The Importance of IoT Device Management

The sheer scale in the number of sensors and other devices in an IoT network will transform the face of device management. So how will enterprises keep IoT devices running reliably with the same levels of uptime they expect from the rest of their network?

Device management is essential for an enterprise in order to securely manage company applications and information on mobile devices and has become routine for their IT folks. But the responsibility of device management, encompassing device provisioning, software and firmware updates, and device monitoring is a whole different ballgame when you're looking at masses of IoT devices without a user interface.

For all but a few enterprises, that will mean involving a third party-provided device management service.

According to ABI Research, enterprise use of IoT device management services will drive a more than $20 billion market within the next five years, with the bulk of that spending done by companies in industrial, automotive, and telematics.

Ryan Harbison, a research analyst at ABI Research, sees it like this: "As IoT solutions continue to shift toward performing more processing and computing at the edge, devices need to constantly be updated to maintain solution security and improve overall analytics solution value.

"If a device is not able to be updated, its long-term value ceases. As a result, operations teams need central tools such as device management solutions to enable efficient remote maintenance. With potentially hundreds of thousands of devices in a solution, it is simply not feasible to fix and update devices after they are deployed."

Reaching Critical Mass

Sprint partner, Nishi Kant, agrees that IoT device management services are going to be crucial once the number of devices reaches a critical mass.

"First of all, when you are dealing with such a scale, it is not possible to do anything manually," Kant says. "At the scale of hundreds, you could still do things by hand even though it would be tedious. But when operating at a scale of several thousand or a million, you simply don't have that option."

He also points to the different impact when it comes to managing mobile devices (handsets and tablets) compared with IoT devices.

"Let's say that your system managing BYOD handsets crashed. Nothing drastic would happen to the devices," Kant contends. "They would still have their functionality.

Enterprise applications would continue to work and users could make phone calls. When the system came back up you could resume management, such as pushing enterprise certificates for Wi-Fi access for a new employee. That is why mobile device systems don't need to have 24 by 7 availability."

But, Kant says, "With IoT, the device and data management could be part of mission-critical processes, such as factory output, or mining operations, or pipeline safety. If that device stops providing you the information, it is serving no purpose. Its value goes from 100 to zero immediately."

Consider, for example, the monitoring system for a delivery truck full of temperature-sensitive dairy goods on a hot August day. If a system glitch – conceivably a software version mismatch – prevents the dairy company from proving via cargo data that the right temperatures were maintained to avoid spoilage, the store could refuse the delivery. That would translate into a loss of revenue and wasted product for the dairy company.

The Key Elements

Clearly, what an enterprise will need is the ability to manage its IoT devices with the levels of reliability and uptime that have been a characteristic of carrier services for years. And except for a select few enterprises that might be able to do this on their own, the rest will be looking to reliable service providers to keep everything going.

The ability to scale to vast numbers of devices and to ensure a global view are the essential elements to an IoT device management solution.

"When IoT is mission critical, it's not just device management you are interested in at that level, but it is about how your whole business is making use of IoT, and how your operations have been instrumented with it," Kant says. "Even if your device management is from a third party, you will need close cooperation with that provider so that your operation can run with confidence."

With IoT instrumented operations, Kant sees device management becoming an underpinning of the "enterprise services bus architecture," with all the workflows and processes riding on top.

That kind of integration, Kant adds, requires a network that can accommodate it with unparalleled reliability and security. He advises that enterprises make sure their provider's network is equal to the task and says that one thing to look for is that the network is dedicated to IoT.

"Instead of trying to stretch the mobile broadband consumer network to serve IoT, what is best is an IoT-centric dedicated network with frictionless provisioning and operation," he explains. "With that kind of separation, you can be sure that you eliminate the chance that error propagation from a consumer network will bring IoT down."

As he notes, the value in IoT isn't in the connectivity, since that is just the means of moving the data. Instead, "The value is removing the friction, so that the data flows seamlessly to the analytics engine."