Internet of Things – when problems can be hidden in a billion places

By Brent Lees

The promise of the Internet of Things era is that all things can be connected and so all things can be efficiently tracked and controlled. But when billions of things are connected, there are also billions of points of contact to sift through to identify faults, says Brent Lees, Senior Product Marketing Manager at Riverbed Technology.

On the face of it, the Internet of Things (IoT) promises a world of unparalleled convenience for ordinary people. Soon, you will control your devices and appliances remotely, your fridge will automatically reorder goods that are running low and your car will proactively book its next service. Pioneers in the field are already taking products and services to market that connect everything from toothbrushes to fitness products. According to Gartner's report "The Future Smart Home: 500 Smart Objects Will Enable New Business Opportunities", a typical family home, in a mature affluent market, could contain several hundred smart objects by 2022.

For governments, utilities and services providers, IoT presents opportunities to monitor and manage assets, automate processes and save significantly on resources and manpower. Utilities are already using connected meters to track usage and pre-empt surges in demand or faults. Connected patient systems are already allowing healthcare providers to track the health status of outpatients and adjust treatment or send help where necessary. Every area of life – from work, to transport, healthcare, government service delivery and entertainment – stands to benefit from the innovations and efficiencies possible in a fully connected world.

From an environmental point of view, when lighting and power-hungry appliances such as heaters and air-conditioners are automated to work only when needed, we will see massive power savings and lower CO_2 emissions.

However, there are some hurdles to overcome. In Southern Africa, the biggest challenge is connectivity. IoT demands a significant number of homes to have reasonable high speed internet connections. Globally, key challenges are concern about security, control of the connected devices and control over the flood of information to emerge out of IoT. While there is already a wealth of personal information in the cloud, IoT is set to exponentially increase the amount of deep personal data moving through the internet. People are understandably cautious about how this data will be protected, who will have access to it and how it will be used. Many are reluctant for others to have this level of insight into what they eat, what they watch on TV, where they go, what they buy and other aspects of personal life.

Much like online shopping and banking, IoT may face some caution in its early stages, but it will become part of ordinary life as people see the benefits outweighing the risks, and we are already experiencing the start of it. Within 5 years, we can expect to see the most mundane trappings of ordinary life connected, and making life easier. In fact, big name brands are banking on an explosion of IoT.

Riverbed sees IoT as an inevitable stage in the evolution of connectedness. As end users require simplicity and convenience is enhanced, so the layers of technologies underpinning that convenience become ever more complex. This is partly because many industries still have decades-old mainframe programs still doing heavy lifting at the substrate level, with a client-server layer, laid down on top in the '80s and '90s, followed by a Web layer on top of that in the '90s and now, SaaS delivered from public clouds, private clouds, hybrid clouds, multiple clouds.
All of this creates islands of infrastructure. Infrastructure at data centres, at replication sites, in the sprawl of branch offices, in remote offices from kiosks to home offices to planes, in billions of mobile devices, in the private cloud, in multi-tenant public clouds shared with others.

Today, as a result, users, applications, and data are everywhere. IT

must provide an environment where users can access applications, data, and the underlying infrastructure located on-premises in data centres and private clouds and consumed as services from public clouds. This environment, the hybrid enterprise, must contend with both where the apps are hosted and how they're delivered. Private networks (MPLS links) are being joined by public networks (Internet transport) to offer choice in delivery channels: more costly private networks for mission-critical apps, cheaper public networks for recreational traffic, SaaS apps, and bulk loads like backup.

In an IoT world, the endpoints, transmitters, extensive connected networks, cloud-based data centres, storage and associated technologies will become increasingly burdened by massive volumes of data and commands moving through the systems. If a fault should arise, locating and addressing it rapidly could become a significant challenge within this massively complex network.

But not doing so can cost organisations revenue and customers, and cause consumers to lose faith in the IoT concept. In cases where connected devices are running critical infrastructure or keeping patients alive, there is no margin for error in identifying and rectifying problems. Maintaining an always-on network in the IoT era will depend in part on world class management and visibility tools that give service providers full visibility of every component of their network, enabling proactive maintenance, network performance monitoring and diagnostics.

The expected boom in IoT technologies opens the playing field for a range of business opportunities. While developers of innovative connected devices and applications stand to gain, the real market growth is likely to come from the service providers who enable the IoT. This sector now has opportunities to develop solutions that address the range of concerns an IoT environment raises, ranging from encryption to secure data storage, interoperability and transmission technologies, and – crucially – the management of the systems running the IoT world.