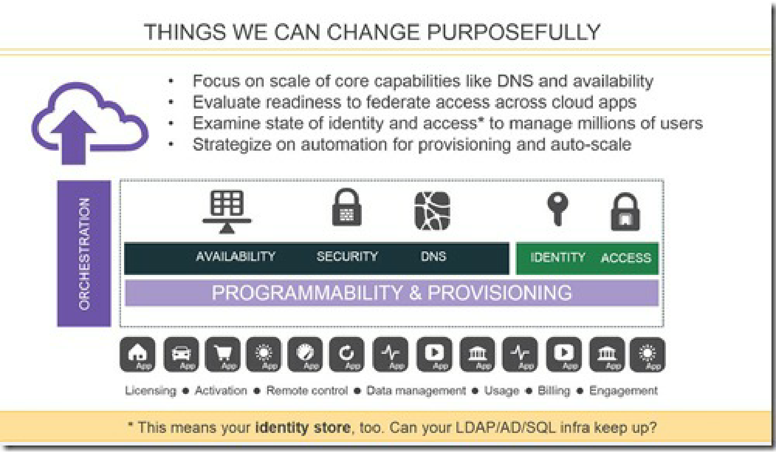
# IoT Effect on Applications

**Peter Silva, 2015-28-04**

As more applications are needed to run those Things, traditional infrastructure concerns like scale and reliability will become paramount. Additional challenges with identity and access, improving the user experience, and the need for faster provisioning of services could overwhelm IT departments. A robust, scalable and intelligent infrastructure will be necessary to handle the massive traffic growth.

IT professionals are tasked with designing and building the infrastructure that's ready for the challenges that lie ahead, including IoT. But many of today's traditional architectures will buckle under the increasing demand of all the connected devices. According to IDC, the rate at which applications double in the enterprise is every four years. This is likely to be cut in half as more IoT devices need applications supporting them and organizations need to be ready for the deluge.

The Domain Name System (DNS) is the most likely method for connected devices to locate needed services, and it's potentially the means by which people will locate the devices themselves. There might be other schemas in the planning process, but those would require the adoption of a new technology naming standard, which would be costly, slow and highly unlikely.



THINGS WE CAN CHANGE PURPOSEFULLY

- Focus on scale of core capabilities like DNS and availability
- Evaluate readiness to federate access across cloud apps
- Examine state of identity and access* to manage millions of users
- Strategize on automation for provisioning and auto-scale

ORCHESTRATION
AVAILABILITY
SECURITY
DNS
IDENTITY
ACCESS
PROGRAMMABILITY & PROVISIONING
App
Licensing ● Activation ● Remote control ● Data management ● Usage ● Billing ● Engagement

* This means your **identity store**, too. Can your LDAP/AD/SQL infra keep up?

Clearly, security must also be present since Iot has the potential to weave vulnerabilities throughout the system. Unless organizations remain proactive, the ubiquity of connected devices presents a gold mine for attackers. Outpacing attackers in our current threat landscape will require more resources in order to minimize risk. Organizations will need to continue to harden our own infrastructures and look to cloud services like DoS mitigation to lessen the effects of attacks.

At the same time, the explosion of embedded devices may well be the event that drives more mainstream IPv6 adoption. There are several advantages to IPv6 such as a large namespace, address self-configuration, and the potential to remove Network Address Translation (NAT) problems. The data center will require some planning to embrace this shift. Components such as routers, firewalls, and application delivery controllers will need to be IPv6-ready, capable of understanding the protocols and data that devices will use to communicate.

To ensure security, intelligent routing, and analytics, networking layers will need to be fluent in the language your devices use. Understanding these protocols within the network will allow traffic to be secured, prioritized, and routed accordingly. Recognizing and prioritizing these messages will enable better scale and manageability of the onslaught of device traffic and data. Intelligence will also be needed to categorize what data needs attention (like a health monitor alert) and what doesn't (temperature is good).

According to TechTarget, to ensure high availability of IoT services, enterprises must consider boosting traffic management and monitoring. This will both mitigate business continuity risks, and prevent potential losses. From a project planning standpoint, organizations need to do capacity planning and watch the growth rate of the network so that the increased demand for the required bandwidth can be met.

ps

Related

- The Digital Dress Code
- Is IoT Hype For Real?
- What are These "Things"?
- IoT Influence on Society

- CloudExpo 2014: The DNS of Things
- Intelligent DNS Animated Whiteboard
- The Internet of Me, Myself & I

Technorati Tags: devices,f5,iot,m2m,security,sensors,silva,things,wearables,dns,applicatons

Connect with Peter: Connect with F5:

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com