FLUKE networks

White Paper

BYOD Without Tears

The Impact and challenge for Network Engineers

Bring Your Own Device (BYOD) is as much a sign of cultural change as it is an indicator of prevailing technology trends. Shifting work patterns and the need to be smarter and more flexible have neatly coincided with the proliferation of connected devices like smartphones, tablets and netbooks.

For most it's a marriage made in heaven. Users like the freedom, spontaneity and instant-on availability of mobile and portable devices. Employers like the creativity, productivity and extended working they encourage from staff. But network performance and security concerns can arise when employees want to use their personal devices at work. Yet it is now regarded as restrictive and outmoded to not allow such use.

With the analyst firm Forrester predicting there will soon be an average 3.2 devices per user in the enterprise, it is clear that it is a trend that cannot be ignored nor halted. BYOD is here to stay whether we like it or not. However, steps must be taken, and taken now, to ensure companies are ready for BYOD. This white paper looks at the challenges of integrating BYOD with corporate networks in a way that BYOD does not compromise connectivity or performance for established wired and wireless users.

Table of contents

Introduction

Not so long ago company desktops and laptops were the only powerful computing devices that staff had access to while at work. Today, those same employees probably carry more computing power around with them than they have on their office desk. It's all thanks to the burgeoning market in high tech consumer devices such as smartphones and tablets.

Originally purchased for personal use, the sheer utility of these devices is leading to them being used more and more in a business role too. The increasing adoption of Web-based software-as-a-service line of business applications is also playing a part. As a consequence the BYOD roller coaster is gathering pace, and there is no sign of it slowing down any time soon.

Of course no runaway technology trend comes without a price. In the case of BYOD it is at the cost of corporate WLAN performance and security. And that impact tends to land squarely on the desk of network support staff.

Some network managers have already embraced the BYOD paradigm with enthusiasm. They have taken steps to minimise the impact of connected personal devices on their networks while still ensuring the devices themselves deliver a good user experience.

For those businesses and network managers ready to embrace and provision for BYOD, some key questions remain. How to keep a tight grip on security when network client machines are no longer nailed down? Can it be possible to administer the relative chaos of an ever changing population of devices? How do you keep pace with multiple device types and operating systems?

And that covers just the hardware. Behind every device comes a legion of apps. or more accurately applications, each from a different software house, by a different author, requiring unimpeded access to a different set of network assets.

Compared to the buttoned up, locked down environment of the traditional corporate network BYOD is a different world.

Challenges Facing Network Engineers

Network performance hits are probably the most visible of the BYOD challenges. All but the most rudimentary of business WLANs will have been planned and sized to match the capacity and throughput demands of known corporate wireless assets, for example company supplied laptops and portable IP phones.

With unchecked growth in the devices carried by employees into the workplace the original wireless planning assumptions go out of the window. Not only is there more contention for available wireless channels and bandwidth, reports from Gartner suggest that many personal devices can gobble significantly more network resources than, say, conventional laptops because of their lower powered and less well specified wireless modules.

The often random behaviour of personal devices can also have a big impact on corporate WLANs. Company-owned assets will have been chosen for their exemplary manners in a shared network environment, or will at least behave in a known and controlled way that does not disrupt the network for other users. Personal, consumer market devices on the other hand often compete aggressively for network resources, restricting access for other users.

As WLANs and BYOD itself become more important to the business and handle increasing volumes of critical data, it is vital that network engineers respond quickly to solve performance issues. Indeed many engineers are now being assigned WLAN responsibilities yet may lack specific wireless skills. Intelligent software tools providing visibility, insight and troubleshooting guidance are invaluable in maintaining network performance and connectivity.

Security

Less visible but potentially more serious are the security implications of random, roving personal devices connecting to the corporate WLAN and accessing networked applications and data.

There are two sides to this particular problem. The first is one of network access. A tablet or smartphone together with its owner - if they have not been approved and registered by the network administration team for full access - may lack the right credentials to log on to the WLAN in a secure and trusted manner. They will then of necessity use open guest access via a second insecure WLAN. To do so means data flowing to and from the device is open to eavesdropping and interception by a third party, an act which may well never be discovered.

The second aspect to security applies even to those devices which have been properly approved and registered for secure access and which log on through an authorised and encrypted connection. The issue here is one of data leakage - the transportation of secure and restricted documents or other data outside the corporate environment. This may happen through storing corporate data locally on the device itself or through the use of cloud storage solutions like Dropbox.

At such times - and for example when employees leave an organisation - is important that a mechanism exists for revoking any access privileges that may have been accorded to particular devices. Also some devices offer a remotely triggered erase facility for deleting any stored business data.

Management

Being essentially consumer devices, many tablets and smartphones come without the management tools and interfaces of their more professional counterparts. Additionally the sheer number and the diverse proprietary nature of devices, along with a constant stream of software, firmware and operating system updates presents a very real support and management headache for IT teams. This is doubly problematic as the rise of BYOD and the need for full visibility and management is coinciding with growing downward pressures on headcount and resourcing. Companies can ill afford to locate skilled WLAN specialists at every branch office, prioritising the need for effective remote monitoring and management of networks as well as the devices themselves.

This is especially challenging in the case of BYOD since many devices do not have proper diagnostic interfaces. And for those that do – regardless of the management solution chosen – there will invariably be delays pending the release of a new OS or proprietary extension. For example there are currently no remote administration or diagnostic agents for Apple® iOS® devices. Some Android devices do offer proprietary extensions for logging and diagnostics, but most have only limited APIs that do not aid remote trouble shooting. As a consequence there is a temptation for many misbehaving devices to remain unsupported, yet continuing to drag down WLAN resources and performance. Furthermore the devices themselves are now so ubiquitous, with seemingly almost everyone of working age possessing one, that IT teams are overwhelmed and simply cannot afford the staff time needed to support them all correctly.

Display Name (32)	ACL	OS	Model
HTC:E8:D2:D0	U	Android/Windows	HTC
APPLE:3F:6B:33	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:81:4E:F8	U	iOS	iPhone 4/iPhone 4s/iPad
SAMSUNG:6D:C...	U	Android/Windows	Samsung
APPLE:CE:79:CE	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:A6:66:ED	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:1F:42:7E	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:18:C3:75	U	iOS	iPhone 5/iPad 4/iPad Mini
SAMSUNG:4A:8...	U	Android/Windows	Samsung
SAMSUNG:21:5...	U	Android/Windows	Nexus
APPLE:81:E4:91	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:2D:B4:08	U	iOS	iPhone 4/iPhone 4s/iPad
SAMSUNG:C1:0...	U	Android/Windows	Samsung
ASUSTEK:CC:A...	U	Android/Windows	Nexus 7
APPLE:0D:86:96	U	iOS	iPhone 4/iPhone 4s/iPad
SAMSUNG:0D:B...	U	Android/Windows	Samsung
APPLE:4C:73:7C	U	iOS	iPhone 5/iPad 4/iPad Mini

Inventory management too poses a problem. IT departments are responsible for making sure all software in use is properly licensed and kept up to date. This is relatively easy across an estate of accredited and registered hardware using known operating systems and software suites. In the case of BYOD the homogeneity of operating system and apps. makes it very difficult indeed.

Business Impact

As these issues illustrate sweeping the impact of BYOD under the carpet risks reducing business efficiency, increasing operating costs and compromising security and confidentiality. Instead BYOD should be - and can be when properly integrated - an asset to the business.

Compliance

More and more companies are having to meet ever-stricter compliance and governance obligations. In the case of financial, insurance, healthcare and similar areas these obligations are often mandated by statute. Examples include the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act. In some cases companies make their own internal rules like those at IBM banning the use of iCloud and Dropbox. In more extreme situations BYOD may be outlawed altogether as is now the case with almost 50% of companies in India following fears of information leaks.

Successfully Integrating BYOD

Plan, predict and design

For successfully integrating BYOD with the corporate WLAN, proper planning and design is essential. Key to this is a thorough understanding of current Wi-Fi capacity and coverage: for example current AP locations, the position of walls, doors and metallic structures, the locations of especially busy areas like meeting rooms, staff restaurants, reception areas and waiting rooms, which departments currently rely most on wireless access.

Due attention should also be paid to the underlying wired network infrastructure that will support the APs. With 802.11n offering wireless data rates of up to 300 Mbit/s, Cat 6 cabling and a 1 Gbps capability is virtually essential.

Device types should also be factored in. For example most pocketable devices will be optimised for low power consumption and for small physical size. This places constraints on RF performance and antenna gain, leading to such devices having to be closer to an AP and providing lower transmission rates than say a laptop or a wireless printer. Also earlier devices are unlikely to support the 5 GHz band or channel bonding, and will consequently contend for the more heavily used 2.4 GHz band, leading to congestion.

Applications are also a consideration. Bandwidth priority will need to be given to real-time applications such as VoIP and video conferencing/ streaming and these will require careful QoS allocation. The coming impact of emerging voice over wireless (VoFi) telephony will be more testing still if call quality and continuity is to be maintained, especially when handsets roam between access points. Due attention must also be given to the fact that users may access personal or third party content through their devices when on company premises. Legality and bandwidth issues may need to be considered.

Contemporary network design tools have revolutionised the way wireless deployments are made. Using information about site and building layout, existing network infrastructure, the prevailing radio frequency environment and anticipated wireless device populations and usage, such tools can predict accurately WLAN coverage and performance. Designs can be fine-tuned iteratively by adding and/or moving devices to simulate BYOD growth and office changes.

From this modeling can come an accurate shopping list of materials for network build out including comparisons of specific APs, vendors and antenna radiation patterns. All of this saves much valuable time later on during surveys and deployments.

Survey, Verify and Deploy

With any wireless system - because of the unpredictability of how radio signals travel - it is important to verify the findings of software planning tools with actual on-the-ground surveys. Using the theoretical design as a baseline, placing APs, conducting coverage walk tests and verifying data rates will allow the design to be iteratively improved until final locations can be confirmed. These will also to a degree be determined by the locations of existing network and power wiring, and physical access for fitting and subsequent servicing

Once all these factors are finalised APs can be located and fixed, guided by the insight produced during the planning and verification process.

Detect and Eliminate Interference. As wireless systems evolve and grow new sources of interference are likely to arise. Effective software tools can monitor continuously for such occurrences and flag alerts to network engineers. In the case of interference from other Wi-Fi devices this is most easily eliminated by changing channels on one or more devices in the vicinity.

This can be especially problematic in the case of BYOD. Many devices may have both Bluetooth and Wi-Fi enabled, effectively saturating the 2.4 GHz band in their proximity. This applies even when there is no BYOD (and therefore no direct network connection) permitted, since these devices will still be repeatedly polling and attempting to connect.

Interference may also come from non Bluetooth or non Wi-Fi sources. These include DECT telephones and microwave ovens, both of which share the same frequency band as Wi-Fi. A recent survey revealed that 82% of respondents had experienced WLAN performance problems due to interference from such non WLAN devices. When this kind of interference is encountered it may require the re-siting of equipment or the addition of screening.

> ***"AirMagnet Survey Pro has made installing wireless networks approximately 50 percent less expensive than it used to be because it reduces the amount of time taken to identify and overcome installation problems. This not only brings down cost in the short term but also minimises the need for maintenance in the long term, giving Logicalis greater competitive edge."***
>
> *– Jon Shorten, Principal technical specialist - Logicalis*

Maintain Security

A key part of any BYOD strategy should be maintaining security of the entire wireless environment. While hardware vendors may offer rudimentary security tools, only a dedicated wireless intrusion prevention system (WIPS) can achieve this in an adequate and robust manner automatically across multiple sites.

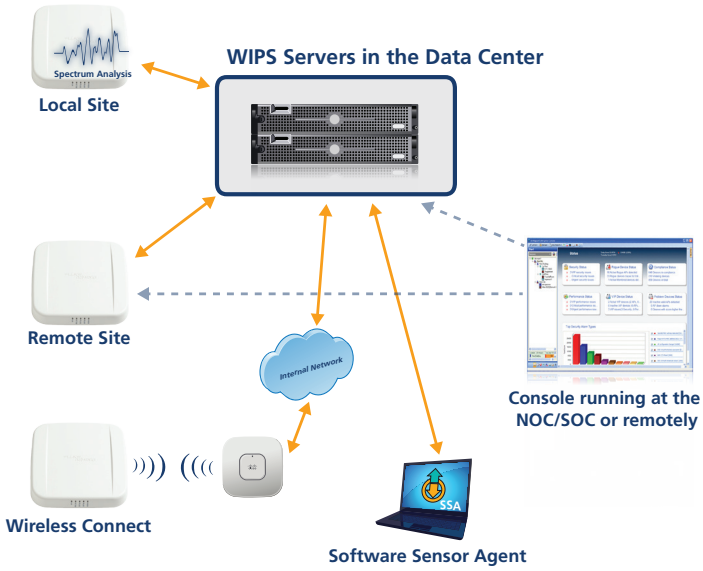
A WIPS works in two ways. It monitors the radio spectrum for any unauthorised wireless devices (detection) and automatically stops these devices accessing the WLAN (prevention). Large organisations in particular are susceptible to threats from bogus access points which could expose the entire network to anyone within wireless range. The WIPS will detect these using MAC address filtering and, to guard against MAC spoofing, device fingerprinting which uses characteristics unique to each device. The WIPS will also detect and flag the attempted use of any wireless attack tools.

Contemporary WIPS tools involve three separate elements: intelligent active sensors that scan the radio spectrum and capture data packets, one or more distributed servers which communicate with the sensors and analyse any captured packets, and a centrally located user administration and reporting station.

This configuration makes it possible to deploy multiple remote sensors and/or servers across all the sites in a network and provide true 24x7 end-to-end monitoring and detection. Central alarms generated by WIPS will then alert the on-duty network engineer and security personnel to any attempted intrusions.

> ***"The ability to remotely utilize the integrated spectrum analysis capability allows our team to pinpoint the exact physical location of WLAN interference and deploy staff already at remote sites to help remediate. Being able to proactively understand the exact source and impact of these problems allows us to restore critical network service as quickly as possible to all users."***
>
> – *Ron Bird, Network and Technical Services Manager - Jordan School District*

With the proliferation of BYOD and wireless, and the consequent rise in vulnerabilities and threats, another key element of security is regular updates as new threats – and defences against them - are discovered. While device vendors might offer infrequent updates which may include some security components, a dedicated WIPS can centrally manage frequent updates across the organization with ease, without requiring specialist local on-site intervention.



Manage Performance

To achieve acceptance of BYOD in the enterprise devices must not compromise network performance for other users. But as already outlined there are many obstacles to achieving a happy medium between traditional wireless devices and the new flood of personal devices brought into work by employees. The issue is one of managing a growing number of different and ever-changing devices while running over a shared wireless medium with unpredictable and often heavy traffic flows.

It should also be remembered that the end users' network experience is not determined solely by the performance of the wireless portion of the network. The underlying wired network connecting the APs also plays a part, as do the servers hosting any cloud applications or data in use. This underscores the need for true end-to-end monitoring, identifying and measuring the entire path between service and user and the role that it plays in the overall user experience.

Hardware-focused legacy network management systems designed for static environments do not cut it in the world of BYOD. Such systems should instead centre around the user. Only in this way can network engineers understand the perceived experience of all users on the network, so gaining maximum advantage from BYOD. Equally support should be provided on a per user basis.

Truly proactive management requires that individual network interactions be captured and analysed with a view to spotting exactly where issues are taking place, introducing the need for true end-to-end visibility across the physical and virtual infrastructure.

It might be frequent occurrences of short term activity on the network, it might be prolonged multimedia streaming associated with teleconferencing where speech and movements on camera cause a temporary surge in data rate. Either way these events are transient in nature

hence the need to capture them locally using intelligent sensors on-site which then report into a central server for aggregation and reporting. From this raw management data can be derived valuable insight on where a problem is, what caused it, and what is its impact on users.

Couple this with continuous wireless testing to reveal points of congestion, high error rates, degraded data rates and other problems and the network administrator has everything they need to be proactive. Rather than chase down problems once they have occurred it becomes possible to concentrate instead on preventing such issues in the first place.

Saving Money

One aspect of BYOD that is not yet receiving much airtime is its potential to reduce operating costs within the enterprise. It might seem that adding network infrastructure, incorporating new network management tools and procedures, and adding to the workload of network administrators can only increase costs. And to a degree it is true with a modest capital outlay required for network hardware and software.

But the network administration burden need not be significantly greater than it was prior to BYOD. Support and user hand-holding aside the job of managing devices, security and performance is eased greatly by contemporary software tools. It is now possible to distribute intelligent monitoring, using software agents and hardware sensors around the network, across multiple sites if need be, and collect all the results centrally. With automation to pinpoint trouble spots, derive actionable information and measure the results of any changes there may be no need to increase the size of the IT team to run an efficient and secure BYOD infrastructure.

This applies in equal measure to conventional wired networks too. BYOD, having forced the move to more advanced, more sophisticated automated network management tools, will also bring benefits in supporting users connected via cabled networks. Wired and wireless can be monitored and managed together as one common network fabric, rather than the two separate entities they otherwise tend to be, bringing further opportunities for savings.

Further there is evidence to suggest that with BYOD employees are able to work more on the move than was possible before which tends to offset any extra costs resulting from the need to manage and support personal devices. Moreover as companies move increasingly to virtualisation and cloud computing for their mainstream applications, there is still further potential for operational savings stemming from BYOD as work can continue anywhere there is Internet access.

Enhancing Mobility

Thus far only the WLAN aspect of BYOD has been considered. The move towards mobile convergence is leading to a second network medium that must also be considered - the 3G and emerging 4G/LTE networks of the mobile operators to which a good proportion of devices also have access. This makes it perfectly possible for staff to use their devices online from areas not served by Wi-Fi and while on the move, or for staff and visitors to make and receive telephone calls on their smartphones.

While the burden of network support in this case belongs with the mobile operator, some larger companies and a lot of indoor public spaces have turned to technologies like Femtocells, Picocells, Microcells and Distributed Antenna Systems to provide enhanced indoor and campus coverage for those using the established mobile networks. This may introduce an additional management and support requirement where such technologies have been deployed by the site owner rather than a mobile carrier.

About Fluke Networks

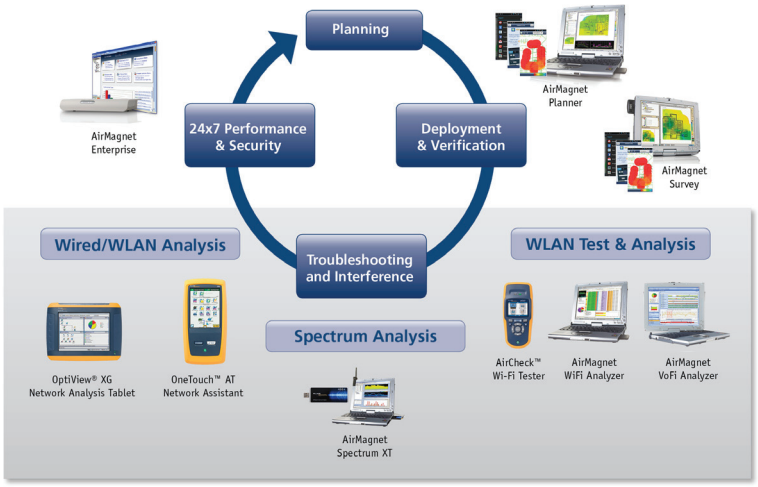
Fluke Networks is the world-leading provider of network test and monitoring solutions to speed the deployment and improve the performance of networks and applications. Leading enterprises and service providers trust Fluke Networks' products and expertise to help solve today's toughest issues and emerging challenges in WLAN security, mobility, unified communications and datacenters. Based in Everett, Washington, the company distributes products in more than 50 countries.

For more information on our wireless solutions, visit **www.FlukeNetworks.com/wlan**

"We've tried many tools from many other vendors over the years, but none of them delivered the complete package like AirMagnet. The level of functionality allows our teams to build and support better wireless networks, which in the end means happy customers." – *S.D. Bishop II, Vice President and COO - ShowNets*

Solutions from Fluke Networks

Fluke Networks offers its AirMagnet product line to help solve the BYOD challenge. It spans the entire WLAN lifecycle, ensuring security, performance and compliance. Automatically discovering employee-owned mobile devices it assesses their impact on the corporate network, reduces unwanted side effects and facilitates trouble-free and appropriate use.



AirMagnet Wireless Solutions

AirMagnet enables predictive modeling of enterprise WLANs, provides advice on AP placement and channel allocations, and runs what-if analyses on the impact of BYOD growth. After WLAN deployment, AirMagnet measures actual coverage and verifies true end-to-end performance and provides an Android app. to visualise coverage.

More information at **www.flukenetworks.com/byod**

OptiView XG® – Automated network and application analysis

The OptiView XG is the first tablet specifically designed for the Network Engineer. It automates root-cause analysis of network and application problems allowing the user to spend less time on troubleshooting and more time on other initiatives. It is designed to support deployment of new technologies, including unified communications, virtualization, wireless and 10 Gbps Ethernet. The result is that new initiatives get up and running faster and network stay productive even in these days of smaller teams.

More information at **www.flukenetworks.com/xg**

OneTouch AT™ – Client to Cloud troubleshooting in 60 seconds

The OneTouch™ AT Network Assistant greatly reduces troubleshooting time through a streamlined, three-step approach:

1. The unique AutoTest replaces multiple tools and an hour of troubleshooting time.
2. A powerful set of network performance measurements to troubleshoot wired and Wi-Fi networks.
3. It enhances team collaboration through a simple web-remote interface and easy-to-use inline packet capture capabilities.

More information at **www.flukenetworks.com/OneTouchAT**

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**

Corporate Office:
Fluke Networks
P.O. Box 777 Everett, WA USA 98206-0777
1-800-283-5853
e-mail: **info@flukenetworks.com**

European Office:
Fluke Networks
P.O. Box 1550, 5602 BN Eindhoven
Germany **0049-(0)682 2222 0223**
France **0033-(0)1780 0023**
UK **0044-(0)207 942 0721**
e-mail: **sales.core@flukenetworks.com**