ISSUE PAPER

DNS

The naming service for IoT

AN AFNIC PERSPECTIVE

ISSUE PAPER

WHAT IS IT?

The term "Internet of Things" (IoT) encompasses several meanings depending on the communities/technologies being involved. The basic purpose is to connect the "Things" in the physical world to the Internet infrastructure. The things could be anything from computers to people to medicines to books.

The things could be connected to the Internet infrastructure *directly* or *indirectly*. A Computer or a mobile phone could be connected to the Internet directly by means of an IP stack and some type of layer-2 connectivity, such as Wi-Fi, Ethernet etc. People or books will have *indirect* connections to the Internet, which may be enabled via some intermediate equipment, which is typically a non-IP carrier device such as sensors, RFID, NFC etc., tagged with the things.

These carrier devices do not use the Internet protocol suite (TCP/IP) for communication. Rather, they use their proper communication technologies such as Radio Frequency (RF), Bluetooth, Near Field Communication (NFC), Long Range, low power wireless platform (LoRA) etc. In order to link the non-IP-capable devices to the IP network (i.e. the Internet), there is a need for a *gateway* device, which can handle communication at two levels: on one hand with the non-IP-capable devices, and on the other hand, with the IP network; thus bridging between non-IP and IP worlds.

/// NEED FOR MAKING "THINGS" SMART

The basic idea for IoT is to make the "things" smart, which are otherwise considered dumb by default, from a technical perspective.

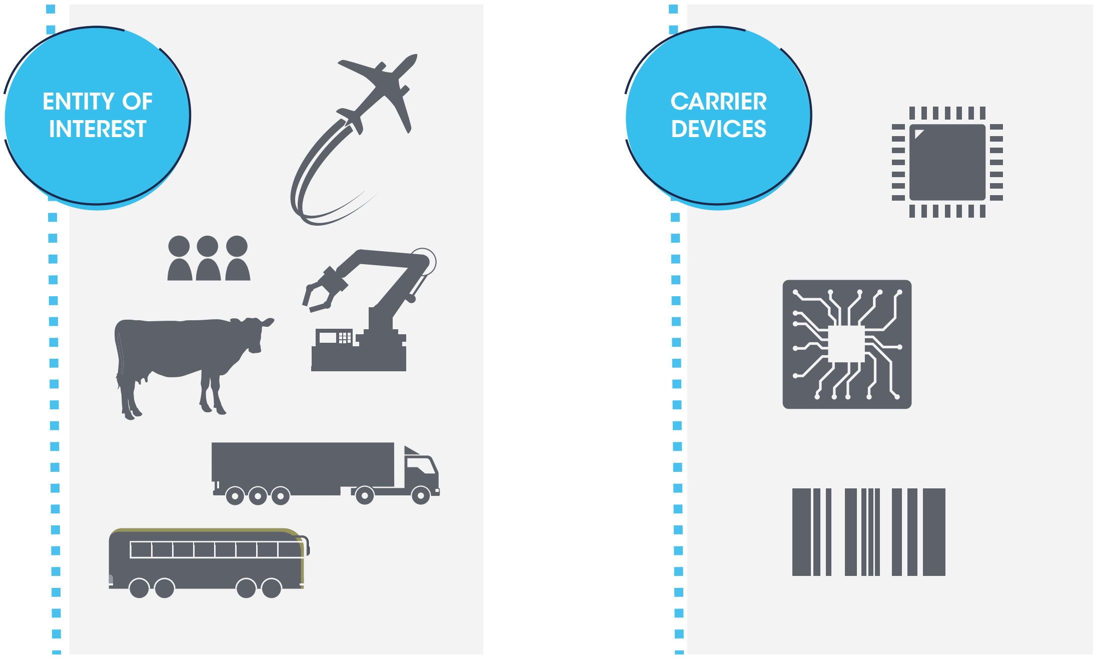


Figure 1 : Making the things smart by tagging carrier devices such as sensors, RF-ID, barcode

Let us take the example of a cow in a herd, which is an entity of interest (Figure: 1) for the farmer. Every 21 days, the cow has a 12 to 18 hours window, which is considered as the optimum period for mating[1]. The cow is highly active during this window, and hence the IoT application is attaching pedometers to the cow. The pedometer tagged to the cow periodically sends information, and a message is triggered to be send to the farmer, when the cow is walking more than its normal average. There is such plethora of applications, when things in the physical world can be tagged with things to make it smart.

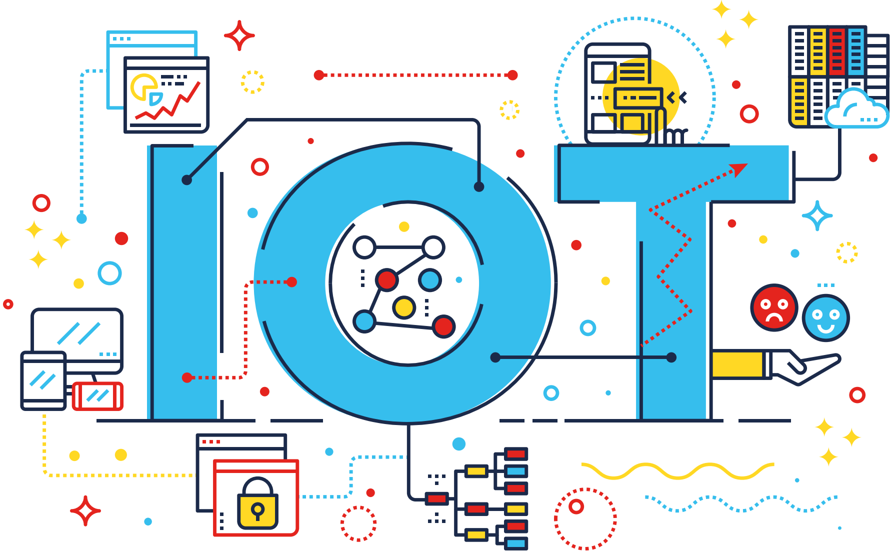
The progress in the hardware development, decline of size, cost and energy consumption has enabled the feasibility of tagging non-IP devices to the physical things. This is the reason why there is much talk about IoT currently, even though the idea is not new[2].

(1) http://www.basvankaam.com/2017/04/04/iot-use-case-the-connected-cow-yes-really/

(2) https://connected.messefrankfurt.com/2016/04/08/the-internet-of-things-not-new-but-more-important-than-ever/

/// THE ISSUE OF IDENTIFICATION IN IOT

Taking the cow example described previously, the farmer needs to identify a cow individually in his herd. For this purpose, the pedometer tagged to each cow in the herd should have a unique identifier. The scope for the uniqueness of the identifiers is limited within the herd.



But, IoT envisions billions of devices connected with the Internet. Hence, the identifier for each thing should be unique in the IoT. In the current Internet infrastructure, identification of a thing (a computer or a router is also a thing from IoT perspective) uniquely on the Internet is based on IP addresses (either IPv4 or IPv6). The IP addresses follow a specific **naming convention** [3]. There is a hierarchical structure[4] which provisions the IP address, and makes sure that there is no **duplicity** (i.e. no two devices in the Internet has the same IP address). Some other things may not use global IP addressing, using private addressing instead. Things having a private address are still connected to the Internet, with the help of a gateway device, which uses a global IP address to transport data from private network to the Internet and vice versa.

As mentioned earlier, IoT involves non-IP capable devices; hence they do not use IP addresses for identification. The way these devices are identified could be classified into *legacy* and *emerging* ones. The legacy identifiers have their existing naming conventions, their proper structure to provision their identifiers to end-users, well before the emergence of the IoT theme. These legacy identifiers range from EUI-48, EUI-64 for MAC addresses to Digital Object Identifiers (DoI) for electronic content to Electronic Product Code (EPC) for RFID, barcodes etc. The emerging ones are new naming conventions with their proper provisioning structure, developed to satisfy specific needs of a particular section of the IoT industry.

One possible way for solving the issue of heterogeneity in naming conventions is for a standardization organization to develop a global/unique naming convention, and ask all the stakeholders in the IoT domain, either legacy or emerging to migrate to it. 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 (who uses RFID and barcode), we feel [5] that it will be nearly impossible to have one global naming convention for all the «things». Industries like consumer, automobile, defense have been using their own proprietary naming conventions for a long time. Migrating to one global naming convention for identifying things, will impact their infrastructure considerably, and does not seem to be a feasible solution. Imagine, asking Walmart and Carrefour to use IPv6 instead of barcodes for labelling a product.

[3] https://en.wikipedia.org/wiki/Naming_convention

[4] https://tools.ietf.org/html/rfc2050

[5] « We » or « Our » instances in this article represents Afnic

/// NAMING SERVICE

The question raised here is that with such heterogeneity in identifier naming conventions and provisioning structure, will it be possible to communicate between 'things' that use different identifier naming conventions?

There are two possible solutions: **disruptive** or **evolutionary** approach. There are number of disruptive approaches[6] for the IoT. Most of them tend to be proposals from the academia, implemented in a laboratory environment (or) tested in specific use-cases.
The evolutionary approach is to use existing technologies which has withstood the operational strains of the Internet. The Domain Naming Service (DNS) is one such technology, which has been there from the beginning of the Internet and still remains it's corner stone. Even though the Internet evolved with a scale that was not even dreamed initially, the DNS remains the basic infrastructure for resolving information in the Internet.

DNS was basically conceived for translating *human-friendly* computer host names on a TCP/IP network into their corresponding *machine-friendly* IP addresses. Besides translating host names to IP addresses, DNS is used for instance by Mail transfer agents to find out where to deliver mail for a particular address, a general mechanism for locating services in a domain using SRV records, resolution of identifiers that do not have traditional host components through DNS using NAPTR resource records etc.

For IoT, there exists already overlay mechanisms services such as Object Naming Service (ONS)[7] and Object Directory Service (ODS)[8]) , which uses the DNS infrastructure to resolve the IoT identifiers (using legacy naming conventions) to its related digital information in the Internet.

/// OUR INVOLVEMENT IN LEVERAGING DNS FOR IOT

It was in late 2008, that we started looking at IoT after the conference "Internet of Things – Internet of the Future" in Nice, which discussed the opportunity to layout, the perspectives for an «Internet of the Future».

The discussions were focused on the ONS, a global look up service, which leverages DNS to map an RFID tag to its information in the Internet. According to the ONS standard V.1.0.1[9], there is a there is a single ONS root zone (onsepc.com), containing the whole ONS name space, and managed by Verisign Inc. Under this single ONS root, there could be delegation at different levels for different Countries providing distribution of the overall ONS database.

Political and technical issues pertaining to a single root scenario, is a déjà vu [10]. in the DNS case. The European Governments (especially France and Germany) insisted the need for a distributed ONS architecture, that is to say, a collection of ONS roots that are sovereign, geographically dispersed and have equivalent functionality.

[6] *Named Data Networking A promising architecture for the Internet of things (IoT) (https://hal.archives-ouvertes.fr/hal-01575110/document)*

[7] *https://en.wikipedia.org/wiki/Object_Naming_Service*

[8] *http://www.itfind.or.kr/Report01/200611//TTA/TTA-0079/TTA-0079.pdf*

[9] *https://www.gs1.org/sites/default/files/docs/epc/ons_1_0_1-standard-20080529.pdf*

[10] *https://www.theguardian.com/technology/2016/oct/04/us-government-internet-control-iana-address-book*

We proposed the «Federated-ONS (F-ONS)» architecture[11], wherein there should be multiple ONS Peer Roots (OPRs), each managed by a regional organization (e.g. based on continents). Below the root there should be DNS zone delegations to either national or local organizations (e.g., a national zone, a single company zone, a consortium of company's zone, etc.).

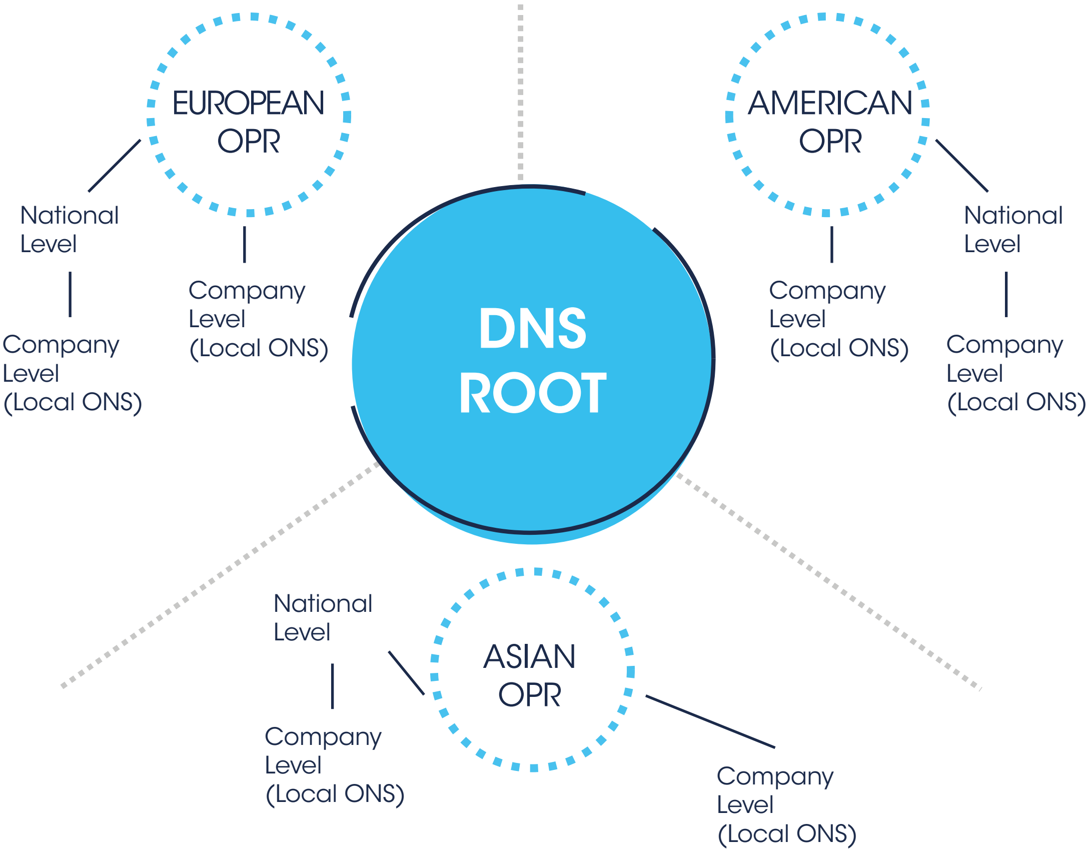

EUROPEAN OPR
National Level
Company Level (Local ONS)
Company Level (Local ONS)
AMERICAN OPR
Company Level (Local ONS)
National Level
Company Level (Local ONS)
DNS ROOT
National Level
Company Level (Local ONS)
ASIAN OPR
Company Level (Local ONS)

Figure 2 : Federated ONS architecture proposed by us

As part of the ANR project WINGS[12], we implemented the proposed architecture (Figure: 2) with three OPRs: **ons-peer.eu** representing the European region, **ons-peer.asia** representing the Asian region, and **ons-peer.com** representing the American region.The delegations under the OPRs confirm to the architecture explained in the previous paragraph.

The proposed architecture enables flexibility, wherein companies under a country which is not able to manage its own namespace can have delegation directly from their respective regional OPR (as shown in Figure: 2). If there is a national level delegation for a country, all the companies associated with the GS1 Member Organization (MO)[13] in that country should get their delegations from their national level zone.

[11] *Sandoche Balakrichenan, Antonio Kin-Foo, Mohsen Souissi, "Qualitative Evaluation of a Proposed Federated Object Naming Service Architecture", Compte rendu de la Conférence internationale de 2011 sur l'Internet des objets et de CPSCom 2011, 4ème conférence internationale sur l'informatique cyber, physique et sociale, p.726-732, 19-22 octobre 2011*

[12] *http://www.wings-project.fr/*

[13] *http://xchange.gs1.org/sites/faq/Pages/there-is-no-gs1-member-organization-in-my-country-how-can-i-apply-for-barcodes.aspx*

If in case, a country does not want to be under a regional OPR, it could have its own national level OPR and all the companies associated with GS1 MO in that country should get their delegations from their national level OPR. In addition, we also proposed a revised query format[14], and a procedure for co-operation between the different OPRs.

We also pursued the propositions made as part of the ANR-Wings project with the GS1 standard[15], and all our propositions were accepted for the evolution of the ONS standard[16]. During the first ceremony of the CENTR[17],awards in 2013, we were facilitated[18] for this work.

In late 2016, we joined the LoRa Alliance™ [19] and started working on complementary specifications that include DNS use in the LoRaWan™ network. The LoRa-alliance backend specification[20]that was published recently (in October 2017), specifies that DNS will be used in different phases of establishing LoRa connectivity: for example, for identifying the Join Server in the event of Over the Air Activation, and the network server in the event of roaming.

/// IOT IDENTIFIER ISSUES IN BRIEF

There are number of issues in IoT. It is difficult to deal with all of them in a single document. In this section, we will briefly look at different issues concerning IoT identification.

- **Identifier resolution**

It is a requirement for IoT that we need to have a single protocol for resolving an IoT identifier, uniquely in the Internet. This will allow seamless interoperability, wherein the identifier could use any naming convention; either legacy or emerging. While the definition of new standards is a long and sometimes tedious task, the use of technologies currently available on the Internet should be encouraged.

- **Scalability management**

In addition, the protocol should be able to support millions of devices and has the capability to scale. One of the best understood methods to have scalability in naming is the use of naming hierarchies to limit the scope of a name to a specific hierarchy.

- **Security**

An area of concern is the security of IoT devices. IoT-centric attacks [21] have raised concerns on its adoption/deployment. In protecting against exploits, IoT devices need to secure their communications. Unique identifiers alone are not enough to provide security during identifier resolution. Additional protection mechanisms such as cryptographic keys should be accompanied to protect against the forgery of the identifier.

- **Privacy**

UAnother major concern for IoT relates to privacy [22]. It is clear that all of the privacy requirements cannot be taken into consideration only at the identification schemes, but support for privacy at different levels is a crucial feature. The main issue with a privacy preserving identification scheme has to do with the guarantee that the scheme is able to protect the possibility to link information from a number of devices with a specific person or group of people.

[14] S. Balakrichenan, A. Kin-Foo et M. Souissi, "Qualitative Evaluation of a Proposed Federated Object Naming Service Architecture", Compte rendu de la Conférence internationale de 2011 sur l'Internet des objets (iThings/CPSCom) et de la 4ème conférence internationale sur l'informatique cyber, physique et sociale, 2011, p.726-732.

[15] https://www.gs1.org/standards

[16] https://www.gs1.org/sites/default/files/docs/epc/ons_2_0_1-standard-20130131.pdf

[17] https://www.centr.org/

[18] https://www.afnic.fr/en/about-afnic/news/general-news/7289/show/afnic-r-d-rewarded-for-its-work-on-the-internet-of-things.html

[19] https://www.lora-alliance.org/

[20] https://www.lora-alliance.org/resource-hub/lorawantm-back-end-interfaces-v10

[21] http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/

[22] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7663&no=12

/// OUR VISION FOR IOT

Even though there are multiple naming conventions (either legacy or emerging) in the IoT, most of them have certain common features.

- They are allocated hierarchically

- Control is decentralized

- The nature of allocation makes sure that there is no duplicity.

These features 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.

DNS has withstood the exponential growth of Internet and remained the naming service for the current Internet infrastructure. There exist mechanisms for security [(23)] [(24)] and privacy[(25)] in the DNS which could be re-used in IoT.

We are convinced that DNS is a realistic solution to consider for name resolution in IoT. Our conviction is based on our work with the GS1 standardization organization and LoRa Alliance™. Number of organizations (such as IETF[(26)], RIPE[(27)], ICANN[(28)]) where we are involved, has started concentrating on IoT. As an organization, which has considerable expertise in DNS, it is our role to educate/contribute to enable interoperability in IoT between heterogeneous naming conventions.

(23) https://tools.ietf.org/html/rfc6698
(24) https://tools.ietf.org/html/rfc4034
(25) https://tools.ietf.org/html/rfc7626
(26) https://trac.ietf.org/trac/int/wiki/IOTDirWiki
(27) https://www.ripe.net/participate/mail/ripe-mailing-lists/iot-wg
(28) https://www.icann.org/en/system/files/correspondence/holmes-to-icann-01feb17-en.pdf

USEFUL INFORMATION

To contact Afnic

Afnic
Immeuble Le Stephenson
1, rue Stephenson
78180 Montigny-Le-Bretonneux
France
www.afnic.fr

support@afnic.fr

Tél. : +33(0)1 39 30 83 00

mastodon.social/@afnic

@AFNIC

afnic.fr

About Afnic :

Afnic (the French Network Information Centre) comprises public and private stakeholders, including government authorities, users, and Internet service providers (Registrars). It is a non-profit organisation.

Afnic is the French Registry for the .fr (France), .re (Reunion Island), .yt (Mayotte), .wf (Wallis and Futuna), .tf (French Southern Territories), .pm (Saint-Pierre and Miquelon).

Afnic is also positioned as a provider of technical solutions and services for registries and registrars.

afnic