under SG13's GII Project, there is an examination of the addressing requirements for GII, which may be met by the use of an existing scheme with appropriate interworking mechanisms to other existing schemes. Some kind of extension to the scheme may be necessary to give the necessary capacity. If this is not possible a new universal scheme would be devised. From the user's perspective, names are easier to remember than addresses, and the development of a naming scheme together with the necessary directory system will be considered.

4.3 Issues for UMTS

4.3.1 Internal naming of ISPs - Access Point Names

For both GPRS and UMTS the intention is to use an internal naming system for identification of the ISP that a mobile wishes to log-on to. These names are called Access Point Names (APNs). More information is given in Annex C.

This naming system mostly uses names that are already registered for public use but the GSM Association registers names in other cases. The GSM Association also assembles and provides the information for DNS servers to be used by the operators.

Presumably the GSM Association will continue this role for UMTS.

Access to ISPs from mobile networks may become an area where regulators are concerned to ensure that there is no discrimination in favour of ISPs owned by mobile operators. Therefore it is recommended that published principles are developed about this access including the use of Access Point Names. Further study is needed in this area especially on the protocols used between the GGSN and the ISPs.

4.3.2 External naming

External naming concems the choice and allocation of names to UMTS users so that:

- other UMTS users and other non-UMTS users of the same services can communicate with them, and
- UMTS users can present appropriate calling identification in their communications

For client-host type services external naming is primarily an issue for the ISPs on the edges of the UMTS networks. These ISPs will serve the UMTS customers and register their name - IP address pairs in the global public DNS if the UMTS users are to be publicly accessible. Some UMTS users will choose to operate in private or restricted virtual networks and so will not be reachable from the external world.

Any-to-any circuit switched services under Release 99 & 4 will continue to use E.164.

For any-to-any services from Release 5 onwards the support of name types will become an issue for the mobile network operators and service providers, and will be related to the services provided.

The main issue for external naming is the choice of naming system. This is a separate issue for each service. Internet names are likely to be preferred for established Internet services and other new services. For services with a large number of users on switched circuit technology, E.164 is likely to be preferred. For telephony services provided by on IP under Release 5, the use of E.164 will be essential for compatibility with circuit switched fixed networks.

4.3.3 E.164 issues

E.164 is the number of the ITU-T Recommendation on “The international public telecommunication numbering plan”.

E.164 defines the structure and maximum length of its numbers and lists the values of the first 1, 2 or 3 digits that have been allocated to particular countries, global services or networks.

The allocation system for E.164 is described in Annex D. In mobile networks, the E.164 number is known as the MSISDN number in mobile systems.

For public voice telephony, E.164 is the obvious choice because of the commercial imperative for compatibility with PSTN/ISDN users. In many countries there are also regulatory requirements for the

presentation of CLI at least to interconnected operators for the support of access to emergency services and malicious call detection, and the systems used for these purposes are likely to remain limited to handling E.164 names for the foreseeable future.

Within E.164, the three main issues are:

- which number range should be used for UMTS?
- should portability be required between GSM and UMTS?
- how should new UMTS numbers be allocated - in bocks through operators and service providers or direct to users (individual allocation)?

4.3.3.1 Choice of number range in E.164

This issue and number portability are related in that if portability is required then UMTS will have to use the same number range as GSM. .

There are two forms of numbering and charging used for mobile services:

- calling party pays services with special mobile number ranges, as used almost very widely in Europe
- called party pays for the mobile termination with number blocks from the scheme for geographic services, as used extensively in the USA

For calling party pays, there are three arguments for allocating numbers for telephony on UMTS from the same number ranges as GSM, provided that the services and tariffs are similar:

- the service (mobile telephony) is essentially the same and numbering should relate to services rather than technology

- those operators with both GSM and UMTS licences are likely to want to be able to provide portability for existing customers who wish to migrate from one technology to another. Therefore UMTS must be allowed to use the same number range

- new market entrants who have only UMTS licences need number portability in order to be able to compete for customers of the GSM networks of the established mobile operators

Where new services or new tariffs are introduced that have no equivalent in GSM, the use of different number ranges could be advantageous or essential. For example, the UK is planning a special number range for multimedia services. Where multimedia services include a voice element that is compatible with telephony then the choice of number range will need careful consideration as some customers may wish to upgrade from their plain telephony service to multimedia whilst keeping the same number.

4.3.3.2 Number portability

Europe does not have a common policy on mobile number portability (for calling party pays), although the majority of countries appear likely to require portability. The Commission is proposing that all Member States should require mobile number portability, however it is not clear that all Member States will accept this proposal. The introduction of UMTS is expected to lead to requests for portability from new entrants who do not have a GSM system so that they can compete more effectively for GSM customers. If there is portability between GSM operators and between GSM and UMTS, then portability between UMTS operators can also be provided easily.

Number portability in GSM has included both portability between operators and portability between service providers[3], where number allocation involves service providers. It is not clear to what extent service providers will be involved in the provision of telephony over UMTS but if numbers are allocated through service providers then they should be included in any number portability requirement

[3] Organisations who resell airtime, not to be confused with ISPs

and given equal access to any number portability infrastructure such as a portability transaction database.

In defining requirements for portability, care should be taken over the definition of the services as the category of service may determine the range of numbers to be used within E.164.

4.3.3.3 Number allocation

Numbers for subscribers are normally allocated in blocks to operators and where appropriate sub-allocated in blocks to service providers. Individual number allocation has been introduced in a few countries for services such as freephone, shared cost, and premium rate services and for personal numbering services. Regulators may wish to consider whether there should be any requirements for individual number allocation for mobile services. Individual allocation has most value where users may wish to have memorable or branded numbers. It is unlikely that there will be a very strong case for individual number allocation for UMTS.

For called party pays, the numbering arrangements are part of the geographic scheme and should conform to all the requirements on those schemes, including portability with fixed services.

4.3.3.4 Multiple numbers per terminal

Second generation GSM uses separate numbers for telephony, fax and circuit switched data services provided from the same GSM terminal. With the rapid growth in penetration of mobile terminals, this could precipitate number shortages or number changes in some countries. It can also create difficulties for users. It would be preferable if a single value of E.164 number could be used for all services that are not normally distinguished in a way that is explicit to callers, provided that the tariff arrangements are similar or that there is adequate tariff transparency. The domain name system used by the Internet provides a single multi-service name

4.3.3.5 Data-only terminals

There may be a substantial prospective market for data-only terminals for applications such as telemetry and PDAs. The standards for GPRS and UMTS do not identify clearly which requirements would apply for data-only terminals, and it appears to be assumed that there will always be an ability to make circuit switched connections. This means that data-only terminals will require E.164 numbers (MSISDNs) even if these numbers are not required for any incoming calls. This requirement could increase significantly and unnecessarily the demand for E.164 numbers for mobiles. A possible solution could be to use a separate private numbering scheme if access from the public networks is not needed. This possibility should be studied.

4.3.3.6 Personal numbering

Personal numbering enables calls to be delivered to any terminal on any network according to information supplied to the personal numbering service by the called user. Therefore users who are called with a personal number may have calls delivered to a mobile terminal. This possibility will continue for third generation systems. Universal Personal Telecommunications (UPT), whose numbering scheme is defined in ITU-T Recommendation E.168, is a highly standardised but little implemented personal numbering service. Other non-standardised services are available in many countries.

Personal numbering provides an overlay of personal numbers on top of existing network specific numbers. Therefore it does not affect the numbering arrangements for the networks on which it is provided as it does not replace them.

4.3.4 Internet name issues

Internet names are the names used by the Internet community. This naming system is administered by ICANN (see Annex G). The names are written normally as “user@domain” where “domain” is the

domain name. The domain name is composed of a series of strings separated by "."s, e.g. "companyname.co.uk". The most significant component is to the right and is called a Top Level Domain or TLD.

More information on domain names and resolution into addresses is given in Annex B

Users with their own domain name are expected to wish to continue to use it for UMTS. Individual users at present normally include the identity of their service provider in their name e.g. user@<service provider>, thereby making the name non-portable. This limitation may be removed by the provision of new domain names for individuals. For example the Netherlands is introducing a system of portable names for individuals and a proposals have been made to ICANN for the introduction of a new gTLD .nom for individual names.

The UMTS Forum and the GSM Association have considered making an application to ICANN for new gTLD specifically for mobile users (e.g. .umts, .air. .cell. .mob). However neither had made an application by the deadline of 2 October 2000. It may be some 2 years until the next proposals are invited. Any proposal would have to include the plans for the provision of registry functions and the operation of the domain name servers. Mobile identification could also be included under ccTLDs e.g. .umts.uk but this is not so attractive in view of the increasing internationalisation of mobile communications.

4.4 Summary of conclusions and issues

4.4.1 Conclusions

Names are related to services and each service must specify the form of name to be used

Third generation technology can support multiple services and hence more than one type of name.

4.4.2 General issues

The choice of naming system should be specified in the service descriptions for each service.

Further study is needed on the access to ISPs to ensure that there are published principles acceptable to regulators. This concerns not only the use of Access Point Names but also the protocols between the GGSN and the ISPs.

Further study is needed on the support of data-only terminals and the use of E.164 numbers by these terminals.

4.4.3 Issues for Operators

Operators should:

1. Check that the GSM Association is willing to continue its role with respect to Access Point Names
2. Ensure that there are published and non-discriminatory principles for the registration of Access Point Names
3. Ensure the support of name (number) portability for E.164 numbers for services similar to those provided on GSM.
4. If practicable build in the capability to support the portability of Internet names in order to ensure compatibility with any future requirements
5. Explore the possibility of using a single E.164 number to be used for telephony, fax and data instead of having separate numbers.

4.4.4 Issues for Service providers

Service providers (ISPs) should:

6. Consider the use of a domain name for individuals that is not explicitly related to their service provider

7. Ensure that their administrative systems and procedures can support name (number) portability for E.164 numbers

4.4.5 Issues for manufacturers

8. Consider adherence to ITU-T Recommendation E.161 for the association of alphabetic characters to the numbers of the keypads of UMTS terminals and supplement it with a standard presentation for the "@" symbols.

4.4.6 Issues for regulators

Regulators should consider:

9. Consider if any regulation is needed on the portability of E.164 names (numbers) in countries where it is not already required. This would include portability between operators, between operators and service providers and between different service providers and, for called party pays, portability between fixed and mobile services

10. Consider if any regulation is required on the portability of Internet names

11. Consider which numbering ranges in E.164 should be used for services on UMTS (provided that the services/tariffs are similar, there is a good case for using the same ranges as for GSM as this will enable portability between GSM and UMTS)

12. Consider the use of new ranges of E.164 numbers for new emerging services, especially multimedia services under UMTS Release 5.

5 Addressing

5.1 Introduction

An address is defined as "a string or combination of digits and symbols that identifies the specific termination points of a connection and is used for routing"[4]. Addresses identifies the interface at which the connection is to be delivered without regard to whether the connection continues beyond that interface. They contain location information and in telecommunications this is expressed in terms of the network structure in order to achieve as high as possible a degree of aggregation that reduces the complexity of routing tables in switches or routers.

Addresses differ from names in that addresses contain explicit network information and this information is what makes them usable for routing. In order to route a call or a packet, the called name must be translated into an address which identifies the location in network terms and so can be used in the routing process. When a name is ported from one location or one service provider to another, the address associated with the name changes.

Unfortunately the distinction between name and address is not followed consistently and entities that are names, or closer to names than addresses, are often spoken of as addresses. A Uniform Resource Locator (URL) pointing to a company's web page is often called an Internet address, but is actually based on a domain name

Three types of address need to be considered for UMTS:

- IP addresses
- Mobile station roaming numbers
- Routing prefixes for E.164 numbers

X.121 is not considered because there is very little interest in using it for GPRS or UMTS.

5.2 IP addresses

5.2.1 Use in UMTS

IP unicast addresses identify interfaces, which are end-points for IP packets (multicast addresses identify groups of participating addresses). IP addresses are used in three different ways in UMTS. They are used for:

- end-points within the GPRS/UMTS network infrastructure (e.g. SGSNs and GGSNs, where the addresses are assigned and managed by the GPRS/UMTS operators)
- mobile terminals connected across the mobile network to an ISP, where the addresses are assigned and managed by the ISPs
- mobile terminals in multimedia services (Release 5 only), where the addresses are assigned and managed by the ISP that owns the CSCF although details are not yet specified

The use in the network infrastructure is not visible to the external Internet world in GPRS and UMTS Releases 3 & 4, visibility may be possible in Release 5. These addresses are used by the internal GPRS tunnelling protocol for setting up tunnels between the SGSN and, when roaming, the border gateway. Each tunnel supports a segment of the communications path between a specific mobile and the ISP that it is logged-on to.

Assignment of addresses to mobile terminals is necessary to enable them to communicate with the external Internet world. In Release 99 the IP addresses are assigned to mobile terminals by the GGSN

[4] According to ITU-T Recommendation E.191

that they are using. Communications to and from the mobile use this address, which is carried without alteration or inspection through the tunnel.

IP unicast addresses are functionally divided, in principle, into two parts:

- The identity of the network (the network part)
- The identity of the interface attached to the network (the host address, which is the destination of the IP packet)

The range of addresses allocated to ISPs may be chosen to provide aggregation, i.e. ISPs that are connected to the same transit (backbone) operator may have adjacent allocations.

The identity of the interface is assigned and managed by the network operator.

There are two versions of IP protocols, whose address formats differ significantly:

- IPv4, a 32-bit address, which is used throughout the Internet but which is considered to be in increasingly short supply and whose allocations are being controlled carefully

- IPv6, a 128-bit address, which is just starting to be used and should provide more than adequate capacity for the future.

Annex F gives more information on the structure and allocation of these addresses.

Annex E gives information on the compatibility of these two different forms of address, which are not fully compatible with each other. It also outlines the methods by which nodes that use IPv6 addresses may communicate across domains that use only IPv4.

5.2.2 Support of mobility

The way in which mobility is supported in GPRS and UMTS Releases 3 & 4 is already defined in standards. The method for IP Multimedia (Release 5) expected to differ and is not yet defined (but see 3G TR 23.923 for further work on mobile IP).

5.2.2.1 Support of mobility in GPRS and UMTS Releases 3 & 4

Mobility is supported by providing a virtual connection between the terminal and a GGSN in either the visited or home network. This virtual connection is provided in two segments:

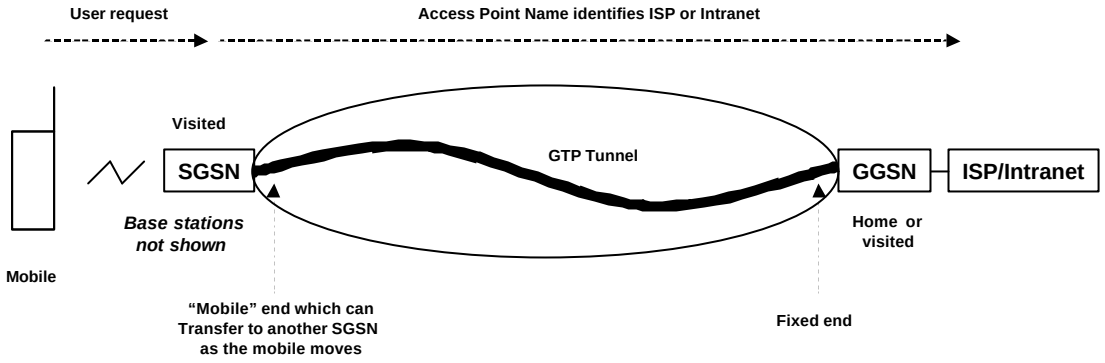
- Between the mobile and the visited SGSN by the procedures used for the air interface
- Between the visited SGSN and the GGSN by the GPRS Tunnelling Protocol (GTP)

This virtual connection is maintained as long as the mobile remains “on” and the mobile end of the GTP can be moved if the mobile moves from the coverage area of one SGSN to another. One can think of the mobile being linked to the GGSN by a global elastic pipe. All communications pass through the GGSN at the fixed end of the GTP. To the external world, e.g. the Internet or Intranet, the mobile appears to be located at the GGSN because the GGSN provides the IP address for the mobile.

The user has a choice of GGSN and can either log-on to the visited or home GGSN. This choice may be influenced by the roaming agreements between the operators concerned and the home operator can prevent the mobile from logging on to the GGSN of another network. The user’s choice is expressed through the Access Point Name (APN).

Figure 7 illustrates this form of mobility.

Figure 7: Mobility in GPRS and UMTS Releases 3 & 4



This process is described in more detail in Annex A and the Access Point Name in Annex C.

The GTP tunnel and the mobility used in GPRS and Releases 3 & 4 has been defined by ETSI/3GPP. This flexible tunnel technique is similar to the Mobile IPv4 enhancement defined by IETF in RFC 2002 and draft-ietf-mobileip-rfc2002-bis-03. In both cases all communications pass through the fixed end of the flexible tunnel.

5.2.2.2 IP Multimedia under Releases 5 & 6

Mobility for IP multimedia may be different because it will be based on IPv6. There is a mobility enhancement of IPv6 (draft-ietf-mobileip-ipv6-12.txt) which can create an association (binding) of:

- A static IPv6 address for the mobile terminal assigned by the home network
- A dynamic "care of" IP address assigned by the foreign agent (visited SGSN)

Both addresses are used in communications and this association allows packets to be routed to and from the mobile without having to pass through the home network, providing more efficient routing. At the same time the use of the static IPv6 address enables the other features of IPv6 such as security to be used, since they depend on the availability of a static address.

It is not yet clear to what extent this feature of Mobile IPv6 will be used in Release 5. Currently mobility for R5 will be based on GPRS and GTP tunnels, with real time handovers at the radio and core network level.

The use on Mobile IP to provide mobility is covered under 3G Release 6 (although there is an initiative to bring this forward) - as are other options to remove GTP and make core network routing more IETF IP based.

Mobile IPv6 also supports the flexible tunnel technique used in Mobile IPv4.

5.2.3 Access to Internet service providers and Intranets

Under GPRS and UMTS Releases 3 & 4, the user may select an ISP or Intranet using the Access Point Name. However, according to the standards, the mobile is assigned the IP address used for external communications by the GGSN and not by the ISP or Intranet.

The standards do not appear to define in detail the relationship between the GGSN and the ISP or Intranet, nor the types of connection that the GGSN may require. For example it could be argued that the GTP should be extended to the ISP or Intranet or that an additional tunnel segment should be added. Equally it is not clear whether the ISP or Intranet must have a leased line connection to the GGSN or whether any ISP or Intranet could be accessed over the public Internet.

This relationship is important commercially and may be of concern to regulators who wish to ensure that there is open access from mobile terminals to any ISP or Intranet. There is a need for agreements and formal documentation giving technical guidelines about the relationships and connection arrangements between network operators and ISPs/Intranets. It should cover items such as:

- interconnect guidelines;
- the implication of interconnect guidelines regarding the allocation of the IP address to the mobile;
- the identification and development of technical specifications required to implement technical guidelines.

The GSM Association should take responsibility for this work. It is a matter of urgency that standardization in 3GPP receives clear advice on these items. The UMTS Forum may assist with expertise, if required.

5.2.4 NATs, Firewalls, security and the end-to-end paradigm

The intention of the Internet was to make all communications end-to-end with stateless networks and public addressing. This would allow the networks to be simple with all intelligence at the periphery giving maximum scope for innovation. Routing would be simple and robust because packets would be routed around any broken links.

Despite this intention, the current Internet is not able to follow the end-to-end paradigm because Network Address Translators (NATs) have been introduced to decouple the internal addressing of corporate networks from the public addresses used, and some firewalls use address translation as a security measure. In summary various solutions have been introduced to handle practical problems for which tools compatible with the end-to-end paradigm were not available. In addition the telecommunications community has moved to IP and brought its own concerns about control, lawful interception, quality of service and billing based on call durations, all of which are not readily compatible with the end-to-end paradigm.

The hope of the IETF community is that IPv6 with its richer set of built in features will facilitate a return to the open network end-to-end paradigm. The introduction of IPv6 will limit the use of NAT to today's level and, in time, as people migrate to IPv6 will eventually restore the end-to-end paradigm of the Internet. However, It is not clear yet which strategy commercial operators will chose with respect to IPv6 implementation. Existing IPv4 Network Service Providers (NSPs) and customers may deliberately migrate from IPv4 to IPv6 (migration scenario) or IPv6 will gradually be integrated into networks and applications to support new services and new customers (integration scenario**).**

The views taken by operators will certainly influence the migration from IPv4 to IPv6. Their decisions will be based on objective analysis but could be influenced by unfounded fears and aggressive marketing by manufacturers

The UMTS Forum cannot judge at this time how well founded the concerns about network boundaries are. No forecast cam be made on how soon operators will be willing to return to or at least towards the end-to-end paradigm. Further study of these issues especially in relation to migration to IPv6 is needed.

5.2.5 Choice of IP version

The GPRS (Release 98) and UMTS (Release 3,4 and 5) specifications allow a choice of IP version (IPv4 or IPv6) in the PS domain but UMTS Release 5 specifies IPv6 for the IM domain.

All GPRS networks today use IPv4. There are many reasons for this with the most significant being that all available infrastructure and terminals today are based on IPv4.

IPv6 appeared only recently on vendor's product roadmaps. Use of IPv6 will probably become practicable during 2001. Terminal manufacturers are faced with decisions on when to introduce IPv6 with dual stack working alongside IPv4 in order to give users the option to use IPv6 based services. The rate of migration will depend on the introduction of IPv6 for Internet services and the advantages

offered for these services. Operators will then be faced with deciding when to migrate from IPv4 to IPv6 with some of them hesitant waiting for more stability in the production lines.

In the absence of any other reason to start earlier, UMTS operators will have to start to introduce IPv6 in the IP Multimedia domain when they start to implement services based on Release 5 of the UMTS Standards from around 2003/4 onwards. The IP Multimedia domain can be considered to be a standalone area of the network and is in addition to the packet domain currently being implemented as part of GPRS etc rather than being a replacement.

The more difficult question is when to migrate the PS domain that has been installed as an IPv4 based infrastructure to IPv6. The PS domain for UMTS Release 5 can be IPv4, IPv6 or dual stack, some compatibility with IPv4 will be required if the installed base of GPRS terminals and services needs to be supported by the common PS.

There are three potential drivers for moving to IPv6:

- Meeting the requirements in the standards, for example IPv6 is required for the IM domain
- Avoiding problems when IPv4 addresses reach exhaustion
- Obtaining benefits from features that IPv6 offers that are not available in IPv4.

We therefore explore these drivers, and then consider the practical issues of migration.

There is however a disadvantage. The IPv4 header has a variable length with the minimum being 192 bits. The IPv6 header has a fixed length of 320 bits, with the possibility of additional extension headers that are normally used only by the end nodes. The fixed header length simplifies the packet handling in routers but the increased length reduces the efficiency of transmission unless header compression is applied.

UDP has 64 bit header and TCP a 224 bit header. Therefore the maximum reduction in efficiency is 33%[5] for a zero length packet. However for speech for a 4kbit/s speech codec with a packetisation delay of 40 ms the speech packet would have a length of 4000*0.04 = 160 bits and the efficiency reduction would be 24%. For data using TCP the minimum reduction for a zero length packet would be 33%. Thus the reduction in efficiency is greater for speech than data.

A significant uncertainty is the speed with which IPv6 will be introduced generally in the Internet world. Here there are two extremes and a continuum of possibilities between them.

- The first extreme is that ISPs will perceive some real operational advantage in using IPv6 and will introduce it as soon as possible in order to capitalise on these advantages.

- The other extreme is that ISPs will regard the introduction of IPv6 as an avoidable expense and will delay its introduction as long as possible, i.e. until the shortage in IPv4 addresses begins to be felt.

There is no common view on these issues within the UMTS Forum.

5.2.5.1 Requirement in the standards

UMTS Release 99 offers options to use either IPv4 or IPv6 (see 3G TS 23.003 V3.5.0 June 2000 section 3.7 and 3.8) for mobile terminals and specifies that either permanent or temporary allocation may be used. In practice they will need to support IPv4 for general compatibility and may choose to support IPv6 as well with a dual stack.

UMTS Release 99 TS 23.003 specifies that the GSN address may use either IPv4 or IPv6, but the GTP specification TS 29.060 specifies that IPv4 is mandatory and that IPv6 is an optional addition.

UMTS Release 5 specifies in 3G TR 23.821 V1.0.1 (2000-07) section 11.1 that:

[5] 100*((320+64)/(192+64)-1)

- network elements of the IP Connectivity services (between RNC, SGSN and GGSN) and IP transport for the CS Domain may continue to use either IPv4 or IPv6
- terminals shall be able to access data services based on IPv4 and IPv6
- network elements for the IP multimedia services shall be based exclusively on IPv6

This situation is summarised in Figure 8.

Figure 8: Standardisation phases

Phase	SGSNs GGSNs etc	Mobile terminals and external services	Network elements for IP multimedia
GPRS Release 98	IPv4	IPv4 or IPv6 In practice it will be IPv4, IPv6 optional	
UMTS Release 99, 4	IPv4, IPv6 optional	IPv4 or IPv6 In practice it will be IPv4, IPv6 optional	
UMTS Release 5	not yet decided, possibly the same as R99	IPv4 and IPv6 (IPv6 exclusively for multimedia)	IPv6 exclusively

For the core network prior to UMTS Release 5, the main issue is the support of the GPRS tunnelling protocol. The specifications concerned are:

- GPRS Release 98: EN 301 347 (GSM 09.60)
- UMTS Release 99: 3G TS 29.060
- The equivalent specification for Release 5 has not yet been drafted.

Implementation of IP Multimedia under Release 5 is expected to start in about 2003, although it could be delayed. IPv6 will be essential for IP Multimedia.

The specifications for the GTP from release 98 onwards accommodate both IPv4 and IPv6 as addresses for terminals. These addresses pass transparently through the tunnel and therefore the version used by the terminal and service is independent of the version used by the core network in support of the tunnel.

Operators are therefore faced with decisions about when to introduce IPv6 into the PS domain of their network, starting with dual stack working, and whether to do so in advance of needing IPv6 for IP Multimedia. This decision will be influenced by their views on IPv4 address exhaustion and feature advantages of IPv6. Cost and availability of mature IPv6 equipment will also be taken into account.

The issue of when eventually to withdraw IPv4 is beyond the timeframe covered by this report.

5.2.5.2 Demand for addresses and IPv4 exhaustion

Many of the arguments surrounding the possible advantages that could be achieved through a move to IPv6 focus on the increase in address space, so this section looks at address space requirements and assesses the demands from the market sectors that will primarily drive demand.

IPv4 has a 32-bit address size and with the introduction of IPv6 the address size will be increased to 128 bits. Although initially IPv4 was considered robust and scalable (it had the ability to uniquely identify over four billion nodes), the rapid increase in demand coupled with the inflexibility of assigning addresses in strict 'Classes' led to problems. Whilst the introduction of CIDR (Classless Inter-Domain Routing) enabled these restrictions to be overcome, there is substantial concern that the capacity of IPv4 will be exhausted within the foreseeable future, possibly within the next few years. In

contrast, IPv6 allows 10 to the 38^{th} power possible addresses, which is in practical terms an almost infinite number and accepted to be more than enough for at least the next 30 years.

Although IPv4 has a theoretical capacity of some 4 billion ($4*10^9$) addresses, in practice a realistic maximum is probably some 200 million hosts. The lower practical limit is the result of the structuring of the address space and is a prediction based on observations of the points at which other numbering schemes reach saturation[6].

It is very difficult to obtain a well founded estimate of the current world-wide situation on allocations or when the effects of exhaustion will first be experienced. According to a paper on the IANA part of the web site[7] of the Information Sciences Institute, there were in October 2000 some 102 unallocated /8 IP addresses out of the maximum total of 256. There were 23 allocations to the Regional Internet Registries who currently handle the allocations to ISPs and large users. The demand for allocations from these RIRs is doubling every year according to RIPE, suggesting that a further 2-3 years' growth can be accommodated without making other changes. However the remaining 131 values are allocated to organisations and large corporate and eventually some of this space could be released if necessary.

There are many 'variables' that make estimation of the remaining life of IPv4 difficult to quantify including:

- the use of Network Address Translators to increase the utilisation of IPv4 address space,
- WAP proxy server deployment (similar to NATs in terms of saving IP address space),
- the impact of dynamic address assignment in an 'always on' environment,
- the possible impact of Windows 2000 which will include IPSec and lead to an increase demand for secure end to end communication, (currently the use of NAT inhibits end to end IPSec),
- new demands from the 'plug and play' (auto configuration) market.

Estimates of the number of IPv4 addresses needed for GPRS/UMTS are made separately for infrastructure and terminals:

- For infrastructure, the GSM Association estimates suggest there are potentially 400 GPRS/UMTS operators and that each operator is likely to need to address up to 2000 elements. BT in contrast has estimated that addresses for up to 1000 elements will be needed within a five year period. This gives a total of 0.4 – 0.8 Million addresses for infrastructure purposes, which should not pose any significant problem.

- For terminals, some sources, including the EMC World Cellular Database, forecast that demand for GSM, GPRS and UMTS terminals is most likely to be around the 500 million mark by the 2004/2005 timeframe. This would be much more than the capacity that is available in practice if every terminal needs an IP address, but there will be some economies from dynamic allocation and use of existing spare capacity within the allocations already held by some ISPs.

In conclusion it does appear likely that some effects of IPv4 address exhaustion will begin to be felt in the 2004-2006 timeframe.

When eventually IPv4 becomes seriously exhausted, new allocations will be possible only from IPv6. This will mean that equipment with only IPv6 addresses will be able to communicate only with other equipment that have IPv6 and therefore communications with the IPv4 world will not be possible. This will be a significant commercial issue and therefore the introduction of IPv6 should be encouraged in order that it can become as widespread as possible before IPv4 exhausts so that the loss of compatibility will be minimised.

In view of the prospective exhaustion of IPv4 and its continued use as the default protocol for the core network for all services other than IP Multimedia, operators should take early steps to obtain adequate IPv4 allocations for their core networks. The GSM Association should work with the IPv6 Forum to develop guidance on the introduction of IPv6 in UMTS networks.

---

[6] See RFC 1715 by Christian Huitema

[7] http://www.isi.edu/in-notes/iana/assignments/ipv4-address-space

5.2.5.3 Feature advantages of IPv6

The following are the main advantages of IPv6 some of which are relevant to the mobile environment:

Addresses: IPv6 has an enlarged address space that will enable all terminals to have a globally unique IP address for the duration that it is connected to the network. This will enable services and applications to be developed without having to take into consideration network issues like NAT etc. Usage of multiple addresses for one interface is also supported in IPv6, that can be useful for creation of services.

Conservation: IPv6 will restore the paradigm of end-to-end functionality. This was disrupted by NAT (Network Address Translation), where the address of a packet from the internal network (mostly using private addresses, not routable in the Internet) has to be exchanged for an official IP address to be routed on Internet. This is decreasing performance as every packet has to be analysed and its header changed. This breaks checksums, end-to-end Security and applications, that needs a fixed IP address such as some forms of IP Telephony.

Routing: IPv6 uses a routing hierarchy with aggregation. In the old days of the Internet the address spaces have been distributed all over the world without any really idea how the routing can be constructed based on this distribution. This changed with the introduction of CIDR (Classless InterDomain Routing), and the registries created allocation policies supporting route aggregation and appropriately sized address ranges. This has slowed down the dynamic growth of the routing tables in the whole Internet but it cannot reverse the mistakes of the first ten years and the large and unstable routing tables that remain. Renumbering is difficult and changing the provider either involves renumbering or creates holes in the aggregation block of the old provider, increasing the routing tables. IPv6 will provide hierarchical address allocation that theoretically limits the number of entries in the routing tables to about 8000 compared to some 90,000 with IPv4 at present. In practice if routers operate in a dual stack mode their routing tables will be a combination of the IPv4 and IPv6 routing tables i.e. larger. In time as IPv4 diminishes the routing tables will reduce in size but not to the theoretical minimum because of private sTLA peering arrangements. The true advantage of IPv6 to routing is that it is probably impossible to operate an IPv4 network with Billions of users but is conceivable possible with IPv6.

Plug&Play: IPv6 reduces the administration and management overhead by making plug & play really work. Autoconfiguration works together with the Dynamical Host Configuration Protocol and the Domain Name System, so the system administrator is not forced to configure every workstation and PC manually. The address is a combination of a routing part (prefix, 64 bits) and a host ID (EUI-64, 64 bits). The autoconfiguration mechanism reads the MAC address or any other IEEE address available on the adapter and composes a network wide valid ID. The prefix is provided by a local facility and can be changed if necessary (change of provider) without difficulty and without manual reconfiguration of the hosts. The cost savings in administration and management can be quite substantial.

Mobility: IPv6 supports mobility much better than IPv4.. All IPv6 networks and nodes are ready for mobile IPv6. IPv6 Neighbour Discovery and Address Autoconfiguration allow hosts to operate in any location without a special support. The performance is improved because of traffic optimisation. The flexible address structure is well suited for roaming. Extended security concepts might be adopted to meet the higher requirements from the mobile world.

Header structure: IPv6 has an optimised header structure. Unlike IPv4, the header of IPv6 has a fixed size and fewer fields. This may lead to faster hardware based routers although most first generation implementation will not be hardware assisted. The fixed length streamlined header structure will also enable firmware oriented implementation to be possible and support effective compression. The header structure also allows for extension headers that in the interest of efficiency are only processed by nodes that require access to the information. The extension header structure of IPv6 also provide some degree of future proofing, as new features and facilities can easily be added.

Security: IPv6 will provide means for privacy and security as an integral part of the standard rather than as a separate protocol. With IPv4 the IPSec protocol is used, which is not different in principle to

IPv6, but is very complex and difficult to use. Before IPSec can be used in a communication, it requires a check to see if the peer is supporting IPSec at all and what are the implemented features.

5.2.5.4 Areas of IPv6 that are currently being investigated

There are a number of areas relating to IPv6 that are currently being studied and investigated. Below is a non-exhaustive list of items that will have to be resolved before any large-scale deployment of IPv6 can occur:

- Interworking: IPv6 is not backward compatible with IPv4. The IETF has been very actively working on this topic and has specified a multitude of interworking mechanisms. There is still a very active ongoing debate as to the most appropriate migration and interworking mechanisms that mobile networks should employ. It is up to the user to make a choice which tools are matching his special needs best.

- There is currently very little commercial development for an Operation Support System (OSS).

- IPv6 has a very good hierarchical address structure. This however does not lend itself to efficient multi homing. Current proposals for IPv6 multi-homing are as good as IPv4 but work is still ongoing within the IETF.

- All routers employ some form of address based filtering, IPv6 with its longer addresses will potentially require these filtering arrangements to be altered – further research and development in this area is required.

- Header compression especially for small packets (VoIPv6) is important for mobile networks.

- IPsec is mandatory in IPv6, the associated architecture (key management etc) to support this needs to be understood.

- The operational costs of running a dual protocol networks against an IPv6 only network with interworking needs to be quantified.

- New procedures and methods need to be established between operations and customers to enable simple exchange of IPv6 address information.

5.2.5.5 Co-ordination between operators introducing IPv6

Two questions arise about the change to IPv6:

- Will the UMTS operators have to synchronise the changes with each other?

- Will the UMTS operators who change to IPv6 need coordination to enable them to use IPv6 with other such operators?

The answer to the first question is that there is no absolute requirement for synchronisation to maintain compatibility because implementation of IPv4 will remain mandatory and therefore operators will continue to have the option of using IPv4 for tunnels from an SGSN in one network to a GGSN in another and for allocation of IP addresses to visiting terminals. Therefore each operators can introduce IPv6 when they wish to without having to synchronise with other operators. However , some synchronisation of the introduction of dual stack and gateway translation capabilities in GGSNs would be advantageous

The answer to the second question is “yes”, co-ordination will be needed in two areas:

- A new, IPv6 compatible version of the internal DNS will be needed for APNs and any other name resolutions for the mobile operators need.

- Operators will need to cooperate about the use of IPv6 and will therefore need a mechanism for exchanging information about their use of IPv6 and their use of transition tools, e.g. IP addresses used for IPv6 tunnels across IPv4. Whilst exchanges could be bi-lateral, there would be great advantage in multi-casting information through a central email exploder or a web site and in producing guidance on recommended practice.

5.2.5.6 Conclusion on migration from IPv4 to IPv6

Although 3GPP has decided to base the IP Multimedia development on IPv6, there is no common view on the timing for the introduction of IPv6 under the earlier releases. This area needs further study and operators will need guidance and support over the introduction of IPv6. The best way to study these issues is to start to prepare the guidance as this process will help to identify the many detailed practical issues that will need to be worked out.

The recommendations are therefore that:

- The GSM Association should facilitate the introduction of IPv6 by providing mechanisms for operators to exchange information about their plans for introducing IPv6 and the transition tools that they will use

- The GSM Association should produce a guide and recommended procedure for the introduction of IPv6.

Although operators may not need to start migrating to IPv6 immediately, it is important that this work should be undertaken reasonably soon to obtain a deeper understanding of the issues and the time that will be needed for migration.

5.2.6 Temporary or permanent assignment

IP addresses are assigned either permanently or temporarily and the choice is not covered explicitly in the standards yet.

Assignments to core network equipment will almost certainly be permanent and there is no problem with this choice for both IPv4 and IPv6.

For the assignments to terminals, the situation is different for IPv4 and IPv6.

5.2.6.1 Assignment of IPv4 addresses to terminals

IPv4 will be used only with GPRS and UMTS Releases 3 & 4. The IP addresses of the terminals are assigned by the GGSN selected by the user and therefore different GGSNs may be selected at different times. This means that the assignment of IP addresses needs to be temporary. If, however, the home network chooses to prevent the user from setting up PDP contexts to visited GGSNs and allows them to be set-up only to the home GGSN, than permanently assigned addresses could be used.

It is possible also that there could be an assignment of addresses to mobiles by ISPs or Intranets but this awaits further study.

The use of temporary IPv4 addresses should not create any particular problems.

5.2.6.2 Assignment of IPv6 addresses to terminals

There will be potentially conflicting requirements about the assignment of IPv6 addresses to terminals under UMTS Releases 3 & 4.

- If users are to be offered the opportunity to set up PDP Contexts to any GGSN, not just their home GGSN, then dynamic assignments will have to be used.

- Some of the feature advantages of IPv6 need to be supported by addresses where at least the interface identifier is fixed although the routing prefix may change and would be lost with dynamically assigned addresses.

This issue needs further study. One solution may be the use of multiple static addresses each associated with a different GGSN, but the practicability of this approach is very doubtful.

For IP Multimedia (Release 5), the architecture is still under development and there may be a conflict between using static addresses and enabling a competitive service provider market to operate over the top of the network operator market. Users may be restricted to a one-to-one relationship between SIM-IMSI-service provider-static IPv6 address. This area also needs further study.

5.3 Mobile Station Roaming Numbers (MSRNs)

MSRNs are used by GSM operators for routing incoming calls to mobiles. The MSRN is allocated temporarily to a visiting mobile by the VMSC. This arrangement will continue for the support of circuit switched services even when an IP infrastructure is introduced under Release 5.

MSRNs come from the E.164 numbering space although they are not public numbers (they are co-ordinated E.164 numbers). The introduction of UMTS with new operators entering the market will increase the demand for MSRNs but national numbering authorities should be able to satisfy the additional demand without undue difficulty.

5.4 Routing numbers for number portability

Routing numbers compatible with national number portability implementations will be needed for each network. This should not cause difficulty for national numbering authorities.

5.5 Summary of conclusions and issues

There is a need for agreements and formal documentation giving technical guidelines about the relationships and connection arrangements between network operators and ISPs/Intranets. It should cover items such as:

- interconnect guidelines;
- the implication of interconnect guidelines regarding the allocation of the IP address to the mobile;
- the identification and development of technical specifications required to implement technical guidelines.

The GSM Association should take responsibility for this work. It is a matter of urgency that standardization in 3GPP receives clear advice on these items. The UMTS Forum may assist with expertise, if required.

The following summarises the detailed conclusions and recommendations on IP addresses:

13. The protocol and addressing version issues for the SGSNs and internal PLMN core networks are independent from those for the terminals, and connected ISPs or Intranets at least until IP multimedia is introduced. However GGSNs will have to be compatible with:

    - internal network equipment
    - the terminals to which they will assign addresses, both home and visiting terminals
    - SGSNs in other networks to which they support GTP tunnels

14. GPRS/UMTS operators will need IPv4 addresses for their core network infrastructure because IPv4 is the default protocol at least for Releases 3 & 4.

15. IPv4 address exhaustion is difficult to predict but may be felt in the 2004-2006 timeframe and so network operators should ensure that they obtain adequate public IPv4 address allocations for their core networks

16. A new version of the mobile operators' internal DNS that is compatible with IPv6 and IPv4 (eg BIND9.x) will be needed when operators start to use IPv6 in their core networks

17. There is no absolute need for UMTS operators to synchronise the introduction of IPv6 in their internal core networks. However as GGSNs allocate IP addresses to mobiles and establish tunnels with SGSNs in other networks, they will need to know which other networks support IPv6 and therefore they need a system for exchanging information about introduction of IPv6 through dual stack operation. The operators may also wish to set common dates for introducing dual stack to reduce the administrative work so that they can change the arrangements with a whole group of networkes at the same time.

18. The GSM Association should facilitate the introduction of IPv6 by providing mechanisms for operators to exchange information about their plans for introducing IPv6 and the transition tools that they will use

19. The GSM Association should produce a guide and recommended procedure for the introduction of IPv6. Although operators may not need to start migrating to IPv6 immediately, it is important that this work should be undertaken reasonably soon to obtain a deeper understanding of the issues and the time that will be needed for migration.

20. Address assignments to terminals appear to need to be temporary if terminals are to be able to establish PDP Contexts with visited GGSNs. This may conflict with the need for IPv6 to use static assignments for many of the feature advantages of IPv6 to be realised. This area needs further study.

21. The UMTS Forum cannot judge at this time on how well founded concerns about network boundaries are. No forecast can be made on how soon operators will be willing to return to or at least towards the end-to-end paradigm. Further study of these issues especially in relation to migration to IPv6 is needed.

Regulators will need to make additional allocations of MSRN numbering space and routing numbers for number portability, but this should be a routine matter.

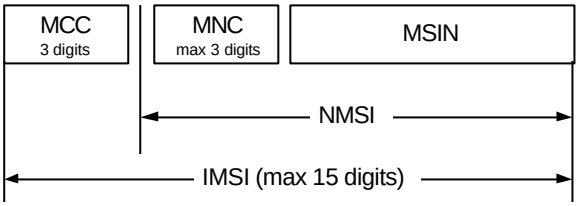
6 Other identifiers

6.1 IMSIs and their Mobile Network Codes (MNCs)

6.1.1 IMSI structure and administration

The International Mobile Station Identifier (IMSI) is defined by the ITU-T E.212 Standard and used as the primary identification of the SIM card. The IMSI is used for network internal purposes including the logging on procedure and billing and is not normally visible to the subscriber. IMSIs are network specific because they contain the Mobile Network Code (MNC). The structure of the IMSI is shown in Figure 9.

Figure 9: Structure of the IMSI showing the MNC



MCC Mobile Country Code
MNC Mobile Network Code
MSIN Mobile Station Identification Number
NMSI National Mobile Station Identifier
IMSI International Mobile Station Identifier

An MNC identifies one specific mobile network. MNCs are used both in 2nd and 3rd generation mobile networks for identification and routing purposes. These purposes include:

- Identification of the home network of a roaming mobile during registration
- Preparation of billing information relating to roaming mobiles
- Analysis in support of fraud detection and prevention

The E.212 standard gives the option of using either 2-digit long MNCs together with 10-digit long MSINs or 3-digit long MNCs together with 9-digit long MSINs. E.212 originally specified 2 digit MNCs only. Thus only 2 digit MNCs were allocated in Europe. However, in order to incorporate the US into the standard, E.212 was revised to also include the legitimate use of 3 digit MNCs. Therefore, it is only as a result of history that there is a mix of 2 and 3 digit MNCs.

The relevant specifications for GSM and UMTS/Release 99 have identical requirements for MNCs: GSM 03.03 (R98) => 3GPP 23.003(99) and GSM 03.23 (R98) => 3GPP 23.122. They state that (with the exception of North America during a transition period) within a single country (or area identified by a MCC) all networks shall broadcast a 2-digit MNC code, or all networks shall broadcast a 3-digit MNC code. A mixture of broadcast 2- and 3-digit MNC codes is not permitted within a single country (or area identified by a MCC).

Whereas MCCs are defined by ITU, the administration of MNCs is up to the NRAs (National Regulatory Authorities). It is also up to the NRAs to grant 2 or 3 digit long MNCs. Therefore the number of MNCs allocated and the number of digits used vary per country. At present, out of a total of 300 MNCs actually in use, there are only 14 3-digit MNCs. Furthermore, there are no assignments for 3-digit MNCs outside the US. These allocations correspond to 1.7 % of the GSM Operators.

6.1.2 Demand for MNCs

MNCs are needed by:

- Each UMTS network operator with radio licence
- Each UMTS virtual network operator who operates an HLR but does not operate a radio network

Because of spectrum considerations, the number of radio licences to be issued will be low in countries with national services but could be larger where local-only operators are licensed. Therefore the main need for a substantial number of MNCs will come in countries where virtual network operators are licensed. Countries that have national systems and do not license virtual operators are unlikely to experience a shortage of 2-digit codes. However personal numbering and mobility for customers of fixed networks may lead to the use on MNC codes by operators of fixed or technology independent

services and these developments may create pressure for an earlier move to 3digits than would otherwise be necessary.

Some GSM operators that will also become UMTS operators may wish to use the same MNC value for both technologies since, for example, they may wish to enable their subscribers to use dual mode terminals with a single SIM. These operators may provide UMTS coverage in only the denser parts of their GSM coverage.

It is not expected that service providers would need MNC codes. Service providers normally obtain blocks of IMSIs from operators for allocation to customers.

In some countries, TETRA technology is being used for public networks and interworking between TETRA and GSM/UMTS may be allowed. This may lead to additional demand for MNCs from TETRA operators. Various organisations, including ETSI, are studying how the allocation of TETRA MNCs for use within TETRA should be handled. In addition, it is probable that other future mobile or converged (fixed-mobile) services will require these E.212 resources as well.

The prospective growth in the demand for MNCs led to concern about whether enough values would be available if the policy followed by many countries of allocating 2-digit values continues. This issue is being studied by ETSI, the European Numbering Forum (ENF) and the Project on Telecommunications Numbering (PTN) group of ECTRA.

The ENF convened a workshop in September 2000 which concluded that:

1. There is no immediate problem (no need to move to 3 digit MNCs in short term). It was recognised that at the present there is not a problem of scarcity of MNC resources but that conservation is best started early.

2. The introduction of 3digit MNCs implies changes and cost. A clear demand that would necessitate the introduction of 3 digit MNCs has still to be proved but could not be excluded.

3. If, in the future, there is a need to move to 3 digit MNCs, two possible solutions would need to be investigated further:
   - Co-existence behind the same MCC of mixed 2 and 3 digit MNCs,
   - Separate MCCs for 2 and 3 digit MNCs.

6.1.3 IMSI allocation

The current system of IMSI allocation is inefficient and may lead to premature exhaustion of existing MNCs. Currently blocks of IMSIs are allocated to service providers by operators through the distribution of SIMs. Individual values are sub-allocated when SIMs are given to a customer. There is a high degree of churn in the mobile market and many customers change operator every 1-2 years. This churn is likely to increase with mobile number portability being introduced or improved in many countries. When a number is ported although the E.164 number does not change, the IMSI changes. Some customers may have already left a trail of several relinquished IMSIs. Thus churn will increase the rate at which IMSIs are consumed and the space within MNCs is used. At some stage a mechanism for recovering and re-using IMSIs after an appropriate sterilisation period may be needed.

6.2 IMEIs

The International Mobile Equipment Identifier (IMEI) identifies the mobile terminal. It is used for tracking stolen terminals and for fraud prevention. It has also been used in relation to type approval. The GSM Association has developed assignment rules for the IMEIs and these identifiers are registered by the Association.

The current IMEI format is structured in the following way:

- Type Approval Code (TAC): 6 digits. The first 2 digits constitute the code allocated to Notified Body = Reporting Body Identifier(1900 MHz phones in USA and test terminals have different coding)
- Final Assembly Code (FAC): 2 digits
- Serial Number: 6 digits
- Check digit

These digits are presented in BCD format.

Before the R&TTE Directive regime was established in Europe, the IMEI allocation procedure was based on the involvement of notified bodies. IMEI has been so far a regulatory requirement. However, this has now been removed. under the new regime, the IMEI has become even more important for network operators. The use of the IMEI may be affected by the voluntary certification scheme.

The industry considers IMEI an important market requirement therefore the advantages of IMEI must be secured. Manufacturers and operators' are presently jointly reviewing the IMEI scheme and the allocation procedure.

The review of the IMEI system should enable:

- a fair, transparent and secure allocation procedure meeting the interests of network operators and manufacturers
- a common scheme to be used for GSM and UMTS terminals as multi-mode terminals as expected to be used.
- global support if at all possible
- Changes from the existing system to cause minimum operational disruption

The review has started in the "Global IMEI Strategy Forum" with the agreement on a number of important issues, among them:

- Mobile Manufacturers and Network Operators aim to have a world-wide recognised central body / organisation administrating and allocating IMEI Type Allocation Codes (TACs) worldwide for all GSM/3G related terminals incl. Multisystem terminals.
- Where multi mode devices are introduced and one band is GSM or 3G, the IMEI scheme must be used.
- The Final Assembly Code (FAC) will be used as digit 7 and 8 of the serial number (SNR). This would increase the potential number of serial numbers for a specific TAC to 100 Million.
- The TWG Guideline Document TW.06 shall be used for a basis of a new common document setting out the structure and allocating procedure for IMEI globally.

Up to now the operator’s side could not agree to a Change Request (CR) in 3GPP standardization allowing the application of a hexadecimal format of the IMEI.

6.3 Issuer Identifier Numbers (E.118)

6.3.1 Background

To meet a cross industry (banking, finance, travel, healthcare, telecommunications, entertainment, and others) requirement, the International Organization for Standardization (ISO) jointly with the International Electrotechnical Commission (IEC) have specified in ISO/IEC 7812 "Identification cards - Identification of issuers" a numbering system for the identification of issuers of identification cards used in international and/or inter-industry exchange. This means the exchange of card originated/activated transaction data between two or more different entities/institutions based on an agreement between the participants and, for example, includes credit card and charge card transactions.

Part 1 of ISO/IEC 7812 refers to the numbering system to be applied. Part 2 of this standard provides the application and registration procedures. However, Issuer Identification Numbers (IINs) beginning with "89" are for use in the telecommunication sector and are administered by the International

Telecommunication Union (ITU) (see ISO/IEC 7812 - Part 1, § 4.2.4). The ITU Telecommunication Standardization Sector (ITU-T) has published Recommendation E.118 (The International Telecommunication Charge Card) to define the necessary rules and procedures in line with ISO/IEC principles.

According to Rec. E.118, Issuer Identifier Numbers (IINs) for telecommunication applications have a variable length, with 7 digits as the maximum. The structure is a follows:

1.	Major Industry Identifier (MII):	fixed to "89"
2.	Country code (CC):	variable, 1 to 3 digits, for simplification, CCs of ITU-T Rec. E.164 are used.
3.	Issuer Identifier:	variable up to the limits that the length of the whole number (MII+CC+Issuer Identifier shall not exceed 7 digits). The length is constant for each value of the Country code.

The length of the Issuer Identifier is constant for each value of the Country code and therefore either 99 or 999 are available per country depending on the length of the Country Code.

6.3.2 Use of IINs for UMTS

IINs are not used by mobile networks for their own GSM/UMTS specific operation and accounting but it is a necessary prerequisite for potential supplementary applications. The IIN has to be stored electronically and, at least partly, printed on SIM cards. Details can be found in the respective ETSI Technical Specifications (GSM 11.11 and TS 100.977, here under the designation ICCID = Integrated Circuit(s) Card IDentifier) Since the complete IIN (or ICCID) identifies uniquely each of the SIM card series in use in a particular network, it can provide a very useful tool for the operators' internal SIM card management. .

For the SIM card of the GSM system, the necessary agreement can be found in the GSMA Permanent Reference Document SE.13, Section B10. For practical reason (roaming between the systems) the same principles have been extended for the USIM of UMTS.

The procedure in SE 13 stipulates that a request of a card issuer (usually the network operator) for an IIN has to be addressed to the national administration (or the numbering administration of a world zone, where appropriate) of the operator. Generally, the national administration allocates an IIN and passes the information back to the applicant and, in addition, to the ITU for registration. The ITU publishes periodically, usually once a year as part of its "ITU Operational Bulletin", an updated "List of Issuer Identifier Numbers for the International Telecommunication Charge Card (In accordance with ITU-T Recommendation E.118)".

6.3.3 Conclusion

National regulatory authorities should ensure that national rules for allocation of issuer identifiers according to ITU-T Recommendation E.118 are in place, and that they take account of the limited number available and the increasing importance of identification cards in an emerging M-Commerce environment.

6.4 Other identifiers

No other identifiers are being considered in this first version of the report.

6.5 Summary of issues

6.5.1 General issues

The need for 3-digit should be reviewed jointly by regulators and operators and a cost effective migration path to 3-digits established as and when necessary. No firm decisions to move to 3-digits should be taken until an adequate migration path has been established.

6.5.2 Issues for operators

Operators should review the arrangements for IMSI allocation and introduce a system of IMSI re-use when the level of relinquished IMSIs becomes unacceptably large.

Operators should review the system for IMEI allocation an use so that an integrated system can be used by both GSM and UMTS, which will also take account of changes in type approval requirements.

6.5.3 Issues for regulators

National regulatory authorities should take care that national rules for allocation of issuer identifiers according to ITU-T Recommendation E.118 are in place which take account of the limited number available and the increasing importance of identification cards in an emerging M-Commerce environment.

7 References

[1] UMTS Forum Report No. 1: "A Regulatory Framework for UMTS", June 1997.
[2] UMTS Forum Report No. 2: "The Technical Vision", September 1998.
[3] UMTS Forum Report No. 3: "The impact of licence cost levels on the UMTS business case", October 1998.
[4] UMTS Forum Report No. 4: "Licensing Conditions for UMTS", September 1998.
[5] UMTS Forum Report No. 5: "Minimum Spectrum demand per public terrestrial UMTS Operator in the initial phase", September 1998.
[6] UMTS Forum Report No. 6: "UMTS/IMT-2000 Spectrum", December 1998.
[7] UMTS Forum Report No. 7: "Candidate Extension Bands for UMTS/IMT-2000 Terrestrial Component", March 1999.
[8] UMTS Forum Report No. 8: “The Future Mobile Market”, Global trends and developments with a focus on Western Europe, March 1999.
[9] UMTS Forum Report No. 9: "The UMTS - 3rd Generation Market - Exploring the Services Revenue Opportunity", September 2000.
[10] UMTS Forum Report No. 11: Enabling UMTS/3rd Generation Services and Applications
[11] ERC Report 60: “Global Circulation of IMT-2000 Terminals", September 1998.

Annex A: Description of how names and addresses are used in GPRS and UMTS

A.1 Addressing and routing currently used with GPRS

The UMTS architecture will be based initially on that developed and currently being brought into service for GPRS. This architecture introduces several concepts that need to be distinguished carefully to understand the naming and addressing requirements.

The GPRS networks are designed to provide access connections (the technical name is PDP Context) between mobile terminals and an IP network selected by the terminal. The IP network may be:

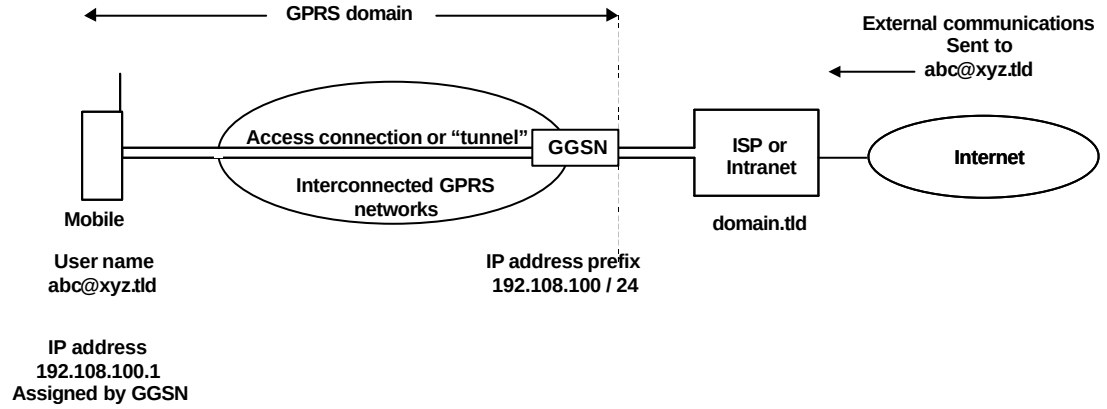
- any ISP with which the terminal user has an account
- a corporate IP network e.g. an Intranet

In practice, a GPRS operator may also own and run an ISP that is connected to the GPRS network and may use this ISP to provide general Internet access for all users, but the following explanation treats these two functions separately.

A.2 The access connection across GPRS

When the GPRS networks are interconnected and provide roaming, this will mean that a terminal has world-wide access to its ISP(s) or Intranet. The access provided by GPRS is analogous to a dial up connection over the PSTN to an ISP or a leased line connection to an ISP. The access connection (PDP Context) can be thought of as a "flexible tunnel" through the GPRS networks. The arrangement is shown in Figure 10.

Figure 10: The GPRS access connection



The mobile terminal will be assigned an IP address by the home or visited GGSN to which the ISP or Intranet is connected. This address may be public or private and may be assigned permanently or temporarily. In Figure 10 the terminal has the address 192.108.100.1 from the range 192.108.100 /24 allocated to the ISP. This IP address is not seen by other nodes in the GPRS networks as it passes unexamined through the access connection.

The user identifications (names) used on the mobile terminal will be specific to the service or services supported. These names will be related to the ISP or Intranet and may not be known to the GPRS network. For many services a name of the form user@domain will be used. The "domain" may be the identity of the ISP (e.g. for an individual subscriber) or a domain name that is served (connected) by

the ISP but is in principle portable to another ISP. In Figure 10 the user has the name abc@xyz.tld from the ISP or corporate network xyz.tld.

Thus the mobile terminal always appears to the outside world, e.g. the Internet, as reachable via the GGSN, even though it may be on any GPRS network, either its home network or a visited network when roaming.

The mobile terminal is able to select the ISP or Intranet that it accesses and may have different names on different ISPs/Intranets (similar to a user logging into different email accounts with different names).

A.3 The structure within GPRS

GPRS networks have a structure similar to the GSM network:

- the Serving GPRS Support Node (SGSN) is equivalent to the MSC and connects to the radio base station controller that handles the radio base stations in an area.
- the Gateway GPRS Support Node (GGSN) is equivalent to the GMSC and provides the connection point to other networks

The GPRS nodes are interconnected on an IP network and the IP networks of each GPRS network are interconnected on an inter-PLMN IP backbone. The Inter-PLMN backbone will be an isolated IP network and is not connected to the public Internet. However the GSM operators have arranged to use public IP addresses for interfaces on this network to ensure uniqueness and forward compatibility (if ever this network is connected to the public Internet). These IP addresses are used to identify interfaces on the SGSNs and GGSNs.

The section of the access connection through the Inter-PLMN backbone between the SGSN serving the mobile and the GGSN is established by the GPRS Tunnelling Protocol (GTP).

When a GPRS terminal logs on to its home or a visited network, it selects which ISP/Intranet it wishes to access. This is done by specifying the Access Point Name (APN) of the ISP/Intranet. The access connection may go through the visited GGSN or the home GGSN depending on the connections available, so for example a roaming terminal can access a local node of its ISP via the visited GGSN. The following example is for a roaming terminal accessing an ISP or Intranet via the home GGSN:

1. The user identifies the requested ISP or Intranet by the network ID part (xyz.com) of the APN and the terminal sends this information to the SGSN. Although the network ID part (xyz.com) of the APN is internal to the GPRS networks, it has been agreed that where the ISP or Intranet has a publicly registered domain name only this name should be used for the network ID, i.e. additional names should not be created for internal GPRS use. For connections without public registered domain names a new name is prefixed to the operator's own domain name e.g. smallcompany.t-mobil.de, anothercomp any.t-mobile.de etc.

2. The SGSN adds the operator ID of the visited network to give "xyz.com.mnc001.mcc007.gprs" where the visited operator ID is mnc001.mcc007. (mnc = mobile network code prefixed with 0 if the code is 2-digits; mcc = mobile country code). This string is the whole APN.

3. The visited network interrogates its own local DNS but the resolution of that APN fails as xyz.com is not known in the visited network

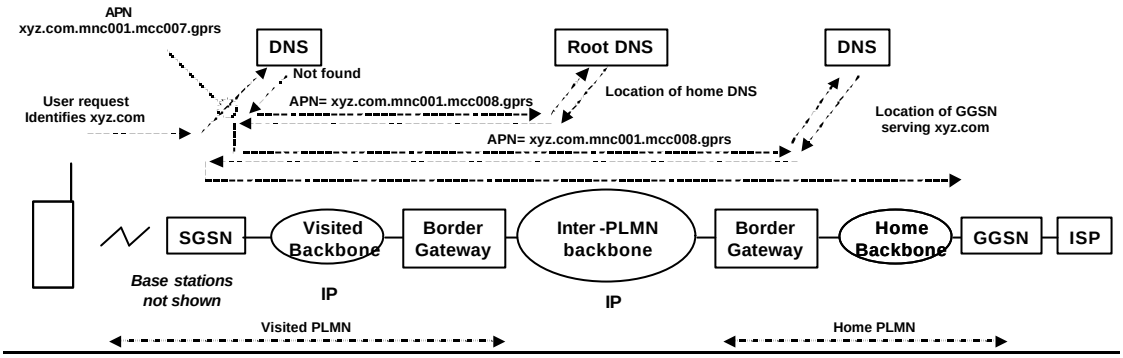
4. The SGSN then changes the operator ID to the home operator ID and sends the request to the root DNS (not one of the 13 public root DNS servers but a private server exclusive to the GPRS networks on the inter PLMN backbone. The root server forwards the request to the home network's local DNS

5. The home local DNS resolves the APN to the IP address of the GGSN that connects to the requested APN.

6. The SGSN establishes a tunnel to the GGSN using the GPRS Tunnelling Protocol (GTP) and then a virtual access connection is created between the roaming terminal and the requested ISP with the section between the SGSN and the GGSN using the GTP.

The sequence of interrogations is shown in Figure 11.

Figure 11: Establishment of an access connection

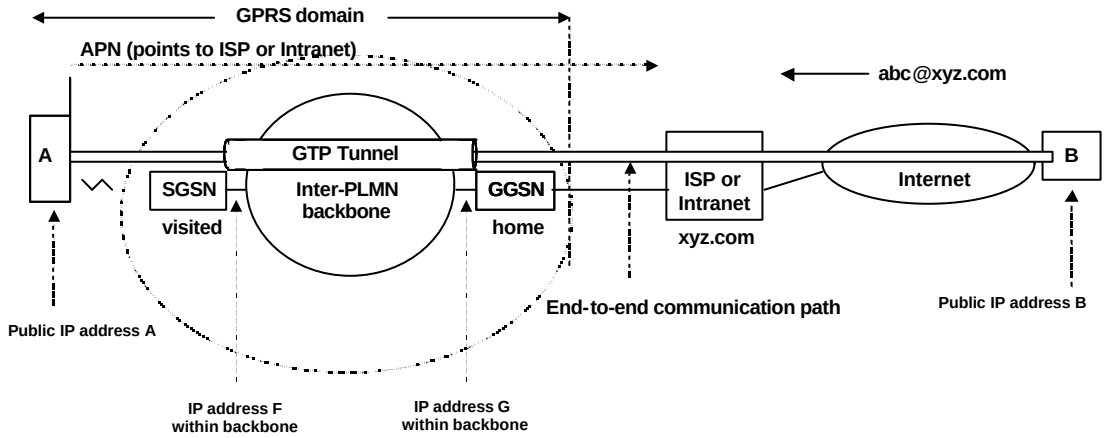


The access connection is connection orientated and is held as long as the terminal remains logged on (always-on) . It extends from the mobile to the ISP.

For the tunnel between the SGSN and the GGSN, i.e. the section across the Inter-PLMN backbone, there is a tunnel identifier (TID) distinguishing each user's tunnel. The tunnel ID relates to the GTP protocol running between the SGSN and the GGSN, and there are IP addresses for the source and destination SGSN/GGSN interfaces at each end of the tunnel.

Figure 12 shows communications in progress between a mobile and an entity in the public Internet.

Figure 12: Naming and addressing for the tunnel and access connection



Packets pass transparently between A and B with the public IP addresses of A and B. The address of A was allocated by the GGSN. The packets use the GTP tunnel across the Inter-PLMN backbone.

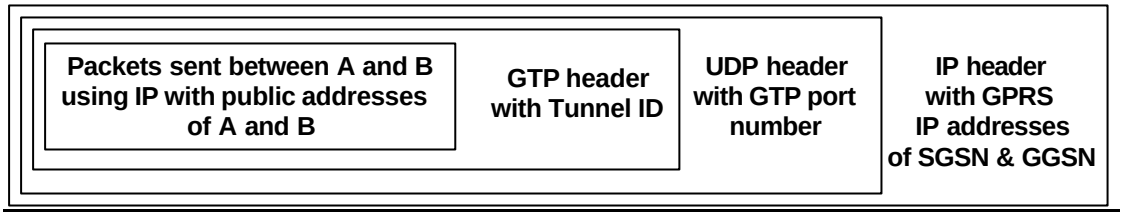
Between the visited SGSN and the home GGSN, these packets are encapsulated (wrapped up) in the following additional headers and footers that correspond to different protocol layers, in the following order working outwards.

1. Tunnel ID from the GTP
2. UDP port to identify that the GTP is used from the UDP protocol that supports GTP

3. IP addresses for the visited SGSN and home GGSN

This is shown in Figure 13.

Figure 13: Encapsulation of headers within a tunnel



Annex B: Domain names

There are two types of Top Level Domain (TLD) names:

- Generic domains (gTLDs): (.com, .org, .net, .edu, .gov, .mil, .int[8]; .arpa is used for Internet management purposes)
- Country code domain names (ccTLDs) (e.g. .jp, .de, .uk) issued in accordance with the ISO 3166 standard.

TLDs may be either open to any use or limited to a specific use or charter. In practice, although .com, .org and .net were intended for specific applications (chartered) they have become open to any use.

ICANN decides whether, how, and when to add new generic top-level domains (gTLDs) to the domain name system. A number of plans have been proposed to create new gTLDs, such as .firm, .store, .law, and .arts., and some companies have even taken orders for them. ICANN commenced a formal process of inviting proposals for new TLDs in August 2000 and decisions on the allocation of new TLDs are expected around the end of 2000.

According to ICANN, there are many arguments both for and against new gTLDs: for example, those in favour argue that new gTLDs are technically easy to create, will help relieve perceived scarcities in existing name spaces, and are consistent with a general push towards consumer choice and diversity of options; those opposed point to greater possibilities for consumer confusion, the risk of increased trademark infringement, cybersquatting (use of a name without payment) and cyberpiracy (taking someone else's traffic). In practice many large companies with valuable names will register their names under all available TLDs in order to protect their identity.

Unlike E.164, the domain name system is supported by a global domain name server system (DNS) that resolves domain names into IP addresses which are then used for routing Internet traffic. DNS is a hierarchical system of servers at the top of which are the root servers.

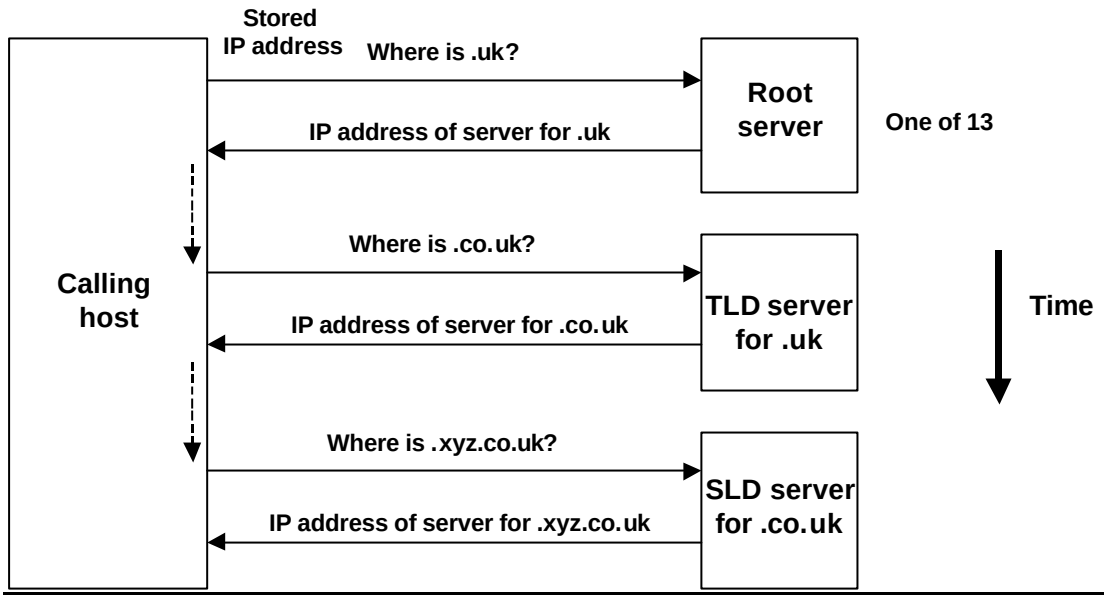
The choice of the domain name has an implication for the portability of IP addresses as described earlier in this report. It is also considered relevant for the marketing of services. However the advantages and disadvantages are not so obvious and detailed investigation in this aspect would be helpful.

ICANN handles the management of the root server system which consists of a set of thirteen file servers, which together contain authoritative databases listing all Top Level Domains. Currently, NSI, under an agreement with ICANN and the US Department of Commerce, operates the "A" root server, which maintains the authoritative root database and replicates changes to the other root servers. Different organisations, including NSI, operate the other 12 root servers (including Lynx in UK, which runs a server for RIPE, and a server in Stockholm). The U.S. Government has played a role in the operation of about half of the Internet's root servers but the ICANN Root Servers Committee is taking over the responsibility for the functionality of the root server system.

The function of the root servers is to resolve from the Top Level Domain name to an IP address by which a Top Level Domain Server can be contacted. The Top Level Domain server then resolves the Second level Domain name into an IP address by which a Second Level Domain server can be contacted. The process is repeated until eventually the IP address of the host is found. Figure 14 shows the sequence for resolving the name: xyz.co.uk into an IP address.

[8] Additional gTLDs were agreed in ICANN in November 2000

Figure 14: Example of domain name resolution



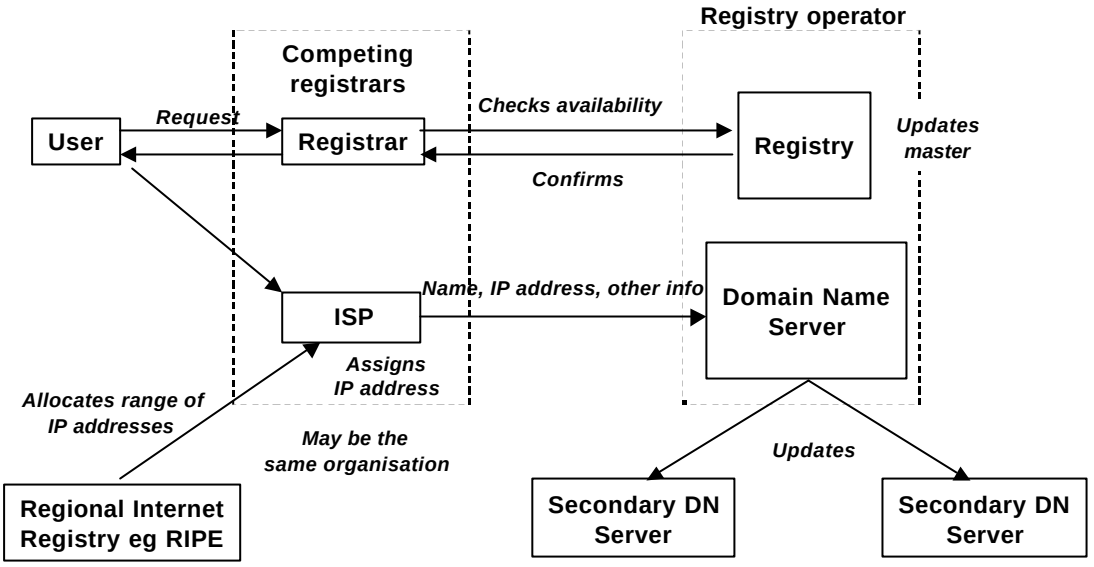
A master registry is maintained for each TLD name. Allocations of Second Level Domain names (SLDs) are made by registrars who update the registry.

For .gov, .edu .mil and .int there are only single registrars, but for .com, .net and .org there are now competing registrars who issue Second Level Domain names. The system was changed in 1999 from single (monopoly) registrars to the new shared registry system in response to proposals from the US Government in its Green and White papers.

The registry for .com, .net and .org is run by InterNIC®, which is a co-operative activity between the US Department of Commerce and Network Solutions Inc (NSI). Network Solutions is the largest registrar and was formerly the only registrar. There is now a rapidly increasing number of accredited and operational registrars. The process of accreditation is handled by ICANN and takes up to 30 days. ICANN has published a proforma agreement that has to be entered into by Registrars.

Figure 15 shows the flow of the process of obtaining a domain name either via an independent registrar or an ISP and having the domain name - IP address pair registered in the domain name server run by the registry.

Figure 15: Registrar, Registry and DNS functions



The DNS resolves domain names to IP addresses. There is a one-to-one relationship between domain names and IP addresses and so provision has been made for the reverse process, from IP address to domain name. However, because the DNS servers are structured by domain name, it is not possible to know which server holds the record with the IP address used for a reverse query. Therefore a special pseudo-domain has been created called “in-addr.arpa”. Under this domain, the IP address is stored in the pointer record (PTR) in reverse form. For example:

For the mapping of a names to an address, an address (A) record is used:

kapella.dfn.de	A	192.76.176.10

For reverse mapping a pointer record (PTR) is used:

10.176.76.192.in-addr.arpa	PTR	kapella.dfn.de

To enable reverse mapping, the assigned IP address has to be registered under the “in-addr.arpa” domain. The “in-addr.arpa” name space is divided according to the reverse of the IP addresses. Therefore 193.in-addr.arpa is delegated to the owner of the addresses starting with 193 and this organisation is responsible for giving the real domain name that corresponds to the address. Thus the name space under “in-addr.arpa” is structured according to addresses rather than the real domain names.

Reverse mapping is likely to be important for lawful interception.

For a more detailed description of DNS see RFC1033, RFC1034 and RFC1035.

Annex C: Definition of Access Point Name

(Based on 3G TS 23.003 V3.5.0 (2000-06) Release 99)

In the GPRS backbone, an Access Point Name (APN) is a reference to a GGSN. To support inter-PLMN roaming, the internal GPRS DNS functionality is used to translate the APN into the IP address of the GGSN.

C.1 Structure of APN

The APN is composed of two parts as follows:

- The APN Network Identifier which defines the external network or service that the user wishes to connect to via the GGSN. This part of the APN is mandatory.
- The APN Operator Identifier which defines in which PLMN GPRS backbone the GGSN is located. This part of the APN is optional.

The APN Operator Identifier is placed after the APN Network Identifier. An APN consisting of both the Network Identifier and Operator Identifier corresponds to a DNS name of a GGSN and has a maximum length of 100 octets.

The syntax of the APN shall follow the Name Syntax defined in RFC 2181 and RFC 1035. The APN consists of one or more labels. Each label is coded as one octet length field followed by that number of octets coded as 8 bit ASCII characters. Following RFC 1035 [15] the labels should consist only of the alphabetic characters (A-Z and a-z), digits (0-9) and the dash (-). The case of alphabetic characters is not significant. The APN is not terminated by a length byte of zero.

NOTE: A length byte of zero is added by the SGSN at the end of the APN before interrogating a DNS server.

For the purpose of presentation, an APN is usually displayed as a string in which the labels are separated by dots (e.g. "Label1.Label2.Label3").

C.1.1 Format of APN Network Identifier

The APN Network Identifier shall contain at least one label and shall have a maximum length of 63 octets. An APN Network Identifier shall not start with the strings "rac", "lac","sgsn" or "mc" and it shall not end in ".gprs". It shall also not take the value "*".

In order to guarantee uniqueness of APN Network Identifier within the GPRS PLMN(s), an APN Network Identifier containing more than one label corresponds to an Internet domain name. This name should only be allocated by the PLMN to an organisation that has officially reserved this name in the Internet domain. Other types of APN Network Identifiers are not guaranteed to be unique within the GPRS PLMN(s).

An APN Network Identifier may be used to access a service associated with a GGSN. This may be achieved by defining;

- an APN that corresponds to a DNS name of a GGSN and is locally interpreted by the GGSN as a request for a specific service, or;
- an APN Network Identifier consisting of 3 or more labels and starting with a Reserved Service Label, or an APN Network Identifier consisting of a Reserved Service Label alone, that indicates a GGSN by the nature of the requested service. Reserved Service Labels and the corresponding services they stand for are to be agreed among operators.

C.1.2 Format of APN Operator Identifier

The APN Operator Identifier is composed of three labels. The last label shall be "gprs". The first and second labels together shall uniquely identify the GPRS PLMN (e.g. "<operator-name>.<operator-group>.gprs").

For each operator, there is a default APN Operator Identifier (i.e. domain name). This default APN Operator Identifier is derived from the IMSI as follows:

"mnc<MNC>.mcc<MCC>.gprs"

where:

"mnc" and "mcc" serve as invariable identifiers for the following digits.

<MNC> and <MCC> are derived from the components of the IMSI defined in subclause 2.2.

This default APN Operator Identifier is used in inter-PLMN roaming situations when attempting to translate an APN consisting of Network Identifier only into the IP address of the GGSN residing in the HPLMN. The PLMN may provide DNS translations for other, more human-readable, APN Operator Identifiers in addition to the default Operator Identifier described above.

In order to guarantee inter-PLMN DNS translation possibility, the <MNC> and <MCC> coding to be used in the "mnc<MNC>.mcc<MCC>.gprs" format of the APN OI shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits
- If there are less than 3 significant digits in MNC, one or more "0" digit(s) is/are inserted at the left side to fill the 3 digits coding of MNC in the APN OI.

As an example, the APN OI for MCC 345 and MNC 12 shall be coded in the DNS as mnc012.mcc345.gprs.

C.2 The Wild Card APN

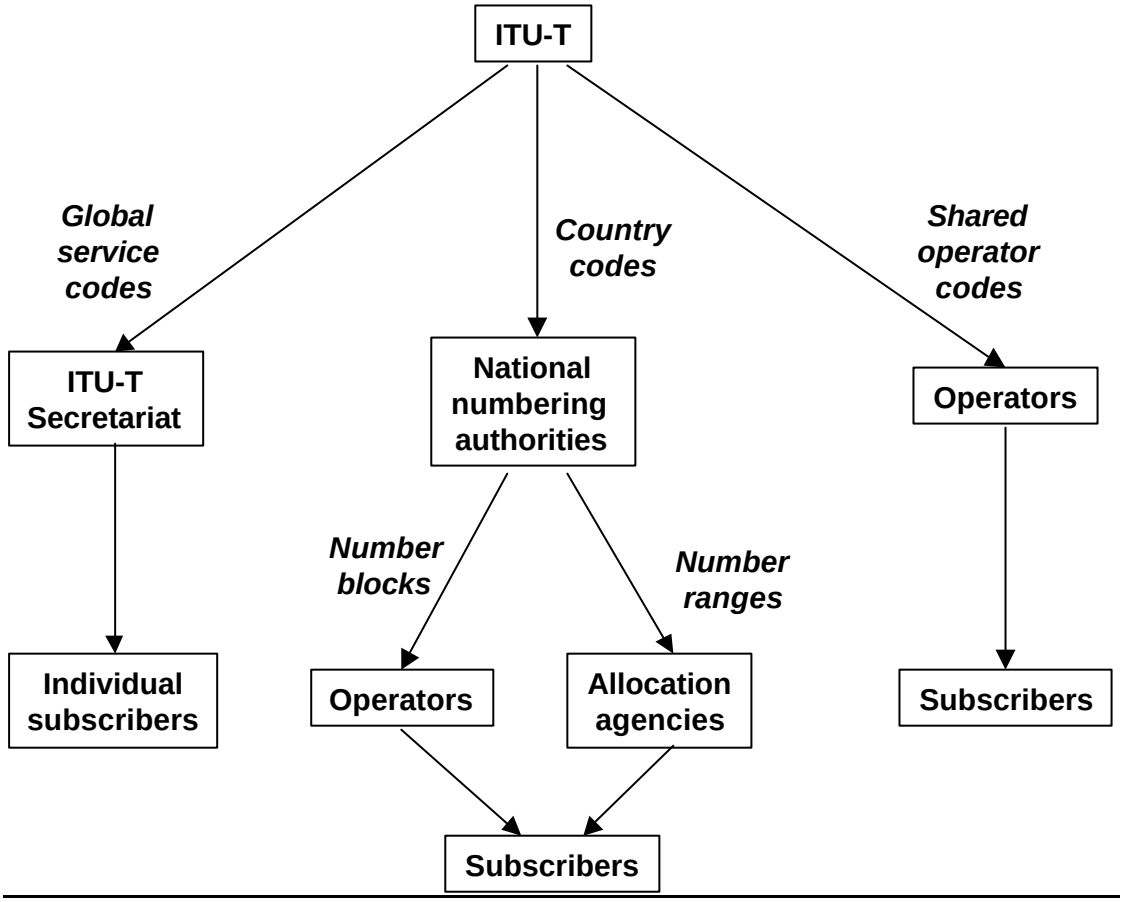
The APN field in the HLR may contain a wild card APN if the HPLMN operator allows the subscriber to access any network of a given PDP Type. If an SGSN has received such a wild card APN, it may either choose the APN Network Identifier received from the Mobile Station or a default APN Network Identifier for addressing the GGSN when activating a PDP context.

The wild card APN is coded as an APN with "*" as its single label, (i.e. a length octet with value one, followed by the ASCII code for the asterisks).

Annex D: Allocation of E.164 names

The allocation procedures are shown in Figure 16:

Figure 16: ITU-T Allocation procedures



Although all public telephone numbers are coordinated with E.164 so that there can be no dialling ambiguity, not all telephone numbers are formally recognised as E.164 numbers. True E.164 numbers always are capable of expansion into the full international form and should be reachable from any county. The following are examples of numbers that are not formally part of E.164 but fit into the national dialling plans alongside true E.164 numbers:

- short codes (e.g. 100 for the operator)
- national freephone or shared cost numbers not reachable from outside the country concerned
- routing numbers that cannot be activated by user dialling (e.g. location routing numbers in the North American number portability solution)

E.164 numbers are used for both names and addresses, although with the growth in demand for operator portability they are increasingly used as names rather than addresses, i.e. they are not related exclusively to a particular network.

E.164 names are used by the following services:

- telephony
- fax
- circuit switched data
- mobile Short Message Service

Telephony and fax are not normally segregated into different number ranges. Data and SMS numbers may be segregated at a national level but this is not recognised by callers.

In addition, within the general heading of telephony, E.164 names are used for:

- geographic services (the most common use)
- mobile services
- satellite services
- paging
- global freephone
- global shared cost services
- global premium rate services
- personal numbering services including Universal Personal Telecommunications (whose numbering is defined in Recommendation E.168) with local, regional or national options

The top part of all E.164 numbers (country code, global service code or shared network code) are allocated by ITU-T Study Group 2. The remaining part is allocated by the next authority level e.g. the National numbering authority for country codes. Most numbers are allocated in blocks (typically 10,000 numbers) to network operators or service providers who then allocate individual numbers to customers. In some cases numbers are allocated direct by the numbering authority or its agent to the end customer.

Annex E: IPv4 and IPv6 Interoperability

Reference: RFC 2893 - Transition Mechanism for IPv6 Hosts and Routers

E.1 Introduction

IPv4 uses 32 bit addresses whereas IPv6 uses 128 bits. The two forms of address are therefore only compatible in one direction.

Networks are built using either or both technologies. DNS will provide separate record for each type of IP address. It will provide an

- "A" record giving an IPv4 address, and/or
- "AAAA" (quad A) record giving an IPv6 address
- "A6" a new record type designed to facilitate network renumbering and multi-homing, will replace AAAA (see RFC2874)

depending on the information provided to DNS by the ISP that is serving the name in question. DNS servers that support IPv6 are currently available in the form of BIND9, they are however not widely deployed.

A key problem of the introduction of IPv6 into the Internet of today is to provide compatibility between the two protocols. A whole set of tools and mechanisms for this transition or migration is becoming available. IPv6 hosts and routers will use these mechanisms to interoperate with and across the IPv4 world for a long time to come

E.2 Compatibility constraints

The compatibility relationships for the two protocols are as shown in Figure 17.

Figure 17: Compatibility table

	Receiving network technology		
Sending network technology	IPv4	IPv4 + IPv6	IPv6
IPv4	Yes	Yes	No Because the address field in IPv4 used by the sender cannot contain the IPv6 address
IPv4 + IPv6	Yes	Yes	Yes
IPv6	Possibly because the address field in IPv6 used by the sender can contain the IPv4 address	Yes	Yes

The circumstance that is incompatible is where a user in an IPv4 protocol domain wishes to communicate to an IPv6 only domain, because the IPv4 domain cannot handle the IPv6 address that is to be sent. The only way in which this can be overcome is if the IPv6 address is made compatible with IPv6 by using only the first 32 bits in the header and setting the remaining 96 bits to zero. This is not an adequate solution because the objective of IPv6 is to provide more addresses than are available within IPv4.

A network that uses only IPv6 will be able to send packets to networks that implement IPv4 because it can put the IPv4 address in the front part of the IPv6 space in the packet but the receiving network will need to know how to handle the incoming packet.

E.3 Transition Mechanisms

The IETF WG "ngtrans" is developing tools to facilitate communications during the transition period when there is a mixture of IPv4 and IPv6 protocols in operation.

RFC2893 gives detailed information on the tools available, but the choice of tool depends very much on the individual circumstances of the operators.

The Internet-Draft "On overview of the introduction of IPv6 in the Internet (draft-ietf-ngtrans-introduction-to-ipv6-transition-04.txt) examines different case studies that are expected to be typical

The following gives a brief overview of the main mechanisms relevant to GPRS/UMTS operators:

E3.1 Dual IP Layer Operation (dual stack)

The most straightforward way for IPv6 nodes to remain compatible with IPv4-only nodes is by providing a complete implementations of both IPv4 and IPv6. Both protocol stacks can be enabled or disabled as necessary and the version can be chosen that matches the capability of the other party to the communication.. Dual stack nodes would be configured with both IPv6 and IPv4 addresses. This means that every dual stack equipment might still need an IPv4 address.

However the Dual Stack Transition Mechanism (DSTM) overcomes this problem by providing a method to assign temporary global IPv4 addresses to IPv6/IPv4 nodes over a native IPv6 network using dynamic tunnels within an IPv6 network to carry IPv4 traffic.

Dual stack is expected to be used widely in the transition period and new products are likely to be dual stack (support both protocols) .

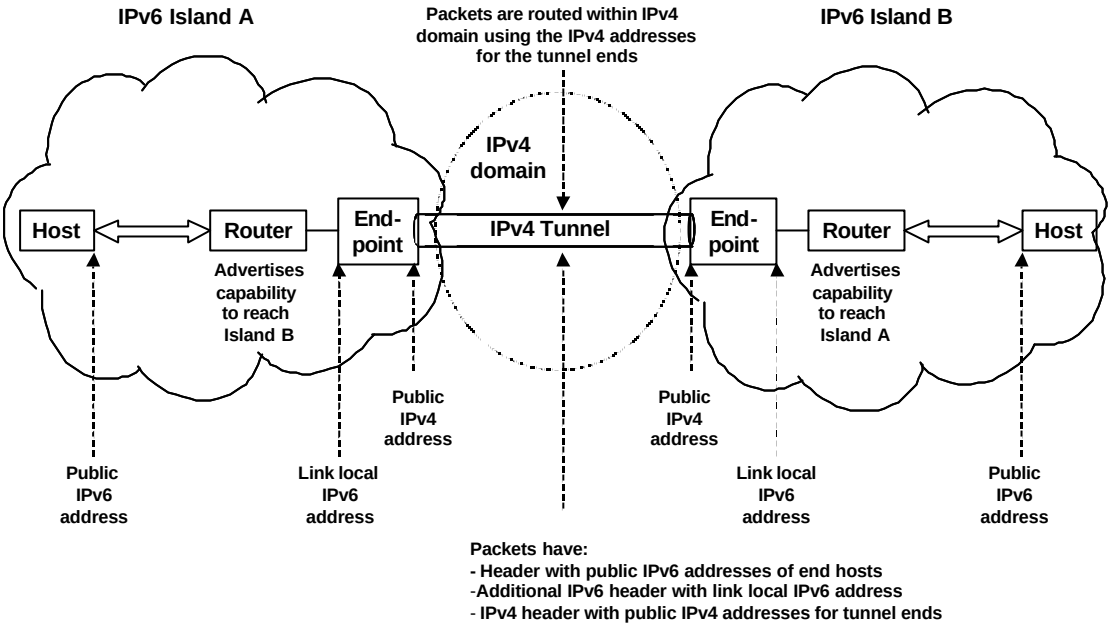
The dual stack approach can be applied to nodes that initially supported IPv4 only. One method of doing this is to use Bump-in-the-stack (BIS, RFC2767), which adds the necessary components to communicate with the IPv6 world (these are essentially a name resolver, an address mapper and a translator). In this way an IPv4 host can be "upgraded" to communicate with IPv6 peers.

E3.2 Configured and automatic Tunnelling Mechanisms

Tunnelling provides a very effective way to use an existing IPv4 routing infrastructure to carry IPv6 traffic. Therefore a node with IPv6 can communicate with another such node across an IPv4 network by using a tunnel.

The IPv6 packets are encapsulated within IPv4 packets and the tunnel endpoints are each identified by an IPv4 address that enables them to be routed across the IPv4 network. The tunnel endpoints also have a link-local IPv6 address where the last 32 bits contain the IPv4 address. This link-local address facilitates the operation of the routers at the ends of the tunnel. The situation is shown in Figure 18:

Figure 18: Configured tunnel across IPv4 domain



The tunnel can span any segment of the path, router-to-router, host-to-router, host-to-host or router-to-host.

There are two types of tunnelling:

- "configured (or manual) tunnelling" where the destination address of the packet differs from tunnel end point and additional configuration information is needed. Configured tunnelling is used to provide permanent tunnels between routers or other situations where there is a regular and frequent stream of traffic

- "automatic tunnelling" where the end point is equal to the destination address. Automatic tunnelling is used to provide temporary tunnels that are set up before communication and torn down afterwards.

During decapsulation the IPv4 header that was added during encapsulation is discarded. After the IPv6 packet is decapsulated, it is processed almost the same as any other received IPv6 packet and so the features offered by IPv6 options are preserved.

Many of the tunnel techniques cannot work if an IPv4 address translation happens between the two ends of the tunnel because both endpoint addresses need to be known to configure the tunnel.

E3.3 6 to 4

This method belongs to the automatic tunnel configuration tools. An IPv6 address is derived from the IPv4 address of the node, a special TLA is used for that purpose. With this mechanism, sites can start to deploy IPv6 without having to ask for IPv6 address space from the registries i.e. by using the values of IPv4 address that they have already been assigned.

E3.4 Gateways and Protocol Translators

Gateways and protocol translators are alternatives or supplements to dual stack for enabling IPv6 nodes to communicate with the IPv4 world.

Gateways operate at the application layer and are specific to particular applications, i.e. they run the application protocol.

RFC1928 describes a SOCKS gateway that accepts connections from IPv4 hosts and relays them to IPv4 or IPv6 hosts. It is basically a method to traverse firewall systems based on an authentication procedure. SOCKS are located between the transport (TCP/UDP) layer and the application layer.

Translators operate at the network layer and provide translation from one form of address to the other.

The Stateless IP/ICMP Translator (SIIT, RFC2765)describes a method to translate IP headers between IPv6 and IPv4 in a stateless mode. The IPv4 address will be assigned to the IPv6 node temporarily.

NAT-PT (RFC2766) uses a stateful dedicated translation service for a site. An application layer gateway is included to support DNS requests and answers.

Annex F: Description of IP addresses and their allocation

F.1 IPv4 addresses

IPv4 uses a 32 bit address field. The main type of address is the unicast address, which identifies an interface on a host or node. Although this address is a binary field, it is normally written in the form of four groups of 1-3 decimal digits, e.g.:

192.108.100.1

The unicast address has two parts, the network identity and the host identity. Initially this space was structured to give three different classes of unicast address with a different boundary between these identities so that address space could be used more efficiently given that there is a wide distribution of host network sizes. (see RFC 791). However when the rapid growth of the Internet started, putting special pressure on Class B addresses, the class definitions with their fixed boundaries were withdrawn in 1993-4 and replaced by the Classless Inter Domain Routing (CIDR) allowing the boundary for each network to be adjusted to the requirements of the network plus a small allowance for growth.

The network identity is generally called the "prefix" and a prefix is normally written with a suffix of /n where "n" indicates the length in bits of the network identity or prefix, e.g.

192.108.100 /24

The allocations of network identities were initially "flat" and unstructured. This meant that routers needed to analyse the whole network part of the address in order to decide on routing. This resulted in the problem of the size of the routing tables in the routers growing faster than the capability of the router processors. To overcome this problem, CIDR also introduced the concept of aggregation at the higher level of the addresses. This meant that addresses were allocated so that all networks that were connected to the same backbone had the same early part (called prefix) of the address. This reduced the amount of analysis to be undertaken by most routers and reduced the number of routes that had to be announced to the outside world and included in routing tables. CIDR also increased the effectiveness of the usage of address space allocated to a site, because the size of the space could be better fitted to the needs

At present with IPv4, aggregation has reduced the rate of growth of routing tables to a manageable rate (i.e. they are growing more slowly than processor capability), however the growth rate is increasing again.

Because aggregation was not started at the beginning and because the relationships between networks and backbone networks can change, there is not 100% aggregation in practice. The exceptions are called holes and should be avoided wherever possible as they increase the size of the routing tables. However the extent of the aggregation achieved is acceptable.

Most of the address space is allocated as provider aggregated space (PA), where the identity of the interconnected backbone network is contained in the identity of the network. This means that a site has to give back the address space to the ISP when it changes to another ISP and introduce new values for the address space. Thus renumbering is a serious issue in IPv4 . Changes of addresses would require:

- changes in routing tables and routing policy for the site networks
- changes in the Resource Records in the DNS system
- changes in host addresses within the network

The external changes to networks unavoidably require some effort to change routing tables and update the DNS system. Changes internally can be labour intensive for network administrators. A work-around term solution sometimes suggested by the registries is for the network administrators to use private addresses and Network Address Translators (NATs) instead of globally routable addresses. NATs are used at the boundary of the network to enable a private addressing scheme to be used within

the network. The private addressing scheme can remain unchanged when external connections change and thus they reduce the renumbering problem.

However NATs introduce disadvantages, see:

- Internet-Draft "Architectural Implications of NAT" (draft-iab-nat-implications-09.txt) by T. Hain
- "Protocol Complications with the IP Network Address Translator" (draft-ietf-nat-protocol-complications-02.txt) from the IETF NAT WG.

One of the biggest problems with is that NATs affect the transparency of the end-to-end connectivity, a fundamental assumption in the Internet design (see also RFC2775 "Internet Transparency" by Carpenter). Loss of transparency:

- disables a whole set services like IP security
- introduces a single point of failure, and
- makes the network less robust because in a failure situation the state values stored in the NAT will be lost making recovery in most cases impossible.
- create problems when two companies with "uncoordinated" private addresses merge

A further method of reducing the demand for IP addresses is to use dynamic rather than permanent assignment of addresses. This solution is used by many dial-up ISPs, where addresses are allocated for each dial-in session. The protocols that support this are Dynamic Host Configuration Protocol (RFC 1541) and Point-to-Point Protocol (RFC 1661).

These developments, together with somewhat stricter assignment policies that now require evidence of need, have reduced the risk of the IPv4 address space being exhausted at least within the next five years with the current rate of growth in the fixed networks.

F.2 Current allocation method for IPv4 addresses

IP addresses are allocated by Regional Internet Registries (RIRs) in accordance with policies set by ICANN and its predecessor IANA. There are currently three RIRs although new ones for South America and Africa may be created:

- Asia Pacific Network Information Centre (APNIC)
- American Registry for Internet Numbers (ARIN)
- Réseaux IP Européens (RIPE NCC), located in Amsterdam

Each RIR allocates IP addresses to Local Internet Registries, which are commonly Internet Service Providers (ISPs). These Local IRs operate under the authority of the Regional IR and hold allocations for assignment to users. The term "allocation" is used for space held by IRs for future assignment to users. Only assigned space is used by networks.

The goals of the allocation and assignment system are:

- uniqueness
- aggregation, to facilitate routing
- conservation
- registration

Aggregation and conservation are sometimes conflicting because to maintain aggregation in a growth scenario spare space for growth must be included around allocations and if this space is not used eventually it may not available for other users without creating a hole in the aggregation

Two types of address space are used:

- provider aggregatable address space, where the aggregation is with respect to the connection to a backbone network.
- provider independent address space, which may incur extra routing charges because of the additional complexity caused for routing tables and is assigned only under special conditions

If a user with provider aggregatable address space changes its interconnection arrangements, then it will have to release its addresses and obtain new ones. It will then have to change any internal addresses that are visible to the public Internet.

F.3 New arrangements for IPv6

IPv6 has a much larger address space than IPv4 and is structured differently so that aggregation is built in to the structure. Thus there is no provider independent address space as there is with IPv4. The RIRs have published a draft set of common principles for IPv6 allocation. However this draft received some criticism because its allocation strategy was too conservative and it is to be rewritten as soon as possible.

The allocation hierarchy of IPv6 is

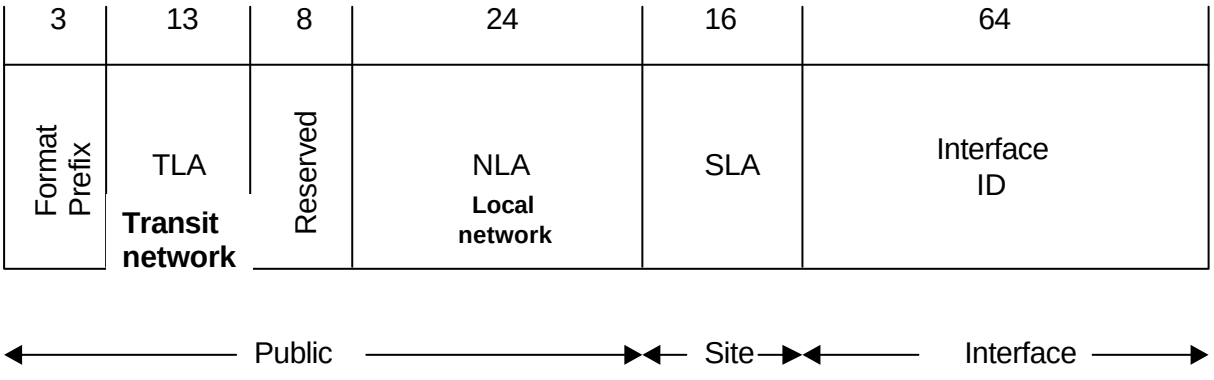
- ICANN
- RIRs, who allocate TLAs to LIRs (Local Internet Registries)
- LIRs (also known as TLA Registries), who may be transit operators and allocate NLAs and SLAs
- NLA registries, who are ISPs
- end-sites

NB: The terminology is confusing. "TLA Registry" means "a registry that is a TLA"; NOT "a registry that allocates TLAs".

Because of the network hierarchy of IPv6, TLA registries, which are transit operators, carry out functions similar to those that RIPE NCC carried out for IPv4.

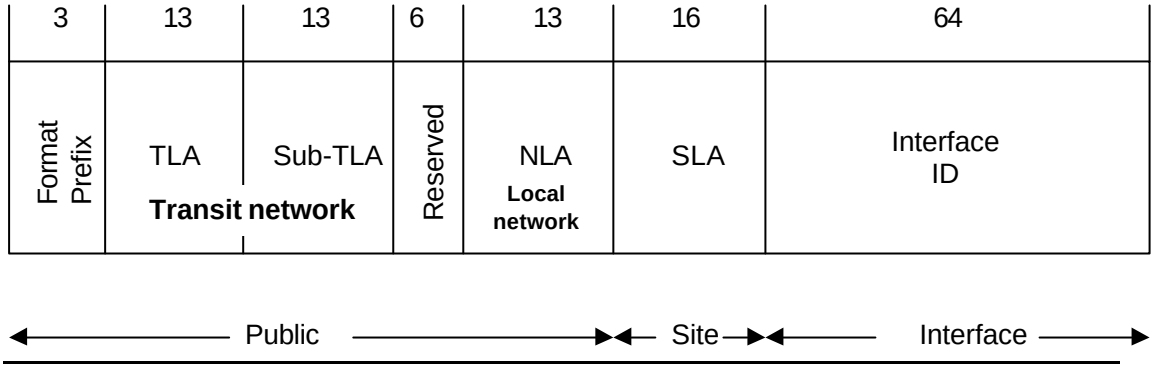
Figure 19 shows the mains structure of IPv6 addresses. Only 8192 TLA ids are available for transit operators and so they need to be assigned with care.

Figure 19: General structure of IPv6 addresses



Consequently a different initial structure will be used where one TLA value (0x0001) will be shared and sub-TLAs will be allocated out of it to the applicants for TLAs. These transit operators will use this allocation for assignments to ISPs (NLAs) until it is 80% used. Only then will they qualify for a full TLA assignment or a further sub-TLA. Figure 20 shows this initial structure as used by RIPE NCC.

Figure 20: Initial structure of IPv6 address used by RIPE NCC under prefix (TLA 0x0001)



For purposes of a "slow start" of a sub-TLA, the first allocation to a TLA Registry may be a /35 block (representing 13 bits of NLA space). The Regional IR making the allocation will in this case reserve an additional six bits for the allocated sub-TLA. When the TLA Registry has fully used the first /35 block, the Regional IR will use the reserved space to make subsequent allocations to the same NLA.

Regional IRs will only make an initial allocation of sub-TLA address space to organisations that meet criterion (a) AND at least one part of criterion (b), as follows:

a. The requesting organisation's IPv6 network must have exterior routing protocol peering relationships with the IPv6 networks of at least three other organisations that have a sub-TLA allocated to them.

AND either

b(i). The requesting organisation must have reassigned IPv6 addresses received from its upstream provider or providers to 40 SLA customer sites with routed networks connected by permanent or semi-permanent links.

OR

b(ii). The requesting organisation must demonstrate a clear intent to provide IPv6 service within 12 months after receiving allocated address space. This must be substantiated by such documents as an engineering plan or deployment plan.

For an initial bootstrap phase, b(1) is replaced by:

c. The requesting organisation must be an IPv4 transit provider and must show that it already has issued IPv4 address space to 40 customer sites that can meet the criteria for a /48 IPv6 assignment. In this case, the organisation must have an up-to-date routing policy registered in one of the databases of the Internet Routing Registry, which the Regional IR may verify by checking the routing table information on one of the public looking glass sites).

OR

d. The requesting organisation must demonstrate that it has experience with IPv6 through active participation in the 6bone project for at least six months, during which time it operated a pseudo-TLA (pTLA) for at least three months. The Regional IRs may require documentation of acceptable 6Bone routing policies and practice from the requesting organisation.

TLA registries must register all end-sites.

Annex G: ICANN

G.1 Introduction

The Internet Assigned Numbers Authority (IANA) was originally the central coordinator for the assignment of unique parameter values for Internet protocols, being chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters. The IANA responsibility is now largely incorporated into the Internet Cooperation of Assigned Names and Numbers (ICANN).

ICANN is a non-profit organisation operating under Californian law. It is based in Marina del Rey, California.

The formal objectives of ICANN as set out in its articles are to:

"pursue the charitable and public purposes of lessening the burdens of government and promoting the global public interest in the operational stability of the Internet by

(i) co-ordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet;
(ii) performing and overseeing functions related to the co-ordination of the Internet Protocol ("IP") address space;
(iii) performing and overseeing functions related to the co-ordination of the Internet domain name system ("DNS"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system;
(iv) overseeing operation of the authoritative Internet DNS root server system; and
(v) engaging in any other related lawful activity in furtherance of items (i) through (iv)."

The Corporation is required to:

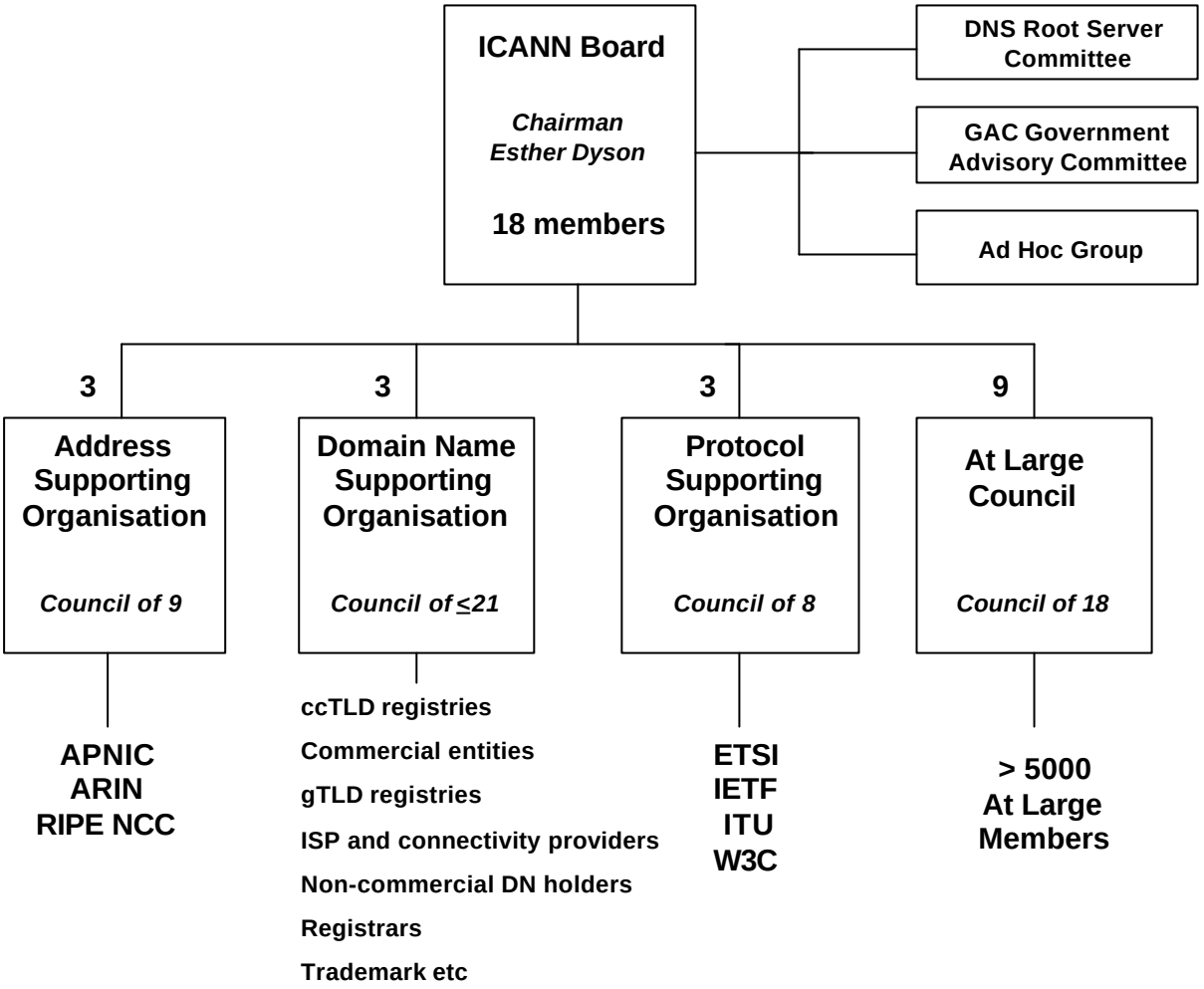
"operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this effect, the Corporation shall co-operate as appropriate with relevant international organizations."

ICANN is controlled by a Board of elected Directors, from which elected politicians and Government officials are excluded. Initially there was an Interim Board but a permanent one was elected in October 1999, consisting of 19 people:

- Chairman: Esther Dyson
- 9 Directors representing the three Supporting Organisations (three each)
- 9 Directors representing the At Large members

There are three Supporting Organisations and an At Large Membership. The overall structure is shown in Figure 21.

Figure 21: Structure of ICANN



G.2 Address Supporting Organisation (ASO)

The ASO is run by the Address Council of nine members, three from each of the three Regional Internet Registries (RIRs). There is an open General Assembly once a year. The work is governed by an MOU which defines the functions as:

- definition of global policies for the distribution and registration of Internet address space (currently IPv4 and IPv6);
- definition of global policies for the distribution and registration of identifiers used in Internet inter-domain routing (currently BGP autonomous system numbers); and
- definition of global policies concerning the part of the DNS name space which is derived from the Internet address space and the inter-domain routing identifiers (currently in -addr.arpa and ip6.int).

G.3 Domain Name Supporting Organisation (DNSO)

The DNSO is run by the Names Council of up to twenty one members, three from each of the seven constituencies;

- ccTLD registries;

- commercial and business entities;
- gTLD registries;
- ISP and connectivity providers;
- non-commercial domain name holders;
- registrars; and
- trademark, other intellectual property and anti-counterfeiting interests.

There is also a General Assembly open to all members. The function of the DNSO is to advice the Board on policy issues relating to the Domain Name System. The DNSO has the following working groups:

B - Famous Trade Marks
D - Business Plan and Internal Procedures
E - Global Awareness and outreach

G.4 Protocol Supporting Organisation (PSO)

The PSO is run by a Council of eight members with two each representing the four member Standards development organisations:

- Internet Engineering Task Force (IETF)
- World Wide Web Consortium (W3C)
- International Telecommunications Union (ITU);
- European Telecommunications Standards Institute (ETSI)

The function of the DNSO is to advice the Board on policy issues relating to the assignment of parameters for Internet protocols.

G.5 At Large Membership

The At Large membership was created in response to the proposal in the US White Paper that ICANN should "preserve the tradition of bottom-up governance". At Large members are individuals who may in future pay a small membership fee to cover the costs of membership. Provided that there are over 5000 such members, they may elect the At Large Council or up to 18 members, which selects nine Board members. The At Large membership is due to be created early in 2000.

G.6 Government Advisory Group (GAC)

A Government Advisory Committee provides advice to the Board on those activities of ICANN that relate to concerns of governments, particularly matters where there may be an interaction between ICANN policies and various laws, and international agreements. ICANN recognises that Governments have ultimate public policy authority over their ccTLDs. GAC does not itself make decisions for ICANN. Membership is open to all national governments. Some 31 Governments sent representatives to the last meeting. Discussions focused on the delegation and management of ccTLDs.

Members of the Governmental Advisory Committee are representatives of national governments, multinational governmental organisations and treaty organisations, one representative each.

Annex H: IETF

Ref: "The Organizations Involved in the IETF Standards Process", RFC 2028, BCP 11

The Internet Engineering Task Force (IETF) is an open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is important to note that the IETF is not a corporation: it is an unincorporated, freestanding organization.

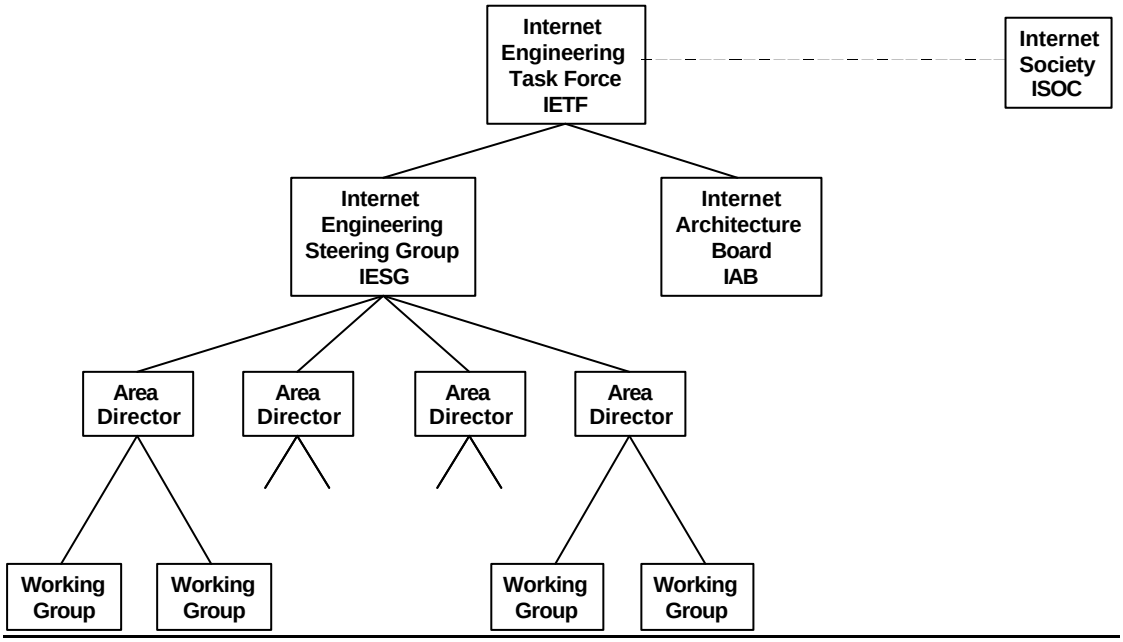
The IETF is partially supported by the Internet Society (ISOC). ISOC is a US-based non-profit membership corporation with thousands of individual and corporate members throughout the world who pay membership fees to join. The Internet Society provides many services to the IETF, including insurance and some financial and logistical support.

As described in BCP 11, Internet standardization is an organized activity of the ISOC, with the ISOC Board of Trustees being responsible for ratifying the procedures and rules of the Internet standards process. However, the IETF is not a formal subset of ISOC; for example, one does not have to join ISOC to be a member of the IETF. There is no board of directors for the IETF, no formally signed bylaws, no treasurer, and so on. The structure of the IETF (its leadership, its working groups, the definition of IETF membership, etc) are described in detail in BCP 11.

The actual technical work of the IETF is carried out in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

The IETF working groups are grouped into areas, and managed by Area Directors (Ads). The ADs are members of the Internet Engineering Steering Group (IESG). The Internet Architecture Board (IAB provides architectural oversight. The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB. The structure is shown in Figure 22.

Figure 22: Structure of Internet organisations



Working groups exist only until the work according to the charter has been completed. New working groups will be established when there is a consensus in the community that this is useful, this is normally achieved by a BOF (an informal group called “Birds of a Feather”).

Further information on meeting dates, persons acting as ADs or WG chairs, RFCs, internet drafts etc can be found at http://www.ietf.org.