www.pipelinepub.com
Volume 20, Issue 9

Network Visibility Requirements for IoT - and the Questions CSPs Need to Ask

By: Miguel Carames

As the IoT population looks to surpass the number of non-IoT devices by the end of the decade, it's time for CSPs to change the way they think about their business and their network. IoT calls for greater precision and network intelligence that acknowledges that IoT will create a hyper-segmented ecosystem. To fully monetize the opportunity behind connected things requires all aspects of the technology stack to come together in synergy, and to do this requires acute network visibility that enables CSPs to address the hard problems. Questions such as: Do you have the network intelligence to detect low-powered IoT, how do you identify mission-critical IoT vs. consumer, or what's your level of confidence that roaming IoT is performing as required? The IoT era is here: Do you have the network visibility necessary?

We are about to witness massive IoT growth. The numbers tell the story:

- 5.8 billion: the number of licensed-cellular IoT devices by 2030, up from 3.5 billion in 2023 (GSMA).
- 46PB (petabytes): global cellular IoT data generated in 2028, up from 21PB in 2024 (Juniper Research).
- Wholesale IoT roaming will reach $8 billion by 2028, a 16 percent average annual growth between 2023 and 2028 (Kaleido Intelligence).

In this context, it's important that CSPs ensure that all corners of their networks are equipped to not only meet the demands of IoT but also help identify opportunities to maximize revenues. Here are the top questions CSPs need to ask.

Do I Have the Network Visibility Required to Maximize IoT Roaming Revenues?

Kaleido Intelligence projects that wholesale IoT roaming will reach $8 billion by 2028. However, the diversity of devices and use cases is making it difficult for CSPs to fully monetize this opportunity. For example, low-power IoT devices and sensors, commonly used to remotely monitor environments such as smart cities, agriculture, and manufacturing, are increasingly joining the IoT roaming category. Juniper Research projects that there will be more than 490 million low-power IoT roaming connections by 2028, a growth rate of 560 percent from 2023. However, because these devices consume less data and have intermittent connectivity, it can be difficult to identify them, which is especially true for devices inbound roaming onto a visited network. This creates a huge potential loss in revenue for CSPs, particularly when Kaleido forecasts that IoT roaming connections that consume less than 10MB per month will represent 59 percent of the total IoT roaming connection base by 2028.

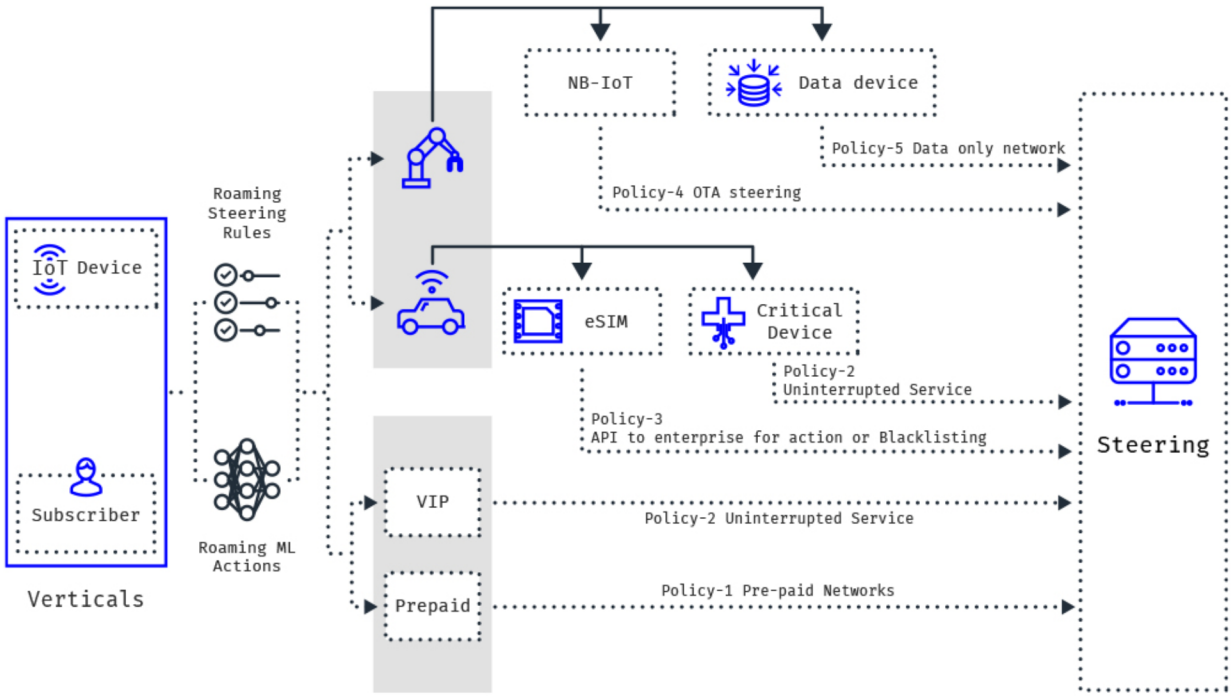

Figure 1. Roaming Steering

A few years ago, GSMA defined the machine-to-machine (M2M) roaming transparency initiative. However, practical experience proves that detecting low-power devices is only possible with AI-based deep analytics. AI-based analytics is required to detect, monitor, and analyze the billions of IoT devices connected to the network in order to form a 360-degree view of the IoT ecosystem. This, in turn, gives the CSP visibility to monitor the network and service performance delivered to IoT devices so that they can provide superior connectivity and experience on every IoT device.

But it's not just detecting the devices that's important. CSPs must also understand the different device categories to ensure the right traffic and pricing policies are consistently applied. This is where IoT Packet Printing plays a critical role. It combines carrier-class security, behavior analysis, and traffic analysis to automatically identify the device category, and it can detect misuse and prevent fraud or abuse in the event of compromised or malfunctioning IoT devices. Traffic and pricing policies for IoT are often more complex than those for retail.

Therefore, CSPs need to ask: Does our policy engine have the AI and automation capabilities to manage the complexity and scale of IoT?

Steering of roaming is another area where IoT brings greater complexity than traditional telco services. (See Figure 1 above.)

Not only do IoT steering policies need to be applied based on criteria such as wholesale targets, quality of service, usage, deal conditions, and regulatory circumstances, but they also need to manage the demands of bootstrap IMSIs or SIM profiles, eSIM capable devices, and different steering policies for mobile, nomadic, and static devices. What's more, CSPs need to have sophisticated steering solutions that enable guaranteed service accessibility for critical IoT segments that can match the device and visited network capabilities, that can move IoT devices to low-cost networks when available, and that will prioritize mission critical IoT devices over consumer devices in times of emergency.

CSPs need to ask: Can our steering of roaming solution enable us to steer traffic based on network, experience, segment, service awareness, and business model? Does it have the intelligence to apply specific business restrictions, such as limiting the number of countries where one operator can offer IoT Narrowband services?

Do I have the Network Visibility to Know if the IoT Value Chain is Working Appropriately?

As enterprises and critical services increasingly adopt IoT-based solutions, granular KPIs will need to be collected and strict SLAs will need to be enforced. Assurance for IoT requires continuous monitoring of devices, connectivity, and platforms to enable CSPs to identify service performance issues and take proactive measures before services are impacted. Automation, AI, and ML are critical to collecting and processing large data sets in real-time to detect and monitor performance, identify anomalies, as well as detect fraudulent patterns for further investigation, validation, and remediation.

To assure the full IoT value chain, CSPs need real-time visibility into KPIs, such as connectivity reliability and performance, power-saving features, and platform connectivity. This requires IoT testing that ensures the necessary conditions to launch IoT applications are met. The testing solution must also enable the CSP to easily perform automated regression testing to ensure the IoT solutions are operating at the required quality and performance. Some of the questions that CSPs should be able to answer when testing their IoT network include:

What is my IoT network availability?
What is the APN connectivity and data session establishment latency?
Is the application service accessibility and round-trip time within specification?
What is the data transfer throughput?
Are VoLTE and SMS services working as required for IoT applications that require them?
The low power consumption of IoT devices is a critical feature for the successful implementation of smart sensors. LPWAN technologies, such as NB-IoT, LTE-M, and 5G RedCap, have two essential power-saving features, Power Saving Mode (PSM) and Extended Discontinuous Reception (eDRX), that need to be optimized. To do so, CSPs need to perform testing that ensures that networks support and can negotiate the PSM and/or eDRX timers according to the different IoT application requirements and device capabilities. In addition, CSPs need to be able to verify the performance of data and SMS delivery during and after the devices have left power-saving mode. Test automation combined with real-time analytics is critical to managing the power-saving features of IoT and avoiding any cost overruns if device anomalies are not detected in real-time.

To ensure the success of an IoT service, application developers need to be able to test and monitor the performance of their IoT platform end-to-end. In addition to automating how their applications are monitored, developers should also have the capabilities to test the IoT platform's availability and authentication and ensure data integrity transfers under different payloads.

Network visibility is critical to assuring the end-to-end IoT value chain. CSPs need to ask: "Do we have the automation and AI capabilities to expertly monitor KPIs, such as connectivity, power-saving features, and platform connectivity, and assure that our IoT services are meeting their performance requirements?

In the IoT era, gaps in network visibility can create huge headaches for CSPs. From the ability to monitor KPIs, meet SLAs, track performance issues, and take the proactive measures needed before services are impacted, CSPs need to make the investments required today to ensure they capture the full potential of IoT now and into the future. Purpose-built IoT enablement and assurance solutions that have a foundation of automation and AI/ML are needed to extract the deep network insights CSPs need to monetize IoT. Now is the time for CSPs to invest in these capabilities to ensure they capture the full opportunity.