# A strategic numbering review

## Annexes to a report to the DGTP

John Horrocks
David Lewin
Claire Milne

**7 februari 2000**
TCA88

# Inhoudsopgave

# Annex A Basic characteristics of domain names

## A1 Introduction

The domain name is the centre of the Internet naming system and is used by various different protocols. Examples are:

- email address: dml@ovum.com
- document URL: http://www.ovum.com

In both cases the domain name is "ovum.com" and currently upper and lower case letters are not distinguished from each other. For the email address, "dml" is a local identifier under the Simple Mail Transfer Protocol (SMTP) for email. For the document URL:

- http indicates the protocol to be used
- www indicates the server to used at the Ovum host

Domain names are structured. The highest part is at the right hand end of the name which is called the Top Level Domain (TLD). Values within each TLD are assigned by competing Domain Name Registrars under rules established by the Domain Name Supporting Organisation of ICANN. The assignments for each TLD are held in a single registry (one per TLD) and updated by the registrars.

## A2 The domain name server

The domain names are supported by the Domain Name Server (DNS) system which stores Resource Records. The function of the DNS system is to "resolve" a domain name to an IP address and other information relating to the name. The IP address is used by the routers which handle the packets.

The process of resolution is a sequence of interrogations (question/response) interactions between the terminal and the domain name servers. The software in the terminals[1] stores permanently[2] the IP addresses of the 13 "root" servers that are the fixed entry points to the system. They are shown in Figure 1.

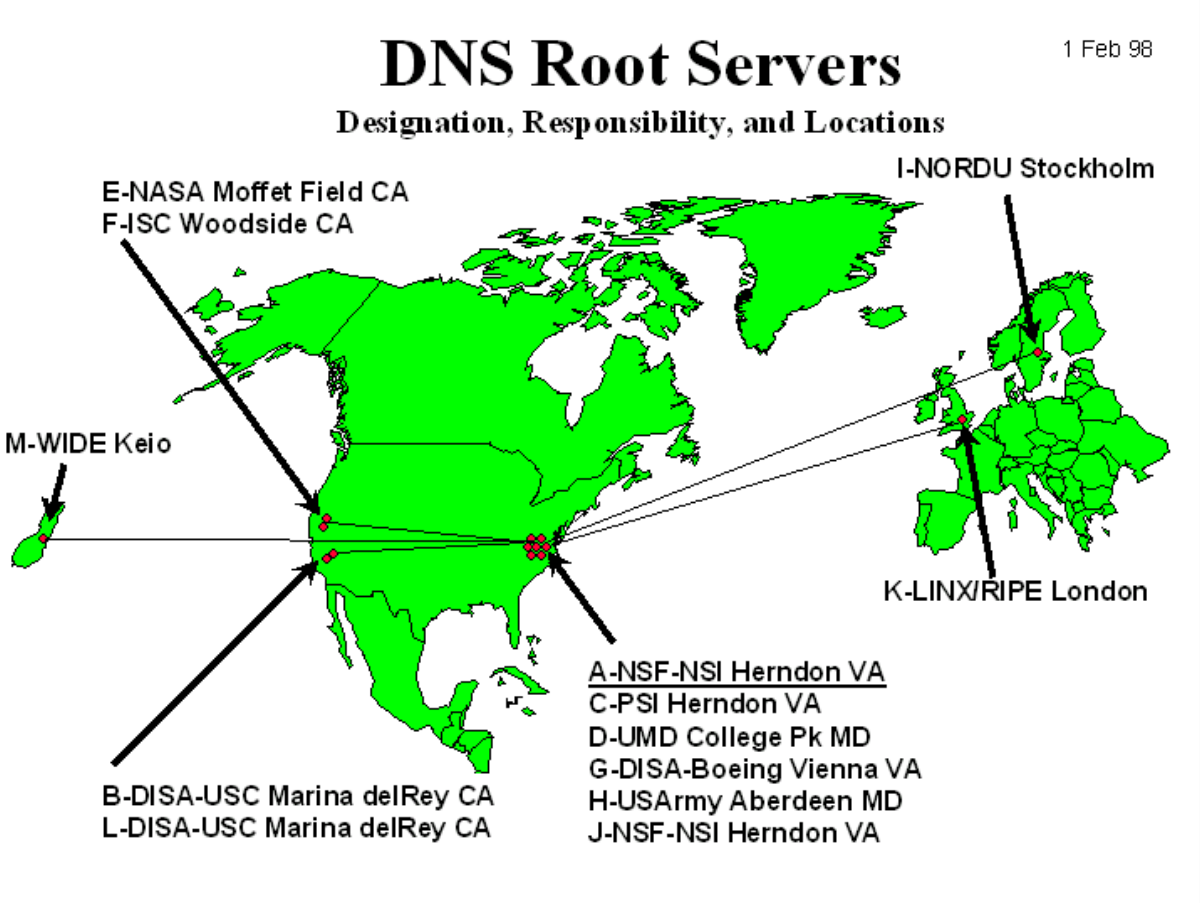
These servers are interrogated first and respond with the IP address of the server for the top level domain. The terminal then makes a second interrogation to this server. The server may respond with a final answer, or point to a further server. This process continues until the name is fully resolved to the relevant host. The sequence is shown in Figure 2 for the domain name ***ovum.co.uk***.

There is frequently some confusion about what is a host and how hosts relate to terminals and ISPs. In an SMTP email address such as John.Smith@ovum.com, ovum.com is the domain name for the email server host (Mail Transfer Agent) of Ovum. There is one domain name entry in DNS and one corresponding IP address (for the email server). All email to Ovum is sent to that address and the email host (a proxy = forwarding server) forwards the email to the users' terminals. Thus only the Ovum host knows the local routing arrangements for John.Smith. The same arrangement would apply for John Smith's private email received by John.Smith@compuserve.com with dial-up access

[1] eg browsers

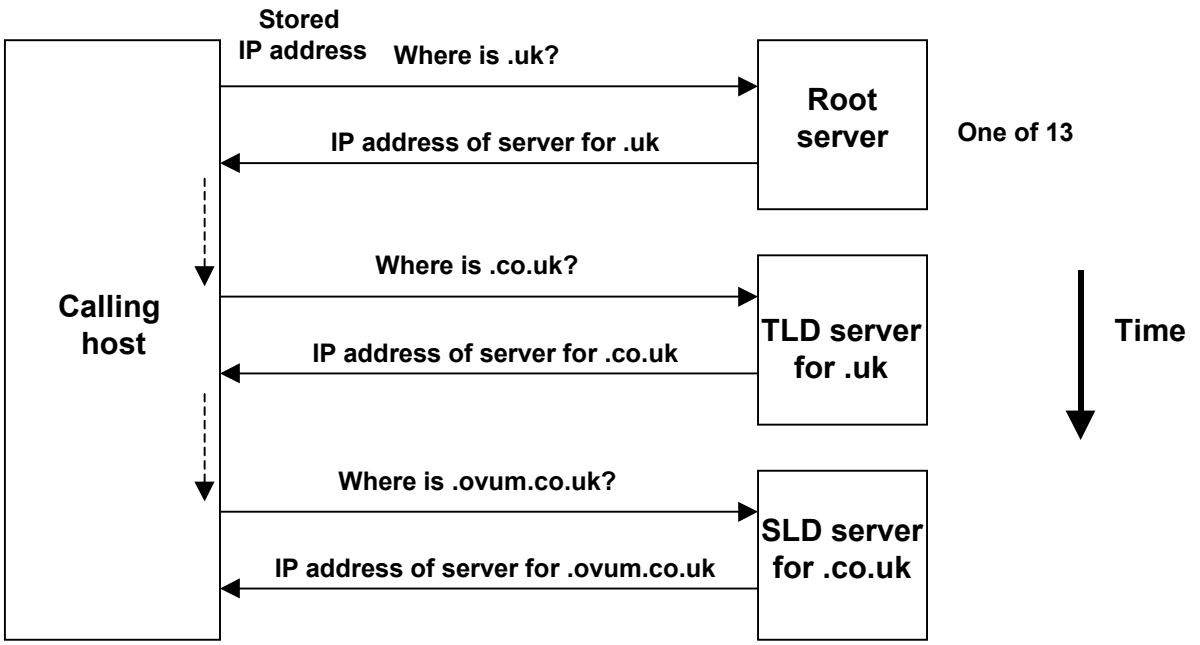
[2] ie the addresses are part of the software

**Figure 1 DNS root servers**




Source: http://www.wia.org/pub/rootserv.html

**Figure 2 Example of domain name resolution**




For some applications such as web browsing, John Smith's terminal, whether connected to the Ovum LAN or by dial-up to a Compuserve node, is allocated an IP address either temporarily or permanently. Temporary allocation is most common for dial-up. This means that the terminal is temporarily a host and IP packets are sent to it directly. However there would be no separate domain name for the terminal and so no individual entry in the DNS system.

It is possible for a mail server host to be run on a terminal such as a LAN terminal at Ovum. In this case the server would have its own domain name such as johnsmith.ovum.com and the SMTP address of the user would be say John@johnsmith.ovum.com. The main Ovum server (ovum.com) would provide the final stage of the DNS resolution for the domain name johnsmith.ovum.com.

In practice, both terminals and servers temporarily store information about the responses to queries that are frequent. This is called caching and cached information reduces the number of queries needed in practice.

In order to provide resilience in DNS, information is always stored in at least two DNS servers.

## A3 Portability

Domain names are portable because of their separation from addresses. A user that registers its own domain name can use that domain name on any ISP. However a user that does not register its own domain name but takes a name that is a subsidiary of an ISP's domain name cannot port their name because it is tied to the ISP.

For example: Ovum is registered with its own name "ovum.com" and can take service from any ISP. But if it used the ISP Pipex as "ovum.pipex.com", then it would not have portability. Only Pipex could port such names, not Ovum.

## A4 Relevant IETF RFCs on domain names

RFC 2606: Reserved Top Level DNS Names.

RFC 2303: Minimal PSTN address format in Internet mail

RFC 2181: Clarifications to the DNS Specification

RFC 2136: Dynamic Updates in the Domain Name System

RFC 1035: Domain names - implementation and specification

RFC 1034: Domain names - concepts and facilities

# Annex B Basic characteristics of IP addresses

## B1 Introduction

IP addresses are strings of binary digits that are used to identify the destination of a packet by the routers that handle the packet in the IP Layer.

Currently the version of the IP protocol used almost universally is IPv4, but a later version has been defined (IPv6) and networks are starting the process of migrating from IPv4 to IPv6. See later in this section for more detail.

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

- the identity of the network (eg the ISP)
- the identity of the host (the destination of the IP packet)

The identity of the host is assigned and managed by the network.

## B2 IPv4

IPv4 uses a 32 bit address field. Initially this space was structured to give three different classes of address with a different boundary between the identities of the host and the terminal port. The purpose of the classes was to manage the addressing space more efficiently given that there is a wide distribution of host network sizes. Figure 1 illustrates.

### Figure 1 Classes in IPv4

| *Class* | *Format* |
|---|---|
| A | 7 bits for network identity; 24 bits for host identity |
| B | 14 bits for network identity; 16 bits for host identity |
| C | 21 bits for network identity; 8 bits for host identity |

The fixed boundary was used for a period but 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 /n that follows an address indicates the length in bits of the network identity.

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 length of the number that needed to be analysed by most routers.

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

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 require fuller analysis. However the extent of the aggregation achieved is sufficient.

Aggregation introduced the problem that the identity of the interconnected backbone network is contained in the identity of the network. If the interconnection arrangements change, either the addresses have to change or expensive holes are created in routing tables. Changes of addresses would require:

- changes in routing tables in the interconnected networks
- changes in the Resource Records in the DNS system
- changes in host addresses within the network

The external changes to networks can be accomplished reasonably easily as routing tables can be updated automatically as can the DNS system. Changes internally can be labour intensive for network administrators. A solution for the network administrators is provided by Network Address Translators (NATs) used at the boundary of the network that enable a private addressing scheme to be used within the network. The private addressing scheme can remain unchanged when external connections change.

NATs are becoming quite widespread, and have been pushed heavily by vendors, but the Internet Addressing Board is against their use because they:

- Balkanise the Internet, ie divides up what was meant to be a homogeneous whole into separate network (this is just what the telecom operators may need to do)
- introduce a single point of failure (the NATs)
- fail to support applications that can use IP addresses at the application layer (actually bad practice)

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 largely removed the risk of the IPv4 address space being exhausted at least within the next 20 years with the current rate of growth.

## B3 Routing

The Internet consists of interconnected autonomous systems (individual networks) where an autonomous system is defined as an area under the same control. For ease we will call them networks in the reminder of this subsection. There are three types:

- stub networks, connected to one other network only
- multi-homed networks, connected to more than one other network, but not willing to accept transit traffic
- transit networks, connected to more than one other network and designed to carry transit traffic.

The transit networks form the backbone and know the address ranges of the stub and multi-homed networks connected to them.

The transit networks are interconnected to each other in an unstructured manner. Each network needs to build up and maintain routing tables so that it knows how to route outgoing traffic. The protocol designed for exchanging and updating this information is called the Border Gateway Protocol and version 4 (BGP-4) is currently in use to support IPv4 with CIDR aggregation.

The main routing method is called per-hop routing where each network decides on the path down which to route each packet and leaves the subsequent routing decision to the next network. The alternative to this is called policy based routing where the source determines

the policy for the route to be taken. Although BGP-4 is used mainly for per-hop routing, it does include some capability for unstandardised information exchange that can be used for exchanging policy information.

BGP-4 is used to exchange and update information on the range of addresses that can be reached by each transit network. This information is expressed through the a prefix (the first part of the network identity in the address) that is associated with a path identity (eg an output port). Information on the ease with which the prefix area may be reached may also be included. The networks maintain an Information Base of this information and use it for making routing decisions.

Each end of a BGP-4 connection is called a speaker, because it tells the other end what traffic it can handle. The process of telling the other end is called “advertising”.

## B4 IPv6

IPv6 is a complete revision of the IPv4 protocol. The introduction of IPv6 is currently starting.

IPv6 is not backwards compatible with IPv4 and this means that there are two different technology domains within the Internet with gateways handling conversions from one domain to another. Hosts that both use IPv6 can communicate with each other across IPv4 by using tunnels where the IPv6 protocol messages are carried inside IPv4 messages.

IPv6 contains a huge 128 bit IP address space ($2^{128} \simeq 10^{39}$). The addresses identify interfaces or sets of interfaces. There are three types:

- unicast: An identifier for a single interface
- anycast: An identifier for a set of interfaces where a packet is delivered to any one of the set, normally the nearest
- multicast: An identifier for a set of interfaces where a packet is delivered to all of the set.

Addresses may be written as ***x:x:x:x:x:x:x:x*** where “***x***” is a hexadecimal value (up to 4 characters where leading digits may be suppressed) of the eight 16 bits of the binary address. An example would be:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

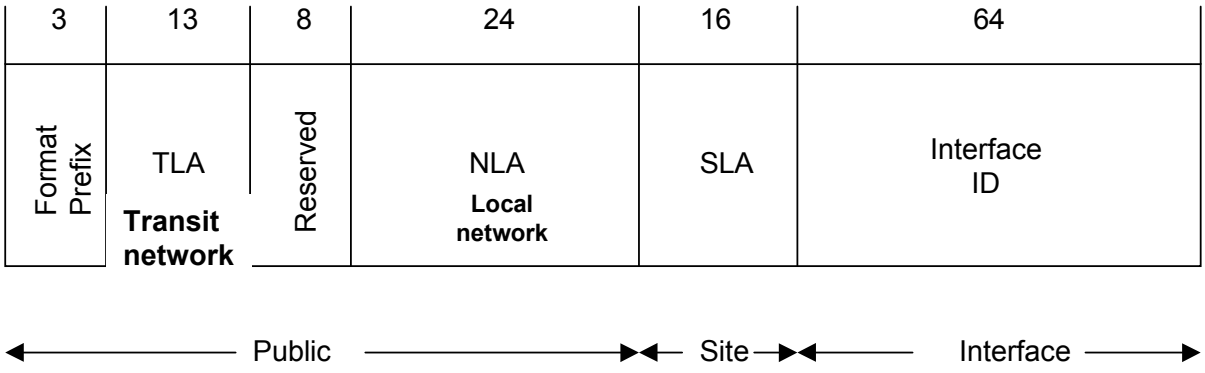
There are additional rules for shortening the presentation if there are groups of zeroes.

Prefixes are written in the same way as part of an address but followed by /xy where xy gives the length of the prefix in bits. An example is:

12AB:0000:0000:CD30:0000:0000:0000:0000/60

The form of the IPv6 address is shown in Figure 2. Because there are only 8192 TLA values available, there is a different initial form where a single TLA value is shared and the share has to be at least 80% used before a full TLA is allocated. Chapter 7 of the main report provides more detail.

**Figure 2 Structure of an IPv6 address**




The figures indicate the number of bits for each field eg for:

- the TLA or Top-Level Aggregation Identifier which is used by transit operators who are called TLA Registries[3], and who allocate NLAs
- the NLA or Next-Level Aggregation Identifier, which is normally used by ISPs who are also NLA registries
- the SLA or Site-Level Aggregation Identifier
- The Reserved field gives some flexibility for expansion of either the TLA or NLA fields.

There are currently two other alternative forms:

- a form where an IPv4 address is embedded into the IPv6 address, it uses the last 32 bits
- a form where an NSAP address is embedded into the IPv6 address (RFC 1888)

The first is comprehensible, the second is reprehensible. It involves embedding a name (an NSAP is really a name) in an address and this is architecturally strange. According to one of the main technical people in the IPng Working Group of IETF that prepared the IPv6 specification, the option to use NSAPs was a political compromise to resolve differences between two groups. Many of the people in IETF hope that the NSAP option will not be used. However the architectural issues of mixing names and addresses do not seem to be fully appreciated in IETF. Currently there is no sign of NSAPs being used.

## B5 IPv4 vs IPv6

The following are the main differences and improvements that IPv6 offers in comparison to IPv4:

- aggregation in the addresses that simplifies routing without having the holes that IPv4 has due to its initial allocation policies
- no need for NATs
- no need for dynamic assignment as each host can have its own address
- better security features with a standard method of checking authenticity
- auto-configuration of addresses, which significantly reduces the administrative task when networks change their interconnection arrangements, because the host can easily amend the IP addresses of the terminals

[3] The terminology is confusing. “TLA Registry” means “a registry that is a TLA”; NOT “a registry that allocates TLAs”.

- the new anycast feature
- a 20-bit traffic flow identification field that can be used for the support of QoS features

The transition from IPv4 to IPv6 is only just starting and it is not clear how rapidly the migration will proceed.

## B6 Relevant IETF RFCs on IPv4

RFC 2101: IPv4 Address Behaviour Today

RFC 1771: A Border Gateway Protocol 4 (BGP-4)

RFC 1661: The Point-to-Point Protocol (PPP)

RFC 1541: Dynamic Host Configuration Protocol

RFC 1519: Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy

RFC 1518: An Architecture for IP Address Allocation with CIDR

RFC 791: Internet Protocol

## B7 Relevant IETF RFCs on IPv6

RFC 2460: Internet Protocol, version 6 (IPv6) Specification

RFC 2374: An IPv6 Aggregatable Global Unicast Address Format

RFC 2373: IP Version 6 Addressing Architecture

RFC 2304: Minimal fax address format in Internet mail

RFC 2303: Minimal PSTN address format in Internet mail

RFC 1888: OSI NSAPs and IPv6

# Annex C Protocols for enabling VoIP

## C1 Introduction

There are two main rival protocols for carrying voice over IP ie:

- SIP and the associated PINT for PSTN and Internet interworking
- H323.

We describe them in this annex.

## C2 SIP/IPTEL

The Session Initiation Protocol (SIP) is a simple application layer text based protocol for establishing, changing and ending calls between one or more IP based terminals. The protocol is based on the protocols used for email and web pages, which follow a client-host model, and much of the syntax of these protocols is re-used. Consequently each terminal has two components:

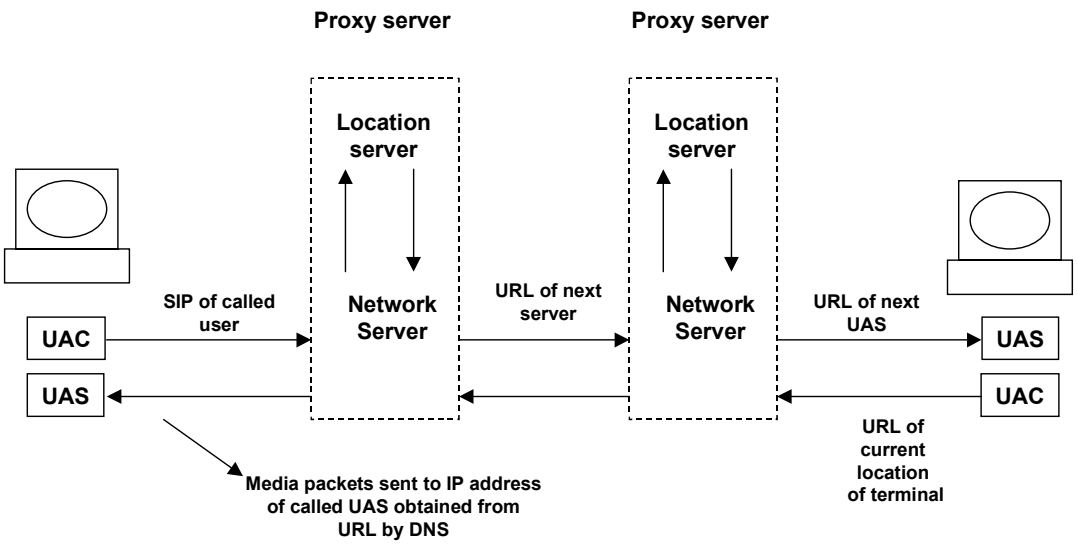
- User Agent Client (UAC) for sending calls
- User Agent Server (UAS) for receiving calls

SIP is supported in networks by a server that controls the calls. There are two types of network server:

- a proxy server that receives requests for calls, determines the location of the caller and forwards a modified request either to the next such server (next hop routing) or direct to the far end terminal (UAS). The forwarding normally uses the domain name of the next server.
- a redirect server carries out the same functions but replies to the calling UAC giving it the necessary information to contact the next server or far end directly.

The main function of the network server is to provide name resolution and user location. SIP uses SIP names that have the same form as email addresses. The sequence of a SIP call set-up using a proxy server is shown in Figure 1. As the SIP call set-up proceeds, translations are carried out as necessary at the name level (not name to IP address) to route the signalling to the far end. The purpose of this possible series of translations at the name level is to provide some control over the route of the call signalling and to provide scope for mobility and call re-direction. Responses from the far end are sent back through the same proxy servers, though subsequent signalling may be sent direct end-end. The Session Description Protocol (SDP) carried within SIP defines the addresses and ports for the media channel in terms of IP addresses. A proxy server can insert itself into the media stream by over-writing the SDP information but this destroys end-end authentication.

## Figure 1 Example of a SIP call set-up




SIP calls can be initiated from web pages by including the text in the same way that emails can be initiated eg ***sip:john.smith@ovum.com.*** Also SIP can work with CGI (Common Gateway Interface) to enable programmable user control.

SIP supports both stateless and stateful options, although it was originally designed so that the network server would be stateless. In the stateful option any network server can select an option in the messages that ensures that all subsequent signalling for that call passes through that server. Although the call signalling can be controlled in this way, the media stream normally goes direct end to end.

SIP is seen as being part of a set of basic components that will be used for VoIP. The other main components are:

- the Real-time Transport Protocol (RTP)
- quality of service protocols such as the Resource Reservation Protocol (RSVP)
- authentication, authorisation and accounting
- Gateway Discovery Protocol

- Lightweight Directory Access Protocol (LDAP)

The Internet draft on Telephony Routing over IP (TRIP) describes a framework for the discovery and exchange of routing tables between service providers.

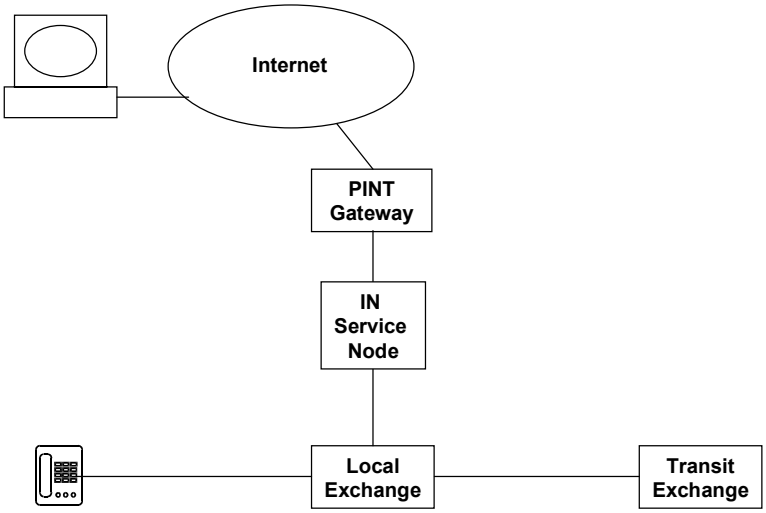
## C3 PINT (PSTN and Internet Interworking)

PINT is concerned with the provision of services where the Internet can initiate or enhance a telephony call on the PSTN, such as

- click-to-dial
- click-to-fax
- click-to-fax-back (to receive a fax)
- web access to voice content (where the web can request information to be delivered over an incoming voice call)

Figure 2 shows the type of architecture under consideration. PINT will be based on SIP.

**Figure 2 PINT architecture**




## C4 H.323

H.323 is an ITU-T standard for "packet-based multimedia communications systems" and it has been taken as the basis for the ETSI work in Tiphon. H.323 was designed originally for end systems such as might be implemented on LANs but require interconnection to the PSTN/ISDN. Its design follows the principles of Q.931 - the ISDN network-terminal signalling system. Consequently it is not perfectly suited for SCN-IP interactions where transit network operations are involved.

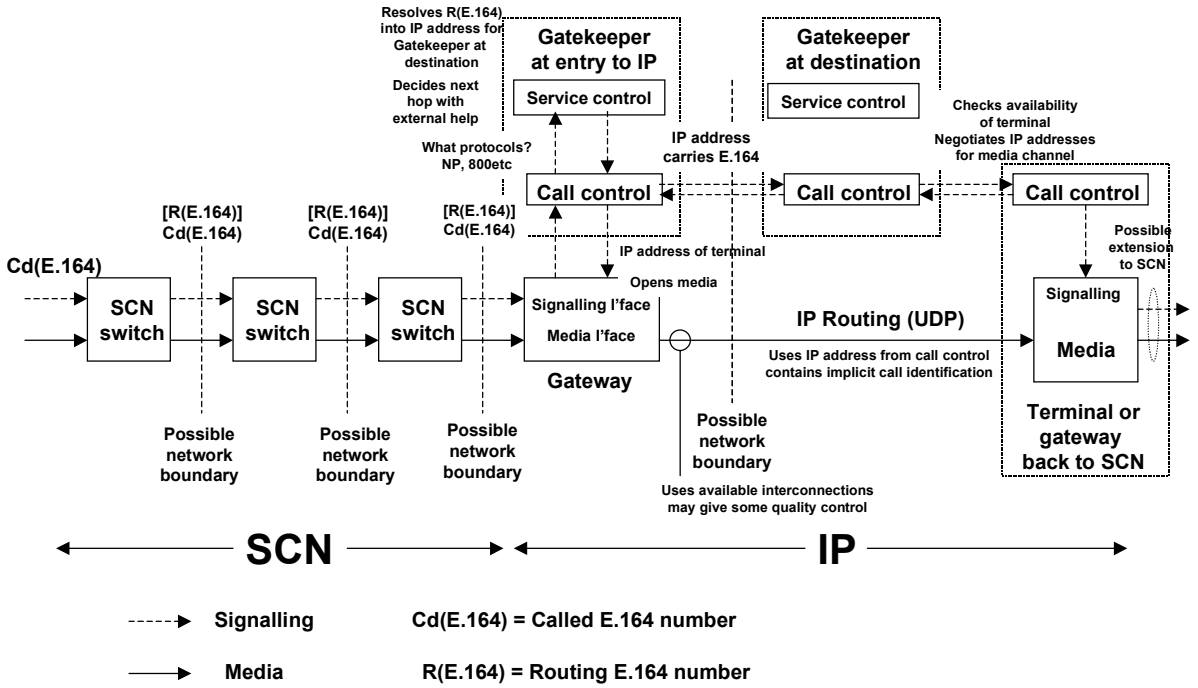
The key elements of H.323 are that:

- signalling and media are separated
- connections between SCN and IP are handled by gateways
- calls are managed and authorised by Gatekeepers whose IP addresses are held in a system modelled on DNS

Figure 3 shows a diagram from Tiphon of process of setting up a call to a customer served on IP or a gateway back into the SCN. The process has a number of important characteristics:

- the call originates with the caller identifying the called party/terminal with an E.164 number. The local switch that serves the calling party analyses at least a part of this number and routes the call in accordance with its routing tables. “Routing” means that the call is passed forward on a channel in a multiplexed transmission system that leads to the switch indicated by the routing tables. As part of the analysis, the switch processor may determine that the number is ported and may add routing information to the called E.164 number. The routing information may indicate a network, switch or concentrator and have the form of a prefix that would be analysed with the called party number or a separate E.164 number that replaces the called number. In the second case, the called number is sent forward in another field and later (eg at the switch or gateway indicated by the routing number) restored to its normal position
- the analysis performed by the switch may be rather basic, eg all calls to a certain country are sent on a particular group of channels, and will be based on the structure of the E.164 number. This structure will not normally indicate the technology used in the destination network as E.164 numbers are normally technology independent
- the call may pass through several switches in the same network or several other circuit switched networks. Eventually the call will reach a gateway at the boundary of the IP technology domain
- different parts of the gateway will provide the signalling and media interfaces. The signalling interface will interact with the SCN signalling by using SS7. The signalling interface sends the called E.164 number to the call control function
- the call control function resolves the E.164 number using whatever information is available. “Resolving” means that it determines from a database the IP address of the gatekeeper of the destination network or an intermediate network. This function is equivalent to the resolution of domain names by domain name servers into IP addresses. Information on the IP address of the terminal itself will not be available at this point. The Tiphon work has identified the different resolutions shown in Figure 4
- the call control sends a message to the call control function of the destination gatekeeper. This message is routed using the IP address of the gatekeeper but carries the E.164 number of the called party
- the destination gatekeeper determines from its local information the IP address of the call control function of the called terminal and signals to the terminal to check the availability of the terminal and determine an IP address for the media channel to use. This address is stored by the terminal’s call control function and when the media packets arrive it identifies which call the packets belong to. This address is only used by one call at a time
- the destination gatekeeper sends the IP address to be used by the media channel back to the call control at the gateway into the IP domain
- the signalling between the call control functions of the two gatekeepers also identifies the IP address to be used by the terminal for packets to be sent to the gatekeeper at the edge of the IP domain
- the gateway completes the signalling process with the SCN and media packets are routed directly between the gateway at the edge of the IP domain and the terminal.

## Figure 3 Handling of an incoming call with H.323 according to Tiphon




## Figure 4 Stages in the resolution of an E.164 number to an IP address

| *Resolution type* | *From* | *To* | *Status* |
|---|---|---|---|
| E.164 Search Engine | Any information | Called E.164 | Public service |
| E.164 Service Resolution | Called E.164 | Routing E.164 for home network | Specific to service or geographical area<br>Not specific to IP technology |
| E.164 - Home Gateway Resolution | Called + Routing E.164 combination | IP of home gateway | Public and global |
| E.164 - Intermediate IP Point Resolution | Called + Routing E.164 combination | IP of intermediate point (sometimes called contact address) | Local to network handling call |
| E.164 - Terminal Resolution | Called + Routing E.164 combination | IP of terminal | Local to home network |

## C5 SIP vs H.323

Articles about SIP and H.323 say that they are converging. SIP started stateless and is developing a stateful option. H.323 started stateful and is developing a stateless option. Both offer various supplementary services defined with differing degrees of precision

It is difficult to assess fully the status of each and their suitability for a general telephony service, but the overall impression is that, whilst both are ready or almost ready to provide a few calls, they need substantial further work before a mainstream interconnected telecommunications service can be implemented on IP.

## C6 Relevant IETF RFCs on SIP etc

RFC 2543: Session Initiation Protocol (SIP)

RFC 2327: Session Description Protocol (SDP)

RFC 2307: An Approach for Using LDAP as a Network Information Service

RFC 2255: The LDAP URL Format

RFC 2251: Lightweight Directory Access Protocol (v3)

RFC 1889: RTP: a transport protocol for real-time applications

Internet draft (iptel-glp): A Gateway Location Protocol

Internet draft (iptel-gwloc-framework): A framework for telephony routing over IP (TRIP)

Internet draft (iptel-cpl-framework): Call Processing Language Framework and Requirements

# Annex D Current VoIP numbering work in standards bodies

## D1 Activities in ITU

ITU-T Study Group 2 is responsible for E.164 numbering. In the period from early 1998 to May 1999 it considered a proposal from some ETSI members for a trial of a country code specifically for telephony on IP. The proposal was not approved but was never finally rejected.

SG2 is proposing to study the future requirements for numbering during its next study period. The main issues will concern:

- Internet telephony
- compatibility of terminal types
- a possible future user friendly all-embracing scheme

SG2 is planning a joint workshop with IETF for 25 to 27 January 2000 for a discussion of the issues of common interest.

ITU-T Study Group 13 has overall responsibility for IP related issues and is working mainly as a co-ordination body. It does not have any particular perspective on numbering as yet, according to its chairman, although it recognises the issue as important.

## D2 Activities in ETSI

### *SPAN 2*

SPAN 2 (Signalling and Protocols for Advanced Networks) is the main technical committee responsible for numbering within ETSI. It has been trying to start work on future numbering issues during 1999 but has received few inputs. The SPAN 2 participants are mostly also participants in ITU-T SG2 and so the approaches and main issues are similar. The underlying objective seems to be to develop a future user friendly all-embracing scheme, probably one that would sit on top of the existing E.164 and Domain Name schemes. As yet there are no clear proposals.

Several of the contributions introduce the concepts of labels. This concept is not very clear but seems to be a globally unique identifier for the top level in the "multi-everything" stack describer in Chapter 3. In other words a person might have several different labels for their different roles.

SPAN 2 is also starting work on standards to support the Internet Registration of Names (IRON). This work will be run by France Telecom/Oleane. Its purpose is to develop the standards needed for communication between competing registries/registrars.

### *HF*

The Human Factors technical committee is planning to start a specialist task force to run for the first half of 2000 to study possible solutions for user friendliness in naming and addressing. Initially the plan was to develop a new universal identification scheme, but the need for this was questioned and it is not so clear now exactly what the task force will do. The focus may move more to the development of directories.

### *Tiphon*

Working Group 4 in Tiphon is responsible for numbering issues (and is chaired in a different capacity by the author of this paper).

Tiphon spent most of the last 18 months developing proposals to SG2 for the use of a global code. Initially the proposal was for a global code for all telephony provided on IP, with the code acting as a form of escape indicator that would enable operators to detect the type of technology at the destination and route the call earlier to an IP gateway. It was assumed, probably mistakenly, that this would lead to lower interconnection charges and enable operators to charge less to callers. Because of a strong lobby that numbering should be technology independent, the proposal migrated to become a proposal for a service called the Full Feature Service which would provide full global portability. By May 1999 this modified proposal was gaining a little more support within SG2, but support for undertaking trials was reducing. Discussions have ceased, but a small group of operators is starting trials of the concepts.

Tiphon WG2 has developed:

- a basic specification on numbering for the Tiphon scenarios (ETSI TS 101 324)
- a short “Guide to numbering options for public networks based on VoIP technology” (ETSI TR 101 327)

The basic specification does not address any of the real problems while the Guide is intended mainly for new entrants that are not familiar with E.164 numbering. The Guide outlines the options and recommends that the numbering options should be chosen with regard to the services that will be supported. Thus various different types of E.164 number will be used by IP based networks, depending on the services that they offer.

WG4 is now working principally in two areas:

- the development of a guide on the implications of number portability for VoIP networks
- the development of an architecture or set of signalling flows showing the various processes involved in setting up a call including the resolution of the E.164 number into an IP address

At its last meeting, Tiphon clarified the service issue by deciding that it is not developing a special new telephony but is working on supporting the existing telephony service on IP, yet may develop some additional special features.

In general the work in Tiphon as a whole is disappointing with insufficient serious development work on the basic issues, nevertheless there are some signs of improvements.

### *3GPP*

3GPP is planning to base its Release 2000 set of specifications on IP. We have attempted to contact the key people without success. Examination of the draft documents available from the server suggests that:

- 3GPP is at a very early stage of considering the implications of using IP technology
- current thinking is to construct a GSM style architecture on the basis of IP. If so there will be little integration of the architectures
- the existing GSM numbering system using the MSISDN is foreseen.

## D3 Activities in IETF

IETF is structured into Areas, and four Working Groups in the Transport Area are working on issues relating strongly to VoIP:

### *SIP (Session Initiation Protocol)*

SIP is the basis of the IETF's approach to telephony. SIP and the related Session Description Protocol (SDP) have already been defined in RFC 2543 and RFC 2327 respectively. The Working Group is currently working on further developments including:

- developing the RFC on SIP further to become a draft standard
- completing the call control specification to cover multi-party services
- developing a caller preferences specification to enable intelligent call routing

### *IPTEL (IP Telephony)*

IPTEL is working on additional protocols to be used in conjunction with SIP for the support of telephony. The main areas of work are:

- development of a Call Processing Syntax to enable the user to interact with the servers who are setting up a call, for example to choose a response if the called party is busy
- development of a service model or framework document
- development of a Gateway Attribute Distribution Protocol for exchanging information between gateways of different networks about their connection and PSTN call handling capabilities. The protocol has to be scaleable and secure.

### *PINT (PSTN and Internet Interworking)*

This group works on arrangements by which Internet applications can request and enhance services where the telephony element is carried over the PSTN. the objectives are:

- to study architecture and protocols for services where an Internet user requests a PSTN call, such as click-to-dial, click-to-fax, click-to-fax-back (to receive a fax),web access to voice content (where the web can request information to be delivered over an incoming voice call)
- to describe current practices for these services
- to develop standards RFCs for a Service Support Transport Protocol (SSTP) between Internet applications and intelligent PSTN nodes
- to consider security issues
- to consider extensions to a wider base of PSTN IN services

Several Internet drafts have been produced including an Internet Call Waiting service which notifies a dial in Internet user that there is an incoming PSTN call on the same line.

### *ENUM*

ENUM has started work only this year and but has already produced a reasonably stable draft.

This working group will define an architecture and protocols for mapping a telephone number to a set of URLs which can be used to contact a resource associated with that number. This work therefore appears to presume that an E.164 number will be translated via a domain name to an IP address.

The rationale for this work comes from the fact that E.164 numbers, which mainly identify network termination points can in practice identify terminals that are used for many different services and protocols, eg ordinary telephones fax machines, pagers, data modems, email clients, text terminals for the hearing impaired, etc.

A prospective caller may wish to discover which services and protocols are supported by the terminal named by a given telephone number. The caller may also require more information than just the telephone number to communicate with the terminal.

The formal aims of ENUM are to specify an architecture and protocols which fulfil at least the following requirements. To quote:

1. The system must enable resolving input telephone numbers into a set of URLs which represent different ways to start communication with a device associated to the input phone number.
2. The system must scale to handle quantities of telephone numbers and queries comparable to current PSTN usage. It is highly desirable that the system respond to queries with speed comparable to current PSTN queries, including in the case of a query failure.
3. The system must have some means to insert the information needed to answer queries into the servers via the Internet. The source of this information may be individual owners of telephone numbers (or the devices associated to the number), or it may be service providers which own servers that can answer service-specific queries. The system shall not preclude the insertion of information by competing service providers (in such a way which allows for the source of the information to be authenticated).
4. The system shall enable the authorisation of requests and of updates.
5. The Working Group will carefully consider and document the security and performance requirements for the proposed system and its use.
6. The Working Group will understand the impact of developments in the area of local number portability on the proposed system.

ENUM is not working on developing protocols for routing calls or locating gateways, nor on the intelligent resolution of the queries that it handles.

The following is a description of what ENUM are planning. It is taken form a draft RFC prepared by Patrik Faltstrom of Tele2 in Sweden.

A new domain name are is created for E.164 numbers with the form (say):

(number in reverse).e164.int

The digits of the number are reversed and separated by dots. An example would be:

+44 20 7551 9000 becomes 0.0.0.9.1.5.5.7.0.2.4.4.e164.int

Thus each terminal with its own E.164 number would have a DNS entry. A query to a DNS with this domain name would receive all the Naming Authority Pointer (NAPTR) records on the various protocols supported on this domain name and the domain names for the called party under each protocol.

This information enables the calling party to select which type of service it wants to use, ie to select from the different services supported eg telephony or fax or email.

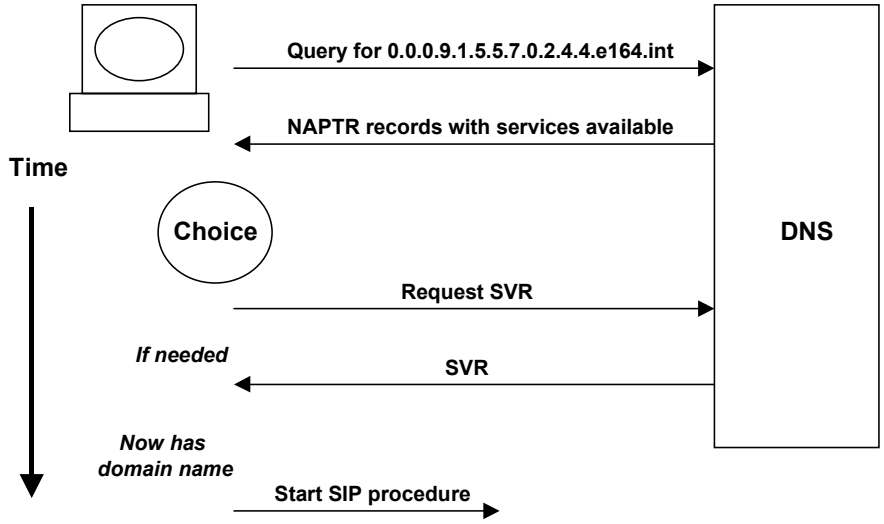
The NAPTR for the selected service may give enough information (domain name) to commence communication with the called party. Alternatively the NAPTR may specify that a Service (SVR) record must be obtained to define the port and domain name of the called host.

The calling party now has the necessary information to commence the communication. This might mean:

- starting a SIP communication
- starting an H.323 communication
- using a gateway to call via PSTN

The process is shown in Figure 1. We can see that the ENUM procedure provides functionality additional to SIP or H.323 and may involve a call using either SIP or H.323.

**Figure 1 ENUM procedure leading to a SIP procedure**




There is also a draft RFC for introducing a new protocol identifier for establishing calls to telephony and fax from within a service domain such as email or a web page. The form is something like:

- tel: +44 20 7551 9000
- fax : +44 20 7551 9091

### *IPv6*

In February 1999, the IETF Working Group on IPv6 considered a draft proposing the embedding of E.164 numbers within an IP address. The aim was to provide a unique addressing scheme for equipment with simultaneous access to the PSTN and the Internet IPv6. According to one of the authors, this was a personal idea that they are no longer pursuing.

# Annex E Possible shortages in the Dutch E.164 plan

## E1 Our approach to quantifying shortages

Our approach to quantifying the impacts of market developments on the Dutch E.164 plan is as follows. We:

- rearranged the developments of Figure 6.1 in the main text so as to:
- - group related developments together

- identify separately the effects on demand for numbers, blocks and ranges in the different parts of the numbering plan
- avoid double counting
- assigned a rough percentage growth figure over current levels of demand for 5 and 10 years ahead, for each of three growth scenarios:
- low growth (10% to 20% probability)
- medium growth (60% to 80% probability)
- high growth (10% to 20% probability)

The figures reflect the Ovum team's best subjective judgement. They are of course open to debate, and the model can be rerun with any desired inputs. Figure 1 shows the developments and the growth estimates which led to the conclusions presented above.

- treated "new service" effects and "increased efficiency" effects rather differently. New services effects, by definition, cannot be quantified in terms of percentage growth over current levels (since these are zero). So the numbers shown in Figure 1 refer to percentages of the capacity of the existing numbering plan at 9 significant digits. In contrast the increased efficiency developments of more portability, smaller blocks and individual allocation are assumed either to happen together, thereby doubling efficiency[4], or not to happen at all.
- combined these growth estimates to produce overall low, medium and high number demand scenarios for each range type[5]
- applied these demand scenarios to base data on the current utilisation of the numbering plan supplied by OPTA and summarised in Figure 2[6].

[4] From 40% to 80% in geographic ranges.

[5] .The developments affecting block demand turned out to be negligible in comparison with those affecting number demand, apart from "more competition". This last was assumed to be counterbalanced by small block and single number allocation effects, so its effects were not calculated separately.

[6] Together with our assumptions used where data were missing

## Figure 1 The developments and their estimated effects

| Development | Number type affected | Number level affected | Low | | Medium | | High | |
|---|---|---|---|---|---|---|---|---|
| | | | 5 yr | 10 yr | 5 yr | 10 yr | 5 yr | 10 yr |
| | | | Percentage growth over current levels | | | | | |
| More operators and service providers[7] | All | Blocks | 10 | 20 | 20 | 50 | 50 | 100 |
| Normal growth, fixed lines | Geog | Numbers | 5 | -5 | 10 | 10 | 10 | 20 |
| Normal growth, mobile subscribers | Mobile | Numbers | 50 | 100 | 100 | 200 | 300 | 500 |
| Normal growth, specially tariffed services | Special | Numbers | 20 | 50 | 50 | 100 | 100 | 200 |
| Machine communications | All | Numbers | 10 | 20 | 50 | 100 | 100 | 200 |
| Voice over IP | All | Numbers | 15 | 20 | 25 | 40 | 50 | 75 |
| Pay for product | Special | Blocks | 0 | 0 | 5 | 5 | 10 | 10 |
| More numbers per line[8] | Geog, mobile | Numbers | 20 | 50 | 50 | 100 | 100 | 200 |
| Alphanumerics | Mobile, special | Blocks | -5 | -10 | 0 | 0 | 10 | 20 |
| New services[9] | Special, reserved | Ranges | *10* | *20* | *20* | *50* | *50* | *100* |
| More portability | All | Numbers | N/a | N/a | N/a | N/a | N/a | N/a |
| Smaller blocks | All | Blocks | N/a | N/a | N/a | N/a | N/a | N/a |
| Individual allocation | All | Blocks | N/a | N/a | N/a | N/a | N/a | N/a |

## Figure 2 Base data on numbering plan utilisation

| | |
|---|---|
| Allocation of geographic blocks | See Figure 3 |
| Allocation of mobile number blocks | Blocks containing 15 m numbers already allocated or reserved; 5m mobile subscribers.<br>Efficiency: KPN ~60%, Libertel ~ 33% |
| Allocation of specially tariffed services (information numbers) allocated | 0800, 0900, 0906, 0909 ranges<br>Long numbers: 28.4m available, 38,500 used (0.14%)<br>Short numbers: 12,000 available, 3,500 used (30%) |
| Allocation of access codes | 100 available, 69 used |

[7] Including virtual network and VoIP developments, so far as they affect block demand

[8] Includes varying roles, distinctive ringing etc

[9] Includes machine communications (entirely new services) and mobile position fixing. Please see text for explanation of meaning of figures.

## Figure 3 Allocation of geographic blocks

| Code | Name | Number of such areas in class | Blocks allocated per area | Blocks allocated per class of area |
|---|---|---|---|---|
| 2-digit NDCs (700 blocks per area each of 10,000 numbers) | | | | |
| 020 | Amsterdam | 1 | 340 | 340 |
| 010 | Rotterdam | 1 | 220 | 220 |
| 030 | Utrecht | 1 | 130 | 130 |
| 070 | The Hague | 1 | 120 | 120 |
| Class 1.1[10] | Others, ave 80 blocks | *6* | *80* | *480* |
| Class 1.2 | Others, ave 60 blocks | *7* | *60* | *420* |
| Class 1.3 | Others, ave 40 blocks | *7* | *40* | *280* |
| Class 1.4 | Others, ave 20 blocks | *6* | *20* | *120* |
| | Total, 2-digit NDCs | 30 | | 2110 |
| 3-digit NDCs (70 blocks per area each of 10,000 numbers) | | | | |
| 0181 | Spijkenisse | 1 | 40 | 40 |
| 0113 | Goes | 1 | 39 | 39 |
| 0180 | Ijsselsteden | 1 | 39 | 39 |
| 0475 | Roermond | 1 | 38 | 38 |
| Class 2.1 | Others, 31 to 37 blocks | 8 | *35*[11] | *280* |
| Class 2.2 | Others, 21 to 30 blocks | 38 | *25* | *950* |
| Class 2.3 | Others, 11 to 20 blocks | 56 | *15* | *840* |
| Class 2.4 | Others, 0 to 10 blocks | 5 | *5* | *25* |
| | Total, 3-digit NDCs | 111 | | 2251 |

## E2 Results of modelling

We consider separately the results of this modelling exercise for geographic and other number ranges.

### *Geographic numbers*

Figure 4 below shows the outcome of combining all these inputs as described. The low scenarios showed few or no area code exhaustion, so for clarity these are not included in the figure. However we see that on the medium and high scenarios, exhaustion rapidly increases. The figure needs to be read in the context of the geographic spare capacity available, which is as follows:

- 10 spare 2-digit codes (assuming recovery of 042 and 014, currently in use for non-geographic applications)
- 89 spare 3-digit codes within groups already in use for 3-digit codes

To a limited extent, these codes can be deployed to relieve exhausted areas without change to existing code boundaries or the structure of the scheme.

However, we see that:

- improved efficiency can avoid large numbers of code exhaustion on any of these scenarios. (Note that the "current efficiency" scenarios would actually be worse than shown, because we have not included the block demand effects).
- even with improved efficiency, the more extreme of these scenarios could require code resources beyond those available, without some area restructuring

[10] Breakdown into classes assumed for the purpose of this exercise.

[11] Figures in italics assumed for the purpose of this exercise.

- the most difficult problems could occur if growth is such that a large number of the smaller 3-digit code areas all require relief
- with area restructuring, possibly extending to much larger (regional or even full national) geographic areas, the total capacity of the geographic ranges remains more than adequate even on the most extreme scenario (the maximum demand envisaged on our 10-year timescale is for around 210m numbers out of the 600m available12).

[12] Within the next decade it should become clearer whether continued growth in demand should be expected for Netherlands E.164 numbering over the following decade, or whether by then saturation has been reached.

## Figure 4 Additional geographic codes needed in assumed scenarios

| Area (or class) | Efficiency as now (40%) | | | | Improved efficiency (80%) | | | |
|---|---|---|---|---|---|---|---|---|
| | Medium | | High | | Medium | | High | |
| | 5 yr | 10 yr | 5 yr | 10 yr | 5 yr | 10 yr | 5 yr | 10 yr |
| 2-digit codes (additional 2-digit codes needed) | | | | | | | | |
| 020 | 1 | 2 | 2 | 6 | 0 | 1 | 1 | 3 |
| 010 | 0 | 1 | 1 | 3 | 0 | 0 | 0 | 1 |
| 030 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 |
| 070 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 |
| Class 1.1 | 0 | 0 | 0 | 6 | 0 | 0 | 0 | 0 |
| Class 1.2 | 0 | 0 | 0 | 7 | 0 | 0 | 0 | 0 |
| Class 1.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Class 1.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total, 2-digit codes | 1 | 3 | 3 | 26 | 0 | 1 | 1 | 6 |
| 3-digit codes (additional 3-digit codes needed) | | | | | | | | |
| 0181 | 1 | 2 | 2 | 7 | 0 | 1 | 1 | 3 |
| 0113 | 1 | 2 | 2 | 7 | 0 | 1 | 1 | 3 |
| 0180 | 1 | 2 | 2 | 7 | 0 | 1 | 1 | 3 |
| 0475 | 1 | 2 | 2 | 6 | 0 | 1 | 1 | 3 |
| Class 2.1 | 8 | 16 | 16 | 48 | 0 | 8 | 8 | 24 |
| Class 2.2 | 0 | 38 | 38 | 152 | 0 | 0 | 0 | 76 |
| Class 2.3 | 0 | 0 | 56 | 112 | 0 | 0 | 0 | 56 |
| Class 2.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total, 3-digit codes | 12 | 62 | 118 | 339 | 0 | 12 | 12 | 168 |

Spare capacity: 10 2-digit codes, 89 3-digit codes

### *Other number ranges*

The **mobile** case is simpler to examine because there is much less structure to the numbers. We assume that this will continue, ie the 06 range will not be split up into significant subranges, and there will be operator portability and small block or individual number allocation throughout 06. This in turn should permit a high level of efficiency, say 80%.

Our scenarios transform the current base of around 5m active numbers[13] as shown in Figure 5. These projections include an allowance for the impact of UMTS.

## Figure 5 Possible demand for mobile numbers

| *Demand scenario* | *Low* | | *Medium* | | *High* | |
|---|---|---|---|---|---|---|
| *Demand after* | *5 years* | *5 years* | *5 years* | *5 years* | *5 years* | *5 years* |
| Number of numbers required | 11m | 22m | 22m | 63m | 90m | 315m |

Capacity of the 06 range at 80% efficiency: 80 million numbers

We see that the scenarios do not exclude exhaustion of the range. However even the most extreme scenario does not exceed the capacity of the same range used at an additional digit length (ie 800m numbers). We therefore recommend keeping open the option of this extension in case a very high growth scenario should materialise.

[13] Note that here, as above, we are speaking of numbers in use by end customers, not numbers allocated to network operators.

Demand for **specially tariffed (information)** services is particularly hard to forecast. Our growth modelling, combined with the very low current utilisation, did not suggest any cause for concern other than in the short number ranges, which have clearly proved very popular and could easily exhaust in a few years.

Allowing numbering space for **new services** amounts to foreseeing the unforeseeable. We commented early in the study, however, that the obvious weak point of the Netherlands numbering scheme is its lack of completely spare numbering space. The first digit 9 can be used either for long-term expansion or for numbering new services, but not both.

Luckily, a high proportion of possible new services requiring numbering space could be for machine to machine applications, where number length is not important. We recommend using a long number length for them, to conserve NDC space.

The first digit 8 should be developed cautiously for new services. If and when its exhaustion seems likely, a decision will be needed on how the first digit 9 will be used. This will have to be considered together with a strategy for fixed network numbering, as discussed above.

# Annex F ICANN

## F1 Constitution

ICANN is a non-profit organisation operating under Californian law. It is based in Marina del Rey, California with fewer than 10 staff. 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 organisations."

## F2 Structure and membership

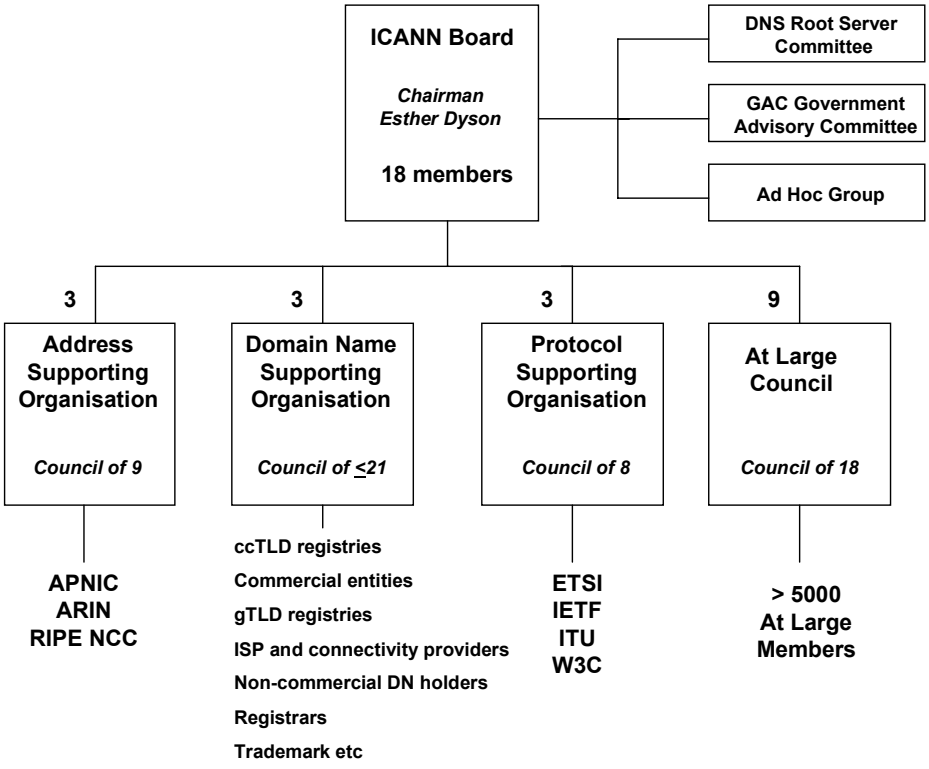
ICANN is controlled by a Board of elected directors, from which Government officials are excluded. Initially there was an Interim Board but a permanent one was elected in October 1999, consisting of 19 people:

- chairman: Esther Dyson
- nine directors representing the three Supporting Organisations (three each)

- nine directors representing the At Large members

There are three Supporting Organisations and an At Large Membership. The overall structure is shown in Figure 1.

**Figure 1 Structure of ICANN**




## *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:

(i) definition of global policies for the distribution and registration of Internet address space (currently IPv4 and IPv6);

(ii) definition of global policies for the distribution and registration of identifiers used in Internet inter-domain routing (currently BGP autonomous system numbers); and

(iii) 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).

## *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:

- A - Dispute Resolution Policy
- B - Famous Trade Marks
- C - New gTLDs
- D - Business Plan and Internal Procedures
- E - Global Awareness and outreach

### *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

### *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 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.

### *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.

The initial chairman of the Governmental Advisory Committee is Paul Twomey from Australia. Members of the Governmental Advisory Committee are representatives of national governments, multinational governmental organisations and treaty organisations, one representative each.

### *Ad Hoc Group*

Following pressure from ETSI, an Ad Hoc group has been formed to identify issues that will affect addressing and numbering in the Internet. The recent ICANN Board meeting

deliberately restricted the group to the identification of issues and not the design of solutions.

Issues to be considered include current trends in globalisation and service and network convergence as well as changes in demand for traditional IP address space. Examples of technology forces to be considered include IMT 2000, 3GPP, and Bluetooth. The spread of these new technologies could require changes to the addressing structure and, potentially with it, how traffic is routed. The new technologies may also increase demand for addresses even with no changes in the structures, by virtue of being layered on top of IP.

The Ad Hoc group has been asked to focus on the future demands and impacts these new technologies will have on IP address space and its administration, with particular attention towards global policy formation and the identification of any requirements for Internet addressing in the future. It should identify technologies and evolution that can be implemented by layering them on top of IPv4/IPv6 and whether technology, rather than merely policy, changes are required.

The group will consist of representatives of:

- the Regional Internet Registries
- the Internet Architecture Board
- the ISP Trade Associations
- industry (eg 3GPP, Bluetooth, IMT2000)
- Telecommunications operators and
- representatives chosen by the ICANN Board.

The current timetable is:

- by Jan2000: identification of key drivers that will affect addressing and numbering in the Internet, including the impact of convergence.
- by Feb 2000: assessment of technologies and evolution that can be implemented by layering them on top of IPv4/IPv6 and whether technology, rather than policy, changes are required, whether new technologies require changes to the addressing structure and, potentially with it, how traffic is routed, and whether new technologies increase demand for addresses even with no changes in the structures, by virtue of being layered on top of IP.
- by May 2000: identification of options to resolve the requirements of the new technologies with the Internet community and the impact on existing structures and policies.

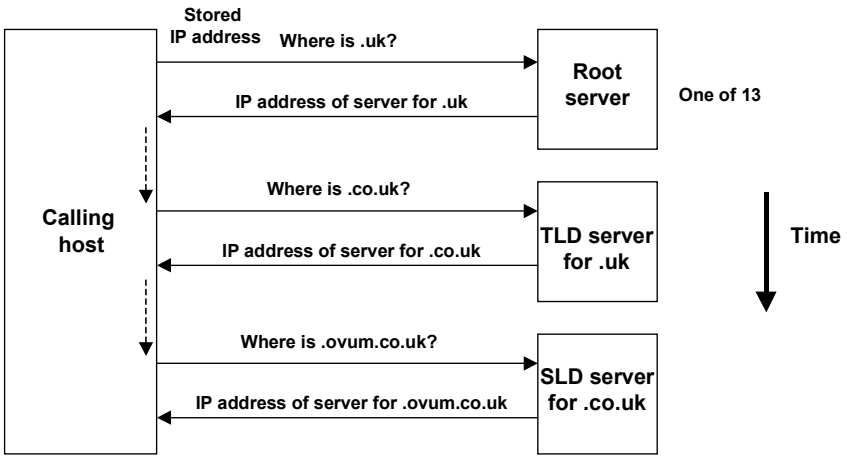
# Annex G Current allocation method for domain names

## G1 The root server system

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 on a daily basis. 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 plays a role in the operation of about half of the Internet's root servers.

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. Figure 1 shows the sequence for resolving the name: ovum.co.uk into an IP address.

**Figure 1 Example of domain name resolution**




## G2 Types of Top Level Domain

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

- generic domains (gTLDs) such as .com, .org, .net, .edu, .gov, .mil, .int
- country code domain names (ccTLDs) such as .jp, nl, .uk issued in accordance with the ISO 3166 standard.

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 has not yet made a decision for or against the addition of new generic top-level domains.

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).

## G3 Registrars and registries

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

### *Generic*

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. Currently there are some 13 accredited and operational registrars and over 50 in the process of accreditation and becoming operational (none in the Netherlands). 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 2 summarises the registrar and registry roles for the root and some TLDs.

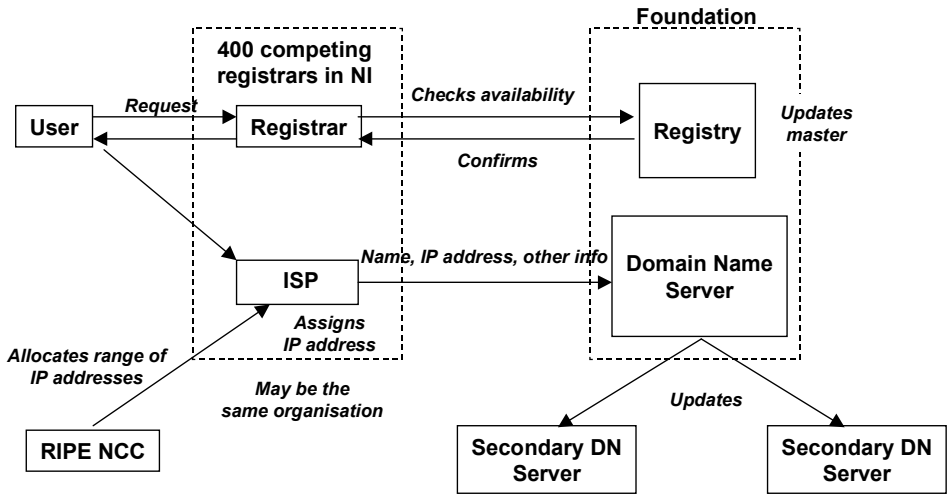
**Figure 2 Summary of registrar and registry roles for root and some TLDs**

| *TLD* | *Registry* | *Registrars* | *DNS* |
|---|---|---|---|
| (root) | ICANN | ICANN | 13 root servers including InterNIC (NSI) |
| .com, .org, .net | InterNIC (NSI) | New shared registrar system (> 50 expected soon) | InterNIC (NSI) and others |
| .nl | Foundation | 400 competing organisations | Foundation plus secondary servers in Europe and USA |

### *Netherlands*

For the ccTLDs, the registry for the Netherlands suffix **.nl** is the Foundation for Internet Domain Names, which also runs the main DNS server for **.nl**. There are secondary servers, three in Europe and two in USA. There are over 400 competing registrars (also called participants in the registry), most of which are ISPs. Figure 3 shows the structure of the relationships. The Foundation is funded by payments for registering the domain names.

**Figure 3 Registrars, Registry and DNS for .nl**




## G4 Principles for Domain Name Management

ICANN is continuing the principles described by IANA in RFC 1591.

Managers are regarded as trustees with a duty to serve the community, and not as the owners of a domain.

Managers are required to:

- be equitable and fair to all groups
- apply the same rules to all requests in a non-discriminatory manner
- publish their policies
- not stipulate that any particular application, protocol or product must be used

ICANN has adopted a Domain Name Dispute Resolution policy. There is a procedure that must be activated if there is a complaint that:

- a domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
- the user has no rights or legitimate interests in respect of the domain name; and
- the domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present. The proceeding is handled by an Administrative Panel established by an administrative-dispute-resolution service provider selected by the complainant.

The following are considered to be evidence of the registration and use of a domain name in bad faith:

a) circumstances indicating that a domain name has been registered primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for a consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

b) the domain name has been registered in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, and there is a pattern of such conduct; or

b) the domain name has been registered primarily for the purpose of disrupting the business of a competitor; or

d) use of the domain name has intentionally attempted to attract, for commercial gain, Internet users by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of a web site or product or service on a web site.

Remedies are limited to the cancellation or transfer of the name registration.

## G5 Accreditation and activities of registrars

For accreditation an organisation must be able to:

- provide the applicant secure, authenticated access to the registry.
- provide robust and scalable operations capable of handling the registration volume reasonably projected by applicant.
- allow for prompt handling of second-level domain ("SLD") holders' requests for changes in registration data.
- achieve a reliable and readily usable daily data backup and archival of all SLD holder and registration data.
- maintain electronic copies of all transactions, correspondence, and communications with the SRS for at least the length of a registration contract.
- provide procedures for information systems security to prevent malicious or accidental disruption of the applicant's operations.
- meet the applicant's obligations under its accreditation agreement.
- provide procedures that permit applicant's customers to change registrars without interruption in use of the assigned domain name.
- have the capacity to engage a sufficient number of qualified employees to handle the registration, update, and customer inquiry volume reasonably projected by applicant. The equivalent of five full-time employees or more will be deemed sufficient, although a lesser number of employees will be accepted upon a showing that it will be sufficient in the circumstances.

- ensure that the registrar's obligations to its customers and to the registry administrator will be fulfilled in the event that the registrar goes out of business, including ensuring that SLD holders will continue to have use of their domain names and that operation of the Internet will not be adversely affected

In addition they must demonstrate adequate working capital and hold liability insurance.

For each registration the following information must be given to the registry:

- the name of the SLD being registered;
- the Internet Protocol ("IP") addresses of the primary nameserver and any secondary nameservers for the SLD;
- the corresponding names of those nameservers;
- the identity of the registrar; and
- the expiration date of the registration.

Updates must be submitted to the registry administrator within 2 days and if a new registry administrator is appointed and full set of information must be submitted within 10 days.

The registrar must provide real-time public access (eg by a “Whois? service” to the following:

- the name of the SLD being registered;
- the Internet Protocol ("IP") addresses of the primary nameserver and any secondary nameservers for the SLD;
- the corresponding names of those nameservers;
- the identity of the registrar;
- the expiration date of the registration;
- the name and postal address of the SLD holder;
- the name, postal address, e-mail address, voice telephone number, and where available fax number of the technical contact for the SLD;
- the name, postal address, e-mail address, voice telephone number, and where available fax number of the administrative contact for the SLD;
- the name, postal address, e-mail address, voice telephone number, and where available fax number of the zone contact for the SLD; and
- any remark concerning the registered SLD name that should appear in the Whois data.

There is a requirement for a Chinese Wall between the competitive registrar activities and the monopoly registry activities of a domain administrator to ensure fair competition between registrars.

SLD registrations are assigned on a first-come, first-served basis by the registry. Existing SLD holders may renew their registrations through the accredited registrar of their choice. Any registrar may take over a registration from another registrar.

Registrars may be required to deposit data under an Escrow agreement (an agreement where data is deposited with a third party and may be released in the event of pre-determined types of failure by the depositor).

## G6 Reverse address mapping

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”. An IP address is stored in reverse form as this type of domain name. For example:

- 193.3.20.100 is stored as the domain name
- 100.20.3.193.is stored in in-addr.arpa

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.

# Annex H Current allocation method for IP addresses

## H1 Overview

IP addresses are allocated by Regional Internet Registries (RIRs) in accordance with policies set by ICANN. There are three RIRs:

- Asia Pacific Network Information Centre (APNIC) with 2001:0200:: /23
- American Registry for Internet Numbers (ARIN) with 2001:0400:: /23
- Réseaux IP Européens (RIPE NCC), located in Amsterdam with 2001:0600:: /23

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.

## H2 RIPE and RIPE NCC

RIPE is the European association of IP networks and is an open organisation without membership fees that has been established for 10 years. RIPE NCC is a not-for-profit organisation with over 1500 members that is 7 years old. RIPE NCC provides services to ISPs including the management of IP addresses within the European and part of the Asian region. RIPE NCC pursues a policy that is controlled openly by its members, and is managed by an Executive Board.

The Working Groups are as follows:

- Anti-Spam Working Group (Fighting the problem of "spam" on the internet)
- Database Working Group (Aspects of the RIPE network management database)
- DNS Working Group (Domain Name System questions and issues)
- European Internet Exchange Working Group (European Internet Exchange's related issues and problems)
- European Operators Forum Working Group (European technical network operation related issues and problems)
- IP version 6 Working Group (IPv6 related Issues and questions)
- Local IR Working Group (Issues and questions related to registration services and Local IRs)
- European NetNews Working Group (Net News related topics. )
- Routing Working Group (Issues dealing with routing architecture for the European Internet)

- Test-Traffic Working Group (Discussion of the Test Traffic project)
- TLD Working Group (Discussion of all TLD related matters)

## H3 Principles for allocation

The goals of the allocation and assignment system are:

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

Aggregation and conservation are sometimes conflicting.

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

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 its internal addresses unless it uses a Network Address Translator to isolate the internal address from the public Internet.

## H4 Arrangements for IPv4 addresses in Europe

RIPE NCC has produce a carefully written and detailed manual about its policy and procedures for the allocation and assignment of IPv4 addresses. The Local IRs are expected to apply this manual in their dealings with users. The general principles are as follows:

- assignments are based on a 2-year forecast of demand
- quite detailed information is required about the network, its traffic and its interconnections
- no reservations of addresses are allowed
- additional address space is allocated to Local IRs only when 80% of the current address space has been assigned

RIPE NCC:

- holds a database of all assignments with quite detailed information about the end users. The database is indexed using the “inetnum” of the end user.
- gives each Local IR an assignment window, which is a maximum size of assignment that the IP may make without obtaining prior approval from RIPE NCC. As a Local IR gains more experience and commands more trust, this assignment window is increased.
- has developed a “slow start” system starting with an initial allocation of /19 (8192 addresses).
- recommends but does not require Local IRs to register all assignments for reverse mapping. A requirement would be better (see later).

Current estimates are that some 60 to 70% of IPv4 address space is assigned, which with the current rate of growth indicates a very serious situation indeed. However the assignment procedures are now make much more efficient use of the addresses and some of the early large inefficient assignments could be recovered and re-assigned, thus estimates are that at the current rate of growth there are enough addresses for another 10 to 20 years.

## H5 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. RIPE NCC has published it principles for IPv6 allocation.

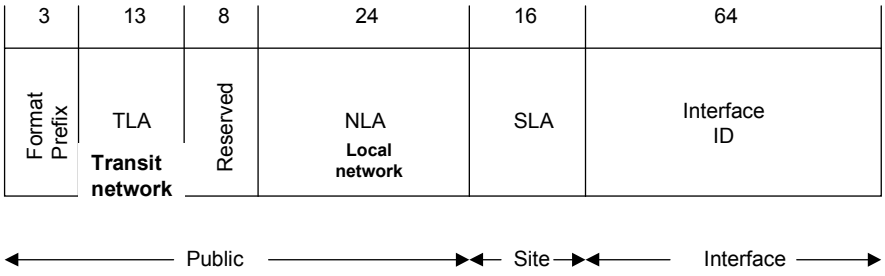
The allocation hierarchy of IPv6 is:

- ICANN
- RIRs, who allocate TLAs
- TLA Registries14, who are transit operators and allocate NLAs
- NLA registries, who are ISPs
- end-sites

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 1 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 1 The main structure of Ipv6 addresses**

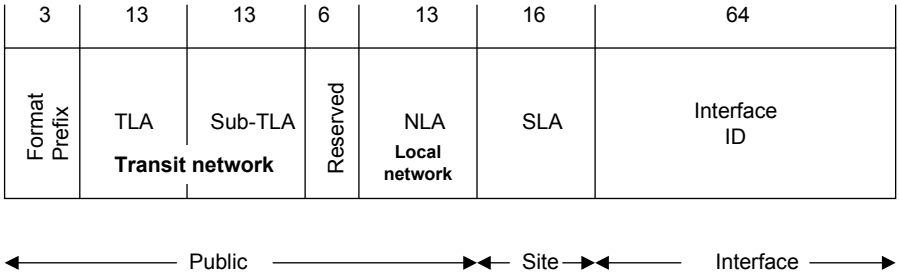



Consequently a different initial structure will be used where one TLA value (0x0001) will be shared and sub-TLAs will be allocated out of it to the applicants for TLAs. These transit operators will use this allocation for assignments to ISPs (NLAs) until it is 80% used. Only then will they qualify for a full TLA assignment or a further sub-TLA. Figure 2 shows this initial structure as used by RIPE NCC.

At the end of November, RIPE NCC had allocated 8 sub-TLAs, slightly more than APNIC and ARIN.

[14] NB: The terminology is confusing. “TLA Registry” means “a registry that is a TLA”; NOT “a registry that allocates TLAs”.

**Figure 2 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 will be a /35 block (representing 13 bits of NLA space). The Regional IR making the allocation will 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(i) 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.

All holders of a /35 allocation who make assignments from that allocation are required to set up reverse DNS for their customers.