Preparing for BYOD

(Bring Your Own Device)

Everything you need to know before you BYOD

AUTHOR PAGE:
Philip Wegner

Philip Wegner is a technology entrepreneur, Founder and CEO of SecurEdge Networks. SecurEdge is an IT Solutions company that has helped hundreds of organizations plan, deploy and support technology that allows for the secure operation of wireless devices.

FOLLOW ME ON TWITTER @PHILIPWEGNER

Share this eBook!

TABLE OF CONTENTS:

Overview of BYOD

What is BYOD?..4
Growth of BYOD...5
What is driving BYOD?...7
Should organizations allow BYOD Network Access?............8
What are the analysts saying? 9
What are the advantages of BYOD?..........................10
What are the disadvantages of BYOD?.......................12

Preparing for BYOD

Build Your Network to Support Mobility.......................14
Application Visibility..15
Security is the Foundation for BYOD..........................17
Integrated Systems..18

BYOD Solution Components

Network Access 20
Network Security 25
Network Access Control 28
Network Management 31
Mobile Device Management 34

How We Help

SecurEdge Networks 38

Share this eBook!

securedge networks
SecurEdgeNetworks.com

CHAPTER 1

OVERVIEW OF BYOD

What is BYOD?

Quite simply BYOD stands for Bring Your Own Device and it means exactly that. BYOD refers to the growing trend of employees bringing their own wireless or mobile devices to the office. Devices such as smart phones, tablets, and laptops can connect to the organization's secure wireless network for personal and/or professional reasons. For education facilities, a BYOD policy may be implemented to cover student users as well.

Bring

Your

Own

Device

Gartner vice president and analyst David Willis described BYOD as "the most radical change to the economics and the culture of client computing in business in decades."

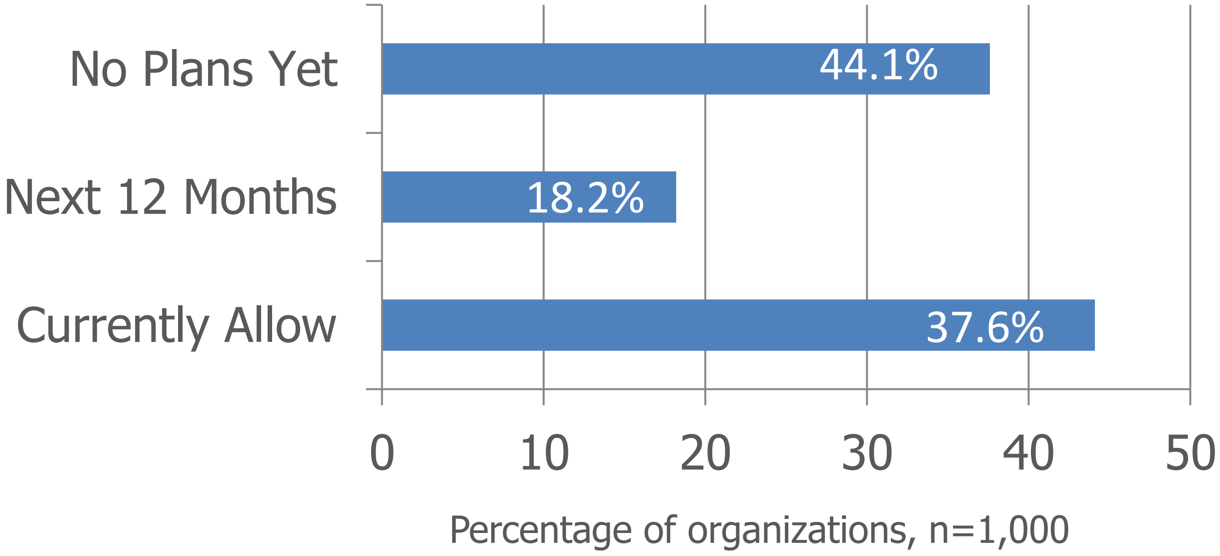
Growth of BYOD

The move toward mobile devices is just too strong to ignore. Many businesses are under a lot of pressure to allow personal mobile device use on the enterprise wireless network. Because of the explosion of smart devices the BYOD trend has taken off.

The BYOD trend started in 2009 and by 2012 over 50% of organizations began to support some form of BYOD. As the smart devices craze continues to accelerate and thrive so does BYOD. BYOD is now a phrase that has become widely adopted throughout various industries all over the country particularly enterprise, education, and healthcare.

Support for BYOD

Chart represents results from ZDNet's BYOD Business Strategy Survey



Share this eBook!

BYOD has gone from small pilot projects to a reality at many organizations. Over the past few years BYOD has seen a meteoric rise in popularity. The average number of connected devices per worker in 2014 will reach 3.3 devices, up from 2.8 in 2012, according to a recent Cisco survey.

Over 70%

of mobile professionals will conduct their work on personal smart devices by 2018

of organizations officially condone BYOD.

Over 50%

Sources: Gartner and Forrester Research

What is driving BYOD?

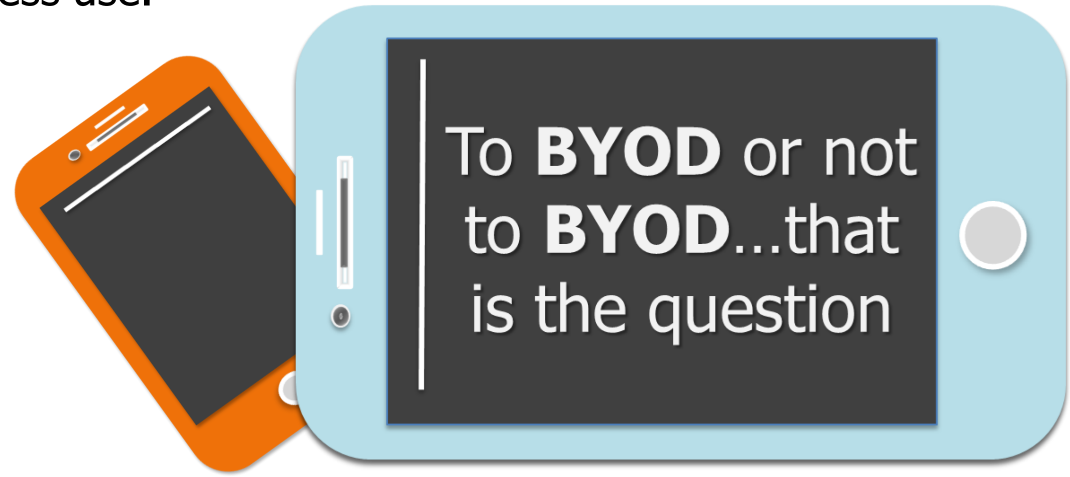
The launch of smart phones and tablet computing (specifically the iPad) is driving the move to BYOD. When you look at devices trending over the past 5 years there has been a significant shift to mobile devices. The rapid adoption of smartphones and tablets including iPhones, iPads and Android devices along with the number of easily accessible apps is driving this trend forward.

According to a report from the Triangle Business Journal, by the end of this year, the number of mobile connected devices will exceed the world's population. Cloud based services, accessible from almost anywhere, are also a key factor. As our world becomes increasingly mobile so does the need for BYOD.

> "By the end of this year, the number of mobile connected devices will exceed the world's population.

Should organizations allow BYOD network access?

This is a corporate policy question, but if you refer to the previous question the answer is that it's going to be hard to stop the demand for access with personal devices. The fact is it's inevitable with or without the organizations approval. According to the US and European Enterprise Decision Maker Survey, over 80% of companies report that employees use personal devices for business use.



From students in class, to hospital employees, to business professionals, BYOD is beyond just being a "cool" trend it's now a necessity across many industries. Getting a BYOD policy is something that every organization has to at least consider allowing in this golden age of technology that is pushing the boundaries of how we do live, learn, and do business. We recommend organizations figure out how to manage it or even embrace BYOD and figure out how to benefit from it.

What are the analysts saying?

In their 2012 "Worldwide Business Use Smartphone 2012-2016 Forecast Update," analyst firm IDC forecasted that, by 2016, worldwide shipments of smartphones will reach 480 million, with 65% being used in BYOD environments. —IDC

About half of the world's companies will enact BYOD (bring your own device) programs by 2017 and will no longer provide computing devices to employees, a new Gartner report predicts. —Gartner Inc.

54% of North American and European companies are developing BYOD programs for smartphones and tablets. —Forrester Research

38 percent of companies expect to stop providing devices to workers by 2016. —Gartner Inc.

What are the Advantages of BYOD?

There is an immense amount of benefits BYOD can offer. The major advantage all industries can expect is cost savings.

For enterprise and healthcare industries, BYOD can save incredible amounts of money with the employee paying for the majority or all of the costs for the mobile devices, services, and other associated expenses.

For schools, BYOD is a way for schools to get closer to that 1 to 1 (every student has a device) model without incurring the higher costs of a 1 to 1 model. It's a cost-effective way to save schools money on technology for staff and students. Of course there is a plethora of other benefits besides just cost savings.

A recent study by Intel showed that every employee was getting 57 minutes more each workday due to their BYOD program!

Here are a few examples of some of these industry specific advantages of implementing a BYOD program.

Benefits in Enterprise:

With BYOD, the enterprise industry can expect to see increased worker satisfaction, enhanced productivity, and amplified engagement in the workplace and after hours. Offering a BYOD on your enterprise wireless network can also help to attract top performing applicants, who seek to work flexibly and often work on-the-go.

Benefits in Healthcare:

In healthcare, BYOD can benefits employees by increasing efficiency, providing easier access to patient records, and improving organization. All of these help improve doctor patient relationship by freeing up more time for them to spend with patients, improving communication and the overall experience.

Benefits in Education:

For schools, BYOD can encourage collaborative education, increase student engagement, and allow opportunities for more personalized learning where students can excel at their own pace. Students' personal mobile devices tend to be more cutting-edge, so schools can more easily stay up-to-date with technology.

What are the Disadvantages of BYOD?

BYOD typically means more devices to support. They are relatively unmanaged, potential security risks, and could drag down employee productivity. Personal devices could easily be misused as a distraction rather than a tool.

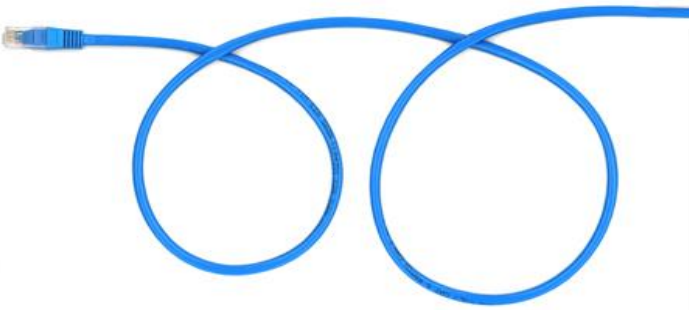
The organization doesn't own the device which means they have less control of the device type, image and security settings. The network has to be designed to control the behavior of the device and manage risks. If you haven't properly prepared your wireless network infrastructure these mobile devices can overload your wireless network as well. Also, if you do not have a well-planned BYOD policy in place you could end up with your IT staff being constantly overwhelmed with questions and device support issues.

CHAPTER 2

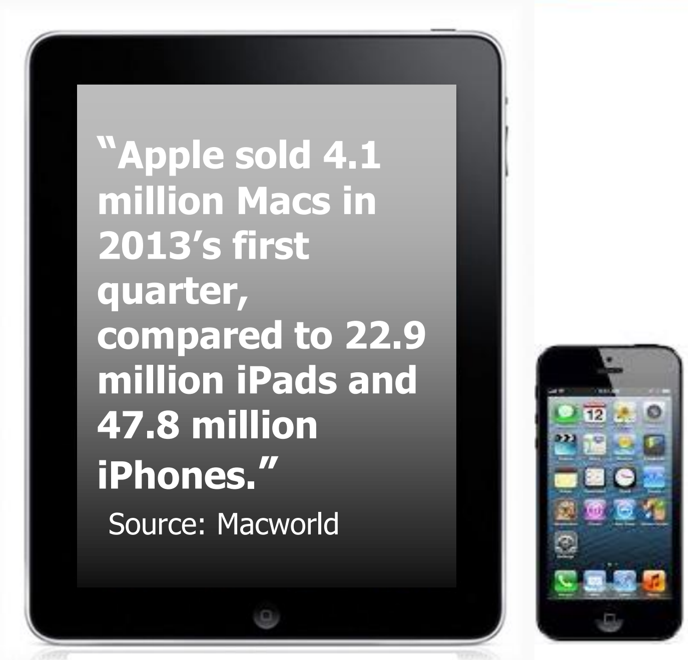
PREPARING FOR BYOD

Build your Network to Support Mobility

This may be obvious, but the users that are accessing the network for BYOD aren't carrying their desktop into your building and jacking into a connection in a wall. They're using a mobile device. At SecurEdge, we've routinely run network traffic studies for customers that support BYOD and the results consistently show that 80-90% of network traffic is coming from a mobile device. So why are we deploying all of this over built wired network capacity?



We should be building our networks to support the users. A good mobile network creates happy users, and happy users make our lives easier in IT. The users are mobile; networks need to be built to support them.



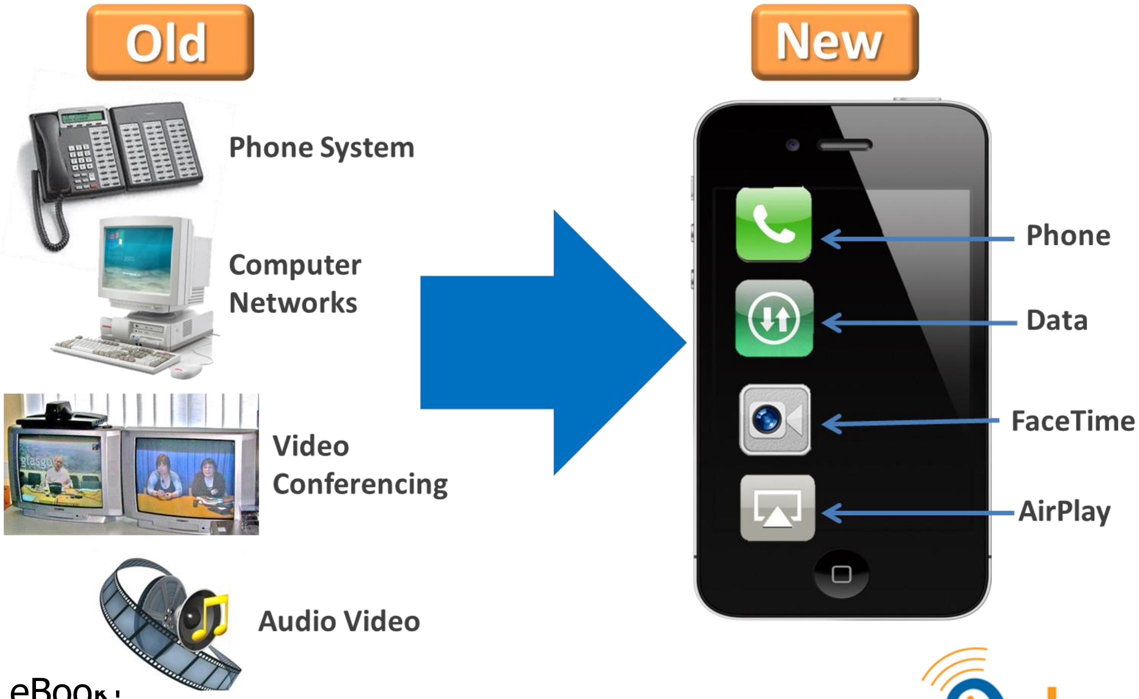
"Apple sold 4.1 million Macs in 2013's first quarter, compared to 22.9 million iPads and 47.8 million iPhones."

Source: Macworld

Application Visibility

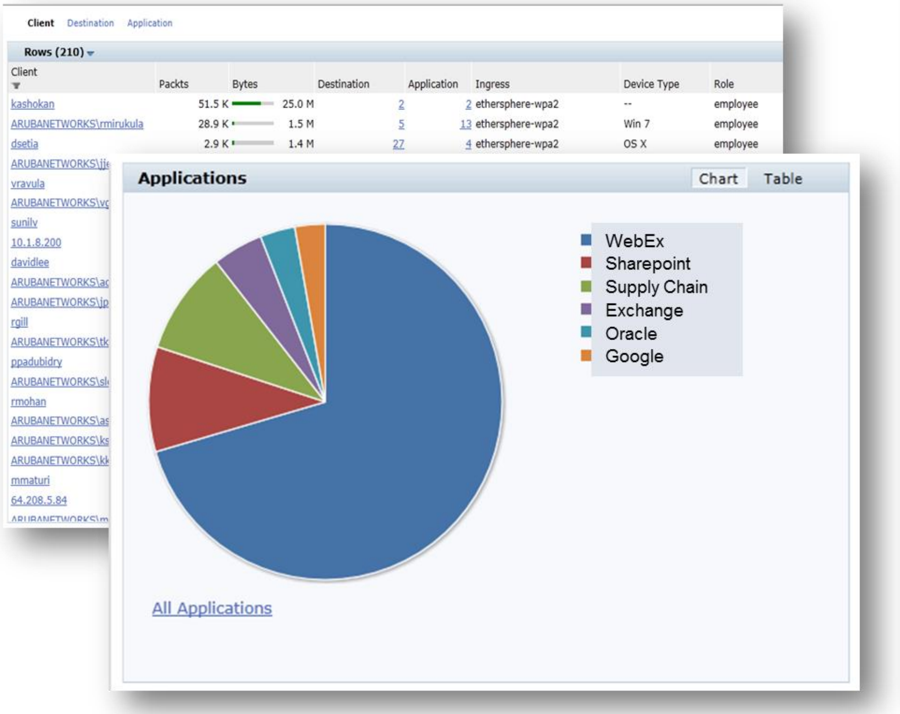
In the old days we built different networks for our different systems. We had a computer network, a voice network, and a video network. We did this so we could segment traffic for security purposes but also so we could prioritize things like video conferencing over someone surfing the web. But that was when our devices were plugged into a wire and we could segment them with a physical switch port or VLAN. But this all changes when the user is on an iPhone.

Consider this:
How do you add a FaceTime session to the Video Conferencing network? FaceTime is an app running on an iOS device. The answer is- you can't. And if you can't prioritize it over someone using Netflix or YouTube, then the performance could be crappy.



Share this eBook!

Application Visibility



Client Destination Application

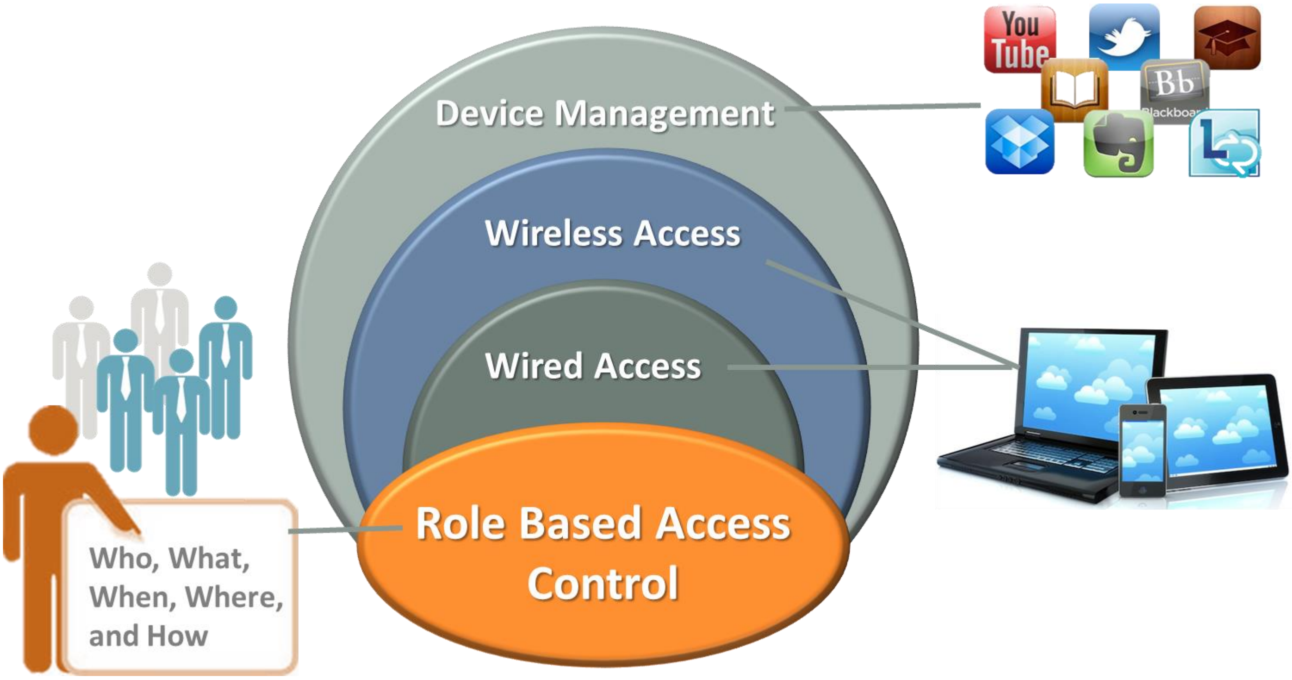
Rows (210)

Client	Packts	Bytes	Destination	Application	Ingress	Device Type	Role
kashokan	51.5 K	25.0 M	2	2	ethersphere-wpa2	--	employee
ARUBANETWORKS\rmirukula	28.9 K	1.5 M	5	13	ethersphere-wpa2	Win 7	employee
dsetia	2.9 K	1.4 M	27	4	ethersphere-wpa2	OS X	employee
ARUBANETWORKS\jje							
vravula							
ARUBANETWORKS\vc							
sunilv							
10.1.8.200							
davidlee							
ARUBANETWORKS\ac							
ARUBANETWORKS\jp							
rgill							
ARUBANETWORKS\tk							
ppadubidry							
ARUBANETWORKS\sl							
rmohan							
ARUBANETWORKS\as							
ARUBANETWORKS\ks							
ARUBANETWORKS\kk							
mmaturi							
64.208.5.84							
ARUBANETWORKS\m							

To support BYOD, we must build networks that can see what apps are running so we can prioritize the stuff like FaceTime over Netflix. Networks have to be software driven and smarter than the traditional segmented networks. We call this Application Visibility and it's a key feature of a network with happy BYOD users.

Security is Foundation for BYOD

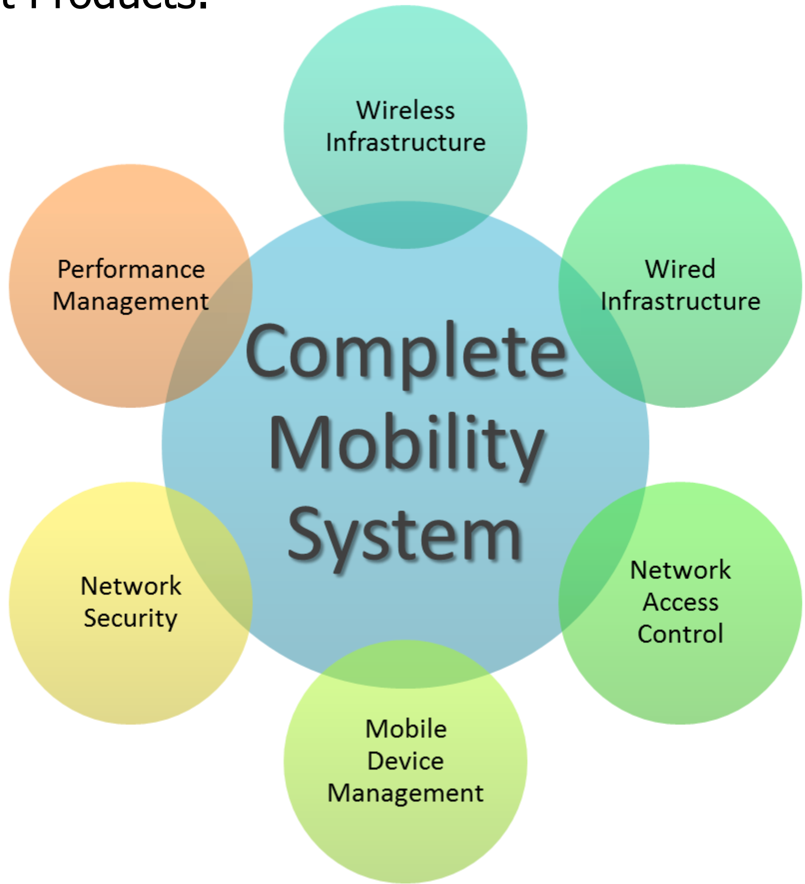
The biggest problem with BYOD and the reason we've never allowed it in the past is of course security. If we did allow someone onto our network with their personal device, we didn't have an effective way to limit what they did on our network.



Security is a big challenge- unless the system is built on what we call "Role Based Access Control". Simply put, it's knowing who, what, when, and how people are connecting to the network, and having the ability to limit their access based upon that profile. Role Based Access Control is the foundation to allow BYOD.

Integrated Systems are the Only Way

Let's think about all of the different parts of network infrastructure required to support BYOD. Wireless networking, wired networking, your firewall and network security systems, server infrastructure….the list goes on and on. They all have to work together. In order to support BYOD you'll need to Think Systems, not Products.



BYOD requires an integrated and systematic approach to design, implementation, and management.

CHAPTER 3

BYOD SOLUTION COMPONENTS

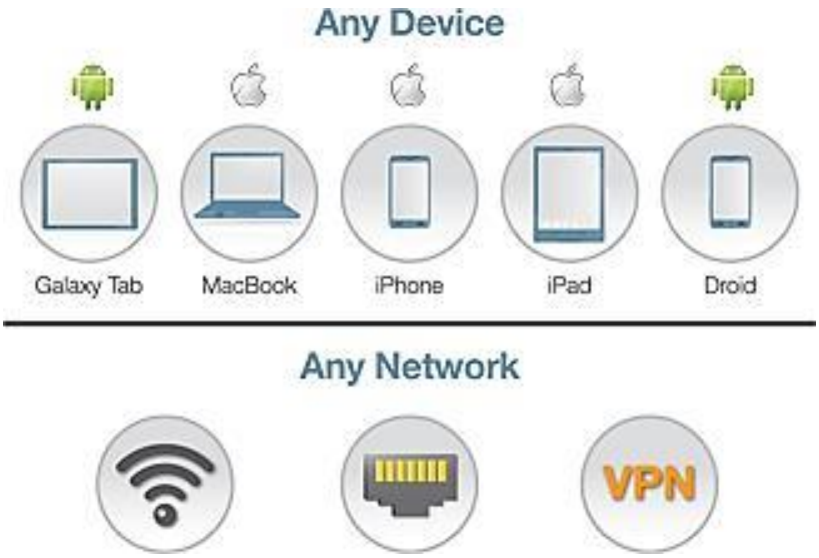
Network Access

This is where the rubber meets the road. This is how users will be allowed to connect to your resources.

There are three ways users can get access to your network:

- Wireless
- Wired
- VPN

Since tablet PCs don't come with a network jack, we're going to focus on building the network to support mobility. We'll start with planning the wireless infrastructure, and then work our way back to the wired infrastructure needed to support it.



Wireless Networking

When it comes to wireless network design there are primarily three things to consider:

1) Coverage- Am I covering the areas where my users will need wireless access? This is a good starting point to look at how many access points will cover a given area. Ideally you'll want to use (or have someone use) RF planning software that shows the predictive coverage of the desired usage area. But don't stop here! Check out #2 and #3.

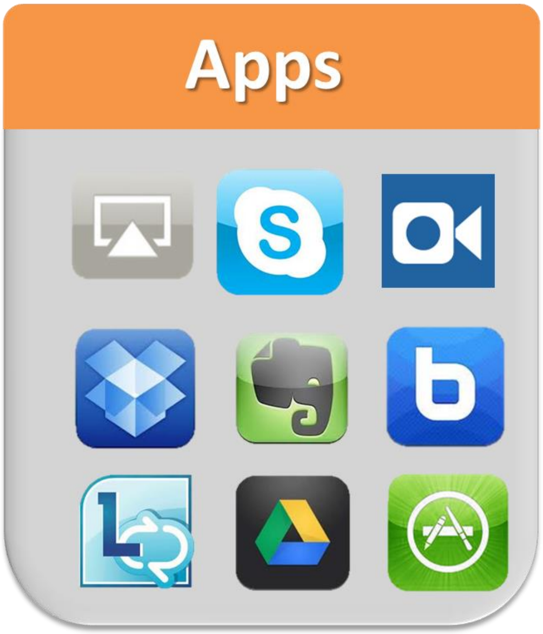
2) Capacity- Do I have enough throughput on the access points in any given area to support my users? This is where most wireless issues happen right here. They fail to take into account how many users will connect to one access point. Access points are a shared medium so when you connect 100 devices to one access point they're slicing the available speeds by 100. If just did a coverage plan, then your users will feel it, if they can even connect.

> **"Networking pros will have to figure how to create infrastructure that makes WLAN a primary way to connect, not just a nice-to-have add-on."** —Forrester

Wireless Networking

3) Performance- Do I have the access points spaced in a way that will be optimal for the devices and the applications that I'm running?

Think about this; a smart phone has 25% the radio strength of a traditional laptop. This simply means that the iPhone needs to be closer to the access point to talk to it than a laptop. To make it more challenging, applications like FaceTime have certain latency requirements. Planning for performance of devices and applications will solve a lot of headaches later.



Wireless Networking

Another way to get into BYOD trouble is to choose the wrong wireless network hardware and software. We can tell you from experience that not all solutions are created equal, and most of them were designed to solve a specific issue.

Here are some features to look for in a wireless solution to solve the BYOD challenge:

- Centralized Management
- Integrated Firewall
- Directory Services Integration
- Layer 7 Visibility
- Spectrum Analysis
- Application, Device, and OS Fingerprinting
- High Capacity Load Balancing
- Ability to adjust channel and power settings in real time
- Scalability
- Ability to communicate with both 2.4 GHz devices and 5 GHz devices
- Real Time Wireless Visibility
- Quality of Service/Application Prioritization
- Redundancy

Wired Networking

Your users are primarily mobile but that doesn't negate the importance of the wired infrastructure! The wired network is backbone of the whole BYOD and wireless network. You're big concern here is to make sure that you're not bottlenecking the wireless users with not enough throughput on the wired network.

For organizations with 1000 or more users, here's what you want to look out for on the wired side:

- Centralized Policy Control for all network access (wired and wireless)
- Integration with your wireless access points & Controllers
- 1 Gigabit Edge Switching
- 10 Gigabit Uplinks from the Edge Switches to the Core Switching
- 10 Gigabit Core Switching
- Switch Stacking capability is preferable.

Network Security

As I stated earlier, security is the most important aspect of a BYOD program. In this section, I'm going to cover two core philosophies in more detail that I mentioned previously in this eBook. But stay with me because this is the section that will deliver you peace of mind.

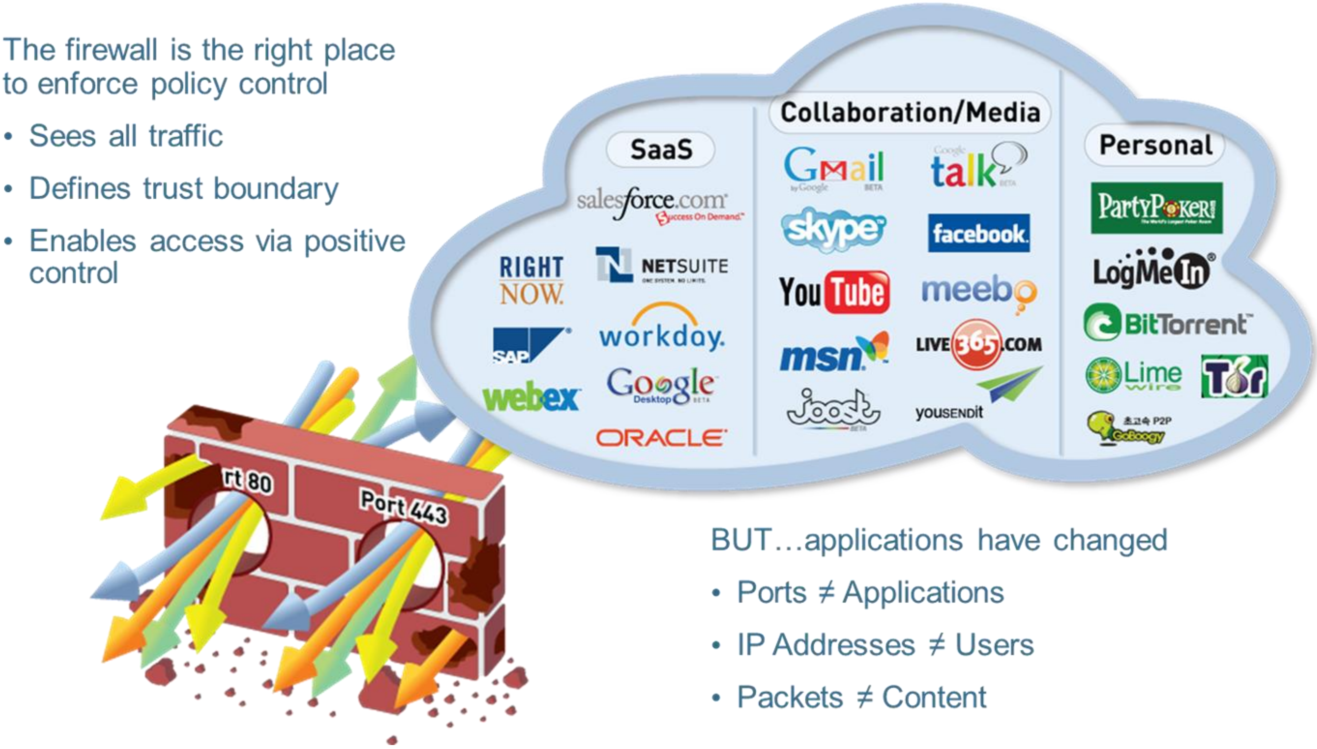
1) Identity Based Security- We mentioned role based access control earlier. Identity based security is the starting point for RBAC. Here's an example of the simple logic using identity based security to deliver RBAC.

- Identify the user- Is this user authorized?
- Validate the device- Is this a registered device?
- Control the access per user- What type of security role should be assigned?
- Classify the traffic- What type of traffic and applications are being used?

Identify
the user
Validate
the device
10110
Classify
the traffic
Control
access per user

2) **Next Generation Network Security-** traditional security products looked at ports, IP Addresses, and packets. BYOD breaks traditional security systems because it introduces issues like peer to peer networking that could be coming from a valid IP address.

Here's how you address network security for the BYOD world:



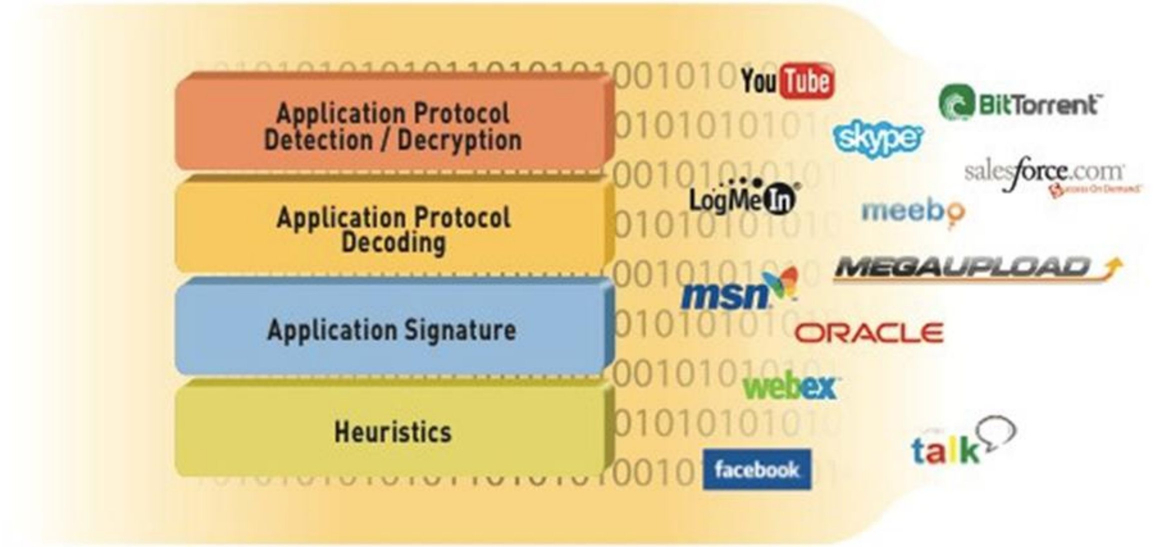
The firewall is the right place to enforce policy control

- Sees all traffic
- Defines trust boundary
- Enables access via positive control

BUT…applications have changed

- Ports ≠ Applications
- IP Addresses ≠ Users
- Packets ≠ Content

- **Application Visibility-** Old firewall technology will group categories such as "Web Services" into one. But application visibility will show you exactly what is being used on your network. You'll see peer to peer, social sharing, business productivity applications, etc. Knowing is half the battle.



- **Application Control-** Now that we can see it, let's lock it down. Application control is more than simply URL filtering, application control gives us flexibility to allow different types of applications based on the user Role. For example: a role for a corporate owned machine might limit FaceBook, but a role for a BYOD device might allow it. The world is yours to control.

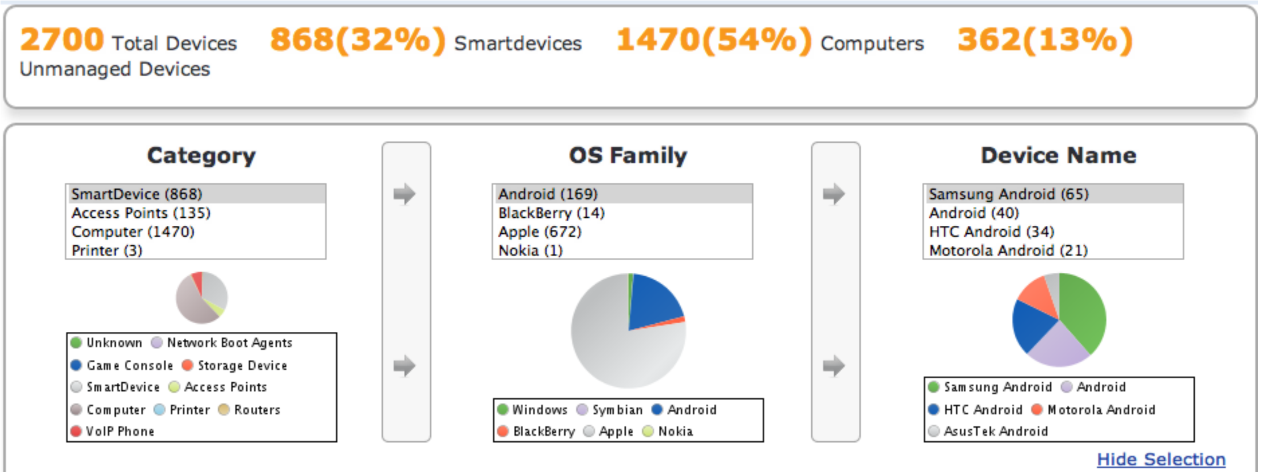
Network Access Control

NAC provides advanced features that when deployed properly, streamline the process of allowing BYOD.

Here are the features you can use to enable BYOD with NAC:

1) Centralized Policy Management- no more having multiple systems to manage your different types of users. NAC provides one place to manage security roles for Corporate Users, Guests, and Contractors.

2) Dashboard Device Profile Views- what types of devices are being used on your wireless network or wired network? Where are they connecting from? You'll need to spot usage statistics and device details to know what network and policy decisions to make in the future.



2700 Total Devices **868(32%)** Smartdevices **1470(54%)** Computers **362(13%)** Unmanaged Devices

Category

SmartDevice (868)
Access Points (135)
Computer (1470)
Printer (3)

OS Family

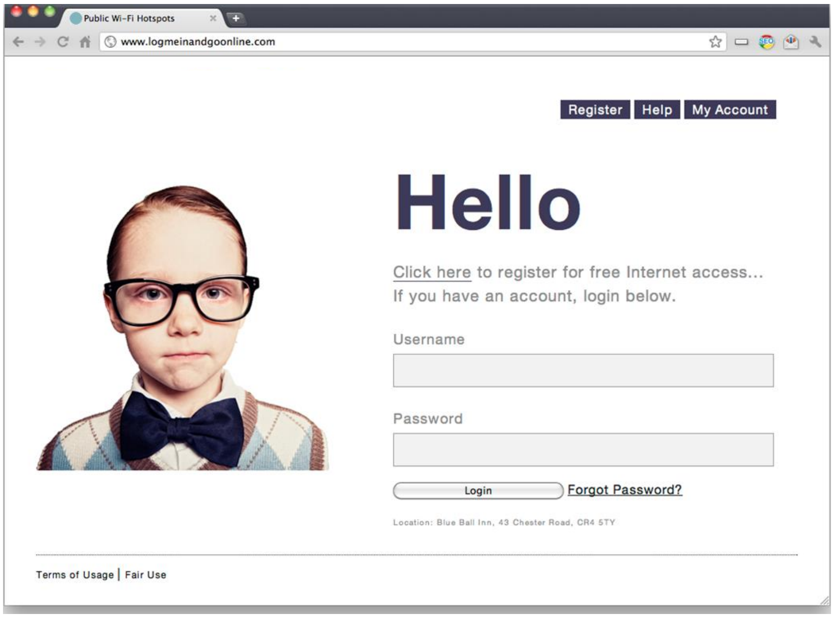
Android (169)
BlackBerry (14)
Apple (672)
Nokia (1)

Device Name

Samsung Android (65)
Android (40)
HTC Android (34)
Motorola Android (21)

● Unknown ● Network Boot Agents
● Game Console ● Storage Device
● SmartDevice ● Access Points
● Computer ● Printer ● Routers
● VoIP Phone
● Windows ● Symbian ● Android
● BlackBerry ● Apple ● Nokia
● Samsung Android ● Android
● HTC Android ● Motorola Android
● AsusTek Android
Hide Selection

3) Self-Registration of BYOD Devices- In Educational Technology, the average users has 3-5 mobile devices (iPad, Android Phone, Netbook, Gaming System, etc.). In the corporate environment you can figure 2.5 devices per person…which means putting your hands on each device isn't feasible. Device Registration for BYOD should allow users to provision their own devices.



Hello

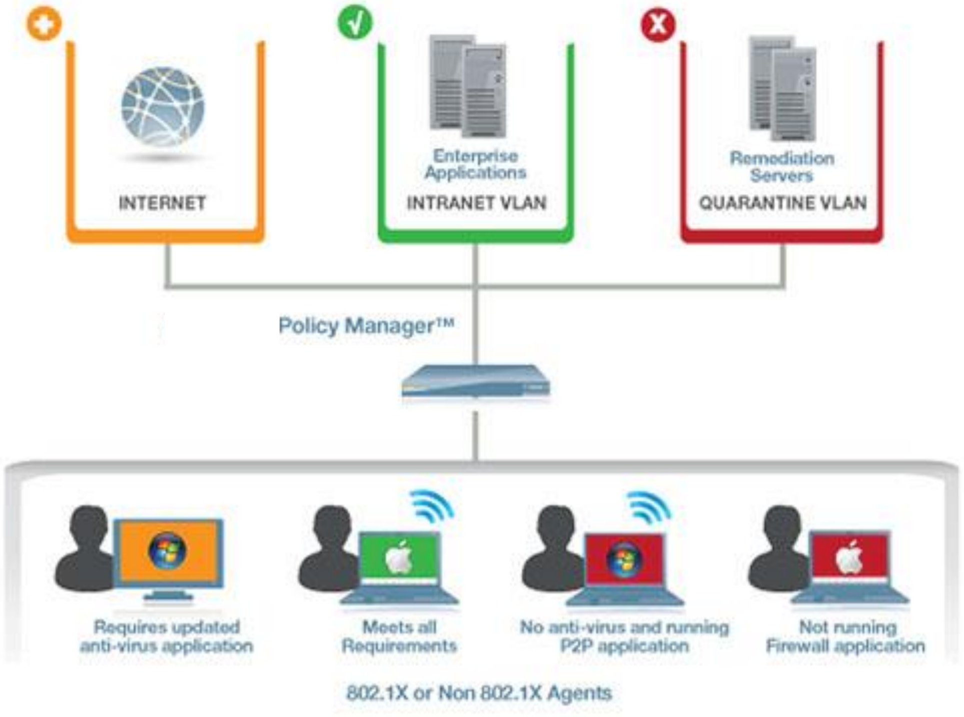
Click here to register for free Internet access...
If you have an account, login below.

Location: Blue Ball Inn, 43 Chester Road, CR4 5TY

4) Secure Guest Registration & Access- Thinking about just handing out a pre-shared key for guest access? If you do, the password will spread like wildfire to other guests and even employees. Today's environment requires that you provide SECURE guest access. This means the user is allowed to register with a captive portal and the system will not provide a password to be shared around the office.

5) Remote Registration & Auto-provisioning of devices- How awesome would it be to email a college student BEFORE she gets to campus to let her register and auto-provision her device? You can do this today. The days of the freshman IT workshop day are over. Let them show up on campus ready to roll.

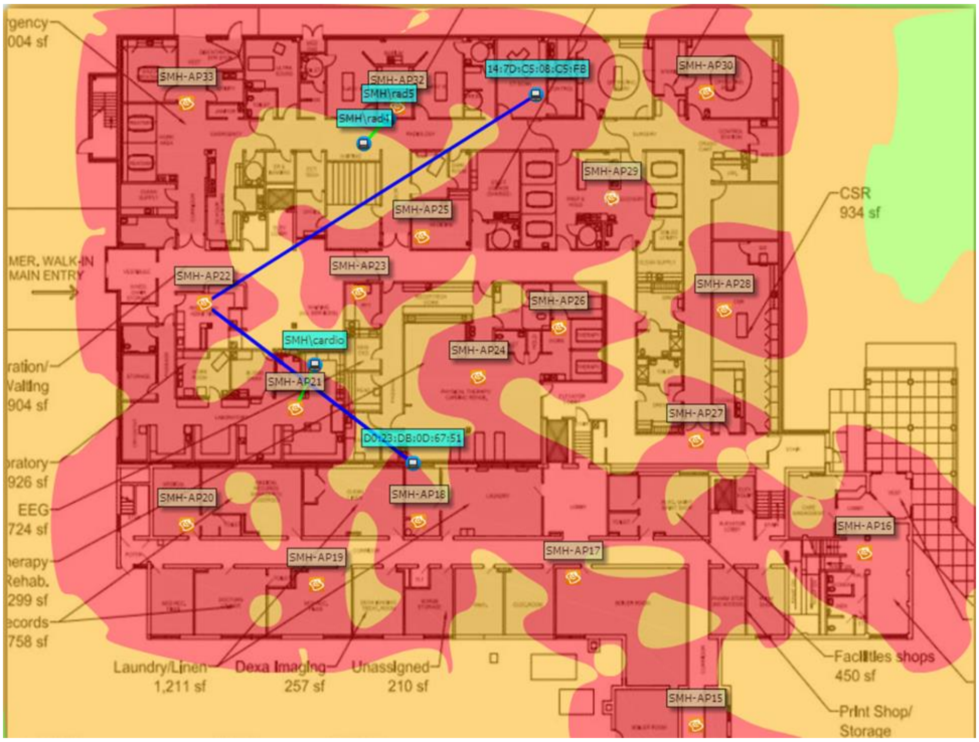
6) Device Health Checks- NAC can run a compliance check on the end user device to ensure that they have important things like anti-virus or a minimum software specification.


INTERNET
Enterprise Applications
INTRANET VLAN
Remediation Servers
QUARANTINE VLAN
Policy Manager™
Requires updated anti-virus application
Meets all Requirements
No anti-virus and running P2P application
Not running Firewall application
802.1X or Non 802.1X Agents

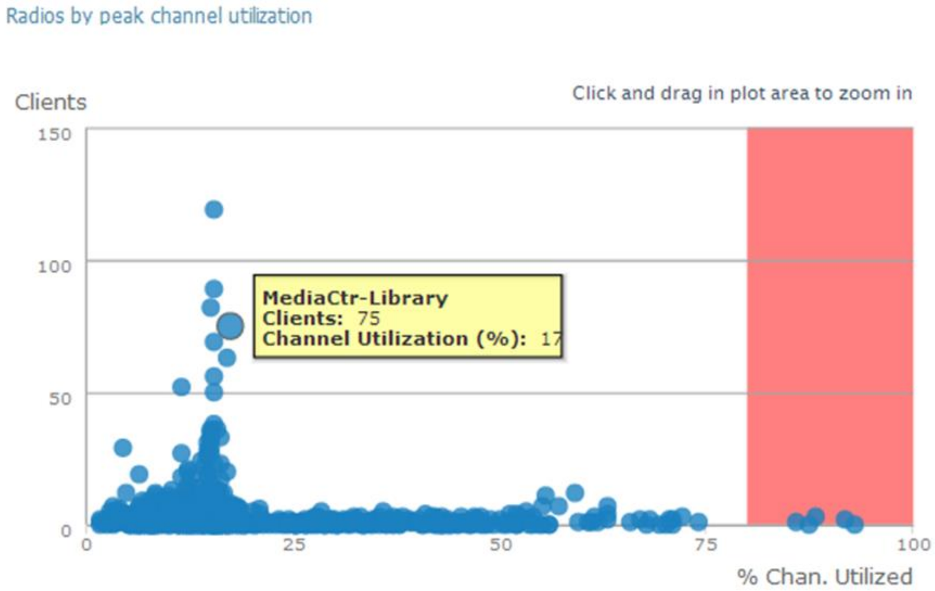
Network Management

Your users are mobile (I really hope we've established that by now), but most of our networking tools were built to manage wired switch ports. Rather than tell you about them, I'm going to show you some examples of the right tools for the job. Here's what Network Management tools you need to have to manage mobile users:

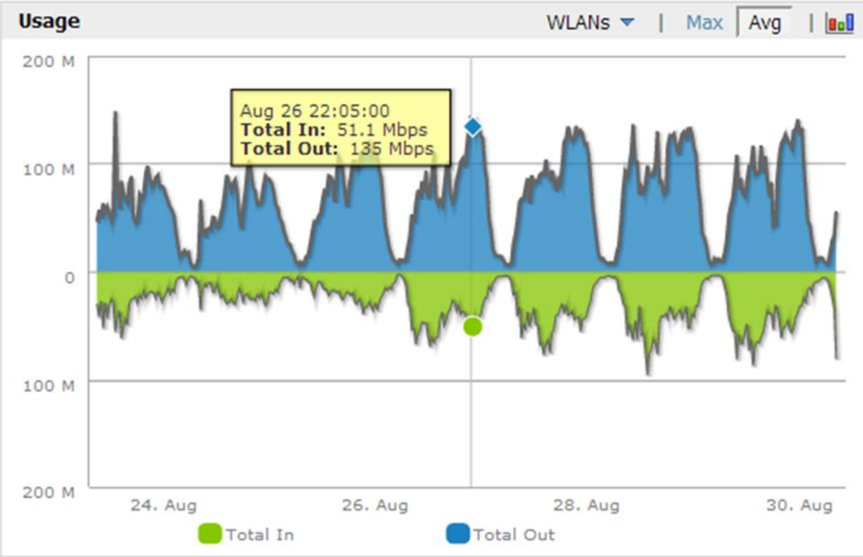
1) Real Time Wireless Visibility-If you can't see the RF you'll be flying blind. Network Management should show you the signal strength, signal to noise ratios, and devices that are connecting to your network.



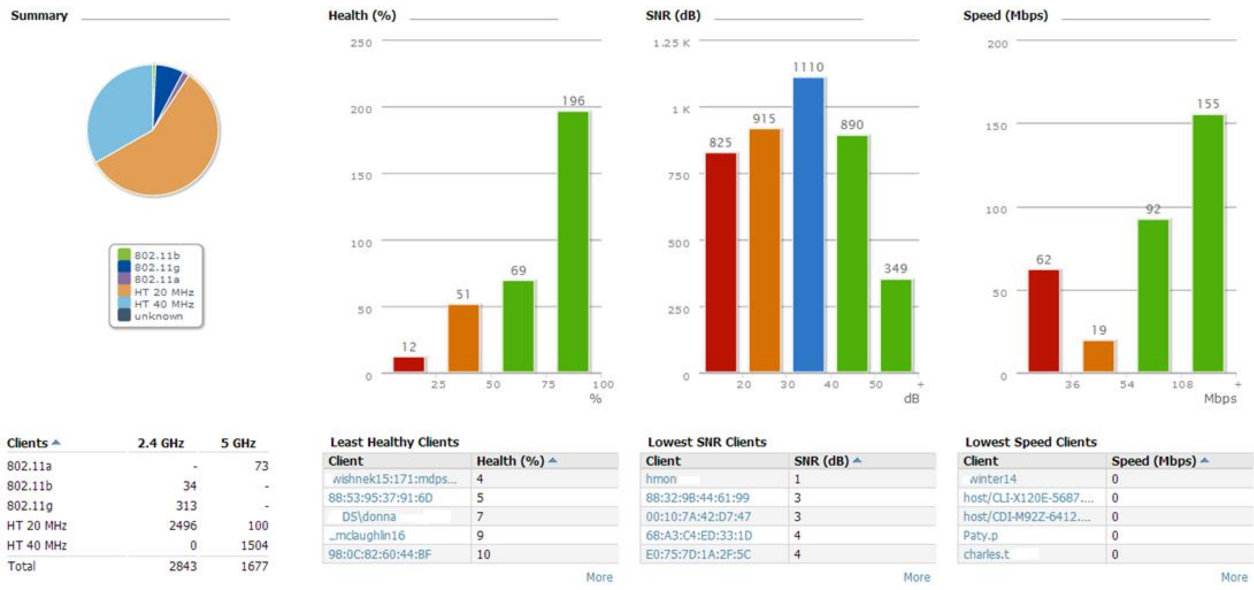
2) Proactive Alerting to Trends-This is the ability to see things on the network that could cause issues down the road. Things to watch out for are over utilized channels or access points.



3) Usage Reporting-It's important to know how much bandwidth is being consumed at any given time, and by whom.



4) Real Time System Health-Performance is predictable. Each application and device has requirements for performance. This screen will show you where your potential issues are.



Clients ▲	2.4 GHz	5 GHz
802.11a	-	73
802.11b	34	-
802.11g	313	-
HT 20 MHz	2496	100
HT 40 MHz	0	1504
Total	2843	1677

Least Healthy Clients

Client	Health (%) ▲
wishnek15:171:mdps...	4
88:53:95:37:91:6D	5
DS\donna	7
_mclaughlin16	9
98:0C:82:60:44:BF	10

More

Lowest SNR Clients

Client	SNR (dB) ▲
hmon	1
88:32:9B:44:61:99	3
00:10:7A:42:D7:47	3
68:A3:C4:ED:33:1D	4
E0:75:7D:1A:2F:5C	4

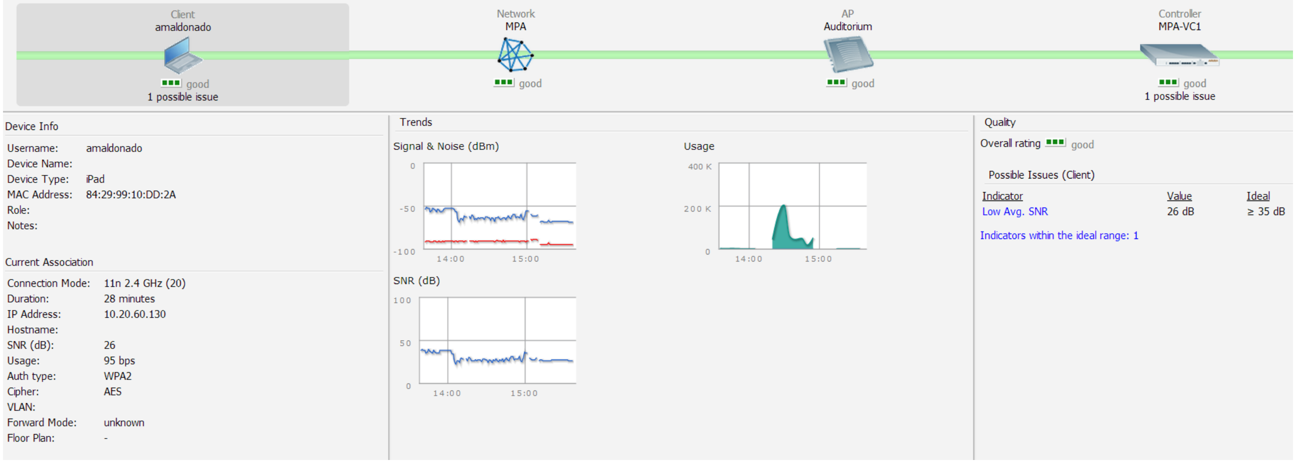
More

Lowest Speed Clients

Client	Speed (Mbps) ▲
winter14	0
host/CLI-X120E-5687....	0
host/CDI-M92Z-6412....	0
Paty.p	0
charles.t	0

More

5) Troubleshooting- Quickly see the status of issues and point to how to solve them.



Device Info

Username:	amaldonado
Device Name:	
Device Type:	iPad
MAC Address:	84:29:99:10:DD:2A
Role:	
Notes:	

Current Association

Connection Mode:	11n 2.4 GHz (20)
Duration:	28 minutes
IP Address:	10.20.60.130
Hostname:	
SNR (dB):	26
Usage:	95 bps
Auth type:	WPA2
Cipher:	AES
VLAN:	
Forward Mode:	unknown
Floor Plan:	-

Quality

Overall rating ■■■ good

Possible Issues (Client)

Indicator	Value	Ideal
Low Avg. SNR	26 dB	≥ 35 dB

Indicators within the ideal range: 1

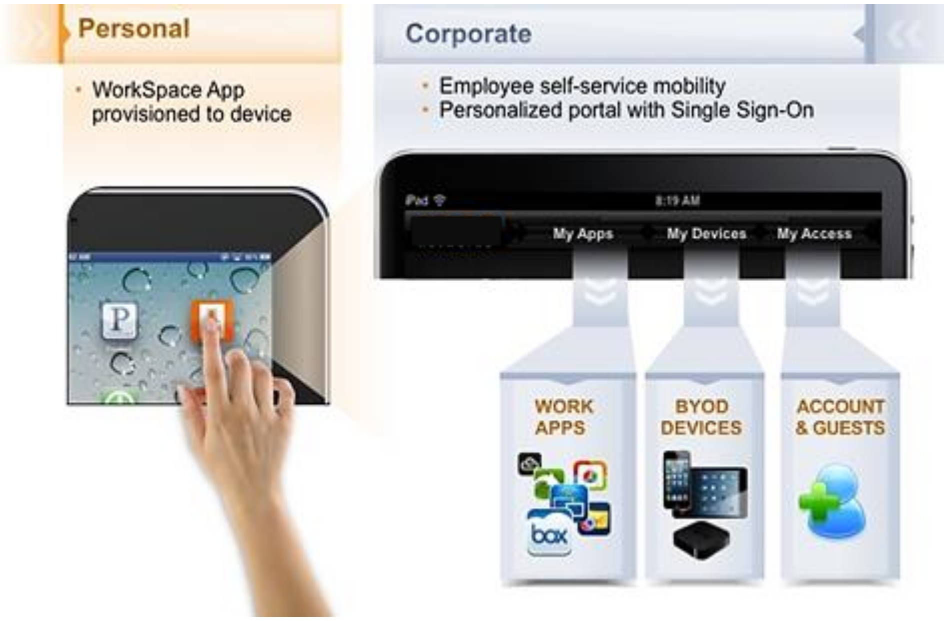
Share this eBook!

SecurEdgeNetworks.com

Mobile Device Management

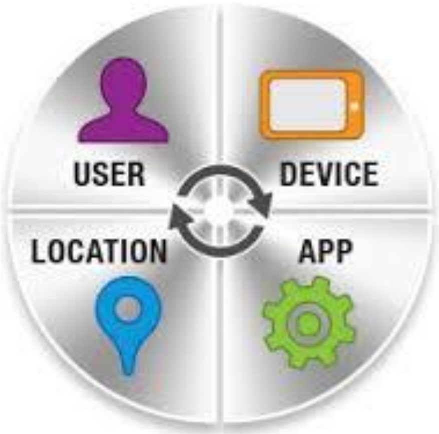
There are hundreds (literally) of MDM vendors that solve the challenge in different ways. So it's best to start with what you're trying to accomplish with MDM and specifically MDM for BYOD.

1) **Segmentation of personal and employee data-** MDM should "containerize" work applications from personal applications.


Personal
WorkSpace App provisioned to device
Corporate
Employee self-service mobility
Personalized portal with Single Sign-On
iPad
8:19 AM
My Apps
My Devices
My Access
WORK APPS
box
BYOD DEVICES
ACCOUNT & GUESTS

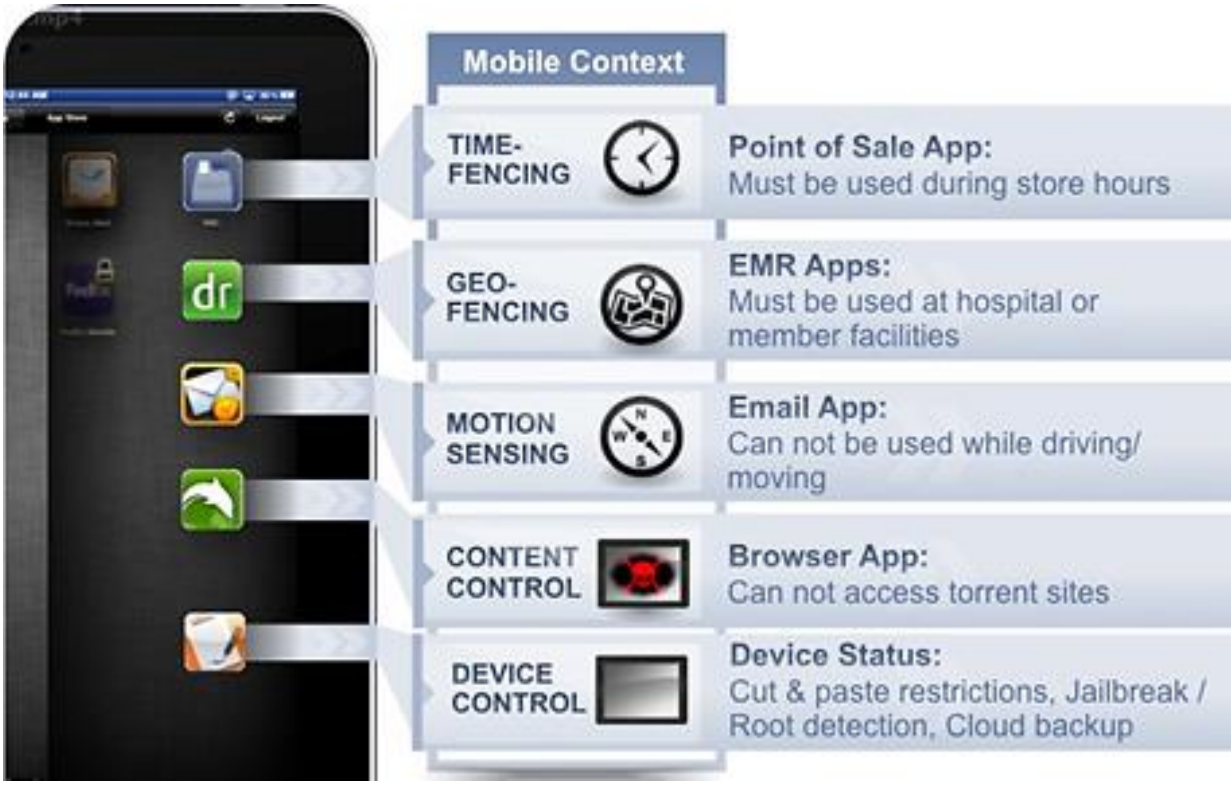
2) **Mobile Security-** The corporate side of the device needs to be encrypted and passcode protected. If an employee leaves or the device goes missing, you should be able to remotely wipe the sensitive data from the device.

3) Application Management- This is your centralized control for all applications you want to want to provide to your users based upon the user role..



4) Application Delivery- When a user logs into the corporate side of their device, MDM should deliver the applications that are loaded for each user profile

5) **Application Control** – Now that you've delivered the right applications. You'll want to control what apps are used in which usage case. This can get pretty granular, see the graph for some ideas.



Mobile Context	
TIME-FENCING	**Point of Sale App:** Must be used during store hours
GEO-FENCING	**EMR Apps:** Must be used at hospital or member facilities
MOTION SENSING	**Email App:** Can not be used while driving/ moving
CONTENT CONTROL	**Browser App:** Can not access torrent sites
DEVICE CONTROL	**Device Status:** Cut & paste restrictions, Jailbreak / Root detection, Cloud backup

CHAPTER 3

HOW WE CAN HELP

SecurEdge Networks

Who We Are

SecurEdge Networks is a specialty IT Solutions Provider focused on mobility and security. We've worked with hundreds of organizations to implement secure BYOD programs.

How we Help

Analyze
Plan
Deploy
Support

Analyze: A thorough discovery of your current environment and your objectives.

Plan: Our design recommendations are based upon your end goal, as well as industry and solution specific knowledge.

Deploy: We can deploy BYOD solutions turnkey or we can work alongside your team to provide guidance on best practices.

Support: We offer managed services and custom support services to ensure the success of your BYOD program.

Get Started With BYOD

SecurEdge has helped hundreds of organizations implement BYOD programs. Register here to talk to one of our mobility consultants about industry best practices to support BYOD.