The Cloud Computing News India

News And Info On Cloud Computing And Virtualization

http://cloudcomputingnews.in/ensuring-the-force-is-strong-testing-wifi-iot-devices/

Ensuring the Force is strong: Testing WiFi IoT devices

26/09/16

September 26, 2016

Areg Alimian, senior director, solutions marketing at Ixia explores the principles that should always underpin WiFi performance and resilience testing for complex IoT environments.

"The Force is what gives a Jedi his power. It surrounds us and penetrates us; it binds the galaxy together." This quote from Obi-Wan Kenobi in the original 1977 Star Wars movie could just as easily refer to the pervasive WiFi networks that surround us and connect Internet of Things (IoT) devices together.

Homes, hospitals, shopping centres and department stores, airports, large manufacturing plants – all are ecosystems with a growing volume and variety of connected devices that rely on WiFi to communicate and function.

Currently, 1 in every 3 IoT devices uses Wi-Fi, and these are being deployed in increasingly mission-critical environments, from hospital wards, to power and water utilities, to traffic-management and public transportation systems. As such, these devices – and the applications that control them – demand good Wi-Fi performance. Having a stable, reliable connection in a range of environments cannot be left to chance: it must be guaranteed.

WiFi-enabled IoT devices have to be able to perform the functions they are designed for, taking into account real-world variables such as the distance from the nearest access point, interference from other radio-frequency sources, as well as interoperability with other devices, and more. To achieve this, a comprehensive, robust Wi-Fi testing approach is needed.

From design to deployment

What, then, does a comprehensive Wi-Fi testing strategy look like? There are two main phases of testing to consider: first, by the manufacturers of the Wi-Fi devices; and second, by the organizations that deploy them as part of their IoT environments, whether a manufacturing plant or a hospital. Robust testing in both phases is essential if the end result is to be an efficient, resilient IoT infrastructure.

This also means that effective Wi-Fi testing must go from the actual design and development of the original devices, all the way through to accurate recreations of the actual environments in which those devices will be deployed. Wi-Fi testing is extremely context-specific. As such, the testing strategy must evaluate devices' performance and functionality across six key areas. Here, I will examine each of these in detail, using the example of a WiFi-enabled medical device used in a hospital environment.

Test one: range

Large hospitals mean, to state the obvious, that Wi-Fi devices within them have to operate across large areas. This means that Wi-Fi coverage is likely to be variable, and some devices will have to respond to being in areas with variable or poor coverage – especially if the device is portable. Qualities like packet loss, retransmissions, latency and jitter are therefore all key KPIs to check whether a particular device will cope across the entire range of the hospital.

Responsibility here lies with both the manufacturer (to build devices that operate across a sufficiently large range) and the hospital (it must test devices to ensure they work according to their specifications in that specific environment).

Test two: roaming and diverse networks

As patients move between wards and departments within the hospital, their monitoring devices must be able to move seamlessly from access point to access point, potentially switching between APs from different vendors too, without compromising performance.

Data loss during roaming could likely result in missing critical alerts, which clinicians are dependent on to provide quality healthcare to their patients. As such, the hospital must emulate its environment and replicate the exact roaming conditions of devices moving within it

Test three: ecosystem

The majority of Wi-Fi problems in complex environments are due to ecosystem issues; that is, the co-existence and simultaneous operation of multiple different devices. In our hospital example, a huge range of different Wi-Fi enabled devices are not only in operation, but also continually changing, as new applications are added or upgraded, and patients come and go. So the test conditions must replicate these real-world environments to ensure that devices function as they are expected to.

Test four: data plane
This stage of testing is all about considering – and accurately emulating – the different forms of data traffic to be transmitted across the Wi-Fi network. In a hospital, this is likely to include scan and test results – visual, audio and video – as well as textual and numeric data. Devices with data plane issues cause unnecessary overheads to the ecosystem – which, as we have seen above, is the major reason for Wi-Fi failures.

Test five: interference
Some background interference, from numerous endpoints operating on same RF frequencies used by mission-critical Wi-Fi patient monitors, and additional Wi-Fi disturbance from patients and visitors bringing in their own devices, is completely unavoidable. Consequently, it is important that the hospitals' critical devices and Wi-Fi access points can cope with the expected level of interference – and even unexpected levels of interference, too.

Test six: channel model
Most Wi-Fi devices within a hospital will encounter a variety of different RF channels, and if their performance on one particular channel is weaker, this can wreak havoc on overall performance. Here, both the manufacturer and the hospital have a responsibility to test devices' performances across a general and specific range of channels.
Real-time, real life

The crucial principle underpinning all of these testing areas is the emulation of real-world operating conditions. Wi-Fi testing is not a theoretical endeavour; it must incorporate traffic simulations, range and roaming conditions, device and application ecosystems that mirror the working environment, and even exceed them in terms of complexity, in order to guarantee performance and resilience in the field.

IoT infrastructures, whether the hospital example we examined here, a factory, a university, a department store or indeed an entire city, are bound together by WiFi. A huge range of devices must be able to connect to diverse networks, often in unpredictable conditions.

While the exact nature of an IoT deployment in months or years to come will always be difficult to entirely predict, real-life, real-time device and network testing will go a long way to ensuring that the environment's connectivity will be strong, always.

(NetEvents)