www.pipelinepub.com
Volume 18, Issue 3

Foolproof IoT Networking

By: Tomer Lavie

What will cellular look like five or 10 years from now? Which of today's network technologies will be riding off into the sunset? Which emerging ones will be as mainstream as 4G is today? And how might operator business models change?

These are the kinds of questions that can mean sleepless nights for CIOs, line-of-business heads, business development VPs and anyone else responsible for their organization's IoT strategy. One scenario is a mobile operator suddenly phasing out a technology much sooner than the marketplace expected — a nightmare that sometimes comes true. For example, T-Mobile plans to sunset Sprint's LTE network by June 30, 2022, while NTT DoCoMo shut down its LTE-based narrowband (NB-IoT) network after barely a year of operation.

Utilities, first-responder agencies, fleet owners and other IoT users often are caught off guard by these kinds of changes. According to a 2020 James Brehm & Associates survey, 47 percent of organizations said their operators never told them that the network they use would be shut down.

"The impending networks sunset is presenting major decisions for these companies," the firm says. "Potential data loss, network service disruption, and damage to business processes and continuity are all compelling risks motivating them to begin planning for migration to 4G LTE, and eventually 5G, solutions."

Evolve along with 4G

Despite the occasional exception, LTE remains a solid foundation for IoT applications, especially ones whose devices need to remain untouched in the field through the end of this decade, such

as smart utility meters. It's worth remembering that LTE stands for Long Term Evolution, meaning its technological framework continues to evolve to meet the changing needs of both operators and their customers. In fact, even as they deploy 5G, many operators will continue to invest heavily in upgrading their 4G networks: roughly $275 billion through 2025, according to GSMA Intelligence.

Some of these upgrades will give IoT providers and end users new options. A prime example is low-power wide-area (LPWA) networks and modules that use LTE-M and NB-IoT. These technologies were designed from the ground up to support low-bandwidth applications, maximize battery life and maintain a stable connection even when signals are weak. LTE-M and NB-IoT are ideal for applications such as smart utility meters and agriculture sensors, where IoT devices are deployed in remote or even underground locations, with batteries that need to last at least a decade.

At the same time, IoT providers and users should be aware that an operator's 5G rollout can affect the performance of its LTE network. For instance, unless they have service-assurance tools that can support multi-generation, multi-vendor networks, operators won't know whether their new 5G standalone (SA) core network is undermining 4G performance until customers start complaining. Another example is spectrum. As they refarm 3G spectrum for 4G use, or 4G spectrum for 5G use, IoT devices using legacy networks could see changes in coverage and signal strength.

By the end of 2021, the number of commercial 5G networks worldwide will hit 220, and 323 by the end of 2023, TeleGeography predicts. This means 5G is steadily emerging as a viable option for IoT applications that would benefit from its advanced capabilities and for organizations concerned about 4G sunsets. The 3GPP 5G standards include three sets of features and capabilities designed to meet many of IoT's unique requirements:

- **Enhanced Mobile Broadband (eMBB)** is designed for bandwidth-intensive applications such as 4K video for surveillance cameras and telehealth.

- **Massive Machine-Type Communications (mMTC)** enables 5G networks to support up to one million devices per square kilometer, such as air quality, traffic and other sensors around a smart city.

- **Ultra-Reliable Low-Latency Communications (URLLC)** provides latencies as low as one millisecond, which is ideal for delay-sensitive, mission-critical applications such as factory automation.

One future-proofing strategy is to choose IoT cards and modules that support both 4G and 5G. This enables organizations to launch their IoT service virtually everywhere today on 4G while providing the flexibility to move to 5G when it makes business and technological sense. Then when 5G coverage reaches a certain point, it could upgrade to 5G.

To understand the business benefits of this strategy, consider how multinational companies such as Alphabet, Deloitte and PwC have decided to allow their employees to keep working from home some or all the time once the pandemic is finally over. A video collaboration provider could offer

those types of companies a bundle of hardware, software and cellular connectivity. This way, remote workers wouldn't have to rely on their home network and ISP, both of which might not be fast enough tosupport work applications alongside multiplayer games, streaming video, and other household applications. The dedicated connection also would eliminate security and privacy risks that come with using a home Wi-Fi network.

By using modules that support both 4G and 5G, the video collaboration provider can target companies that have some employees who live in places where only LTE is available. When 5G becomes widely available, the provider than can leverage URLLC to add enterprise-grade SLAs as a powerful new market differentiator.

Roaming is becoming a moving target

IoT is a major and continually growing source of revenue for mobile operators. But some IoT customers also increase an operator's overhead costs. A prime example is when those devices are roaming on the operator's network for an extended period — or even permanently. As a result, mobile operators are increasingly restricting their roaming agreements, increasing their roaming tariffs, or both.

IoT device vendors, IoT service providers and end users should keep this trend in mind when developing a future-proof strategy. It's easy to assume that these changes will affect only mobile IoT applications, such as fleet telematics. But fixed IoT applications also can incur higher operating costs. For example, IoT solution providers often use a single SIM for devices sold into multiple countries. If roaming partners start increasing tariffs, it can quickly erode the profitability of customers in those markets. It also can undermine that solution's competitiveness with products that aren't roamers.

The regulatory environment is another factor to consider. Some countries, such as Brazil, don't allow permanent roaming, so operators there must cut off service to those devices after a period of time.

IoT gets a new identity

SIMs are another key consideration when developing a future-proofing strategy. The main drawback of the traditional SIM card is that it's tied to a specific operator. Switching an IoT device to another operator means trekking out to each device to pull the original SIM and insert a new one. This swap takes a lot of time — and money — when it's a large-scale deployment, such as a thousand trucks or 100,000 utility meters.

The traditional SIM card also is vulnerable to fraud. The organization paying for IoT service must be able to track each SIM card to ensure that it wasn't removed for use in another, unauthorized device. In both cases, these overhead costs eat into the savings and revenue that IoT enables.

A software-centric alternative is the eSIM, which uses the Universal Integrated Circuit Card (eUICC) standard so multiple operator profiles can be loaded onto a single physical card. eUICC

also enables operators to upload their SIM profiles to eSIM devices in the field. This design means IoT devices can be quickly and inexpensively switched to the network offering the best performance, tariffs and more — all without a truck roll or end-user intervention.

eSIM also significantly reduces the cost and effort of expanding an IoT solution to additional markets, such as from a country to a region or to the world. For example, an IoT solution provider could use eSIM to develop a single-SKU product that can be provisioned to a specific operator in each market.

The next evolutionary step is the iSIM, which integrates the SIM functionality with the IoT module hardware. This design eliminates the physical card and its associated hardware, such as the SIM tray. This makes iSIM ideal for applications that require a low bill-of-materials (BOM) cost or an ultra-compact form factor.

eSIM and iSIM architectures provide flexibility and future-proofing that traditional SIM technology can't match. By leveraging them and understanding how network technologies and operator business models are evolving, every member of the IoT ecosystem — from device vendors to service providers to end users — can avoid sleepless nights. Future-proofing also enables them to take advantage of changes, such as switching to an operator with better service or better tariffs, or to a new network technology that offers longer battery life, lower latency or higher speeds.

What's next for IoT?

We have explored the uncertainties that come with new network technologies, changes in mobile operator business practices and more. There are several major options for future-proofing IoT devices and services so they can accommodate these kinds of changes. IoT service providers should consider partnering with an MVNE that has access to hundreds of 2G, 3G, 4G and 4G LPWA networks around the world, enabling fast rollout of IoT services in a country, region or worldwide. This service provides another key set of capabilities for future-proofing while enabling innovative new business models, revenue opportunities and savings.