THOUGHT LEADERSHIP

Proof of Concept vs. Production Deployments - The Case for an Enterprise IoT Model

As the IoT market steadily matures from the early adopter proof of concept to full-scale rollouts, increasing numbers of connected devices are coming online around the world – IDC forecasts that there will be 41.6 billion connected devices by 2025. However, it has become apparent that companies looking to deploy production networks at scale will face challenges that may compromise overall benefits if not addressed. Particularly, for those organisations that are considering trialling their IoT use cases first on public 'innovation' networks (due to the ultra low cost), there are a number of vital elements missing in such services, which are standard practice in an enterprise-grade production network design. These elements are fundamental to a futureproof, secure and reliable IoT deployment that can stand up to technical and commercial scrutiny.

Nick Sacke, Head of IoT and Products at Comms365, explores these elements and explains how companies can overcome challenges by moving away from, or stop using public networks in the first place. Rather, start the IoT project in a private, enterprise-grade network design, where there is already an advanced set of software features, techniques and seasoned providers ready to deliver a successful IoT phase 1 trial and production rollout.

SLA-Driven Networks - Access No Less!

The backbone of an Enterprise IoT solution is connectivity from device to application. Controlling radio mechanisms, authenticity and authentication is a critical requirement of an Enterprise Network Server. Providing a clear network overview, comprehensive meta-data, gateway insights and management alerting for problems ensures a network design that can be operated and managed at scale.

By contrast, Public, 'open' IoT networks have been designed to encourage innovation for the individual user - and have been very successful in sparking a training ground community of hobbyists, academics and interested parties that can connect and test their IoT devices and use cases. But whilst you can connect an IoT device and pass data, there are limits on further functionality – there is no decoding of data, no management of the gateway, no quality of service on message delivery, or SLAs.

Confidence in Guaranteed Delivery of Information

In a LoRaWAN network, the protocol used between gateway and server is User Datagram Protocol (UDP). Known as a packet forwarder, it simply takes a message and passes it on. But UDP, which is still common in many IoT gateways today, has diffi culties with authentication and the ability to recover from losses on the network. There is a prolific use of these legacy protocols and techniques on public networks which provide no method to guarantee delivery of information.

A successful IoT implementation relies on guaranteed delivery of information from the gateways to the network server. But with legacy protocols used on public networks often being a cause of missing data points, this is a frequent cause of failed Proof of Concepts (PoC), casting a shadow of doubt over the reliability of the end to end solution.

In an IoT model fit for the enterprise, it's imperative to use software on the gateway which guarantees the reliable transfer of the data, and confirms it. A private network design, combined with software that confirms data delivery to the application layer – and can handle retransmission of the data if required – means that the Quality of Service (QoS) can be significantly improved.

If, under all conditions, there is high availability as well as guaranteed secure and reliable data delivery, a PoC will be much safer and more secure. Even in PoC stage, you still need to be able to demonstrate reliability, constant connection, failover and backup of connection, and with an enterprise model built on a single cloud private infrastructure, that can easily be achieved.

Security Measures and Standards in Enterprise IoT

With an enterprise IoT model, there is a set of security techniques and standards that simplifies compliance audits and also requires little or no effort in terms of changing corporate firewalls and proxies – it has all the necessary security elements baked in from the start.

The first consideration for any deployment from the moment the first sensor and gateway are connected should be security. However, in practice it is often only taken into consideration when deployments start to scale or move into production. Building on an insecure platform might not be an immediate concern, but it typically ends with unforeseen problems when a solution is ready to scale.

The Enterprise IoT Network Server components are built with implemented security features at every layer and encourage the use of secure software and integrations. This means it does not compromise on security by using basic insecure software, which is a common scenario with Public Innovation Network.

Automatic Version Updates

Building an IoT network at scale requires powerful operational and management tools, and complete overview of the network, users and resources, ensuring you maintain full control. As a deployment scales, debugging, user management and valuable administrative tools are essential. For example, in an IoT production deployment, there could be hundreds of gateways deployed. So how do you ensure the gateways have the latest security patches and software updates? In an enterprise IoT model, lifecycle management is highly automated. Along with the security and authentication, updates can be securely retrieved, self-updating, and due to this, the new version of software can be remotely installed/ run without any human intervention.

The same cannot be said for a public network – any updates or security patches would have to be retrieved and installed manually. Which, for a large scale IoT rollout would be a significant challenge, potentially leaving the entire deployment vulnerable to attack and incur lengthy downtime.

Conclusion

While public IoT networks have proven successful in encouraging innovation in IoT, when it comes to rolling out an enterprise-grade production network, an ultra-secure model is required that also has essential elements that can demonstrate reliability, security and scalability. It's not enough just to connect to a public network and show data flowing, businesses must pay close attention to these crucial elements, or else the deployment may never move out of PoC, potentially putting business revenues and ROI at stake if the network is being relied upon to deliver key operational data and insights for action.

With an enterprise model that has security and reliability baked in from the start, organisations can be assured that their private network is secure, reliable and can stand up to scrutiny, even in an era of increased regulatory requirements.

www.comms365.com
sales@comms365.com
01234 865880