Why DNS should be the glue in the IoT?

Sandoche Balakrichenan – Afnic
sandoche.balakrichenan@afnic.fr

Context:

To start with, let's have a look at the supply chain industry wherein the term Internet of Things (IoT) was first coined. IoT has multiple use-cases in this industry, such as extended packaging, tracking and tracing of goods etc. Concentrating on the extended packaging use-case, IoT enables a consumer to have additional information about the product he/she intends to buy through their mobile phones. It is enough for a buyer to scan the barcode of the product using an application in one's smart phone, and the application will enable him/her to access a content (such as a website) in the Internet which has additional information to what is currently available in the product's package.

Like the domain name industry wherein we have domain name "Registries", the consumer industry has GS1. Just like the registries which maintain the unicity of domain names, GS1 helps to maintain the unicity of the identifier of a product such as the barcode. The product identifier in the GS1 industry is encoded based on the Electronic Product Coding (EPC) format.

Moving to a second use case, in the Wireless sensor industry, the "thing/object" (i.e. the entity of interest) is associated with a sensor device. The identification of this sensor device could be done in two possible ways: 1. Pre-encoded MAC addresses and 2. Configurable network addresses. Even though the MAC addresses are distributed by single organisation, that is the IEEE, it is well assumed that MAC addresses are not unique.

Problem Statement:

Limiting to the two use cases explained in the previous section, it is clear that one cannot use bar code (encoded using EPC) to identify a "thing" in the Zigbee network nor we can use a sensor device having a MAC address to identify a "product/thing" in the supply chain industry. Such silos in encoding the identification data are a fact in the IoT industry.

Another issue to note here is that there is a conceptual difference between the identifier of an object and the identifier used for resolving the object uniquely in the network. In the extended packaging use-case, the barcode is both the identifier of the object and the one used for resolution, whereas in the sensor device use case; it has two identifiers, wherein the MAC is the identifier of the object, and the network address used for resolving the sensor device in the network may change depending on the location of the sensor device.

One possible way for solving the issue of heterogeneity in identification encoding mechanisms is for a standardization organisation to develop a global identification scheme, and ask all the stakeholders in the IoT domain either existing or new to use the new encoding scheme for identification. With the standardization of protocols such as IPv6 and with the benefits of a large addressing space, it is a possibility.

But in reality, experiences in working with stakeholders in the supply chain industry we do feel that it will be nearly impossible to have one global identification scheme for all the "things" in the world, since most industries have been using their own proprietary coding standards (i.e. identification schemes) for a long time. For this reason, it is highly unlikely that they will move to a different object identification system.

Need for the glue:

As the DNS acts as a "glue" in the current Internet, where its basic feature is to resolve "human-friendly" host names to their corresponding "machine-friendly" IP addresses, in IoT also it is proved, that the DNS could be a glue for certain identification schemes.

In the supply chain industry where we were involved in a project [WINGS] that was awarded the R&D project of the year 2013 by Council of European Top Level Domain Registries, we worked with GS1 in evolving the Object Naming Service (ONS) Standard [ONS standard]. ONS is an overlay mechanism which uses the basic DNS infrastructure. As part of this project, it has been proved with implementation examples that identifiers using EPC encoding scheme (wherein it could be barcode or RFID tags) could be converted into a domain name based on the ONS standard and then use the DNS for resolution and service discovery.

Let's look at an example of how ONS is used to resolve an object attached with an RFID tag (the object identifier is encoded following EPC encoding) to its extended packaging information in the Internet. Since ONS uses DNS, the EPC has to be converted into a Fully Qualified Domain Name (FQDN) to query the ONS infrastructure.

To read the code from the tag associated with the object, an RFID reader is needed. The RFID reader connected to a computer reads the code in Binary form. A conversion mechanism (based on ONS standards) is used to convert the binary data into an URI of the following format "urn:epc:id:sgtin:3102542.000024.46595".

Using the "narrowest to widest" structure for host name, the URI could be rewritten as 4.2.0.0.0.0.2.4.5.2.0.1.3.sgtin.id.example.com as per the ONS specifications. The serial number ("46595") is ignored since the ONS resolution stops at the object reference level. The serial number is used to distinguish between different objects of the same class (for example to distinguish from one nestle product to another). The label (such as example.com) added at the end could be any string, which is added by the conversion tool, based on its configuration. The ONS standard specifies a mechanism, wherein whatever 'label' is added at the end of the identifier during the conversion, is modified and redirected to its destination based on the DNAME resource records, used in the DNS.

The delegation at the DNS could be as follows:

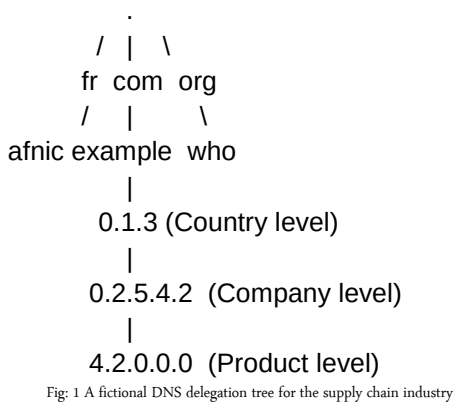

Fig: 1 A fictional DNS delegation tree for the supply chain industry

In the sensor industry, we were involved in setting up a Proof of Concept (PoC) for the Long Range radio network. Sigfox [Sigfox], a pioneer in this business has successfully established a market that enables to communicate with objects (things attached with a sensor device) from a base station, similar to mobile communication. But, the communication here is of low range (In Kilo bytes) and also of low cost (around 12 euros for an object per year). As a pioneer, Sigfox has built a proprietary architecture from encoding the identifier for the sensor device, to the gateway which does the mapping from radio to the Internet, to the cloud which stores the information.

The competition in the sector came in the manner of LoRA alliance [LoRA Alliance] wherein there are multiple stakeholders involved in each segments of the LoRA end-to-end architecture. We at Afnic were involved in looking at how DNS could be used in mapping the MAC address from the object in the radio network to the specific operator for the client in the LoRA network. The PoC helped us to prove that DNS could be used for resolving the object identifier to its destined service.

Conclusion:

Even though there are multiple identification schemes, they all have certain common features. Some of them are: they are allocated hierarchically, control is decentralised and the nature of allocation makes sure that there is no duplicity. These features described previously are similar to the domain name allocation and management, and thus, identifiers in IoT could leverage the DNS infrastructure and software for allocation and resolution.

Leveraging DNS for other uses started with ENUM for telephone numbers, and for IoT; there exists already overlay mechanisms services such as ONS and Object Directory Service (ODS) [ITU-T standard] which uses the DNS to resolve the IoT identifiers (using their respective identification schemes) to its related digital information.

Vision:

It is a requirement for IoT that we need to have a single protocol, which could be used to map an object identifier to its intended service, for any type of identification schemes either existing or new. In addition, the protocol should be able to support millions of devices which are the case for IoT. DNS has withstood the exponential growth of Internet. And, as described earlier in this document, ITU-T and GS1 have already worked on different variants of DNS, since they too felt that the only practical alternative for look up and discovery in the IoT is using the DNS. The vision is that IETF should be in the fore-front in pushing DNS as a look-up mechanism for the IoT as shown in the figure below.

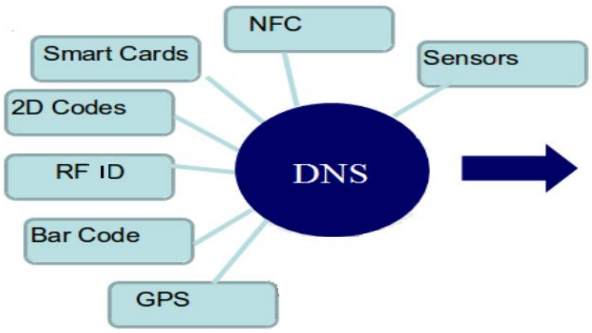

Fig: 2 DNS being the glue for all identification mechanisms in the IoT domain

References:

[WINGS] http://www.wings-project.fr/

[ONS standard] http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf

[ITU-T standard] Object Directory Service for Mobile AIDC services (ISO/IEC 29177)

[WSN Project] http://www.labfab.fr/portfolio/lora-fabian/

[Sigfox] http://sigfox.com/en/

[LoRA Alliance] https://www.lora-alliance.org/