BYOD Use Case

See Kay Leong **(8.5 mins)**

Let me take you through a use case to show how BYOD solution works. I am using a healthcare scenario.

Dr. Tom buys a 4G iPad during lunch. He is walking back to hospital with his new iPad, walk to the IT Department, and says, "Folks, I want to use this for my work, how can you help me, IT team?" Without BYOD implementation, the IT manager will probably reject Dr Tom's request, and instead ask him to fill up a few forms, to request for a hospital-own iPAD of approved devices. Dr Tom will need to wait for this device to be approved, purchased, and set up for use in the hospital network.

With BYOD, the process has changed.

Instead of asking Dr Tom to fill up the forms, the IT manager tells him that using his username and password authentication, he can "on-board" the device. On-boarding means bring the device onto the network for the very first time. With the username and password, the network can see the profile of Dr Tom. The user profile is very important over here, in BYOD context, and is typically tied to the job role and responsibilities of the user, what type of access he has as a doctor in this particular hospital. The network can then apply all the correct policies and approved apps that Dr Tom is allowed to access automatically.

The IT manager knows the importance of keeping network secure, complying with regulations to protect patient data. Things like remote wipe, data loss prevention are very critical here.

As you can see here, the application are defined based on the device-type, the user, the location and the application that Dr Tom is using. This is what we known as 'contextual policies'. Once that's done through the Wi-Fi network, having put in his username and password, which is identity-based access control, Dr Tom is ready to go, as you can see. With the policies being in place, Dr Tom can access to electronic medical records, telepresence systems, email and instant messaging. His system apply contextual policies based on things like device type, users, and location automatically without user intervention.

We have keep it simple for this example, but you can apply policies based on many more attributes.

Dr. Tom has now on-boarded his new iPad. Keep in mind, to enable this seamless experience, the network need to support certain things. First, you need an 802.11n Wi-Fi network which can withstand the challenges of mobility including complex RF interference. Second, you need identity-based network control for the contextual policy which we just touched on. Mobile Device Management is required for functions such as installing enterprise applications or remote wipe if the device is lost. Last but not least, make sure you have a management system for the infrastructure and service assurance manager for visibility into what's going on in the network, and what you need to do if things start going wrong. If you have branches in the hospital, WAN optimization will help network resources be available.

Let's get back to Dr. Tom again. He is attending to his patients in the operating theatre. His contextual policy has been defined from an application perspective such mobile telepresence, email and instant messaging. It is key to note that you can tailor this policy for unique job and regulatory requirements, with the doctor only allowed to access sensitive patient records while in the office due to HIPPA regulations.

Dr Tom goes into the operating theatre. With his policies, as you can see here, he can pulls up EMR, looks at x-ray images, communicates with staff via instant messaging. We know that literally billions of devices are pouring onto the network at hospitals. That presents doctors, administrators, patients, and visitors. Each has unique needs, and along with tablets and smartphones. Healthcare has specialized medical equipment, and Wi-Fi tracking tags, connecting in increasing numbers.

A Wi-Fi network must be designed to meet these challenges, these changing device profiles, application profiles, and device density:

- Capacity and performance to support the influx of clients
- Performance to handle new applications, such as a two-way telepresence with patients, and EMR data hosted centrally for a medical group, and application data now residing in the cloud.
- Acceleration for all client types, even the medical asset tags, slower tablets and smart phones.
- Proactive protection against wireless interference from things like blanket warmers and light controls.
- Location tracking for assets and people,
- Plus, patient data is protected by HIPPA regulations, so that IT must carefully govern when and how this can be accessed.

It's now 2pm, Dr Tom needs his afternoon coffee. He decided to go to the coffee shop next to the hospital, which has a WiFi hotspot.

What happens when he leaves the hospital? Now, his contextual policy becomes a roaming policy defined by the hospital. The policy says that Dr Tom will not have access to EMR while at the coffee shop, but he will be able to use email, telepresence and instant messaging using a Virtual Private Network connecting back to the hospital's infrastructure.

While there, he gets a page from his nurse to have a two-way video chat about his patient. Of course, behind that video call was an infrastructure that made it possible.

Dr Tom goes to his child's soccer game, still with his new iPad, now roaming on 3G network. Again, his VPN has roamed from hotspot to 3G, preventing any interruption or intervention. He has full access to the patient data, but his applications have been throttled to prevent overloading of the 3G network and to prevent application performance issues. Our doctor pulls up his EMR application, checks for updates on patient status, and all is well. He can watch his game in peace.

Time to go home. Dr Tom goes home, connects on home Wi-Fi, He has partitioned access, (VPN) tunnel back to hospital with a personal SSID for family access.

Dr Tom calls in on his IP softphone to talk a colleague about tomorrow's operations. You can see from this slide- he has a teleworker's policy, which allows him to have full EMR access. He can have remote telepresence, email and instant messaging.

Now, while at home, Dr Tom's son started a Call of Duty "Modern Warfare 3" game, but his home router applies QoS (Quality of Service) and prioritizes this lower than his phone call. His call continues with perfect quality.

Healthcare is especially mission-critical, and we can all relate. But the parallels across industries are endless:

- In the Retail world: imagine you have a virtual dressing room, personalized shopping experience.
- Insurance: Agents and adjusters generating quotes on location with customers, with photos and personal data.
- Financial services: portfolio management for client discussions, as well as a branded customer experience in a retail branch.
- In the Education space: students in a large lecture hall, watching multicast video of the lecture, supporting materials and photos.

These are the many uses of BYOD. Businesses in every sector will need to keep up with these trends, and that means investing in a mobility architecture capable of turning these challenges into opportunities.