Parsing hope from hype: should domain name registries care about IoT?

Sandoche Balakrichenan, Afnic

Parsing hope from hype: should domain name registries care about IoT?

It is difficult to explain the role of a domain name registry[1] to someone outside the domain industry. If someone asks me what my company does, the quick answer is that we manage the Internet domain namespace for France and its overseas territories. In addition, we are also backend operators for gTLDs (generic Top-Level Domains).

The impression that most of the people outside the domain industry who get the above answer have is – "oh, you sell domain names, or you are a web design development or an SEO company".

The comparison one could relate to is the World Wide Web and the DNS (Domain Name System). The World Wide Web would not be operational without the DNS, but the DNS does not share the same limelight as the World Wide Web. Similarly, a domain name registrar[2] or a web site development company would not be present without a registry. Nevertheless, a registry and its role in keeping the Internet operational are less visible.

Need for a domain name registry

In the Internet there are two major namespaces: one being IP addresses and the other being domain names.

Domain names became a necessity for two reasons[3]. Firstly, humans remember names better than numeric addresses (i.e. IP addresses). Secondly, when the servers that host web content are reconfigured and their IP addresses change, the generic public uses the same domain name to identify the servers, unaffected by the IP address modifications.

To resolve a domain name to its related information (such as the website) in the Internet, the client software (such as browsers) formulates a DNS query and sends it over the Internet. The objective of the DNS query is to find the authoritative information (e.g. the IP address of the server hosting the information or services linked to the domain name) using the DNS ecosystem.

To enable scalability and minimize storage, the DNS database is designed as a hierarchy, like a pyramid[4]. The DNS query sometimes has to go through multiple iterations from the top of the hierarchy (which is called the 'root[5] servers') downwards until it obtains the authoritative information. Information on how to reach the domain name registries technically identified as TLDs (Top-Level Domains), are stored in the root servers. The TLDs include country-code TLDs such as '.fr' (representing the Internet namespace for France) and generic TLDs such as '.com'. Each TLD includes many second-level domains (such as 'afnic' in 'afnic.fr'), each second-level domain can include a number of third-level domains ('labs' in 'labs.afnic.fr') and so on.

The Internet domain namespace is hierarchically partitioned among domain name registries, which play two important roles. Firstly, they are responsible for administering and operating a TLD, following certain rules. Secondly, they maintain a centralized database for each TLD, thus enforcing the singular association of a domain name to its related information in the global Internet.

1 https://en.wikipedia.org/wiki/Domain_name_registry

2 https://en.wikipedia.org/wiki/Domain_name_registrar

3 Milton L. Mueller, Ruling the Root: Internet Governance and the Taming of Cyberspace 39-40 (Cambridge, Mass.: MIT Press 2002)

4 "The Origins of ccTLD Policymaking" by Peter K. Yu (https://scholarship.law.tamu.edu/cgi/viewcontent.cgi?article=1545&context=facscholar)

5 https://blog.apnic.net/2017/02/15/the-root-of-the-dns/

Need for diversifying the revenue stream

With the boom in Internet usage of the late 90's and early 2000's, the sale of second level domain names created a lucrative business for domain name registries. However, since 2012 the growth in the domain name market has started slowing down[6], and the trend continued into 2018. This has led many domain name registries to diversify their revenue streams[7]. These diversification efforts include providing additional DNS services with respect to infrastructure (e.g. Anycast DNS services), security (e.g. DNS Firewall), monitoring tools (e.g. FRWATCH[8]) etc.

In addition to these services, domain name registries have been eager to capitalize on certain innovations, such as how to use the DNS ecosystem in a different manner from what it was originally conceived for, for example by using technologies such as ENUM[9] ONS[10]. However, none of them have turned out to be killer applications, which could generate a dedicated revenue stream for domain name registries. This is where IoT (Internet of Things) comes into the picture for domain name registries.

IoT and the need for identification and name service resolution

In a nutshell, "IoT" is the Internet. In the Internet there are communication entities (devices) which are interconnected, such as computers, mobile phones, routers etc. The IoT tries to go a step further and connect all sorts of entities (things), such as humans, cattle, bricks etc. to the Internet.

In order for these things to be connected to the Internet, they need the support of carrier devices. Examples of such carrier devices are RF-ID, sensors, barcode, NFC etc. This is the case in the Internet where for a computer to communicate, it needs a carrier device such as a network card.

The carrier devices in the Internet are identified uniquely in the scope of the Internet by identification mechanisms such as IP address, MAC addresses, domain names etc.

To uniquely identify the 'thing', the carrier device tagged to the 'thing' should have an identifier that is unique within its scope. Similarly to the Internet, information related to the things will be distributed globally, and there is a demand for services that map the thing's identifier to its related information or service in the Internet.

The hype

In 2018, there were about 7 billion[11] connected devices, and the number is expected to grow. In comparison, there were approximately 342.4 million domain names[12] registered across all TLDs by the third quarter of 2018. In the event that all devices connected in the IoT were to register a domain name, domain name registries would already have found their El Dorado.

Let's look at the case of home-automation-use in IoT, to check whether there is a need to register a domain name for every IoT device connected to the Internet.

Connected devices at home include televisions, thermostats, bulbs, refrigerators, coffee machines etc. To identify them in a human-friendly manner, they might be configured with a default or personalized name (such as light_kitchen). If you want to connect to one of these devices while still at office, you need to connect to a gateway device (e.g. Amazon Alexa), which is in turn connected to your Wi-Fi network. All the devices at your home, which has been named, do not need to be domain names with global visibility but do need to be unique within the scope of the gateway device. Hence, there is no need to register domain names publicly in the Internet in order to access these devices.

In the Internet, a domain name is indispensable to have a global online presence. But for many IoT applications, the visibility is specific to a particular gateway, application or an industry. Even if there is a need for global visibility, they could be segregated under a designated namespace which may not create a revenue stream for the domain name registries.

---

6 https://www.afnic.fr/en/resources/publications/french-domain-name-industry-report/2015-online-edition/2017-year-of-consolidation-for-the-domain-name-market-1.html

7 https://www.afnic.fr/medias/documents/etudes/Global_Domain_Name_Market_in_2017_FINAL.pdf

8 https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/10510/show/l-afnic-lance-frwatch-un-nouveau-service-de-surveillance-et-de-prospection-de-noms-de-domaine-2.html

9 https://tools.ietf.org/html/rfc3953

10 https://www.gs1.org/sites/default/files/docs/epc/ons_1_0_1-standard-20080529.pdf

11 https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

12 https://www.verisign.com/en_US/domain-names/dnib/index.xhtml?section=executive-summary

The hope

The home automation use case discussed previously did not need a global Internet visibility and it is the same case for many IoT application scenarios. The interaction scope is restricted to a particular brand, cloud platform or to a large-scale alliance of companies. Interoperability between the different IoT applications is not needed.

Nonetheless, with the advent of smart cities, there is a need to break these silos, and there arises a necessity to interoperate with different IoT applications in the Internet to make the correct decision. Let's take a simple use-case where there are two IoT applications: one being the smart grid, which supplies electricity to the city lighting system and the second being the traffic management. Electric supply to the city lighting system could be optimized based on traffic. This example shows how input from a device in one IoT application domain could be needed by a device in another IoT application domain to make an optimized decision. Furthermore, it shows that the identifier for an IoT device should be accessible from the Internet.

In order for all these identifiers to be visible in the global Internet scope, the only possible way is to provision them in the DNS. The Chinese National Identity platform is one such example, wherein there is a Chinese IoT root (cniotroot.cn[13]) zone in the DNS. The number of Chinese IoT namespaces is delegated under this zone.

The Chinese National IoT platform has over one billion registered names[14]. It is true that these registered names will not boost second-level domain registrations and thus generate a direct revenue stream for CNNIC (the Chinese domain name registry). However, bringing in the heterogeneous IoT namespaces to be delegated under the DNS solves two major issues: first, a particular company, industry or an alliance of companies could operate and manage their respective IoT namespaces independently. Secondly, it is possible to interoperate between these different IoT namespaces for identifier resolution and service discovery.

The entities managing the segregated IoT namespaces do not essentially have the technical expertise in managing and operating such large databases, which need to conform to DNS standards. Securely registering a device and resolving it to its information or service in the Internet using DNS on a large scale is a complex process, something which domain name registries have proven to have a track record of over the years.

The roles played by domain name registries could be to act as a back-end registry service provider for the segregated zone, a DNS infrastructure provider, a DNS solution provider and to provide technical advice on using DNS solutions such as DNSSEC, DANE (Verisign has been actively positioning the DANE protocol as a way forward for securely scaling IoT[15]) etc.

The business model for domain registries in IoT will probably not be based on second-level domain registrations, but on providing technical services for IoT device-identity management, authentication, discovery and security.

13 http://www.cniotroot.cn/home

14 https://iotweek.blob.core.windows.net/slides2017/WORKSHOPS/Big%20Data/Globally%20Interoperable%20IoT%20Identification%20RDA%201%2C2%2C3/Tian%20Ye%20NIOT%20Platform%20and%20its%20Applications.pdf

15 https://www.eclipsecon.org/na2015/sites/default/files/slides/01%20-%20EclipseCon-Verisign-IOT-Security.pdf

Council of European National Top-Level Domain Registries

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 54 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries. Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

This paper is part of a series of articles covering industry research, historical data analysis and the future of technologies such as digital IDs, published over the course of 2019 to mark CENTR's 20th Anniversary. These publications do not necessarily present the views of CENTR or of the CENTR community.

CENTR wishes to thank and acknowledge the organisations which have so generously contributed to the efforts of its 20th Anniversary:

Platinum sponsor

Gold sponsor

Silver sponsor

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn