www.pipelinepub.com
Volume 17, Issue 8

Hyperscaling IoT Services

By: Jonas Bjorklund

Growth in “smart everything” is propelling the Internet of Things (IoT) through explosive growth. Amid this acceleration, connectivity becomes essential. It’s anything but simple, though.

Mobile operators that think they can create IoT connectivity services by repackaging existing cellular services need to think again. It’s not just a matter of adding IoT SIM management capabilities to an existing mobile core. Enterprise IoT customers need so much more in terms of flexibility and security.

It’s a giant step to go from offering consumer services, with a handful of subscriber-types and associated policies, to providing complex IoT connectivity services. In IoT, each customer has their own unique requirements.

Some IoT customers need all or part of the traffic delivered in private connections such as APN and VPN. IoT device security is crucial, and customers also want to protect the traffic through firewalls. Many customers want to manage their own connectivity and security policies per device or for device groups from a web interface. Others need local subscriptions in specific countries, including in which permanent roaming is prohibited. And they want a unified experience across all these international networks. This means that operators are facing challenges to maintain things such as policies and IP addresses across partner networks.

The bottom line is that customers need programmable and secure global IoT connectivity. Mobile operators will realize that they cannot deliver this from a mobile core created for consumer services. They need to chart a different course forward to deliver what their IoT customers actually truly need. Let’s take a closer look.

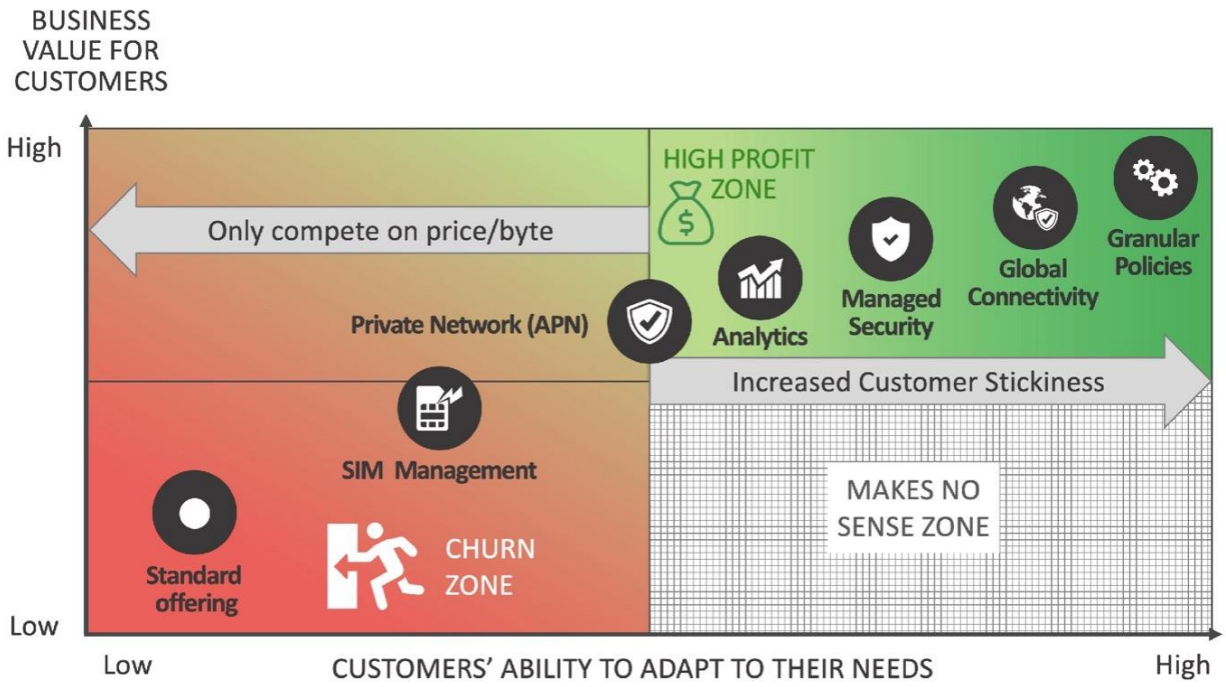

Figure 1: Business value in IoT connectivity
click to enlarge

Delivering what customers need

The matrix above shows two perspectives that we think operators need to consider when creating IoT connectivity services. On the Y-axis is the business value the service brings to the IoT customer. On the X-axis is the customer's ability to adapt the service to their specific needs.

If, as a mobile operator, you simply repackage an existing consumer service for IoT, you end up in the bottom-left corner.

Most operators then add SIM management and offer private connections on top of this. The key word here is *most.* The problem is that this approach delivers a commodity with very little added value. You will only compete on price, and the lowest bidder will replace you. You are in what we call the red "churn zone" in the matrix. This is not a secure place to be.

The farther you move toward the upper-right corner with value-added services, the stickier your connectivity service offering will be for your customers. Additional revenues and higher margins come with value-added services such as analytics, managed security, global connectivity and granular policies. You should also add a web interface for customer self-management, as it enables greater operational efficiency. Customers will also be less cost sensitive, as the service feels like their own when integrated with their business.

So, the green zone, or the high-profit zone, is where you want to be as a mobile operator. The question is: will a dedicated mobile core for IoT take you there? Before we try to answer this question, let's first examine some of the use cases the mobile core and OSS/BSS need to support.

IoT complexity

In the utilities market, a customer may need to connect hundreds of thousands—perhaps even millions—of "dumb" IoT devices such as electrical meters. They are dumb in the sense that they are simple and cheap, so they often lack security features such as VPN connectivity. These devices have a vulnerable position in people's homes. Thus, they need to be protected by firewalls and you may need to detect anomalies in the traffic patterns.

Let's now move to a more complex use case: the connected vehicle. A modern car is a hub of multiple IoT devices. These devices include suspension systems, batteries, brakes, security systems, entertainment systems and more. They all need private connectivity for firmware upgrades and predictive maintenance. So, the mobile core needs to deliver multiple VPN connections from a single physical connection. The car manufacturer needs to be in control of the policies for this. In addition, the Internet connection for the entertainment system may also need complex routing rules. For instance, some traffic needs to go to the home country so that the passengers can watch their local streaming content while abroad.

The small and medium enterprises (SME) market is the direct opposite of the automotive industry in that companies have very limited IT resources. For most small companies, setting up a VPN tunnel is an impossible task. Many of them also have legacy systems with limited security features. In order to address this mass market, mobile operators must offer managed security. To scale with profit, operators likely also need to develop an easy-to-use app for self-management of the service.

Global challenges

For customers with things crossing national borders, operators cannot rely on roaming alone. Regulators in many countries—including Australia, Brazil, China, India and Turkey—prohibit the use of IoT devices managed by foreign operators via roaming agreements. There are also cases in the United States and Canada in which the operators themselves, for commercial reasons, prevent permanent roaming. As a result, compliance with roaming partner and regulator rules has become critical for global connectivity.

The answer is of course to use eSIM (eUICC) and localize the device to the right country by changing the SIM profile over-the-air (OTA). This is important also for stationary things. The analyst firm Transforma Insights estimates that at least 70 percent of cellular connections remain active in just one country for the lifetime of the device.

To see how this plays out, let's look at an example of a manufacturer of coffee machines rented out to coffee shops all over the world. Just imagine the benefits in simplicity and freer capital of

producing a single version of the machine instead of individual versions for each country. Imagine how the risk is lower of being blocked for violating local regulations and rules for permanent roaming. This approach is much simpler than finding a local IoT connectivity provider in each territory and making integrations with each one of them.

But localization introduces new challenges. In order to have full control and also apply managed security and other value-added services, the home operator would have to arrange with each local operator partner to have the traffic home-routed.

In addition, some customers require a unified IoT service in which the device, for instance, keeps its IP address no matter what network it connects to. This is a challenge both in the roaming and localization case, as normally the visited operator assigns the IP addresses.

It is also costly to provide customers with their own private APN and VPNs across territories to create seamless and unified connectivity across partner operators. What if customers want some traffic routed back home through VPNs and the rest routed to the Internet?

The shortcomes of the existing mobile core

It's clear that applying this complexity on an existing mobile core will not cut it.

The focus in our industry is always on whether the equipment has the features to perform a certain task and scale with millions of subscribers. But is this the right discussion to have when it comes to complex IoT services?

Maybe the better question to ask as a mobile operator is: "Will my organization be able to deliver on the agility, speed and cost-efficiency needed in the IoT era?"

We must all respect that the mobile core and OSS/BSS teams prioritize stability before being fast on their feet, implementing every change requested by demanding customers. Wouldn't it be great if mobile operators could have their cake and eat it, too? We think they can!

What we suggest is that mobile operators leave their core networks untouched and then use hyperscalers such as Amazon Web Services (AWS). Here they can add a programmable and flexible layer of IoT security and policy control on top of their mobile infrastructure. There are already vendors that offer this type of value-added functionality as an OPEX-based IoT connectivity control service (IoT CCS).

It is also possible to combine such service with other value-adding functions such as SIM-management systems and services that provide a network of international mobile operators for global connectivity.

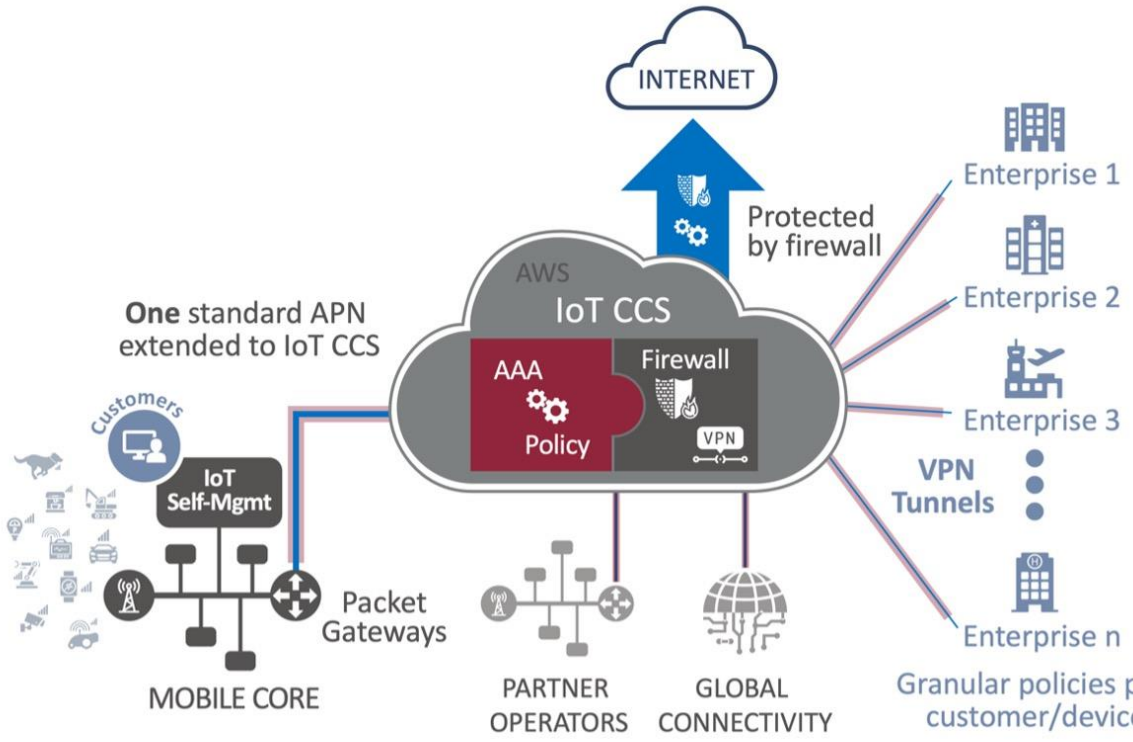

Figure 2: IoT connectivity control service
click to enlarge

With such an IoT CCS service adjunct to the existing mobile core, operators can add other functions to create a smooth, innovative and profitable IoT connectivity service. They can, for instance, add customer self-management portals. This allows customers to control authentication, security, policies, and global connectivity from a single user interface.

Operators can also create automatic provisioning of secure private connections (APN + VPN). When handled manually, this can take days and even weeks to set up. They can also offer managed security at scale by adding firewall functionality included in the IoT CCS service.

To provide global connectivity with local subscriptions, mobile operators can add international MNO partners to the IoT CCS service. They can do so either directly or through the mentioned global connectivity services. By using policy-based IP assignment and central security and policy control, operators can deliver a unified IoT service across all these cellular networks.

We have only seen the beginning of hyperscale solutions for IoT. The concept of network slicing in 5G is very well suited for this approach. Operators will be able to scale their innovations like never before.