

New Domain Name Structure Allows for Consistent Web Presence

Expansion vs limitation, location vs search

An instantly recognisable Internet domain name has become an essential part of establishing a clear corporate identity. Large organisations have the resources to acquire domain names that reflect their name and associated brands. Similarly, they have the resources to design websites to maximise their exposure through search engines. Thus, users can generally locate these sites relatively quickly. Lesser known organisations, however, are sometimes hard to find and generally require perusing deeply into lists generated by search engines. The launch of a second-generation Internet addressing regime stands to change this.

The Internet has grown from a small experimental military and academic data network into a ubiquitous commercial medium. As a result, it has become increasingly difficult to find websites and content quickly. This is largely because the Internet domain name structure was developed to accommodate a much smaller network. The enormous growth of the Internet over the last decade has surpassed the functionality originally designed for the current domain name regime. What is needed is twofold. There needs to be a way for site owners to have addresses that are not limited by .coms already taken and then for users to be able to find sites because the names are intuitive and easy. To understand how this will work and why it is so imperative, it is important to look at how the current system came to be.

The Current Domain Name System

The domain name system (DNS) we use today stems from

the mid 1980s. As a result of its creation, the foundation for the world wide web was laid. Top-level domains (like .com, .edu, .org, .gov), and country codes (like .uk, .kr, .br, .de) have dominated the Internet ever since. These so-called generic top-level domains (gTLDs) and country code top-level domains (ccTLDs) led to a massive proliferation of second-level domain names (e.g. sony.com, adidas.com) and business hubs (e.g. google.com, yahoo.com).

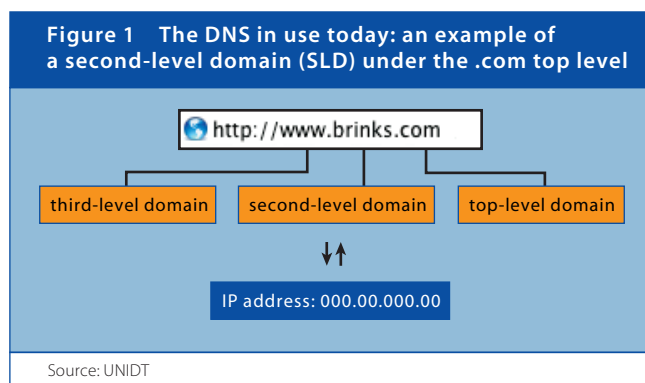
In the beginning, the assignment of domain names and corresponding IP addresses was administered by a group of individuals operating under contracts supported by the US government. In 1998, the US government oversaw the privatisation of the domain name system through the creation of ICANN, the Internet Corporation for Assigned Names and Numbers, which was designed and launched by members of the Internet community. Despite its promising beginnings, the ICANN experiment has been the subject of significant criticism throughout its short tenure, mostly with respect to its exclusive control of the domain name system. Additionally, the influence of special interest groups and the appropriateness of decisions regarding the allocation of scarce domain name resources have further brought ICANN under fire. As a result, there remains a significant demand for a more effective domain name regime that would help organisations that operate internationally establish a web presence in a clear and consistent manner.

There is also an issue around the perceived limited supply of domain names. That scarcity is artificial (i.e. a policy, not a technical limitation) created by ICANN's decisions to restrict the number and type of top-level domains. As a result, the current Internet addressing regime is overcrowded in some TLDs (e.g. .com) and practically unused in others (e.g. .pro). Because the most desirable domain names have been claimed, many site owners are unable to register the domain names they desire.

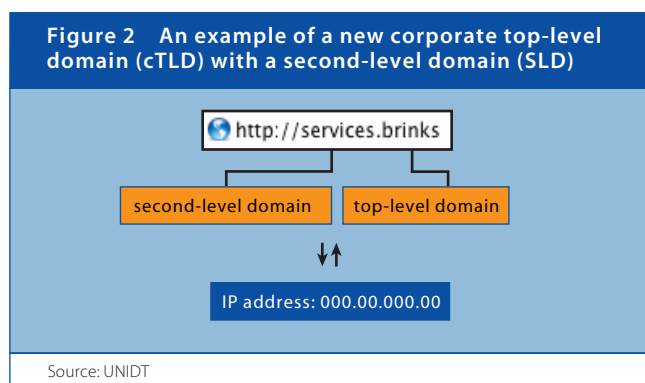
Technical Background of the DNS

How does the domain name system work? First, it is important to understand that computers communicate with numbers, whereas people have a strong preference for names. Computers route information through the Internet

using IP (Internet Protocol) addresses, sets of numbers that provide unique identification. These numbers are linked with specific names. Quite simply, domain name servers located around the world translate domain names into IP addresses, allowing computers to interact. Thus, the DNS system works like an automated phone directory, which links unique names and numbers to avoid duplication (see Figure 1).



This system has obvious limitations, and that is why a new naming structure is needed which will allow for the creation of millions of new TLDs world-wide. This new regime is designed to coexist with the domain name system we use today, while at the same time revolutionising Internet navigation. Finding websites and content will be easier and faster – and websites can be designed more simply. An example of the new naming structure is shown in Figure 2.



Navigation to Sites

The current domain name system leaves little room for a coherent way of naming URLs. Corporations that operate internationally or local organisations that deal with an international audience (e.g. airports, cities, regional or local authorities) often cannot register their preferred second-

level domain (SLD), because it has already been taken. Further, registrants are encouraged to secure SLDs separately under one or more gTLDs or ccTLDs, adding to the confusion about where to find information, particularly 'official' information provided by governmental authorities.

Let us assume a user wants to visit a certain site, but he does not know the exact name or the TLD it belongs to. The user will generally rely on a search engine to locate the site. Search engines, however, have proprietary and esoteric ways of presenting results. Site owners have no control over the summary content presented or the way a site is ranked in the responses. In many cases, links to competitor websites and sponsored links may distract the user from the intended site. By contrast, what this user needs is a simple, intuitive system that allows him to go directly where he wants.

Say the user we just mentioned wants to visit the home page of the Vancouver International Airport, but he does not know the precise URL. It could be www.vancouverairport.ca, www.vancouver-airport.ca, www.vancouverairport.com, or something altogether different. Upon searching for 'Vancouver Airport' via Google, the user finds a link to the official website – at the time of this search, it was ranked number two behind a taxi company. However, the following was also displayed on Google's results page:

Sponsored Links

Try Abbotsford Airport

Vancouver's hassle free alternative

Hassle free, cheap parking

www.AbbotsfordAirport.ca

British Columbia

Presumably, the Vancouver Airport Authority would prefer the user to have a more direct link to its site. For his part, the user generally wants to go directly to the targeted site without having to sift through advertising and questionably related links.

The Solution: Corporate Top-Level Domains

The current DNS system does not reveal much information about a website and its contents. Let us take 'vancouverairport.com' again as an example. Its TLD is '.com', the preferred second-level domain is 'vancouverairport'. With a new 'corporate TLD', Vancouver Airport will be able to use its very own TLD, simply named '.vancouverairport' – nothing more. The airport would not share the .com domain with

Domain names and top-level domain names

In formal computer terms, 'brinks.com' is referred to as 'domain name' – domain being just a fancy term for group. The domain name consists of two parts: the so-called top-level domain ('.com') and the second-level domain ('brinks'). In other words, brinks is a 'child' within the .com 'family'.

The idea of grouping websites into domains was to organise sites according to their purpose, so users (at least in the US) would know whether they were visiting a commercial (.com), educational (.edu), governmental (.gov), military (.mil) or non-profit (.org) website. In October 1984, an Internet standards document introduced 250 top-level domains: six generic TLDs (gTLDs) .com, .edu, .gov, .mil, .org, .arpa and 244 country-code TLDs (ccTLDs). Later, two more TLDs were created: .net in the beginning of 1985 and .int by the end of 1988.

In some countries, like the UK, Japan and Korea, a generic SLD under the ccTLD is used to indicate the type of website. For instance, in the UK, .co.uk, .ltd.uk and .plc.uk are used for companies, .org.uk is used for non-commercial organisations, .net.uk for ISPs, and .me.uk for personal websites. This additional SLD pushes the corporate identity toward the third level.

Regarding gTLDs, second-level domains can be registered in three of these (.com, .net and .org) without any restriction; the other four still have limited purposes. At first, there were very few commercial websites. Today, there are about 40 million sites crowding the .com and .net domains alone. Since the creation of the web, there have been intense debates regarding the introduction of additional gTLDs. The Internet community has sought the introduction of new TLDs, but ICANN has maintained a limited DNS. After protracted consideration – and vocal dissatisfaction among the Internet

community – ICANN approved seven new gTLDs in 2001. Three of the new gTLDs (.aero, .coop and .museum) are 'sponsored', whereas the remaining four (.biz, .info, .name and .pro) are open to SLD applicants.

Generally speaking, an unsponsored TLD operates under policies established by the global Internet community through the ICANN process, while a sponsored TLD is specialised and has a sponsor representing the narrow community most affected by the TLD.

Recently, two additional TLDs have been authorised – .travel and .jobs. Though this expansion of TLDs indicates a move in the right direction, it does little to assuage the broad demand for TLDs across both public and private sectors. To meet this demand, a wholly new domain structure is being launched, which will make corporate and public TLDs (cTLDs and pTLDs) available world-wide. While a corporate TLD equals the name of a company, organisation or brand, public TLDs can be anything else, as long as they do not conflict with any corporate TLD. These cTLDs and pTLDs will not replace the existing DNS but will rather coexist with the original regime.

For further information on domain names, see the following websites:

<http://inaic.net>
<http://iana.org>
<http://unidt.com>
<http://public-root.org>
<http://www.icann.org>
<http://www.internetgovernance.org>

tens of millions of other domain names; 'vancouverairport' is a *corporate* TLD, controlled by the airport itself.

Naming Standard for SLDs

Corporate TLDs also make it possible to develop second-level domains, allowing users to go directly to the page they desire. A standardised naming convention for SLDs has been developed. Each website can adopt this convention and thereby provide visitors with obvious entry points (for example, 'departures.vancouverairport' or 'contact.vancouverairport').

These recommendations are informational and do not reflect any technical specifications or limitations on the operation or the administration of corporate TLDs, nor do they mandate any particular tree structure. Their goal is to assist corporate TLD owners in setting up a consistent naming space that will be used for referring to corporate resources. The naming standard recommends that owners of corporate TLDs reserve a number of SLD labels that identify specific departments, tasks or functions within a company. In particular, mobile Internet users will benefit from simpler, more precise navigation, reducing number of

keystrokes, airtime, and data transmissions. With a cTLD, the owner can decide exactly how to process and distribute information on his domain, providing superior customer service.

The Next-Generation Internet

The new domain name structure is part of several innovations that will modernise the Internet. In order to keep the Internet accessible in the future, there are many improvements being developed under the umbrella of the 'next-generation Internet'. These developments are intended to be an addition and a replacement for a future overcrowded Internet – without the need for a separate physical network.

In addition, multilingual TLDs (or internationalised domain names, IDNs) are expected to become more widespread.

Some examples of second-level domains (SLDs)

cTLD owner: Vancouver Airport Authority

park.vancouverairport finds parking info

taxi.vancouverairport finds info on cabs

weather.vancouverairport or even

monday.weather.vancouverairport to find

specific local weather info

arrival.schedule.aircanada.vancouverairport finds

info on Air Canada arrivals (cf. www.vancouverairport.com/guide/around/arriving.asp?id=canada)

ac722.schedule.aircanada.vancouverairport to find the schedule of flight AC722

pTLD owner: local authorities Vancouver

weather.vancouver finds local weather info

city.vancouver to go to the town hall website

airport.vancouver links to Vancouver Airport

cTLD owner: Air Canada

tickets.aircanada to go to ticket sales and info

vancouver.destinations.aircanada finds the local destination airports

vancouver.trips.aircanada to find specific holiday trip packages to Vancouver

All domain names mentioned here are only possible examples of how SLDs could be structured under a given TLD. They do not have the endorsement of the organisations mentioned.

These enable users to navigate the Internet in languages with characters not based on Latin script. And, web developers can reach and advertise to target audiences in their local languages. This is a critical development in the evolution of the Internet, as more than 500 million people around the world are online daily, yet only one third of them are native speakers of English. IDNs will be a key factor in the transformation of the Internet into a truly global and multilingual resource.

Infrastructural Issues to Accommodate New TLDs

So how is the new addressing regime going to be introduced? Several independent Internet root operators and stakeholders in the Internet community have formed an international, non-profit federation, called the Public-Root. They have established an 'inclusive root' system, which will resolve the domain names of all existing DNS roots (ICANN, New.net, ORSC, et al.) while resolving the new TLDs. A root operator can be any organisation that hosts a root server and operates under certain technical standards. Root servers are an essential infrastructural part of the DNS; they collectively manage the so-called root zone file, a single directory that contains references to all TLD name servers. These authoritative name servers, in essence, 'know' where to find second-level domains under a given TLD.

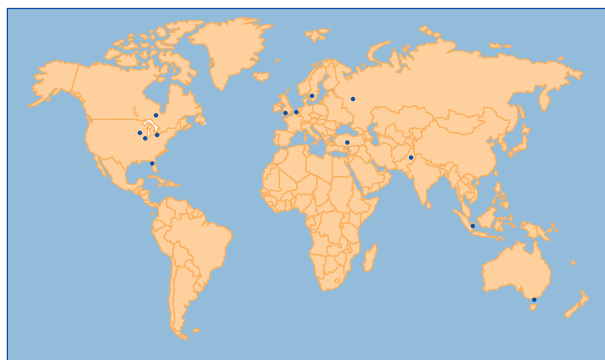
The Public-Root organisation has entered into an agreement with UNIDT (UNified IDentity Technology), a company founded specifically for the coordination, introduction and registration of corporate TLDs. Both organisations are contributing to the development of the next-generation Internet and have developed standards for domain navigation in combination with the use of new TLDs.

The Public-Root operates through a system that reflects the current ICANN regime and follows the standards developed through the Internet Engineering Task Force (IETF). A group of independent operators runs 13 master root servers. This system maintains and distributes the so-called authoritative root zone files, which include all domain names in all other DNS roots. The master root servers propagate the root zone files to affiliated root systems. The system consists of reliable technology that supports universal resolvability of TLDs and eliminates domain name conflicts. The Public-Root is the only DNS root that resolves all TLDs and domain names available on the entire global Internet. In the past, many organisations registered TLDs which ICANN has refused to resolve. The Public-Root however resolves all registered, non-colliding TLDs, disregarding its registrant or its financial power.

The Public-Root system

The Public-Root DNS is robust and secured against tampering, abuse or intrusion. Root operators are required to provide a critical infrastructure to the Internet community and must ensure the security and reliability of their servers. The root is tested technically by its root server operators on a regular basis to address security issues, including a comprehensive review of the geographical distribution of root server systems. The resolution of all TLDs in the root is tested regularly by INAIC (the Internet Names Authorization & Information Center). All of this ensures the continued reliability, performance and response time of the root infrastructure.

Stakeholders in the Public-Root system set standards and operational specifications by consensus. Consideration is given to such matters as hardware selection, host capacity, operating system, name-server software, network connectivity, redundancy and the physical environment. These specifications form the basis of the obligations that bind root-server operators as trustees of the Public-Root. To be affiliated with the Public-Root, operators must guarantee the stable technical operation of the DNS.



World-wide root server locations

The Public-Root has adapted to the key innovations enhancing use of the Internet. It is currently compliant with IPv6 standards (an advanced version of the current IPv4, which exponentially expands the number of IP addresses available) and Internet2 technology (see <http://www.internet2.org>). In the course of 2005, the Public-Root also expects to be fully compatible with the new email standard Email2, which holds the promise of spam-free communication, and internationalised domain names (IDNs), which are in particularly high demand.

cTLD Administration

The Public-Root organisation and UNIDT are responsible for the administration of cTLDs (and pTLDs, see text box on p. 13). However, they have no intention of 'governing' the next-generation Internet. Rather, they will defer to extant or future entities with legitimate authority over Internet policy matters. For its part, the Public-Root coordinates with root-server operators to ensure the resolution of TLDs in a sustainable, state-of-the-art fashion. By contrast, UNIDT maintains exclusive rights to market and sell new TLDs, which it intends to do through hundreds of resellers throughout the world. Registrations are approved by an independent Internet Names Authorization & Information Center (INAIC) Council, which reviews applications in accordance with objective, transparent and non-discriminatory principles. This Council will not refuse to approve any new TLD, except for those that might cause operational or trademark conflicts.

The Public-Root system ensures universal resolvability – a user will get the same answer to the same query from any computer or device on the Internet. This universal resolvability is secured through first-come, first-served delegations, which minimise TLD conflicts and duplication.

Heading Toward the Second-Generation Internet

Corporate and public TLDs are an enhancement for the current domain name system. Their introduction is the first visible sign of the second-generation Internet for end-users. In addition, the imminent launch of the Public-Root infrastructure provides a wedge for new technology, such as IPv6, and, later in 2005, Email2 and internationalised domain names, all of which will improve the web experience throughout the world. IDNs will make the Internet a truly global and multilingual resource, which is increasingly crucial, as the majority of people now online speak non-western native languages.

Corporate TLDs will contribute to an improved, consistent and ubiquitous web presence world-wide, thereby lifting the limitations inherently imposed by country code TLDs or gTLDs. Due to its coexistence with the established gTLD and ccTLD convention, the new naming structure can grow without creating disruption. In doing so, it may very well mark the beginning of a new era in electronic communications.

As the Internet evolves into a much more sophisticated, time-efficient network that hosts advanced applications as

DNS settings to resolve all TLDs

Eventually, ISPs will resolve all cTLDs and pTLDs. But end users can already adjust their network settings to resolve all existing TLDs. The network settings for most operating systems can be found at <http://www.inaic.net>

Windows 2000/2003/XP users who want to change their settings automatically can use the free Internet2 upgrade kit, which will search and test several public DNS servers at different locations. It will update DNS settings with three public DNS servers on three different IP address ranges. The tool can be run as often as required. It will always search, test, and assign the three best servers to the DNS of the user's PC.

All existing TLDs will still be resolved by the new Public-Root DNS.

At the moment, more than 3000 companies and organisations have registered cTLDs and pTLDs in the Public-Root. This figure is expected to grow rapidly in the coming months, as the system is formally released and marketed through UNIDT.

well as accommodates many more gadgets and appliances, the new naming structure will become essential for users. These new TLDs will contribute strongly to quickly access relevant content. The time has come for a new addressing regime that puts power in the hands of website operators and their users.

Marcel Bor

CTO UNIDT

marcel.bor@unidt.com