White Paper

Optimizing Cellular Networks for the Internet of Things

Test and Service Assurance Challenges for Delivering IoT Connectivity

New Devices Bring New Testing Considerations

Network operators and network equipment manufacturers employ rigorous test regimes and operational service assurance methods to ensure optimum network performance and quality of service. But current test methods and service assurance solutions are set to be challenged by the rapid advance of the Internet of Things, which is placing new and very different demands on the network.

This paper introduces the key test and assurance challenges created by the Internet of Things, analyzes the risks of not addressing them adequately, and presents some advice on how best to tackle them.

It's based on Spirent's many years of working with the world's largest telecoms operators, network equipment manufacturers and device manufacturers to address their testing needs.

The Test Challenges of IoT

IoT devices are coming in force, with analysts estimating that 27B connected things will be in use by 2025[1], and by 2018 they will be generating a combined 400ZB of data annually[2].

For many cellular network operators and equipment manufacturers, current approaches to testing and service assurance are geared towards consumer voice and internet services consumed through smartphones and tablets:

- Tests, infrastructure and service assurance solutions are set to handle well-understood smartphone traffic
- Cells have been distributed to cater to high-bandwidth mobile device use with high levels of user mobility
- Networks are optimized for maximum speed, sometimes at the expense of other qualities

But the Internet of Things introduces a completely different class of device, placing completely different demands on the networks they connect to. These new devices:

- Can send unpredictable, volumes of data and signalling through the network
- Can be required to function remotely, and further from cell towers
- Often need to reduce power consumption to extend life expectancy

And that's just the beginning. IoT devices can also demand different network service quality levels and service level agreements. For instance, critical applications like insurance telematics will need a continuous, reliable service compared to applications such as public waste bin volume monitoring, which may only need to connect occasionally. Many networks currently aren't equipped to correctly prioritize traffic to different classes of devices and services.

Similarly, different devices demand different levels of mobility and different tolerances for latency. Mobile vehicles, street light sensors and autonomous cars all have different movement and network speed demands, and will place different demands on the network accordingly. IoT devices can also be deployed in a more saturated manner than conventional mobile devices, creating the risk of network congestion.

Changing Network Landscapes

In addition, Network Service Providers face the challenges of supporting high-volume, low-cost IoT devices in parallel with mission-critical IoT devices and applications.

On average, smartphone subscriptions generate $50 average revenue per user (ARPU), while many IoT devices may only earn the network service provider $1-$2. The risk from low-cost, massive IoT must be offset by serving critical IoT applications that require high levels of service quality—but offer substantially higher ARPU.

These demands require operators to re-think the way networks and equipment are planned, designed, implemented and operated.

Some service providers have already begun to adapt their operations to accommodate IoT. Network Function Virtualization (NFV) deployments are being trialled with Virtualized Evolved Packet Cores that isolate new IoT traffic and services from traditional voice and data services. Other providers are evolving DevOps into the operational network to provide a continuous and automated approach to designing, testing, launching and operating IoT services.

Whatever approach is taken, changes require new testing and service assurance initiatives to ensure IoT devices are supported by the network without compromising existing services.

Old Challenges, New Tests

The Internet of Things doesn't just bring new design challenges. It is also forcing operators and manufacturers to rethink the way they approach existing challenges.

For instance, network security is given another layer of complexity by the breadth of new, potentially insecure devices connecting to the network.

The influx of internet-enabled devices also offers cybercriminals a huge new variety of hosts to co-opt into damaging Denial of Service attacks. Are you able to test your network to see how it stands up to this new era of attack?

The trend towards virtual networks is also complicated by the new spread of IoT traffic. Can you guarantee your virtual (and existing physical) gateways can handle new, growing and more complex traffic from IoT devices?

Similarly, current service assurance solutions and practices are designed around services used by humans, not by machine-to-machine communications. Operators will need to adapt existing service assurance processes to handle the challenges of supporting IoT.

1) Machina Research
2) Cisco

Current Network Test Assurance Methods aren't Fit for Purpose in the IoT Era

The proliferation of new IoT devices demands a new breed of testing. The scale and variety of devices means existing test solutions may no longer be enough to accurately replicate the scenarios your network and equipment will encounter.

The large variety of IoT devices, all with different Quality of Service (QoS) requirements, means many existing network testing solutions can't accurately emulate the varied traffic patterns and behavioral mixes coming to market. The sheer number of IoT devices estimated also means existing test solutions may not be able to realistically simulate the numbers of virtual devices needed to stress-test the network.

There is also no single IoT standard that network tests can standardize on. New cellular IoT standards such as NB-IoT and LTE CAT-M1 demand new, multifaceted testing to consider how a combination of device, traffic and IoT standards will affect the network.

IoT devices also pose a security risk to the network. With potentially less-secure devices joining the network, infrastructure, interfaces and services must be rigorously and continuously tested and validated against realistic traffic volumes, as well as both known and evolving security scenarios.

To support IoT, network operators are also investing in new technologies and practices such as NFV and evolving DevOps into the operational network to provide a continuous and automated approach to the entire IoT lifecycle. Network testing and service assurance must also be able to assess network readiness across this entire IoT lifecycle for this approach to be effective.

Finally, there's the consideration that IoT devices may wind up in locations unused by existing devices, such as soil trackers in agriculture or monitors in offshore oil rigs.

Testing devices in these remote and disparate locations can present a big challenge for network operators. On-site field testing can quickly become prohibitive for testing a full range of critical IoT use cases, for example.

The bottom line is that accurately testing the complex traffic patterns and locations of new connected devices requires a breadth and scale of testing that is often unachievable with existing hardware setups.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

How Spirent Can Help

Spirent offers expert testing that can help you ensure your network infrastructure, processes and equipment are fit for the age of IoT.

The Benefits of Testing with Spirent

Since engaging with Spirent, one service provider achieved a 6x improvement in test cycle times, saved 80% effort for lab sanity checks, and full ROI in just 3 months.

Spirent testing and assurance solutions are able to scale to millions of simulated devices and traffic types, offering you the most realistic testing conditions for your networks and equipment.

With this test data in hand, Spirent can help you turn it into powerful insights that can automatically shape how your virtualized networks respond to complex IoT traffic. By automatically shaping virtual network parameters based on test results, you can keep your network one step ahead of the game.

Offered as both hardware (physical), and software (virtual)—both as a product and as a service—Spirent solutions are flexible and can be matched to your specific IoT testing needs.

NB-IoT and CAT-M Testing with Spirent

The recently launched NarrowBand IoT (NB-IoT) and Cat-M technologies are putting additional strain on network operators and equipment manufacturers looking to embrace and rigorously test the latest IoT innovations.

Spirent is at the forefront of offering cellular testing solutions to validate the networks for these new protocols. With Spirent, you can ensure co-existence with traditional voice and data services, and accelerate your IoT launch with confidence.

Talk to us today about how we can help you ensure your network and infrastructure is ready for the Internet of Things.

spirent™
Promise. Assured.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com