Connecting the Internet of Things

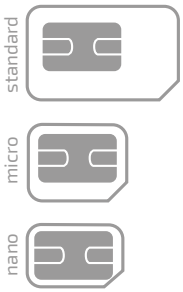
A Guide to SIM Selection

Wireless Logic Group | September 2018

wireless logic

Sitting at the heart of a world of devices - as they become a universe of connected, intelligent machine-based networks– - is the humble SIM.

And while it might be easy to equate IoT SIMs to the traditional mobile or mobile broadband versions we walk around with in our pockets, that's where the analogy ends. An IoT SIM, while it might look the same, is designed, built and supported specifically for purpose. In this White Paper we examine the factors unique to IoT SIMs, which a business needs to have top of mind when building the most efficient network of things.



We will consider the background to selecting IoT SIMs from every angle. Firstly, the content they will carry and the devices they will connect. We then look at the quality of service and the support they require. The White Paper then moves deeper into addressing and connectivity requirements before an addendum which explains why mobile broadband is an inappropriate choice for IoT connectivity, from four perspectives: contractual, development, management and utilisation.

Content

Choosing an IoT SIM requires a discussion as to exactly what content will need to be transmitted and how. And this discussion needs to take place with the knowledge that consumer APNs - or, to be more specific, SIMs marketed as 'mobile broadband' - often do not provide pure internet access. Instead they provide what might be described as a 'walled garden' set of specific internet services, such as web browsing and mobile email. IoT requires much more than this: a wider range of application protocols and use cases, such as FTP and VPN. Additionally, when using a consumer APN, ports can be locked down which requires more flexibility in M2M and IoT when routing the data. A secure private network gives control of policy changes and what ports are closed and open.

As the market evolves, we are seeing many different form factors of SIM - plastic, EUICC and e-SIM (more commonly referred to as soft-SIM). Many businesses are also beginning to use embedded SIM cards mounted onto PCB boards. But in many cases, what needs to be considered are the logistics and provisioning process for each application.

Devices

One relatively straightforward consideration on SIM selection is to ask the question "into what kind of device will it be placed?" Note that mobile broadband terms and conditions state very specifically where such devices can be used. In short: phones, laptops, tablets and dongles. Not only are they not sold to be connected into routers or any IoT related 'things', a MNO can restrict services and connectivity should SIMs be found to be in use within unauthorised hardware. (The same common mistake is also made by using voice SIM cards for data.)

Quality of Service (QoS)

Following on from the above, it should be noted that mobile broadband and consumer APNs may bring with them usage caps and/or throttling of throughput, the polices of which are not always made clear by a MNO. Throttling polices can also be highly complex, so it is not out of the ordinary for unrestricted throughput to be permitted up to a certain quantity of data per month, only for it then to be throttled to a very low rate as soon as that contractual cap is exceeded.

A practical example: If a business was running a remote deployment of CCTV cameras, it would be disastrous if, mid-month, all connections (i.e. all cameras) were throttled. This would result in a complete loss of service.

Additional, policy-based rules are in place as part of MNO edge infrastructure which are distinct from traditional, 'end-to-end' internet design principles. These might include performance-enhancing proxies, network caching, firewalls (which may or may not adhere to protocol designs embodied in IETF RFCs) and policy-based selection of DNS. IoT SIMs and connectivity need to be able to deal with all of these as and when they arise.

A further feature of IoT SIM cards is that, if they have a static IP address, then there is a VPN in the cloud that is always on (one reboot per night). In contrast, a normal SIM card will try and kick itself off the network as often as every five minutes.

Lastly, a private static IP address is off the public internet - unless it is required to be on. This effectively means a deployed base becomes an extension of the user's wide area network (WAN). Compromises to the public internet are common; when you pay for download and upload this can also increase your airtime costs should a compromise occur.

A final, simple point on QoS of IoT SIM versus mobile broadband or consumer SIMs: mobile broadband contracts typically provide uptime of 85%, whereas IoT demands an always-on approach: 99.9% or higher. This is achieved by interconnects that are designed specifically for 2G/3G and 4G, provided by a contention ratio that is far superior to normal SIM cards. Consequently with the correct SIM, M2M/IoT applications just simply work.

Support

By their very nature, IoT SIMs need constant monitoring, 24/7. Thus, as a fleet of SIMs is rolled out, the business has to be confident that there are skilled, IoT-trained support agents on hand at that moment and for the life of the project. Support is equally important during uptime, as connectivity has to be monitored and measured at both the level required by a business and within the context and parameters of IoT.

Consider also the communications between business, MNO and customer. A business running IoT needs to be confident that the support provision at its MNO includes sophisticated, specific incident notification to handle occasions of service degradation and outage. And, as an aside, it is only an IoT-focused MNO and fleet of IoT-specific SIMs that will engender a dialogue between business and customer - for example, about change and problem management. An IoT SIM roll-out should be a collaborative, dialogue-based process, as opposed to 'plug, play and forget'.

By deploying the right SIM on the right private network - and with a static IP address that will always be there for the life of the SIM - you can greatly reduce the need to ever have to visit a device. Especially as, when a SIM is based in the 'middle of nowhere', engineer call out costs can range from £100-£400 depending on location.

Addressing

A network of things will most usually need to be kept agnostic of both MNO and APN. And, at SIM level, a business needs to be sure that the approach to addressing is consistent across every MNO, APN and geographical territory.

It is worth noting that, in the consumer marketplace, APNs often adhere to complex address schemes (built around RFC1918 private addressing and Network Address Translation (NAT), or port-NAT to a range of public internet addresses). Most importantly, the implementation of such a complex architectural approach will vary from MNO to MNO. As a result, addressing could easily be problematic if using a consumer or Mobile Broadband SIM in a network of things.

There are also security aspects to the addressing associated with consumer or mobile broadband SIMs too, if they are placed into the IoT arena. This is because MNOs will often - and without prior notice - change both the internal and CG-NAT addressing of consumer-type APNs. A standard operational security practice, it demands that a client maintains (and instantly adapts to) an extensive knowledge of public address blocks. Failure to open firewalls to newly assigned address blocks results in service disruption. Also, failure to close firewalls to address blocks as soon as they are retired opens significant holes in security.

Connectivity

How is your data treated, the moment it goes from SIM to MNO? It's a question that has to be asked because, at that precise moment, it becomes subject to an MNO's own distinct working practices, all of which are rigid, controlled and non-negotiable.

Let's take three examples: traffic path, session teardown and split tunnelling.

- In terms of traffic path, with IoT SIMs it's simple: for fault resolution, all traffic needs to be kept inside the MNO and/or the customer's network. IoT SIMs and a dedicated APN are required, along with contracted backhaul services, given that other SIMs and consumer APNs will often pass traffic across the open - and, indeed, uncontrolled - internet.
- Session teardown is an MNO's practice of placing timers on mobile devices, and curtailing the duration of time they may remain connected. It varies across MNOs, who may also change their teardown limits on an ad hoc basis, with no advance warning. So this is another aspect that needs to be considered, controlled and, within application-ware, constantly managed.
- The process of splitting data at the MNO edge into two flows - for example, through a VPN tunnel and across the Internet - is often required. Like other connectivity considerations, the amount and frequency of such split tunnelling is dictated by the MNO. Its management is down to the customer, which needs to have business-ready, IoT-specific SIMs in place to handle it. Consumer-type APNs are unlikely to be able to support split tunnelling.

Addendum: discounting mobile broadband

Despite the many and varied technicalities associated with selecting and implementing IoT SIMs, there have in the past been situations - not least in the early days of the industry - where resellers and systems integrators would opt to simply roll out consumer/mobile broadband SIMs to connect devices and things. Although this practice has since diminished, it does still take place and, rather than being cost-saving, can actually jeopardise an IoT project in four key ways, which we examine here:

1. **Contractual:**
   A follow-on from the commentary under Content and Devices above, it is a standard part of the terms and conditions of consumer APNs and mobile broadband SIMs that they should simply not be used for commercial purposes, IoT or otherwise. If this is found be the case then disconnection is a likely outcome.

2. **Development:**
   When mobile broadband SIMs have formed part of IoT projects, it has generally been because connectivity has come as an afterthought. But connectivity - and the enhanced functionality that IoT-specific SIMs can provide - should really be a fundamental pillar of development from the start.

3. **Management:**
   Management platforms - which cover everything from the monitoring of IoT devices to more complex functions such as restricting and redirecting data - are simply not available with mobile broadband SIMs.

4. **Utilisation:**
   An MNO's commercial sales team works to a lower assumed utilisation of mobile broadband SIMs. 70% on average, with more than half of all customers utilising less than 30% of the available data. IoT commercial teams, on the other hand, generally see such SIMs utilising 100% of available data for every user. As a result, mobile broadband prices are clearly unworkable in the IoT arena, in fact an MNO's sales team would never knowingly approve mobile broadband SIMs going into an IoT project as P&L would show a loss from day one.

For more information...
Call **+44 (0)330 056 3300** or email **hello@wirelesslogic.com**

The information and guidance within this paper have been developed by Wireless Logic in conjunction with our strategic MNO partners Vodafone and O2.