



## Technical Briefing

### Introduction

By 2020, it's estimated that there will be at least 20 billion connected devices. How effectively those devices communicate over heavily congested networks will determine whether they succeed or fail so testing their network resilience is essential.

The problem lies in the nature of the IoT itself. It will connect remote devices and systems and provide a data stream between devices and management systems.



Whilst industrial devices have typically only had to operate over reasonable networks (a LAN within a factory, for example) a common commercial or domestic model requires devices to be clients that rely on the manufacturer's cloud-based services to function. For example, an Internet-enabled thermostat and the associated app on the phone that controls it, don't communicate directly. Instead, each communicates independently with the cloud. In other words, the thermostat doesn't need a name because it offers no services -- it's a client and only needs to know how to phone home to the cloud.

### The Lab is not the Real World

When developing and testing IoT devices in the lab, setting up and testing over 'LAN' type networks is easy. The problem is that these rarely reflect the actual (real-world) network environment over which the devices need to operate. Deploying IoT Devices or Applications into real-world networks is a whole other ball game.

IoT developers, Q&A and deployment teams need to deliver applications and devices that "deal gracefully" with variable network connectivity i.e. avoiding meaningless message cycles, preventing hangs & crashes and demonstrating good retry and recovery capabilities.

They also, ultimately need to understand the network criteria under which the app or device is likely to fail.

### Issues with IoT Testing in Real Networks

It really isn't practical or viable to test in a real network because:

- ⇒ Live networks are not manageable - It isn't feasible to provide multiple network types and topologies and regardless, you can't easily induce appropriate transmission issues on demand.
- ⇒ You can't determine the network characteristics and issues being experienced; you really are flying blind.
- ⇒ The network scenarios are not controllable and repeatable. How would you replicate the same conditions to qualify a fix ?

### Network Emulation

The answer is **Network Emulation** technology that creates **Virtual Test Networks** which replicate all the real-world network scenarios and associated transmission issues likely to be encountered in real IoT network environments.



A Virtual Test Network is more useful than the real network because you can replicate, on demand, any network scenario, all the transmission issues and do this in a completely controlled and repeatable manner.

Another invaluable feature of a Virtual Test Network is that you can see what's really happening with powerful inbuilt statistics, reports and graphs providing total visibility in terms of the communication traffic, performance and errors.

iTrinegy's Virtual Test Network technology represents the defining way to deliver the insight, proof and confidence that your IoT devices will perform effectively when deployed.