Five Steps to a Faster, Smarter Wireless LAN

ARUBA networks

What Drives our Market?

ARUBA networks

Mobility Effect #1 – More Mobile Devices

- **2013: More mobile devices than people**
- **2017: 19x increase in mobile data usage**

10 Exabytes. 45% Offloaded to Wi-Fi

Mobility Effect #2 – Cloud Evolution

Local

Cloud Based

- 2012: Public cloud projects surpassed $100B+
- Cloud traffic comes from mobile devices: 70% more in 2013.

Mobility Effect #3 –
Bring Your Own

- **Avg 3.3 connected devices/employee (by 2014)**
- **40% devices accessing business apps are employee owned**
- **Over half the networks were breached in 2012 due to personal devices**

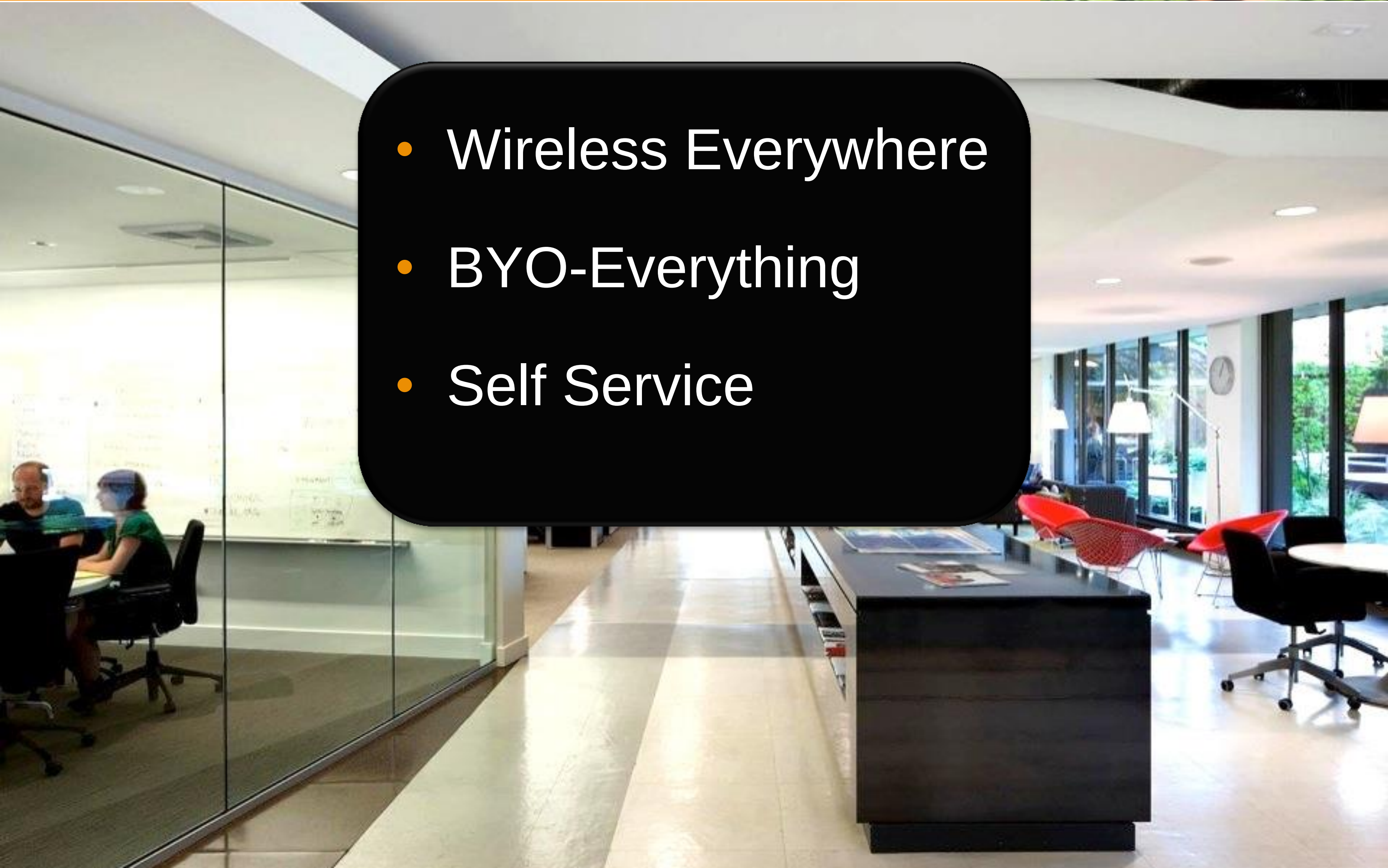
Mobility Effect #4 – There's An App for Everything

Corp/ Business Apps

Custom Apps

Personal Apps

Attributes of Next Generation Workplace



- Wireless Everywhere
- BYO-Everything
- Self Service

Five Steps to a Faster, Smarter WLAN

Session One: Building Your Wireless LAN

- Step 1: Providing faster and smarter Wi-Fi with 802.11ac
- Step 2: Planning your mobility network architecture

Break

Session Two: Supporting Your Users & Their Devices

- Step 3: Smart policy creation and BYOD enforcement
- Step 4: Device and app management
- Step 5: Extending mobile services to visitors and customers

Step 1

Providing faster and smarter Wi-Fi with 802.11ac

Why 11ac ? - Capacity & Bandwidth

More devices

- Average 3 devices per user
- Smartphone, tablets, laptops, ultrabooks

More applications per device

- Average 40 apps per mobile device
- Estimates > 300 billion app downloads by 2016

More traffic

- HD mobile video, video telepresence, collaboration programs
- Tablet traffic ~ 3.4x greater than smartphone traffic

Shift in W-Fi Usage

- Pervasive, primary access
- Mission critical
- Multimedia – Voice, IPTV, older legacy media transport systems (i.e. cable TV)

802.11ac Technology Overview

Think of 11ac as an extension of 11n

11n specification:

- 2.4 and 5 GHz
- 40 MHz channels
- 64-QAM modulation
- Up to 4 streams
- Explicit & implicit beam forming
- Backwards compatible w/ 11a/b/g

11ac introduces

- 5 GHz only
- Wider channels (80 MHz &160 MHz)
- Better modulation (256-QAM)
- Additional streams (up to 8)
- Beam forming (explicit)
- Backwards compatible w/ 11a/b/g/n
  - Refer to http://www.802-11.ac.net for in-depth information

Wider Channels

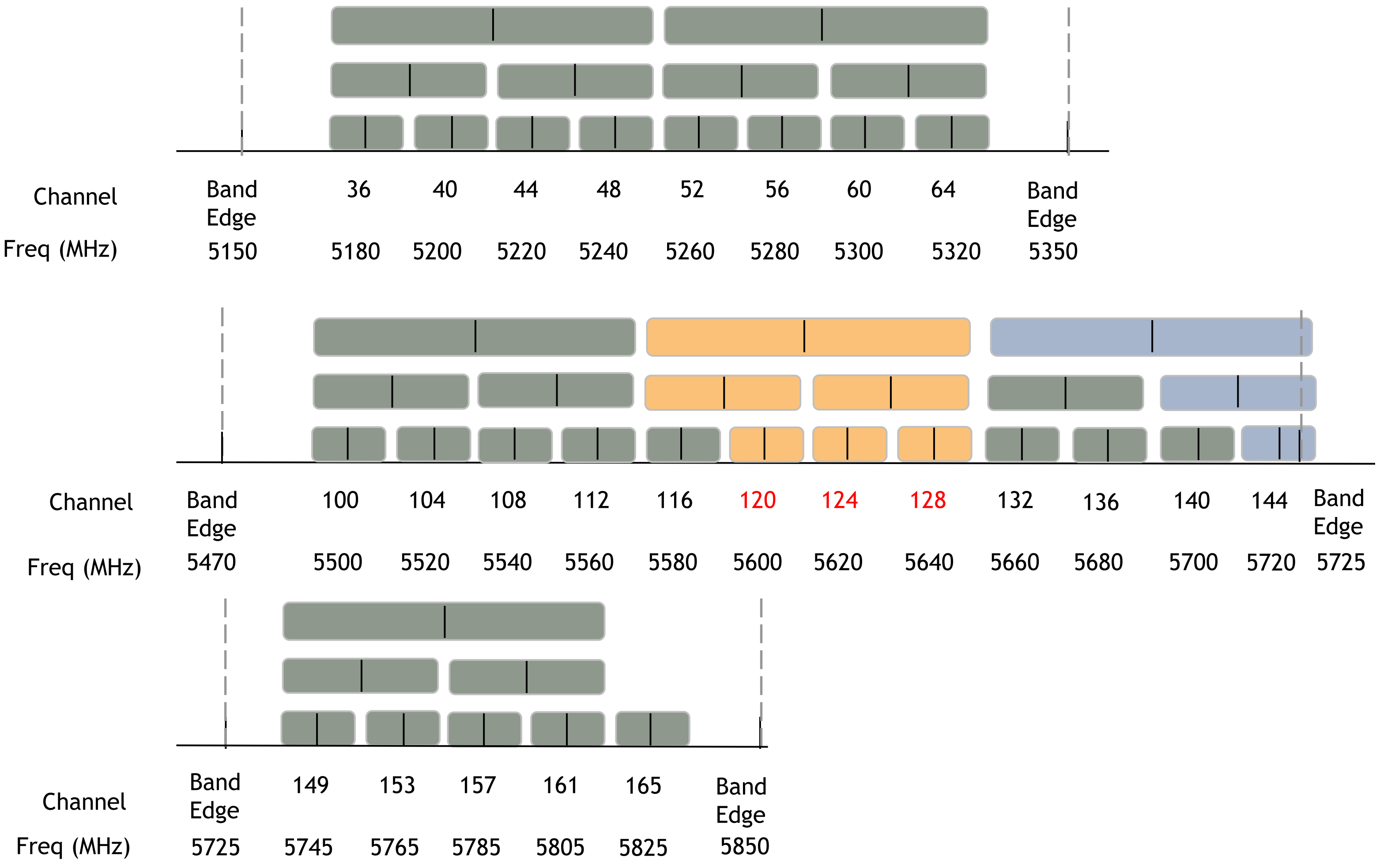
80 MHz channel widths supported in first generation

- 80 MHz is 4.5x faster than 20 MHz
- 80 MHz is contiguous
- Per packet dynamic channel width decisions

Future releases will allow for 160 MHz channel widths

- 160 MHz can be either contiguous or in two non-contiguous 80 MHz slices

802.11ac Channels (FCC)



UNII I and UNII II
2x 80 MHz
4x 40 MHz
8x 20 MHz

UNII II extended
3x 80 MHz
6x 40 MHz
12x 20 MHz

US UNII III
1x 80 MHz
2x 40 MHz
5x 20 MHz

More Spatial Streams

Spec allows up to 8 spatial streams (4 max in 802.11n)

- 8SS performance will only be possible where both devices have 8 antennas
- Space, power and cost constraints will dictate the number of streams supported by the client
  - Smart phones – 1 stream
  - Tablets – 2 stream
  - Laptops – 2 or 3 streams
- Speed of connection is decided by the device with the lowest number of streams.

Adding spatial streams increases throughput proportionally.

- Assuming multipath conditions are favorable:
  - Two streams offer double the throughput of a single stream
  - Eight streams increase throughput eight-fold

AP Throughput > 1Gbps

"How fast can I go?"

- Simple question with very complicated answer
- Depends on many factors
  - Device type
  - Distance
  - Signal to Noise Ratio (SNR)
  - Access Point configuration
    - Channel width
    - Number of Spatial Streams
    - Short/long guard intervals
    - Link aggregation
- Your mileage WILL vary

Max Data Rates per Client Type

Channel bandwidth	Transmit - Receive antennas	Typical client scenario	Max individual link rate	Max aggregate link rate
40 MHz	3x3	PC	606 Mbps	606 Mbps
80 MHz	1x1	Smartphone	433 Mbps	433 Mbps
80 MHz	2x2	Tablet, PC	867 Mbps	867 Mbps
80 MHz	3x3	PC	1300 MBPS	1300 MBPS
160 MHz	1x1	Smartphone	867 Mbps	867 Mbps
160 MHz	2x2	Tablet, PC	1.73 Gbps	1.73 Gbps
160 MHz	4x Tx AP, 4 clients of 1x Rx	Multiple smartphones	867 Mbps per client	3.47 Gbps
160 MHz	8x Tx AP, 4 clients with total of 8x Rx	Digital TV, set-top box, tablet, PC, smartphone	867 Mbps to two 1x clients 1.73 Gbps to one 2x client 3.47 Gbps to one 4x client	6.93 Gbps

11ac Clients are Already Here!

11ac Clients

- Samsung Galaxy S4 (1x1:1 11ac)
  - 20 million units as of July 5th
- HTC One (1x1:1 11ac)
  - 5 million sold in first 45 days
- 2013 MacBook Air (2x2:2 11ac)
- USB dongles (2x2:2 11ac)
  - Look for USB 3.0

No significant impact on client battery life

Pros and Cons of 802.11ac Spec

Pros

1. APs can accommodate more users/devices
   - Increased capacity
2. Standards based Explicit Beam-forming increases SNR
   - Higher data rates over longer distances
3. 256-QAM
   - Increased throughput at high SNRs
   - Improved modulation and coding techniques
4. Multi-User MIMO (future generations)
   - Improved utilization of RF capacity
5. Use of 5 GHz spectrum
   - More non-overlapping channels
   - Quieter RF environment

Pros and Cons of 802.11ac

Cons

1. Hardware update required to support 802.11ac
   - Some features will not be available on legacy devices

2. 802.3at (PoE+) is required to attain full benefit of 802.11ac
   - 802.3af (PoE) can be used on the AP-22x, but it will limit the full features and functionality available with 802.11ac

Planning for .11ac migration

1. ***RF bands (2.4 GHz, 5 GHz)?***
2. ***Channel width per band (20 vs. 40 vs. 80Mhz)?***
3. ***Apps (Voice? MC Video?) now and in the future***
4. ***Real-time location services (RTLS)?***
5. ***Devices per user?***
6. ***Max devices per AP?***
7. ***Wired network capacity & power?***
8. ***Accessible floor plan images?***
9. ***DFS?***

Purpose-built Aruba 220 Series

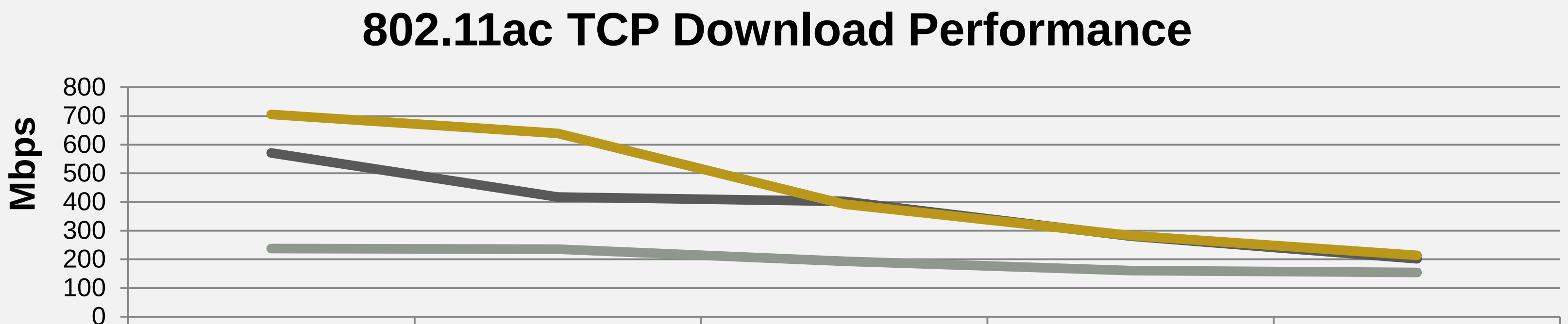
Controller-managed &
Controllerless

- **3x3:3 Dual Radio**
  - 5GHz 11ac: up to 1.3Gbps
  - 2.4GHz 11n: up to 450Mbps (600Mbps with Broadcom clients)
- **2x GE link aggregation**
  - Enabling >1Gbps TCP throughput
- **Operates with 802.3af, requires 802.3at for full functionality**

AP-225 Purpose-built = No Design Compromises

Powerful CPU & memory	Custom antenna design	Smaller & lighter	Cost effective
Higher density	Better RF coverage	Easier to install	$1,295

802.11ac TCP Download – 214 Mbps at 120 feet



	15ft	30ft	75ft	100ft	120ft
1SS	238	235	193	161	154
2SS	572	417	402	281	202
3SS	705	640	393	283	214

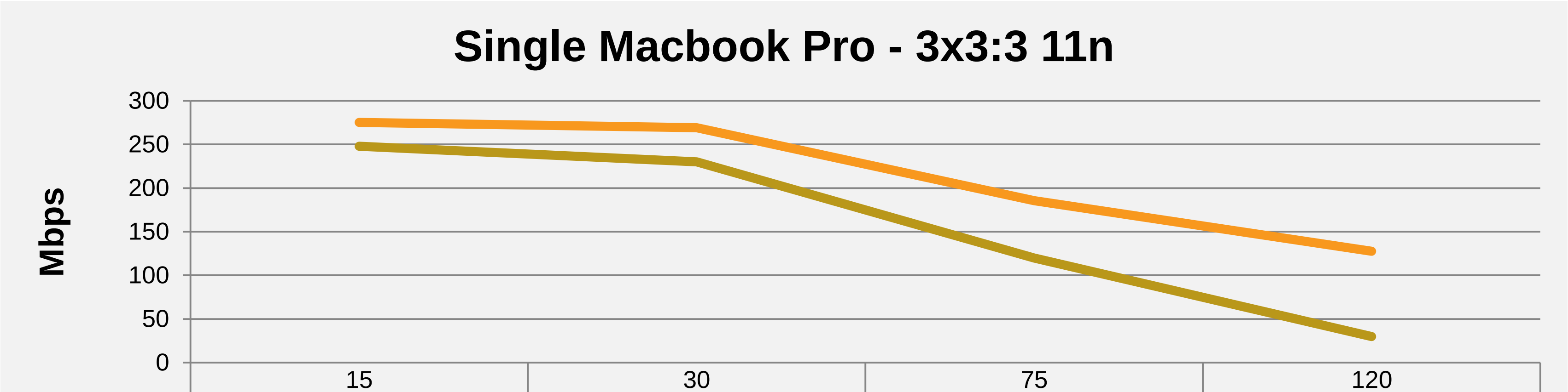
Distance from AP in feet

Test Clients: Windows 7 Laptop with 3 stream 802.11ac radio, Macbook Air with 2 stream 802.11ac client and Samsung Galaxy S4 smartphone with 1SS

Test Goal: Test TCP download performance at increasing distance from AP for devices with varying capabilities

Test Result: Aruba AP-225 delivers peak performance of 705 Mbps. Even at 120ft, the clients gets upto 214Mbps throughput

802.11n TCP Download: AP-225 Delivers 325% More



	15	30	75	120
AP-225	275	269	186	128
AP-135	248	230	120	30

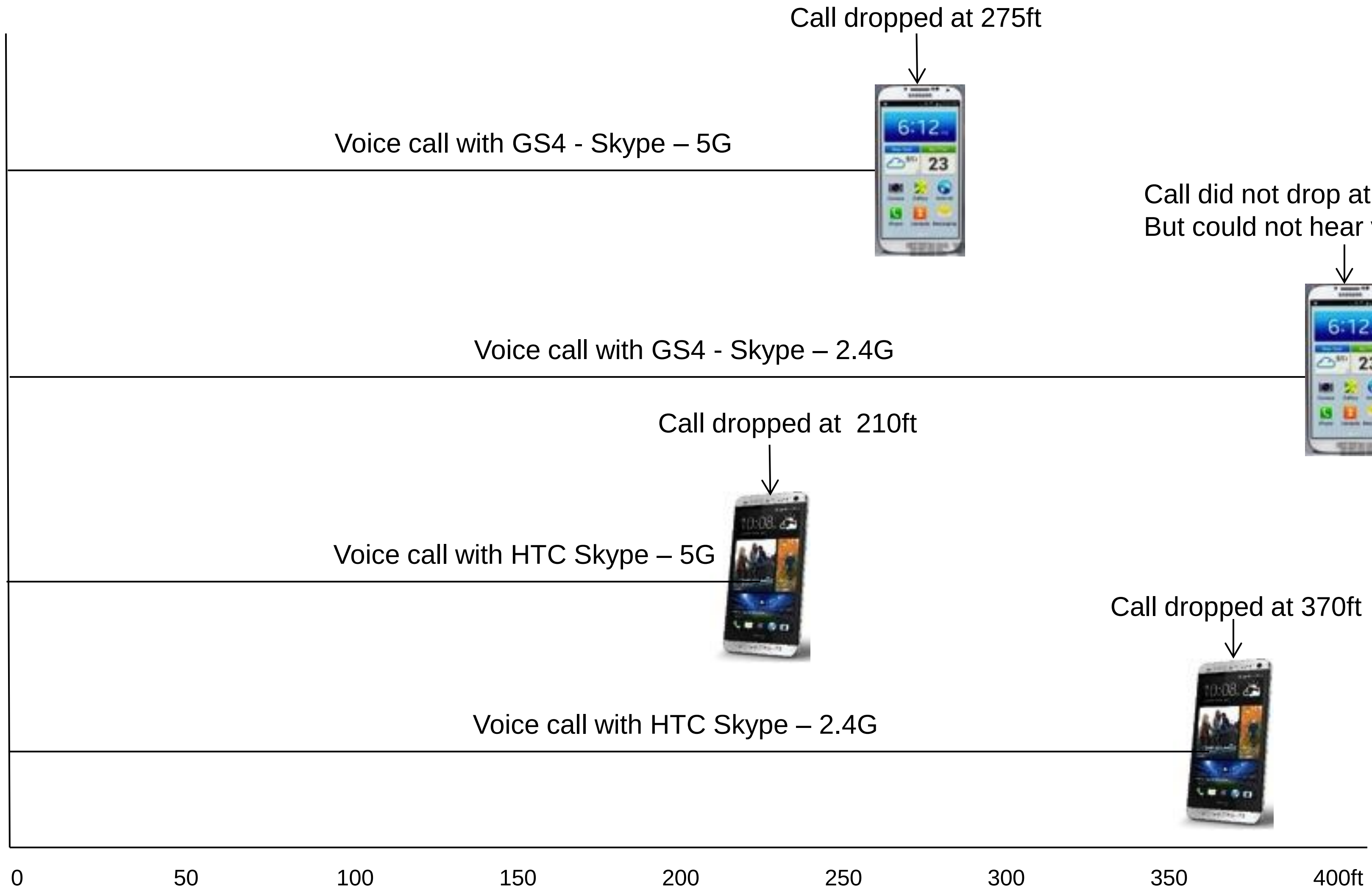
Distance from AP (ft)

Test Client: MacbookPro with 3 stream 802.11n radio

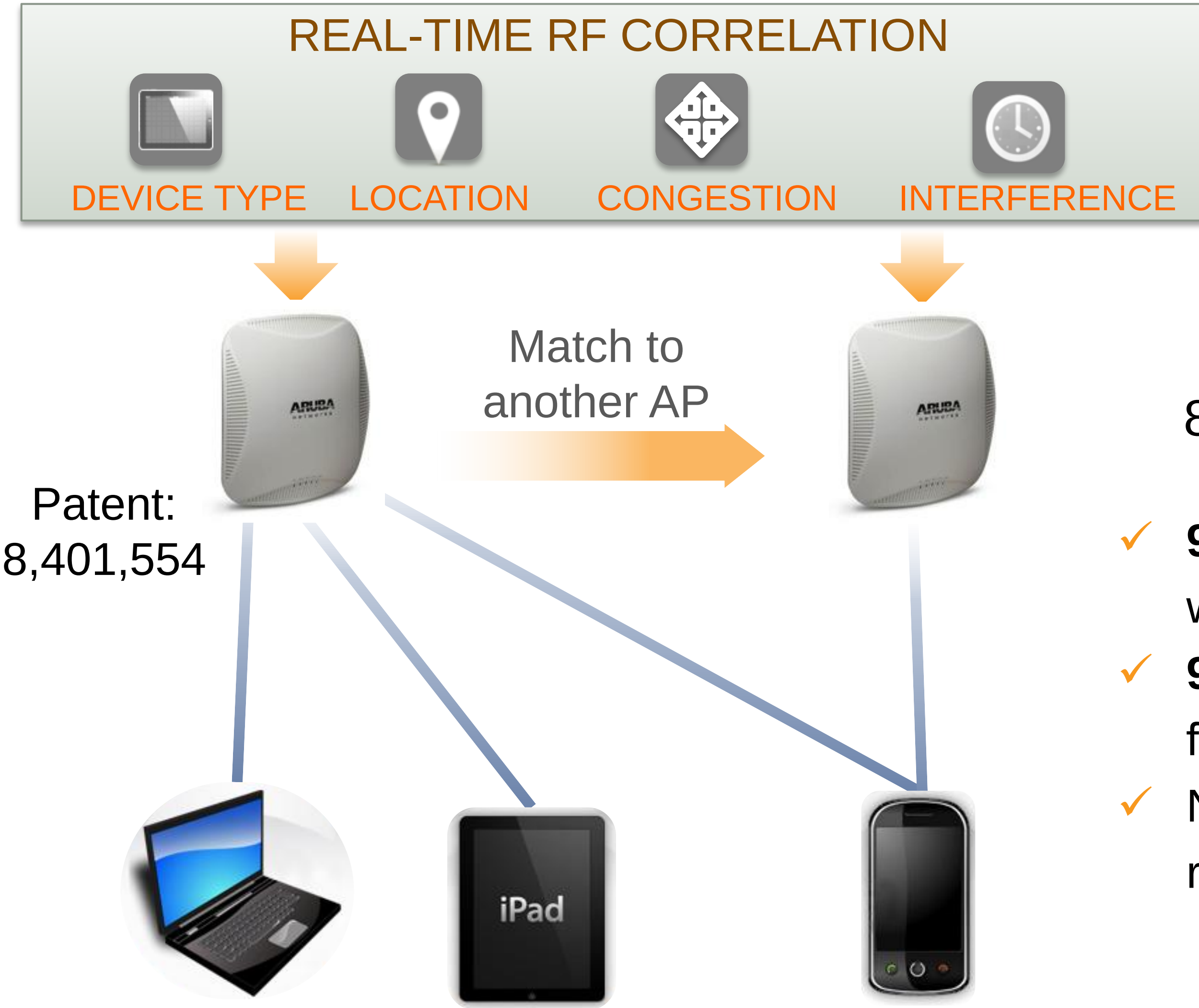
Test Goal: Test TCP download performance at increasing distance from AP to see if 11n client performance is improved on 11ac Access Point

Test Result: Aruba AP-225 delivers upto 325% improved performance for 11n clients compared to 802.11n access points

802.11ac Voice Performance – Almost 400ft Range



ClientMatch™ Enables 802.11ac Wi-Fi

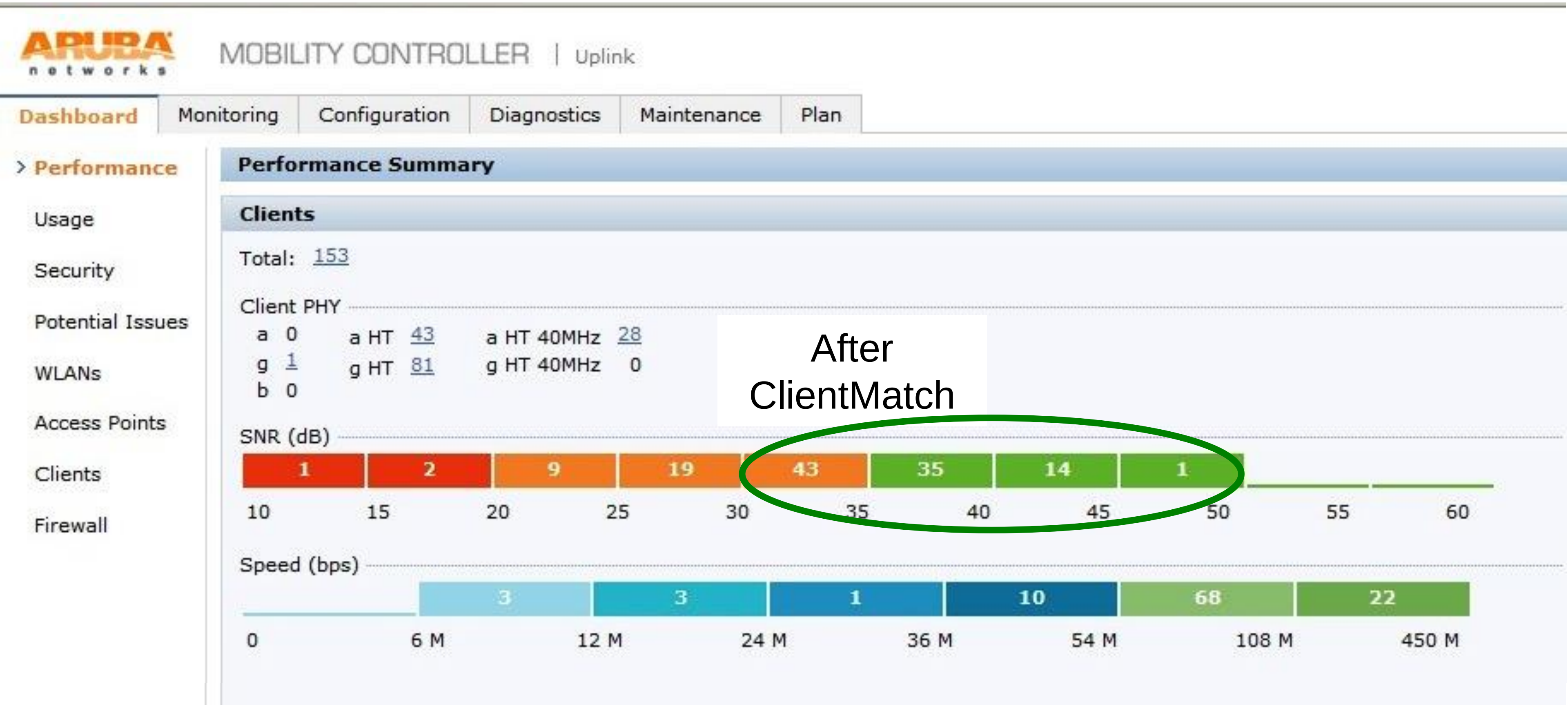


Patent: 8,401,554

Enables use of 802.11ac Wi-Fi rates

- ✓ **98%** of mobile devices with higher signal quality
- ✓ **94%** better performance for "sticky" clients
- ✓ No client-side software required

Client Health Visibility



Demos

Demo 1 – RF Capacity

What you will see:

- AP distribution by channel utilization
- Channel utilization for every AP radio
- Drill down to an AP with high utilization
  - Identify root cause
- Drill down to an AP with low or less utilization
  - Show why this AP is in “green zone”

Why it matters

- Helps identify areas requiring additional capacity
- Identify areas that will benefit with 11ac upgrade

Demo 2 – RF Performance and ClientMatch

What you will see:

- Overall client health
- Drill down to unhealthy client
  - Identify root cause
- Drill down to healthy client
  - See ClientMatch in action

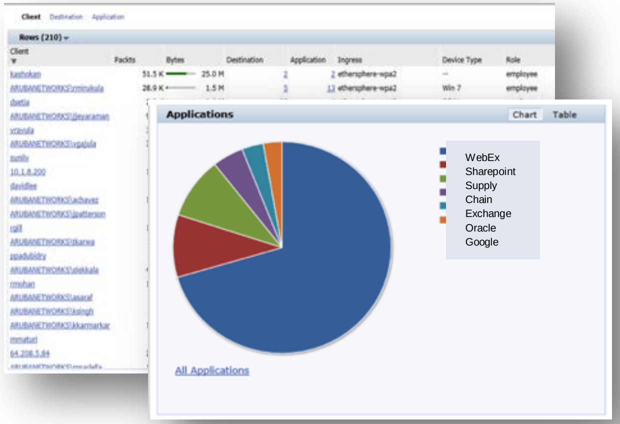
Why it matters:

- Single client with poor performance impacts entire network performance
- Helps identify potential design changes to boost performance

Demo 3: Aruba AppRF Technology

What You will see:

- App usage dashboard
- Identify URL traffic via DNS resolution
- Heuristics and ALGs to fingerprint UC apps
- Prioritize business traffic over personal
- Wired/wireless/VPN



Why it Matters

- Identify web services and UC traffic, and prioritize
- 75% better UC performance
- 30% more video on iPads
- 11x faster mobile apps

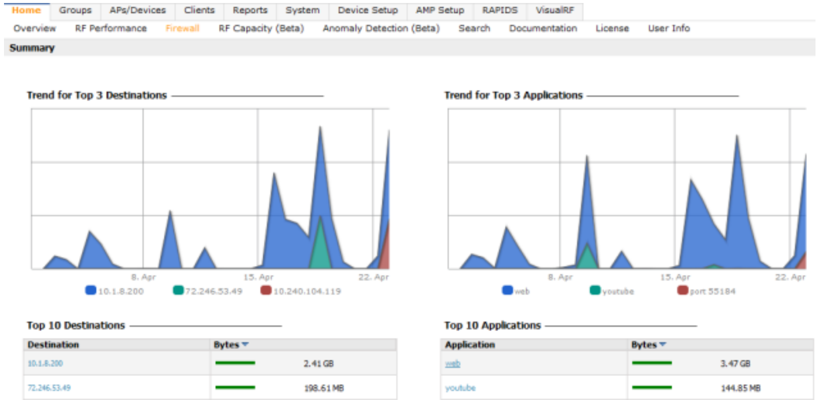
Demo 4: AirWave AppRF

What You will see:

- You can see that you will be able to get historical data of AppRF on AirWave, allowing you to get historical trending
- You can examine new applications as they gain popularity amongst your population

Why it Matters

- While APP RF is nice, you will likely want the history
- You can define better policy



Demo 5: Lync Dashboard

What You will see:

– Lync visibility adds an additional level data points when examining traffic.
– Track usage of voice protocols along side Lync
– Understand prioritization requirements on the network

Why it Matters

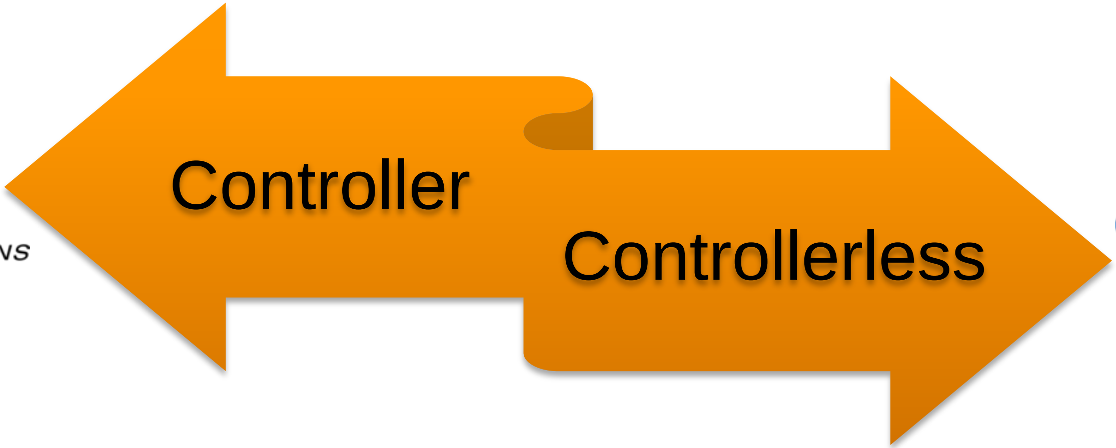
– Speeds up troubleshooting, points to network or client/server issues
– Justify investments in additional equipment, validate investments in technology
– Better Lync call traffic, higher usage, higher customer satisfaction.

Step 2

Planning your mobility network architecture

Two different architectures

ARUBA networks
CISCO
JUNIPER NETWORKS
MOTOROLA SOLUTIONS
RUCKUS WIRELESS
MERU NETWORKS
hp



ARUBA networks
meraki
MOTOROLA SOLUTIONS
Aerohive NETWORKS
XIRRUS

Evolution of the architectures

Autonomous APs
had no coordination

1st generation
128 APs
2,048 devices

2nd generation
512 APs
8,064 devices

3rd generation
2048 APs
32,768 devices

Current controllerless APs have equivalent CPUs and
memory to 1st generation controller architectures

Deployment overview

Controllers

Complex network topologies

Centralized encryption / switching

Larger mobility domains

Advanced services at scale

Controllerless

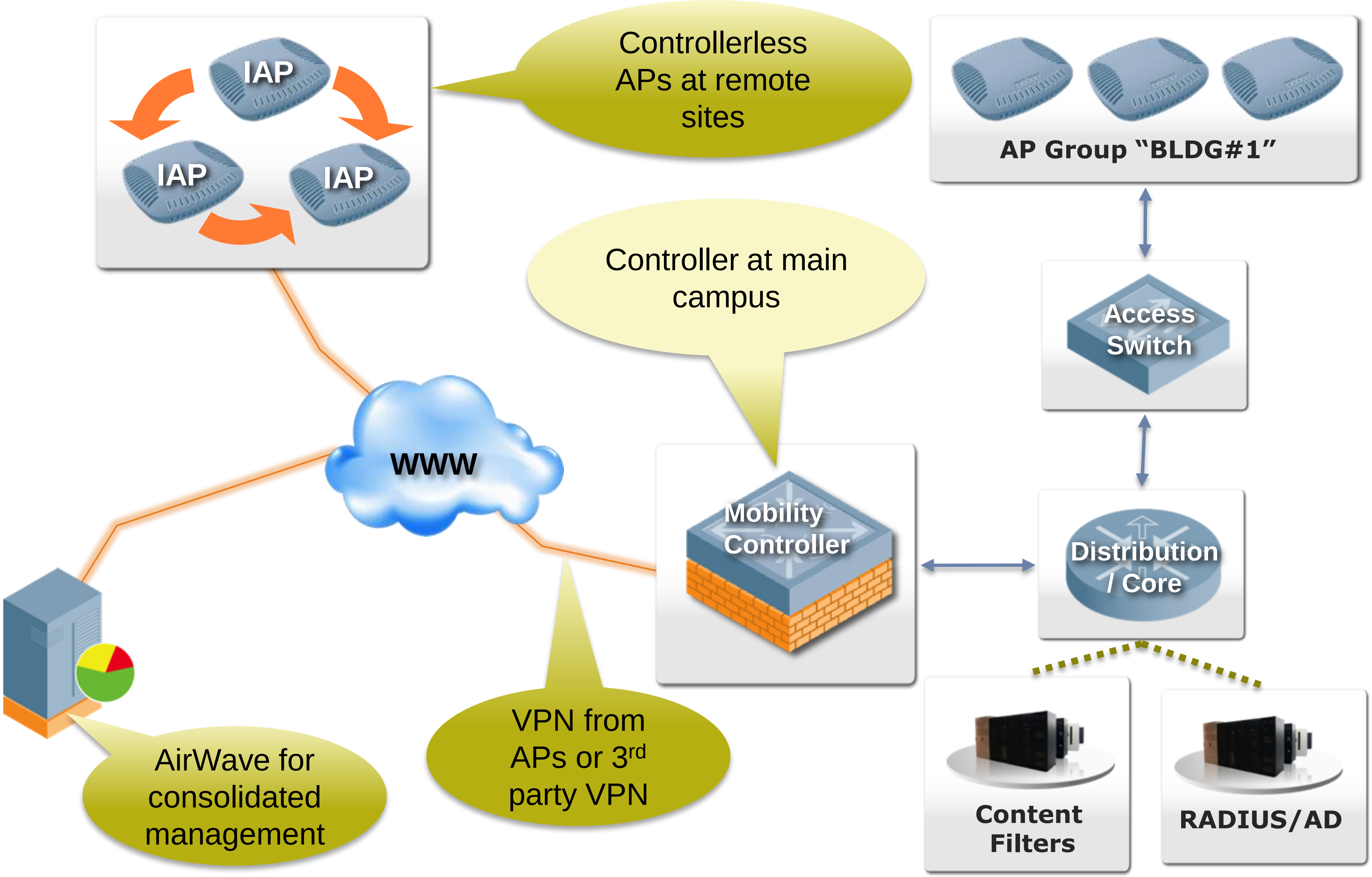
Less complex local networks

Many individual remote sites

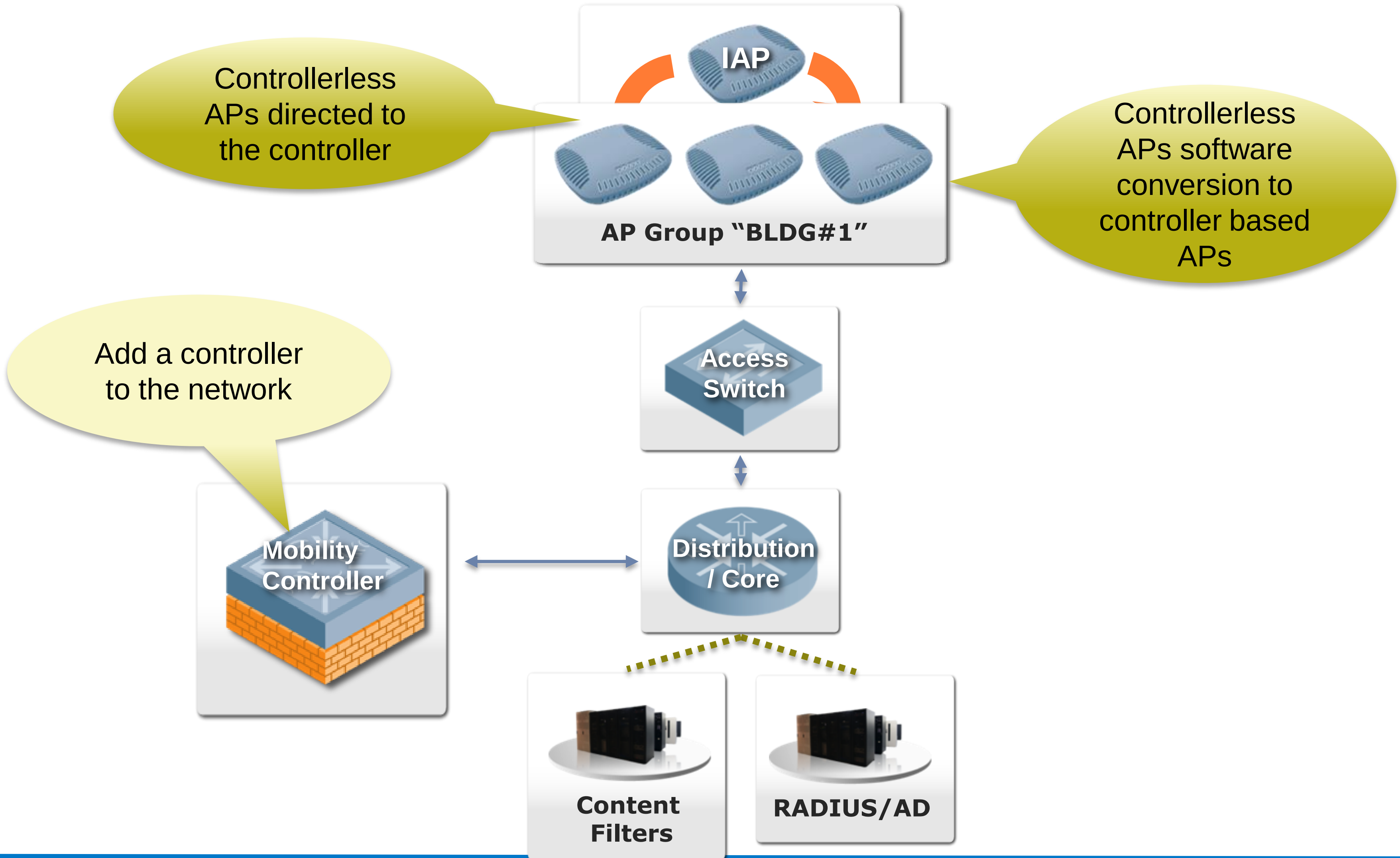
Simplified management

Minimal onsite HW and cost

Mixed Architectures



Convertible Architectures



Cloud Wi-Fi

How Does it Work?

- **Zero-touch provisioning: AP pulls configuration from Aruba Central**
- **AP self-selects as master**
- **Master performs firewall and controller functions**
- **New APs automatically join the master**

Aruba Central Services Platform

Public cloud subscription

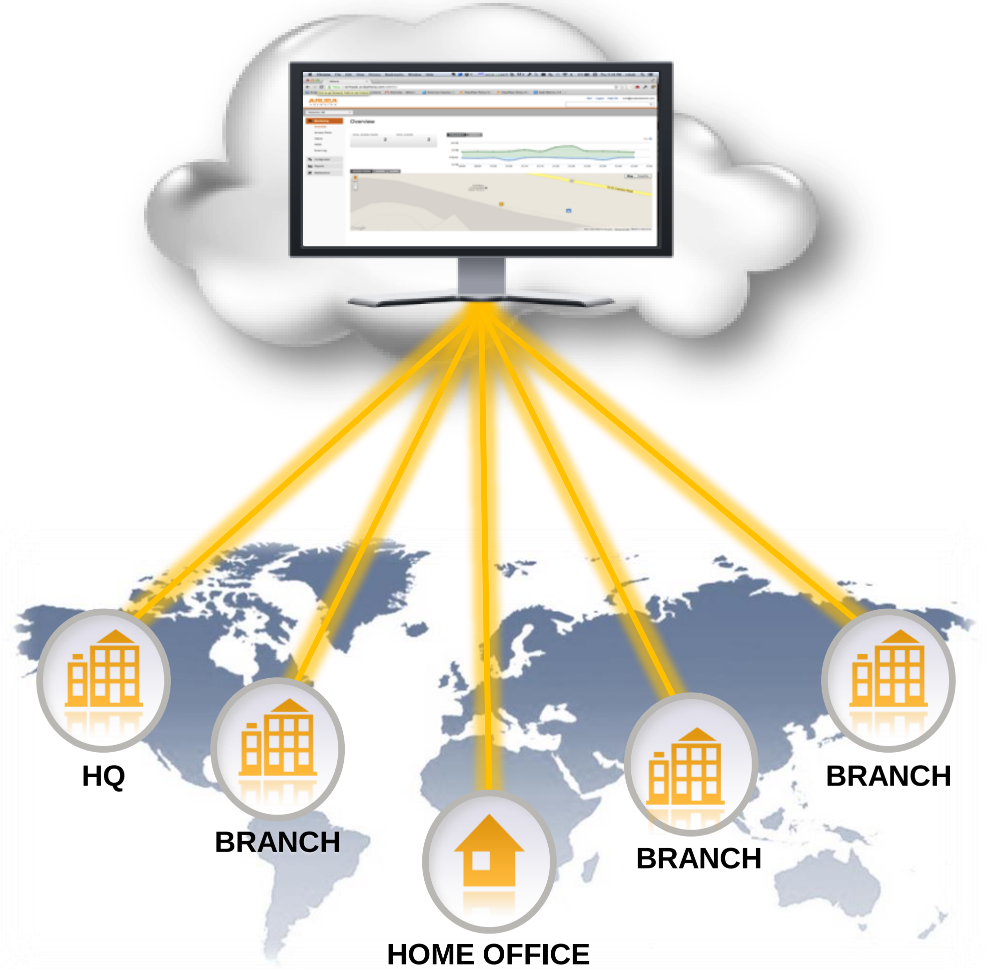
One interface

- Multiple sites
- Multiple clusters in a single site

Enterprise management

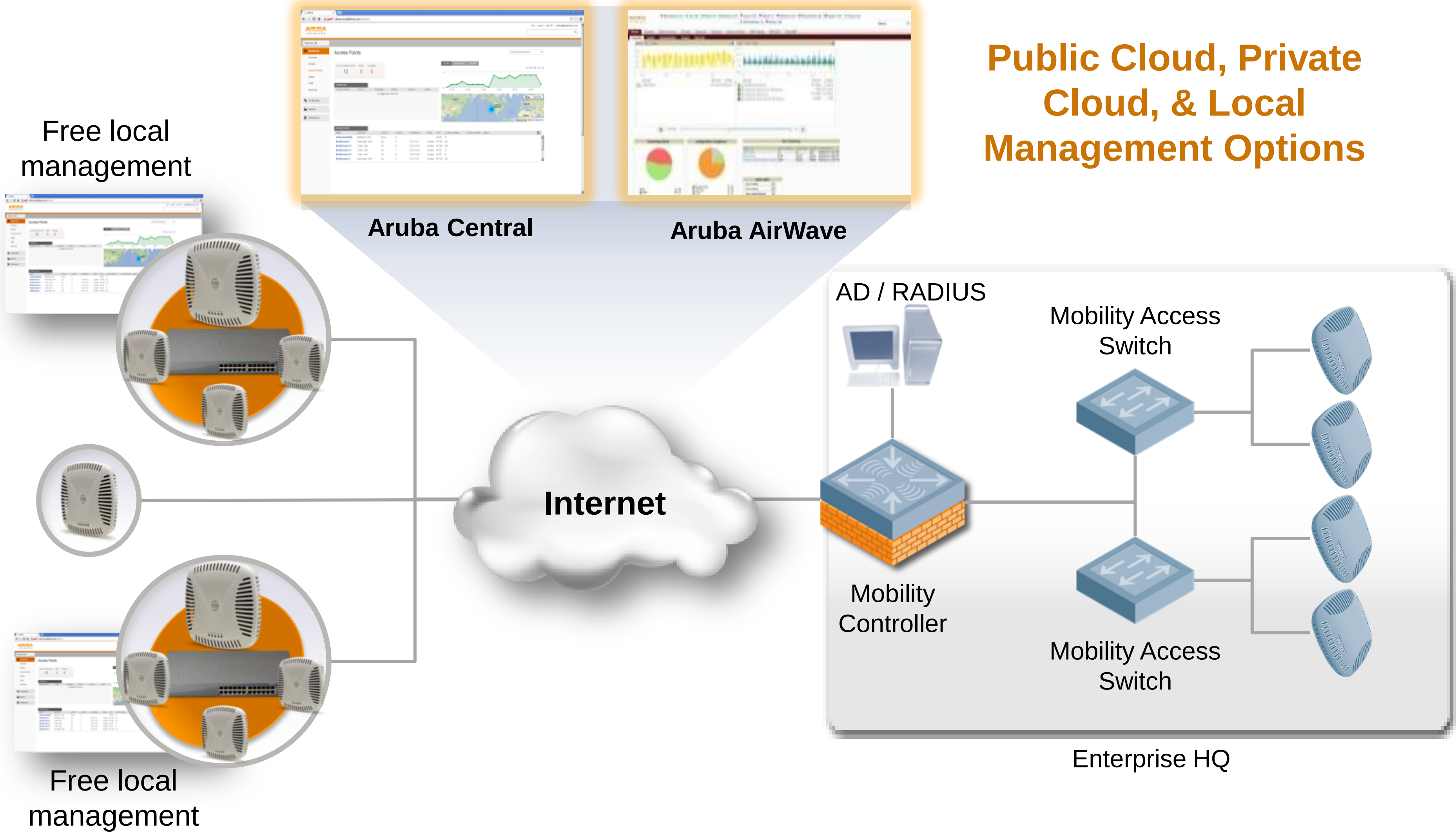
- Remote monitoring & troubleshooting
- Central configuration & firmware management
- Compliance records and historical data
- True Zero Touch provisioning

Comprehensive e-Support and community



Single Architecture, Multiple Modes

Public Cloud, Private Cloud, & Local Management Options



HUNTING FOR FASTER, SMARTER WI-FI?
YOU'RE IN GOOD COMPANY

Demo Aruba Activate & Aruba Central

BREAK

Step 3

Smart policy creation and BYOD enforcement

Why Network Access Control?

Smartphone and Tablet Growth

Users are More Mobile

Rise of Mobile Apps

Enterprise and BYOD Together

Evolving Auth/Authz needs

New policy and AAA dynamics

- No longer just authenticating Windows domain devices.
- Use of more 802.1X to lock down open ports/SSIDs.
- Meeting SSO requirements for cloud applications (e.g. SAML, Okta).

Why context for fine grained Authorization

- Ability to layer multiple authorization rules and conditions.
- Leverages context stored in a variety of 3rd party systems.

Challenges with legacy RADIUS

Visibility and troubleshooting

- No capability to profile devices connecting to the network.
- No contextual awareness (e.g. posture, device type, asset type).
- Poor per session troubleshooting tools and logs.

Scalability and reliability

- Limited performance to handle EAP termination or higher loads.
- Poor active clustering technology and centralized management.

Narrow feature sets

- Limited to core AAA, TACACS+ (ACS/SBR products are EOL/EOS)

Network Policy Best Practices

Most organizations do a fair job of authentication (who the user is) -- But, a poor job of authorization (what the user is allowed to do based on context)

1. Profile and authenticate everything that connects to your network.
2. Place ClearPass close to Active Directory or other Identity/Context servers to reduce latency.
3. Leverage context to provide fine grained authorization.
4. Utilize access infrastructure that supports CoA and role based access control versus VLAN segmentation.
5. Use standards based protocols for enhanced network security.

The ClearPass Platform

High performance AAA

- Up to 300 auths/second for 802.1X with AD.
- Supports distributed, active/active clustering and bursting.
- Hardware and virtual appliance platforms.

Multi-faceted policy services

- Uses standards based Web APIs to receive additional ***context*** from new sources (e.g. identity stores, MDM)
- Supports multiple enforcement actions.

Extensive support for emerging standards and multi-vendor products.

Network Policies Based on Context

Policy Example

Permit /Deny | Whitelist / Blacklist | Remediate | Quarantine | Redirect | Role-based Security | Bandwidth Mgmt | Optimize Multimedia

Use context from ClearPass & external sources to set network policy

WHO

- User/group membership

WHAT

- Device Profile
- OS version
- Endpoint health
- Jailbreak status
- Pincode/encryption

WHEN

- Time/Date
- eg. in semester

WHERE

- Location
- Trusted or untrusted network

HOW

- Application installed
- blacklisted

ClearPass for IT-managed and BYOD

Network Control	Device/User Control	App Control
Device Profiling & Visibility	MDM Services	Contextual Policies
AAA – RADIUS, TACACS+	Device Registration	3rd-party App Security
Policy Engine & Management	Visitor Management	Enterprise App Store
Health Checks	BYOD Onboarding	Work Space Security & Privacy

Demo

Demo: Defining Policies

What you will see . . .

1. **Creating a Wi-Fi service**
2. **Onboarding a personal device**
   – Limiting a 2nd device by the same user
3. **Enabling guest self-registration**
   – Keeping IT-managed devices off the guest network

Step 4

Device and App Management

Policy Enforcement Options

NAC / AAA	• VLAN • ACLs • QoS • Authentication	
MDM	• Device Provisioning & Onboarding • Device Policy • Device Level Encryption • Passcode • Full Wipe • App blacklist / whitelist	
MAM	• Authentication • App Passcode • App Wipe • App Policies • App SSO • App VPN	

Protect Your MDM Investment

ClearPass

Exchange
endpoint context
& trigger policies

3rd Party MDM

CITRIX
SOTI
airwatch
MaaS360 by Fiberlink
MobileIron
JAMF software

Use ClearPass to Enhance MDM/MAM

Wi-Fi based MDM enrollment

- End reliance on SMS or e-mail invitations
- Link MDM agent to captive portal

Auto-remediate non-compliant devices

- Quarantine devices by blacklist
- Redirect to self-service portal
- Push reminders about policy violation

In-built CA for provisioning credentials

- Unique device certificates using SCEP
- No need for PKI to support BYOD

Use MDM device context for network security

- Deny/limit network access to jailbreak or rooted devices

Use MDM Attributes for Network Policy

MDM Attributes

Inventory

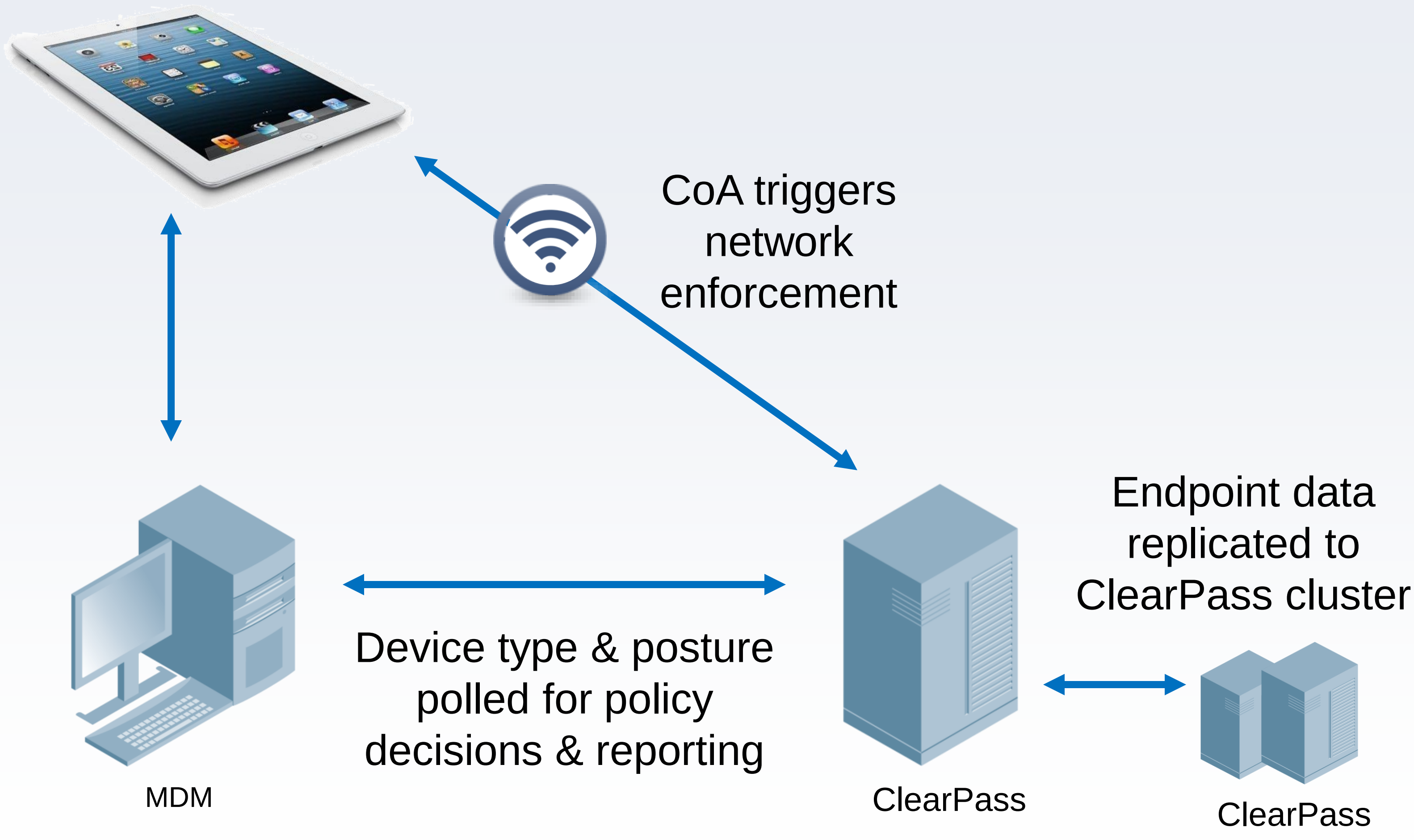
Manufacturer:	Apple
Model:	iPad2
OS Version:	iOS 6.1
UDID	1730235f564094186
Serial Number	79049XXXA4S
IMEI	012416009780168
Phone Number	408-534-2819
Carrier	Verizon
MDM Id	130d0f992t34
Owner	jhoward
Display Name	John Howard
Ownership	Employee Liable

Posture

MDM Enabled	Yes
Compromised	Not Jailbroken
Encryption Enabled	Yes
Blacklisted Apps	No
Required Apps	Yes
Last Check in	01/30/2012 9:03am

ClearPass MDM Integration

Using MDM device information for Policy

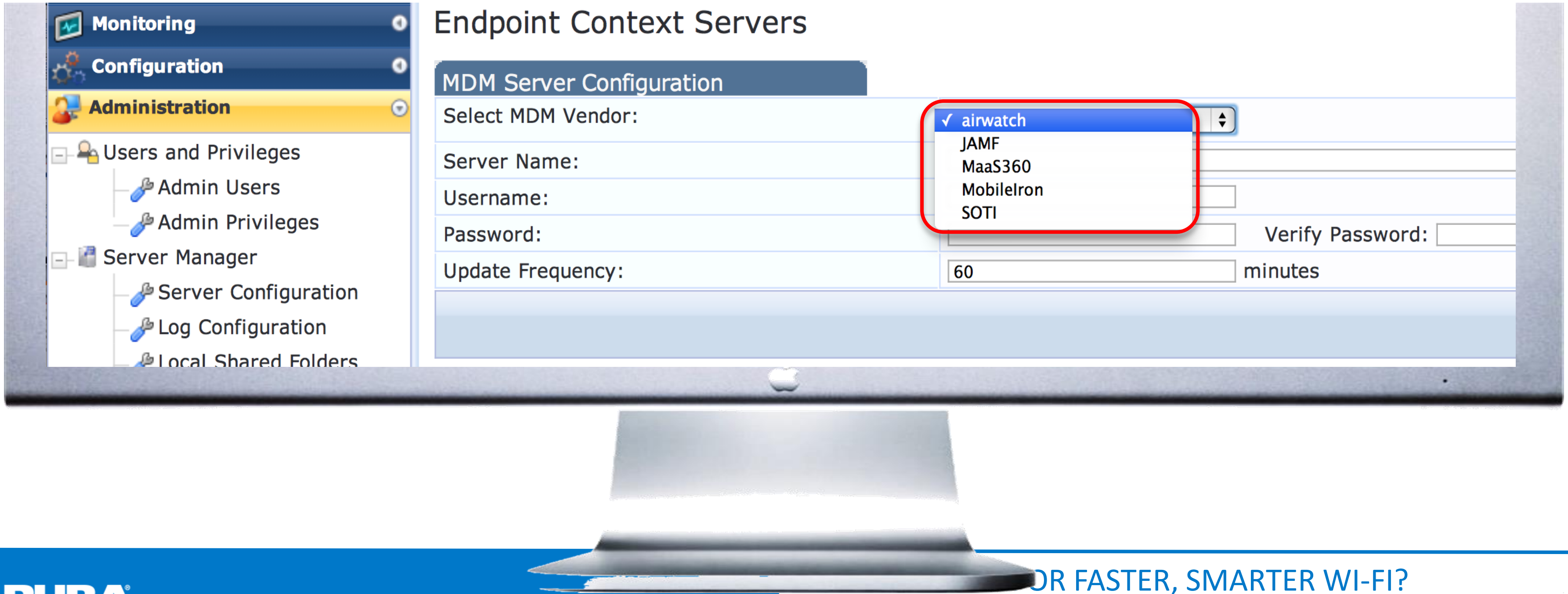


Integrating Leading MDM Vendors

- **ClearPass uses public APIs for:**

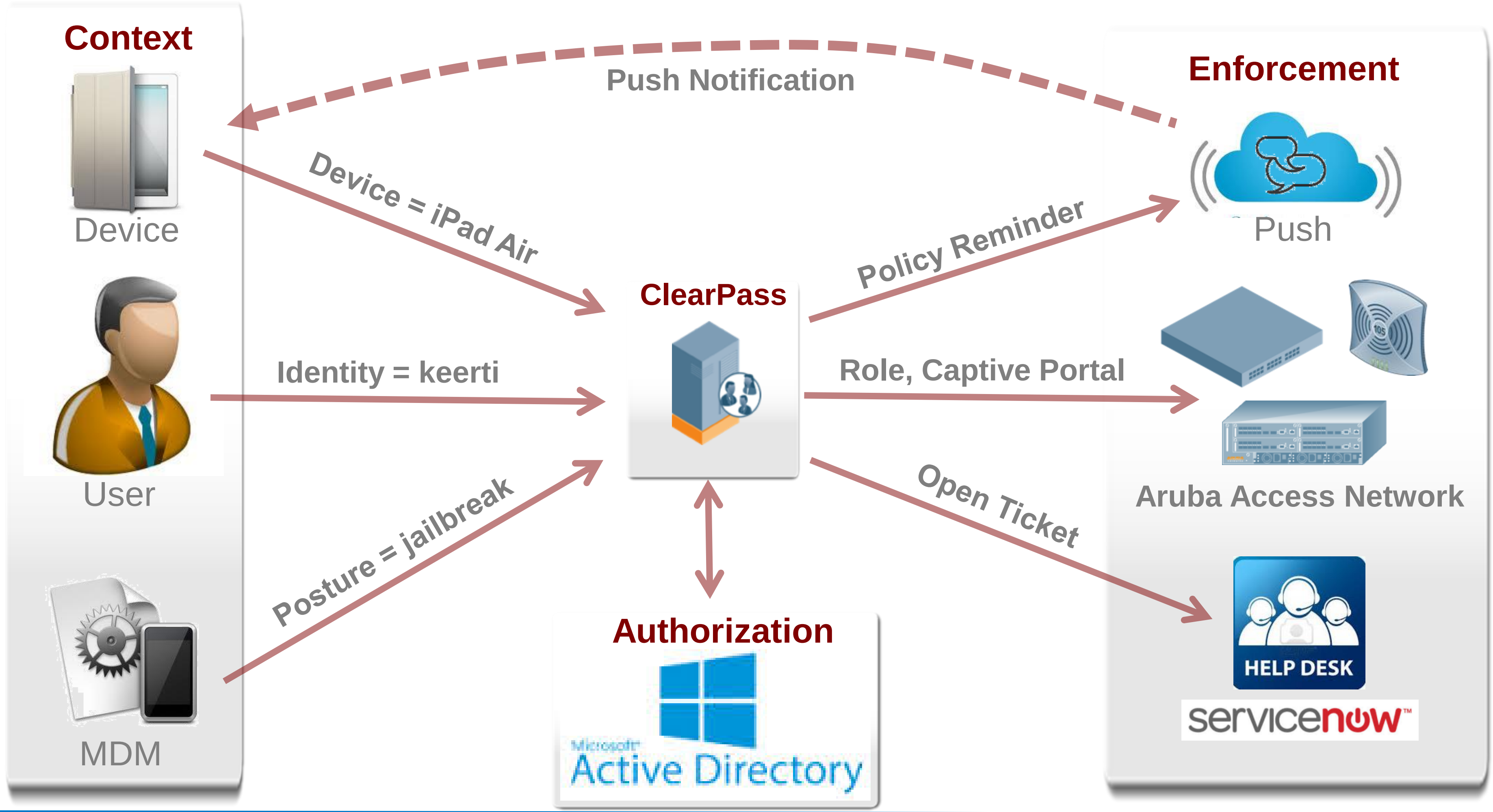
airwatch SOTI MobileIron MaaS360 by Fiberlink JAMF software CITRIX

- **Normalize MDM endpoint data across vendors**



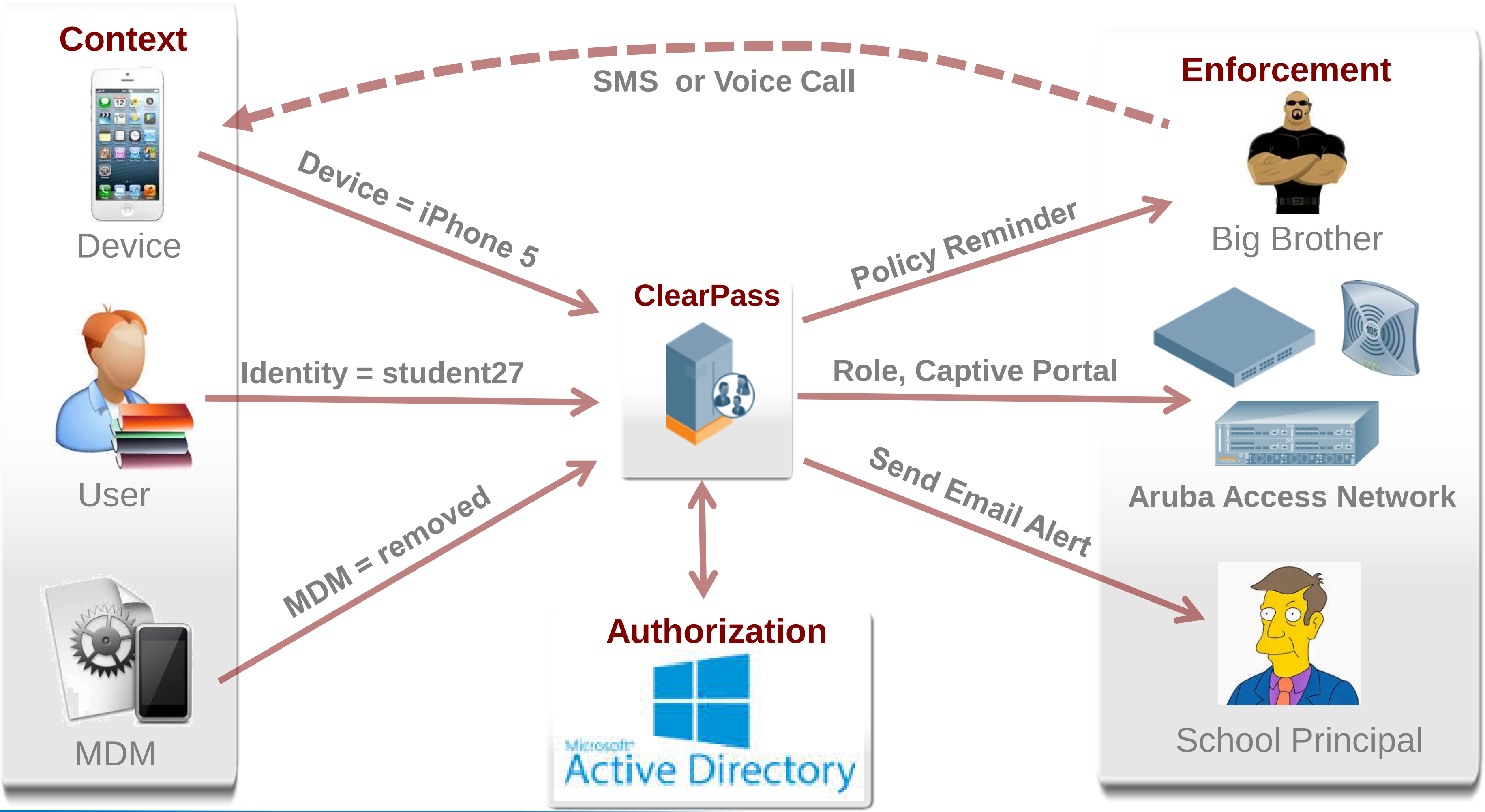
Enterprise Policy Beyond the Network

Use Case: Compromised Device



Enterprise Policy Beyond the Network

Use Case: MDM Profile Removed



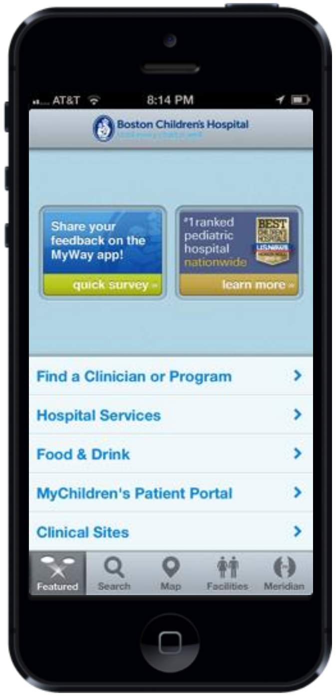
Step 5

Extending mobile services to visitors and customers

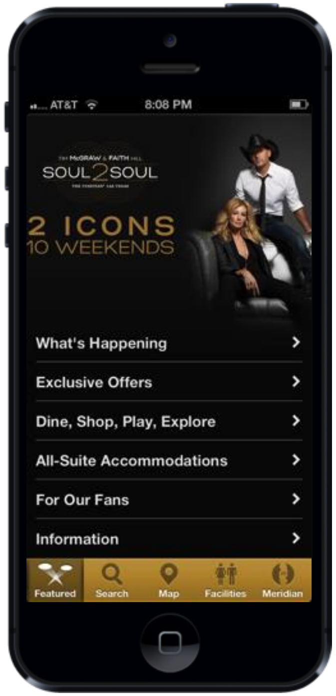
Location-Based Mobile Services on the Rise

Retail

Hospitals

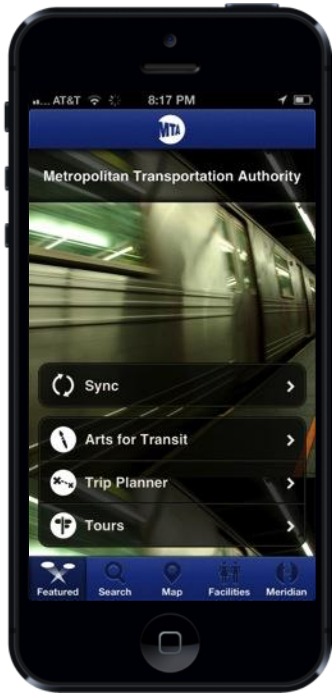


Hotels



Campus

Transportation



80% of the world owns a mobile phone. And we're using them in the venues we visit

27% of companies worldwide intend to implement location-based mobile marketing in 2013

ARUBA networks

HUNTING FOR FASTER, SMARTER WI-FI?
YOU'RE IN GOOD COMPANY

Wi-Fi Concierge Inside Venues

Way-Finding	Indoor turn-by-turn directions
Push Notifications	Time & location relevant messaging
Analytics	Dwell-time and traffic insights

Wi-Fi Concierge Solution Components

Meridian Editor	Aruba Wi-Fi	Analytics Service
meridian "BluDot," Nav, & Zone-based content	Featuring Analytics & Location Engine	Nomi JOINGO nearbuy 20+ third party products

Meridian App (white-label/custom)

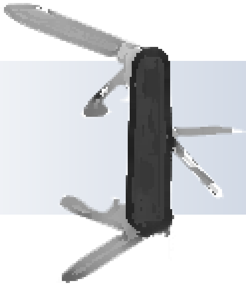
iOS android

Active Wi-Fi Connection Not Needed

Key Take Aways

Integrate Network, Device and App Management

- **Stronger security, simplified rollouts**: Complete solution for BYOD and IT-managed network access policy management



Ensure Multi-vendor Support

- **Integration flexibility:** Standards based enforcement across any Wi-Fi, wired and VPN infrastructure

Plan for Growth and Change

- **Adapt to the environment:** Support a wide variety of use-cases and phased deployment – BYOD, AAA, guest access, compliance initiatives…

ARUBA®

networks