The DNS Role in the IoT World

4 possible IoT structures & DNS roles

Maria Butina, American University, Washington, D.C.
APTLD72, Tbilisi, Georgia
September, 14-15 2017
Find a Panda Among the Snowmen
Find a Panda Among the Snowmen
Once It Was Found, Cannot Be Forgotten
Scenario #1: Local Router
Scenario #2: Manufacturer’s Server
Scenario #3: Common Protocols
Scenario #4: Third Party Applications
Conclusion
Scenario #1: Local Router

**Description:** User controls a device through a router-gateway, which receives a signal from the user and sends it through the assigned port to a certain device.

The router-gateway acts as a firewall against information entering the local wi-fi network, but misses requests of the devices for necessary information from the internet.

**DNS Role:**

- To obtain the user’s router’s IP-address so that the user’s IoT devices can be managed. (When the user only enters the domain name of his router.)
  - Registration of new domain names does not take place.
  - DDNS is an additional function that should be used if a router has a dynamic real IP-address.

**Internet**

- **Port 47111**
- **Port 47000**
- **Port 48777**

**DNS**

- Security
- Possibility of combining devices from different manufacturers in one system

- Complexity of customization
- Complexity of management
  (multiple programs and applications for system management)
Scenario #2: Manufacturer's Server

**Description:** Every IoT device manufacturer offers an application/webpage that only manages its devices.

If a user has IoT devices from different companies, he is forced to manage them via different apps/websites.

To exchange data between the devices of different brands a user has to do it manually.

- Simple ONLY if all IoT devices are same brand.
- Profitable for a manufacturer – holds a user to a particular brand.

- Complexity of management if there are different brands of devices in one system.

**DNS Role:**
To obtain the IoT manufacturer’s IP-address so that the user’s IoT devices can be managed. (When the user only enters the manufacturer’s website.)

- Registration of new domain names **does not** take place.
- Third-level domain names increase.
Scenario #3: Common Protocols

Description:

Manufacturers of IoT devices agree on general rules, so any application / website is suitable for managing any device.

Direct communication between devices is possible.

- Safe for a user
- Simple for a user
- It is unprofitable to a manufacturer (the motivation to buy devices of one manufacturer is lost)
- A complete consensus between all manufacturers is difficult for many reasons.

DNS Role:

To obtain any manufacturer’s IP-address so that the user’s IoT devices can be managed. (When the user only enters the domain name of any IoT manufacturer.)

- Registration of new domain names does not take place.
- Third-level domain names increase.
Scenario #4: Third Party Applications

Description:
An outsider creates software that can provide one application/website for managing all IoT devices from different manufacturers working on different protocols.

+ Simple and safe for a user
+ Creates a new business opportunities for an outsider software developer.

- Errors are possible due to different IoT device protocols.

DNS Role:
To obtain the software provider's server's IP-address so that the user's IoT devices can be managed. (When the user only enters the domain name of the outsider software provider.)

- Registration of new domain names does not take place.
- Third-level domain names increase.
1. **IoT devices DO NOT** need any domain names. (No new names assigned.)

2. In the IoT world, **DNS** will be playing its **CLASSIC APPLIED ROLE** to obtain an IP-address when prompted with a domain name supplied by the user.

3. Third-level domain names registration will increase, but with **NO PROFIT** to the **DNS** systems.

4. Since **DDNS services usage** might increase, **INVESTING in DDNS** might be smart.

**Conclusion**