NOTES ON THE ROOT NAME PRINCIPLE

Three main architectures have been used by the international digital ecosystem:

- Tymnet (1977 – 1986)
- OSI (1987 – 1995)
- Internet (1996 -)

They all obey to the common “root name” principle which is the basis of the networks stability

An history of network innovation resulting from balancing between a global deployment and the support of national and cultural rights …

National ARPANET started in 1969, financed by the US Congress. In February 1972 Tymnet started offering a private national, and then international, commercial packet switch service. In 1974 Louis Pouzin proposed the catenet concept, which became the DoD doctrine, for the concatenation of existing networks into larger network systems. In 1977, the FCC granted Tymnet and Telenet a Value-Added Carrier license, Robert Tréhin and Joe Rinde had to externalise the sovereignty of the Communications monopolies over their national Tymnet public access. They did it in using the root name concept. In 1978, Vint Cerf documented the Internet catenet architecture. Internet started on January 1st, 1983, and connected the International Packet Switch Services through Tymnet in 1984, resulting in the creation of the national ccTLDs to accommodate the constraints of the local monopolies and to interface the local cultures and administrative obligations. The various Tymnet developments lead the international network towards a multilingual, multitechnology and a multiservice for a first short while before being purchased and leave the stage to the sole OSI inter-monopolies standard.

Progressively the US/British deregulation, copied all over, removed most of the national constraints, permitting the deployment of the US ASCII Internet and making it more attractive to support the Web development. Today the WSIS acknowledges the need to reorganise States regalian communications rights and services and to empower cultures in the information society. It is now the turn of the Internet to externalise political and cultural control over the network national and lingual utilisation, through an adequate architectural vision.

Time has come to renew with time proven concepts the Internet have just used the default, needing no more as then an academic effort. The user-centric, multilingual Internet, will be a major architectural change and innovative improvement, as it was for the preceding technologies under similar obligations.

The international digital divide is now being between the States and the Cultures, which control their name and numbering spaces and the context of their exchanges, and the ones, which do not.

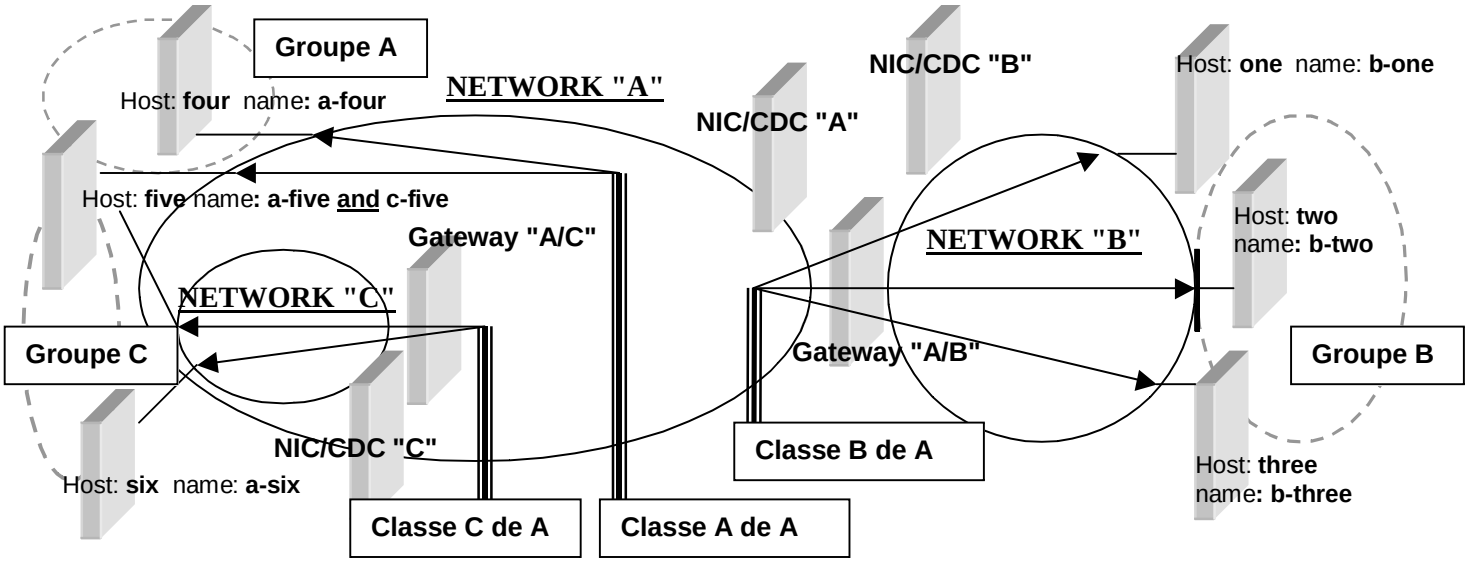
THE ROOT NAME CONCEPT

When the FCC decided to submit the TYMNET packet switch services to a value-added network license, Robert Tréhin and Joe Rinde had to match the ITU framework of the international operators' obligations. They then introduced the "root name" concept, inherited from the telephone numbering plan, to logically partition the network sovereignties. It later on turned to be extremely fruitful in many situations.

INTLNET was created to help documenting and to support its deployment.

> In a network an external network is known by its root name. It is the name of its gateway, of the class of its users, of the group of its hosts accessible to these users, the radical of the names of these hosts, and the name of its Registry and of its context. The gateway can be real, virtual, or to loop back into the network.

To prevent confusion with the DNS, the root name can be also named (Multilingual) ***ExtName*** *(MEN).*



This concept permitted to organise the initial system and to aggregate all the public and private operators, to support the OSI X.121 scheme throughout the international name space (in aliasing addresses with numeric names), to support the first non-ASCII languages dedicated environments, to out-dial and fax into the telephone network, to plug the Internet hierarchical DNS in 1984. I was used in part in the OSI closed user group concept, which permitted the Minitel deployment and had many other applications.

It is now the thirty years old, stable and proven core principle of the global network system. It was first used with a left to right aggregation, making it directly compatible (in using numeric names) with the telephone and X.121 numbering plans. It is applied as a right to left hierarchy in the DNS, where the dot separator gives it more flexibility.

The DNS still supports nearly 50% of the Internet connections. The other name space systems like the Handles of Bob Khan, the ONS for the RFID, etc. also obey to the same root name concept.

EXTERNETS

The term itself comes from the interconnect discussions of the Internet with “external networks”, as for example discussed in RFC 887. They were first implemented in 1977 for the partition of Tymnet into national monopoly spaces, together with numerous features added over time. The most important of these features were the local access permissions and destination limitations, the IRC rotation (rotating the use of several links on a packet basis) and the IRC restrictions (reserving the use of a link to a certain kind of traffic). They were also used for statistics, security, accounting, language support, services, etc. purposes. They were the very basic features of the initial international network deployment and of the OSI transition.

Externets are a consequence of the root name concept. An externet gathers a name, a class of users, a group of members, a registry (NIC), a governance and (now) a context reference centre (CRC) where is stored the description of its context. They permit stable, simple and consistent traffic governance.

A CRC can document an unlimited number of contextual parameters, links and services. Classes, Groups, CRCs and their inheritances and support in subsidiarity give users unlimited ways to shape their granular vision and usage of the digital continuity.

Fully secure externets cannot be implemented with the existing Internet technology, but CRCs and the DNS permit to start studying and deploying them, benefiting from the interest in **multilingual externets**.

THE INTERNET DNS

The DNS is central to the Internet, to the point that its governance is confused with the intergovernance of the Internet. It is a simplified robust adaptation of the root name concept to the Internet catenet structure (one single network made of many networks).

The DNS implements the root concept in the internetting described by Vint Cerf (IEN 48) along the Louis Pouzin's initial catenet vision. This is why the Internet interconnect to the international system was quite standard. Jon Postel documented it in the RFC 920, from which ICANN claims its legitimacy and which has been strictly respected and enforced ever since. This RFC documents the Internet interconnect MoU with external networks such as the value-added public service Tymnet and its international connections.

It introduces externets through "multiorganization TLDs". The Internet only partly use them as specialised TLDs, but has however the general capacity to support them. The DNS support of Classes is very limited (only “IN” and “CHAOS”). There is only one group, differentiating general, e-mail and name servers: this is why the DNS can only supports aggregation by hierarchy (domains and zones). It offers a simple yet robust support of external gateways (extranets) and a closed user group like loop-backs capacity (intranets – virtual private networks). The IANA is a unique CRC for the Internet.

The dot-root test study (see below) carried by INTLNET, leads to think that, in fully tacking advantage of the root name principles, one can use the existing DNS to address most of the today’s challenges: multilingual internet, IPv6, private alias directories, smart network [extended services ubiquity], digital convergence, and NGN.

For example, a FQDN actually is (the descriptors between brackets are DNS defaults):

subname.name.[ascii IDN table].country code.[legacy]

One sees the possibilities of the existing DNS if a proxy located virtual gateway system (an OPES, a plug-ins, an OS filters) can hide/restore/translate these descriptors to the DNS servers, and if they are managed as virtual zones, or for a local view, of the network space.

THE AUTHORITATIVE ROOT MATRIX

In 2002/2003 INTLNET responded the ICANN's ICP-3 call for an applied study of the DNS through the dot-root DNS test bed project study. It fully respected the ICANN requirements: non-profit, reversibility, no pollution of the public operations, and open to everyone from the Internet.

- it used four root hierarchies, one being a replication of the NTIA/RSSAC system as a reference. The three other hierarchies formed a multi-root system, permitting two to one comparisons procedures: if system reports a disparity with an another one, both systems are downgraded and investigated.

- it also wanted to study the TLD governance creation process. To that end it used ULDs ("User Level Domain") as a parallel registration of the domain name both in an experimental ".uld" TLD zone, of the test-bed system, and in a regular ".uld.tld" SLD zone, of the public DNS. This allowed to engage real user registrations and to follow their evolution (one might become a major TLD).

The lack of budget did not permit to offer the dot-root test bed to Universities, to developing countries and to private and individual research projects, as initially intended. But the immediate results of the study and the acquired experience where of interest. Among others, they shown:

- a sovereign State cannot depend, through its name space governance, from a foreign power, which has this way, a de facto e-embargo capacity on its life and economy without needing a UN decision.
- people's life and national economies cannot rely on non contracted private sponsors, non screened voluntaries, without legal responsibility, published procedures, insurance, binding non-disclosures …
- in critical situations, States must be able to immediately take over the management of their national namespace and to best manage their national bandwidth.
- risk containment necessitates a national "virtual firewall" resulting from the availability of national, regional and local roots replications users may depend on, with legally protected logs.
- DNS risks cannot be insured. In most of the countries the legal responsibility of the TLD Managers is not clear, yet the harm can be enormous. Only States can carry this responsibility.
- name and numbering spaces are highly mixed in terms of security and sovereignty. States must be control their numbering space even more than their name space.

- unlike ICANN envisioned it, there is no reason to abandon the notion of single authoritative reference, but there is certainly a different vision to adopt, in line with the "root name" concept:

    - the current centrally **"managed root"** approach is not secure. Top zone data come from the alpha root server, the last updates, rs.internic.org ftp file, and the additions by the TLD Managers. 97,5 % of the calls to the root system are illegitimate.
    - the need is for a **"documented root"** every one can generate and control, in using the Registry Managers data. Registry Managers should publish these data in XML/ASN.1 format on different sites of their announced sovereign choice and subject to the jurisdiction(s) they chose. These data should be considered only if the presentation is identical on two third of the listed sites.
    - **everyone is able to build the root file and name space she wants**. The probable shift of ISP business from bandwidth provision to intelligence support, and a progressive cultural switch from default trust to distrust, the bandwidth and CPU power low cost, reactions to dominances, among others, should lead to a more general demand for individual independence and innovation.
    - open roots experience shows **registry name organisation** (TLD) should be **non-profit and free** to set-up: name owners are the registrants. Who would want to invest in a disputed name?

- every information ("context") the members of a class of users need, when participating to an externet, should be as available in the same way as the DNS information today. Its management should only be

subject to the governance of that externet (as is the management of a naming zone). The netiquette should be a mutual support (subsidiarity) among externet governances as it is the case between zone managers. The architectural rule should be **total user originated flexibility in parameter choice**.

NUMERIC NAMES

Numeric names were first used on a large scale to transparently support X.121 addressing in the left to right international naming scheme. They are extensively used in the handles system.

Numeric names are of interest for a pivotal (language independent) naming and are sometimes easy to manage and remember aliases to sounds. For example, Chinese and Korean use numbers as a convenient way to enter their soundex mnemonics on a non-ASCII keyboard.

Two examples of applications can be considered with the DNS:

- the support of the telephonic numbering plan. there are several manners to do this: one is ENUM. However the load imposed on the DNS seems to be unnecessary, except on a temporary basis: ENUM could be directly supported in using adequately crafted IPv6 addresses. Other schemes, like the UTELNET "TIPI ™" (Telephone user's Individual Presence on the Internet) project would associate a multiservice weblog to every telephone number. Other VoIP projects use similar schemes.

- the support of numbering plans which are not (yet) supported by an IP addressing. This opens a large area of possibilities. For example, the use of post-codes, which are good mnemonics for "grand'place" (city hub) of local services and for teleurbanism ("Webs de France/of America" INTLNET applied project studies).

TRANSPARENCY, NATs AND PADs

Long before NATs, the first IETF response to the loss of network transparency, due to the shortage of IP addresses, was HTTP.1.1. It routes calls within the host servers in using domain name instead of an IP address.

The IPv6 address availability restores transparency (as documented in RFC 2775) and provides again one IP address per virtual host. It therefore permits to access virtual hosts in using their IP address. The appearing complexity of the IPv6 address has lead to forget about this access mode.

- if the IPv6 address construct is simple enough it can advantageously replace naming on occasions in calling directly an IPv6 number entered, in a way similar to a telephone number, or as a simple numeric sequence assisted by the browser entry line or a plug-in.

- IP addresses can be aliased with local names, in using a DNS local root and a name server, or the simple hosts.txt file. These local aliases form a local Private Alias Directory (PAD). Alias can be keywords disseminated by webmasters, externets CRCs, specialised Registries. PADs are highly advisable as a back-up to full DNS in critical situations and for intelligence protection (no DNS log leaks). They permit a simple direct multilingual support of the 20.000 languages of the world (ISO 639-6 [under preparation]). It is likely that "PAD click" will be available some times on web sites, to support access by keyword and multilingual names.

  The organisation of this new name space obviously depends on the easy availability of IP addresses.