# The BYOD Wave: Policy, Security, and Wireless Infrastructure

Ken Kaminski

BYOD & Security Technical Solutions Architect – Northeast

CISSP, GCIA, GCFA, GAWN, GPEN

Cisco Systems

# Agenda

1. BYOD Trends & Policy
2. BYOD Solution Building Blocks
3. BYOD Device On-Boarding
4. Wireless Infrastructure Issues
5. Mobile Device Management (MDM) Vendors
6. Radius Change of Authorization (COA) – Two-way Plumbing

*This presentation focuses on wireless mobile smartphones and tablets – in particular Apple IOS and Android Devices which are the most prevalant*

# BYOD Trends and Policy

# Access Today

| END USER EXPECTATIONS | IT TRENDS |
| --- | --- |
| Over 15 Billion devices by 2015, with average worker with 3 devices | 50% workloads are virtualized — to increase efficiency |
| New workspace: anywhere, anytime | 2/3 of workloads will be in the cloud by 2016 |
| 71% Next Gen Y workforce do not obey policies | 71% of the world's mobile data traffic will be video in 2016 |
| 60% will download sensitive data on personal device | Mobile malware has doubled (2010 to 2011) |

**REDUCE SECURITY RISK**

**IMPROVE END USER PRODUCTIVITY**

**INCREASE OPERATIONAL EFFICIENCIES**

# Spectrum of Customer Requirements

| | |
|---|---|
| ✓ Adoption Policy | Restrict, Limit, Allow, Embrace |
| ✓ Device Ownership | Corp, Employee, Mix, Guests |
| ✓ Support Model | IT managed, IT assisted, Self-supported |
| ✓ Support Level | Production, Guest+, Guest, Best Effort |
| ✓ Data Security | Written |

Many Customers

| Limit | Basic | Enhanced | Advanced |
|---|---|---|---|
| **Environment requires tight controls** | **Basic access for additional devices** | **Any device, anywhere, enhanced security** | **Any device, anywhere, anyone** |
| **IT chosen devices** | **Broader device set** | **Wide range of devices** | **Wide range of devices** |
| **IT managed devices with mainly on-site access** | **IT managed devices with mainly on-site access** | **Corp and employee owned devices with full on-site and off-site access** | **Corp and employee owned devices with full on-site and off-site access** |
| **All other devices prohibited** | **Employee owned and Guest devices with Internet only** | **Device-side security** | **Device-side security** |
| | | **Guest devices with Internet only** | **Guest/Customer devices with enhanced services** |
| | | | **Custom Native applications** |
| | | | **BYOD for Competitive advantage** |

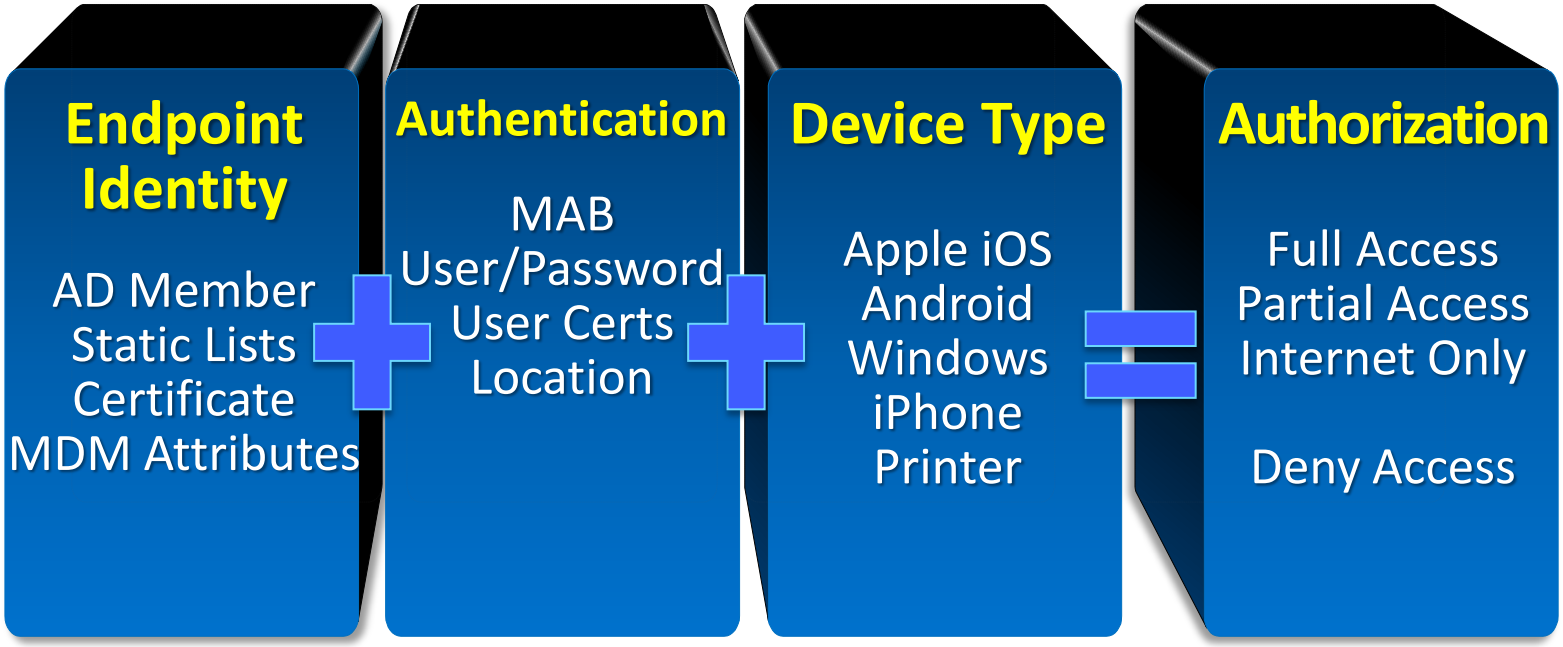
# What Makes a BYOD Policy

The Policy Server is Critical to Meeting Your Goals

**Context-Based Identity and Access Control**

| | | |
|---|---|---|
| **Who?**<br>Known users (Employees, Sales, HR)<br>Unknown users (Guests) | **What?**<br>Device identity<br>Device classification (profile)<br>Device health (posture) | **How?**<br>Wired<br>Wireless<br>VPN |
| **Where?**<br>Geographic location<br>Department<br>SSID / Switchport | **When?**<br>Date<br>Time<br>Start/Stop Access | **Other?**<br>Custom attributes<br>Device/User states<br>Applications used |

# Example BYOD Policy



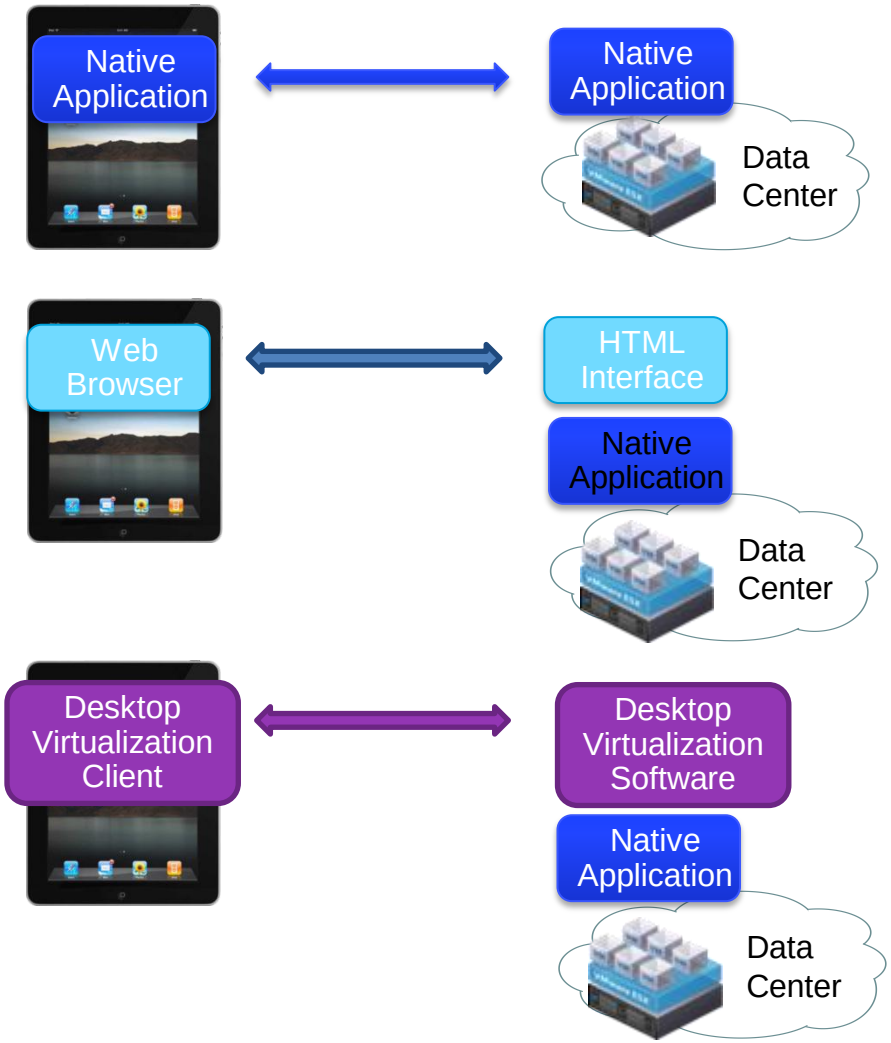
# BYOD Solution Building Blocks

# BYOD Mobile Device Connectivity

# BYOD Smart Solution Building Blocks

| | |
|---|---|
| Collaboration Apps | Lync, Jabber |
| Workspace Management | MDM & VDI |
| Secure Mobility | VPN Clients |
| Policy Management Infrastructure | Radius, Profiler, Posture, Guest, BYOD On-Boarding |
| Core Infrastructure | Wireless Infrastructure & Management |

# Application Models Affect Strategy




**Native**
- ✓ Local data on device
- ✓ Maximum performance
- ✓ Native device experience

**Browser**
- ✓ Local data on device
- ✓ Portable to many devices
- ✓ Browser experience

**Virtual**
- ✓ No local data on device
- ✓ Maximum security
- ✓ Translated experience

BYO isn't about the device, its about securing data security

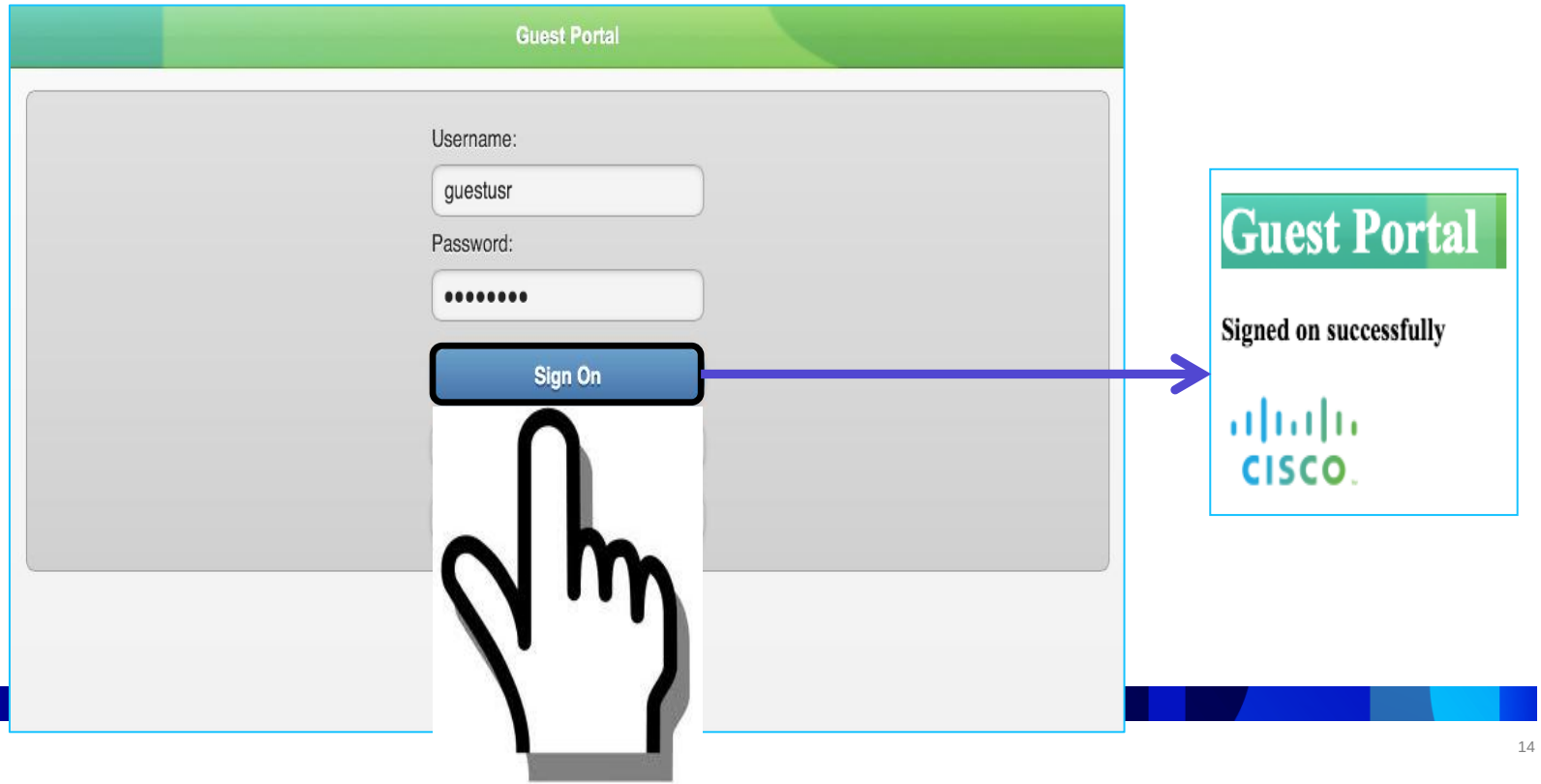
# Integration Trends – One Policy Server

- Radius Server
- Guest Server – Sponsored Guest Access and Guest Portal
- Device Profiler
- Network Access Control (NAC) Posture Server – Windows & MacOSX clients
- BYOD Device Registration Portal – On-Boarding
- Trend: Certificate Authority (CA) Integrated

# BYOD Device On-Boarding

# Key Technology: Web Authentication

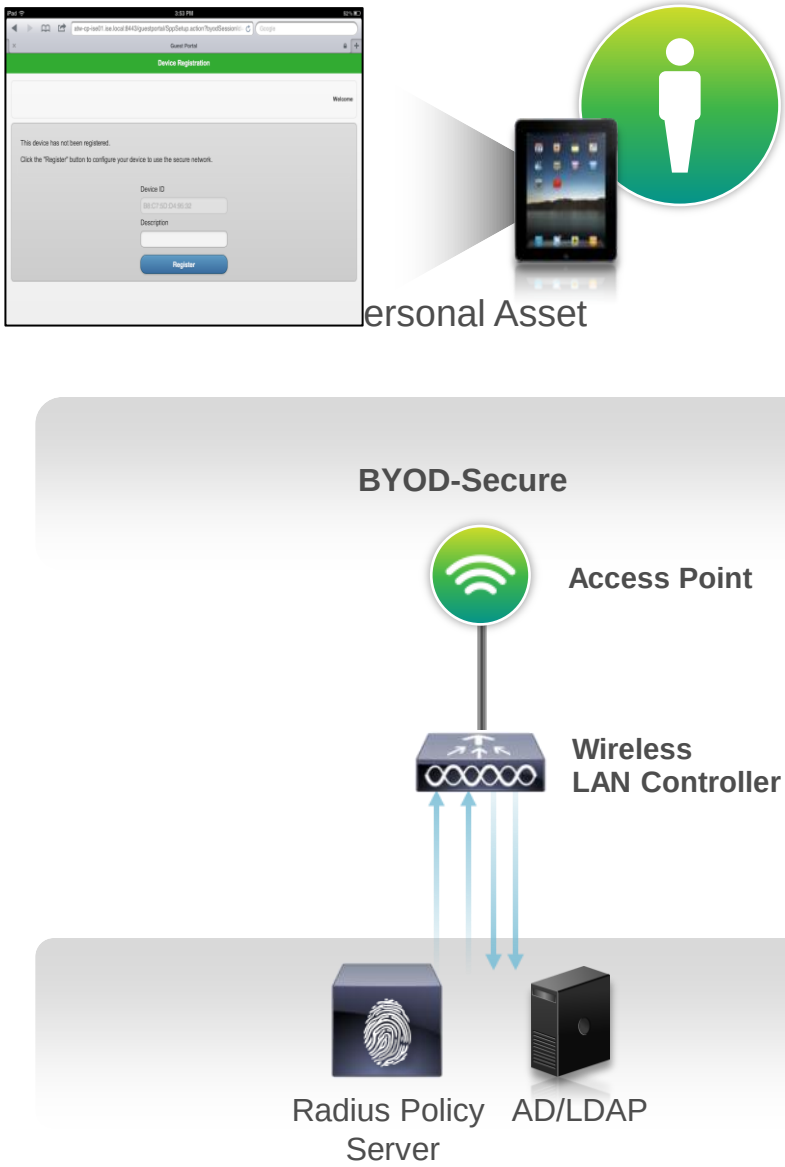
- Used to identify users without supplicants (Classic Guest Captive Web Portals)
- BYOD – AD Credentials for device registration/on-boarding used vs traditional sponsored guest credentials



# BYOD Flow

## Use Case: Single SSID

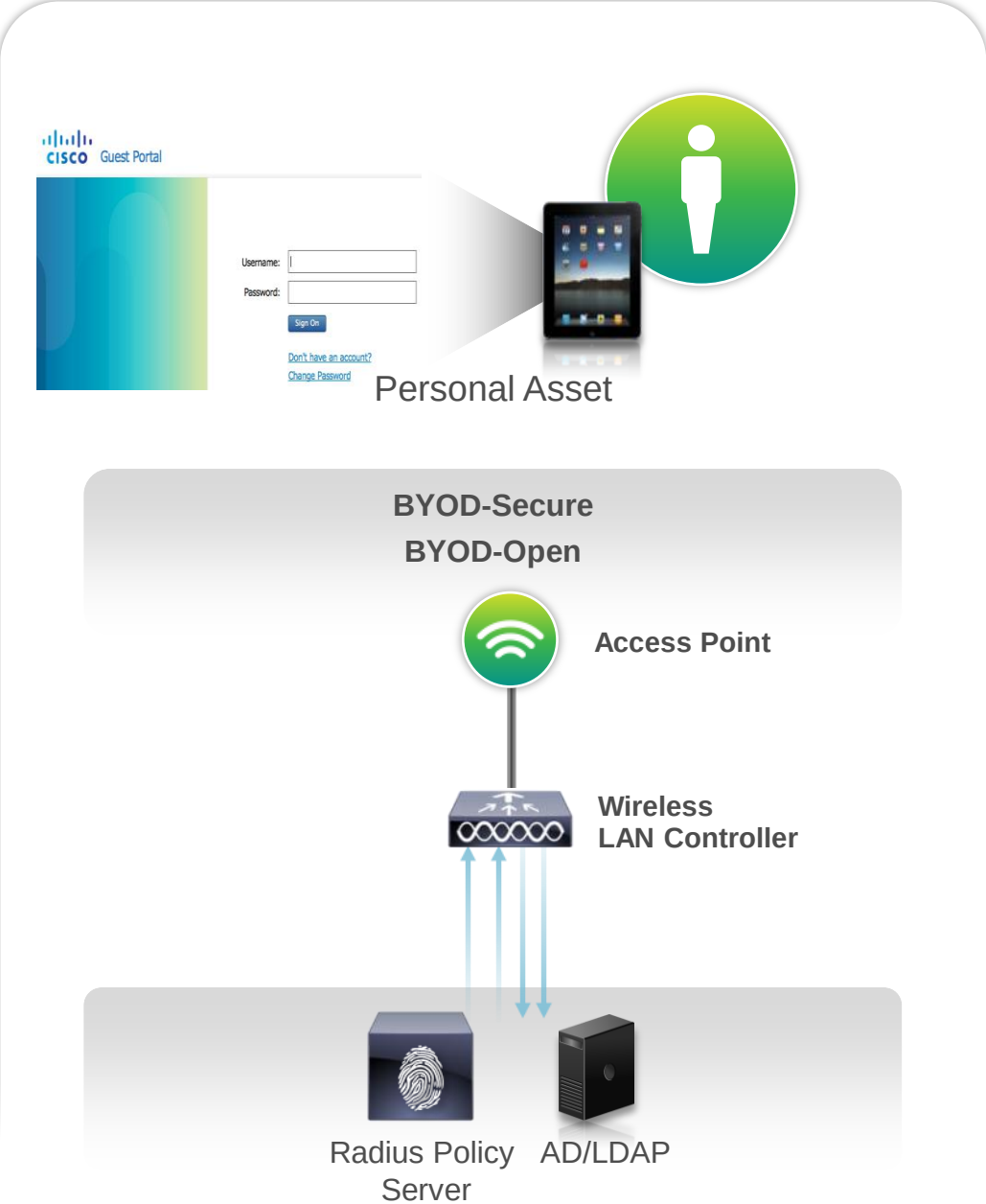
- User connects to Secure SSID
- PEAP: Username/Password
- Redirected to Provisioning Portal – Radius URL Redirect + ACL
- User registers device
  - Downloads Certificate
  - Downloads Supplicant Config
- User reconnects using EAP-TLS



# BYOD Flow

## Use Case: Dual SSID

- User connects to Open SSID
- Redirected to WebAuth portal
- User enters employee or guest credentials
- Guest signs AUP and gets Guest access
- Employee redirected to Provisioning Portal – Radius URL Redirect + ACL
- Employee registers device
  - Downloads Certificate
  - Downloads Supplicant Config
- Employee reconnects using EAP-TLS



# Provisioning Apple ios Devices

- Uses Apple Over-the-Air (OTA) Delivery
- Phase 1: Authentication – use user AD Credentials. Policy Server sends its certificate to device
- Phase 2: Certificate Enrollment
  - Policy Server uses Simple Certificate Enrollment Protocol (SCEP) to proxy to CA – Microsoft calls this Network Device Enrollment Service (NDES)
  - Policy server tells device how to build it's Certificate Signing Request (CSR)
  - Useful CSR: CN=username, SAN=Mac Address (helps with moving a certificate from one device to another) – check MAC in Cert to radius MAC
- Phase 3: Service Configuration/Encrypted Profiles – Configuration profile (as a Wi-Fi Profile) is an XML file

# Provisioning Android Devices

- No equivalent to Apple Over-the-Air (OTA) Delivery
- Need an application to do this function.  Example is Cisco Network Setup Assistant
- Application usually hosted on Google Play – need to allow access to Google Play during the device enrollment phase.  This is usually done via an Access Control List included in the radius exchange
- The diversity of Android vendors and Service Providers and the Android Trust Model makes it difficult to host this application on the Policy Server

# Wireless URL Redirection Considerations

## Apple Captive Network Assistant (CNA)

- Problem: URL redirection on Apple devices may fail due to Apple Captive Network Assistant (CNA)
- Background on CNA:
- Apple iOS feature to facilitate network access when captive portals present that requires login by automatically opening web browser in a controlled window. Feature attempts to detect the presence of captive portal by sending a web request upon WiFi connectivity to http://www.apple.com/library/test/success.html
  - If response received, then Internet access assumed and no further interaction
  - If no response received, Internet access is assumed to be blocked by captive portal and CNA auto-launches browser to requests portal login in a controlled window.
- Solutions:
  1. Disable Auto-Login under WLAN settings (requires user knowledge and interaction)
  2. Configure WLC to bypass CNA



1

# Trend: My Devices Portal

## Devices owned or assigned to the employee managed by the employee

- Employees are able to mark any of their devices as Lost or reinstate a device

Access to the device is terminated immediately

# Wireless Infrastructure Issues

# Expectations for the Network

## Is the Network Ready for Next Generation Applications?

The Wireless network is no longer a network of convenience

Mobile BYOD clients drive advanced applications for Voice, Video, and VXI

Network Infrastructure Will Have To Scale= High Bandwidth Use)

Time to rethink the access network

# Access Point Spacing – BYOD General

- Classic Data AP Spacing – 5,000 sq ft
- BYOD AP Spacing (incl. heavier video apps) – 3,500 sq ft
- Voice  AP Spacing – 2,500 sq ft

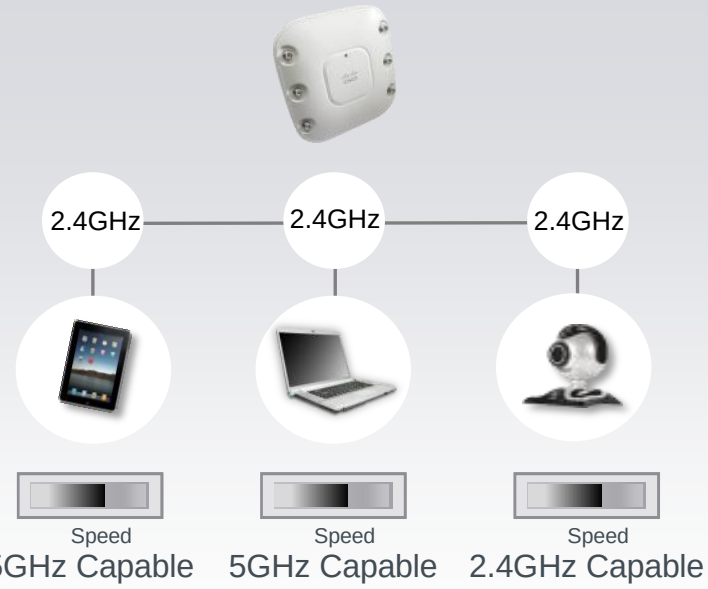
- Check Current Channel Utilization/Duty Cycle to get an idea of where you are at.  Improving the Duty Cycle:

  - 1. Disable Lower Data Rates
  - 2. Beam Forming Technology
  - 3. Spectrum Analysis built into the AP's

# Band Steering Technology

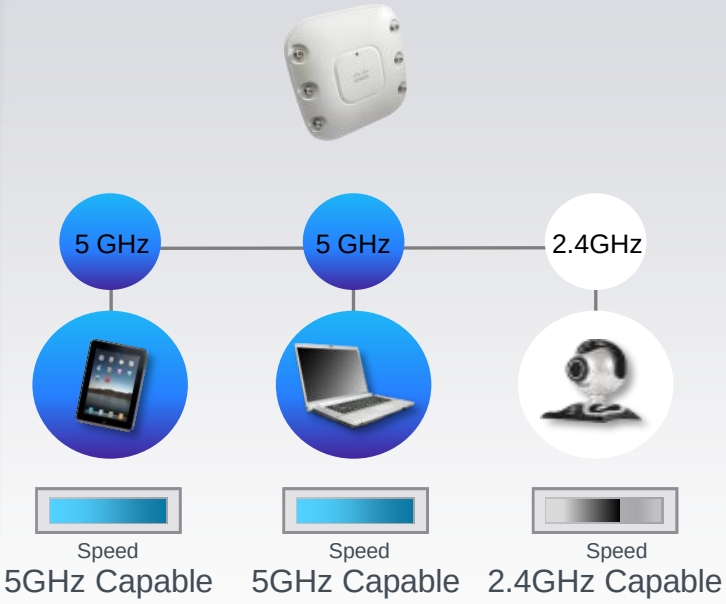
## Automatic Band Steering and Selection For 5GHZ Capable Devices

All clients crowd the 2.4GHz spectrum lowering performance



**AFTER**

5GHz capable clients are automatically moved to cleaner 5GHz spectrum



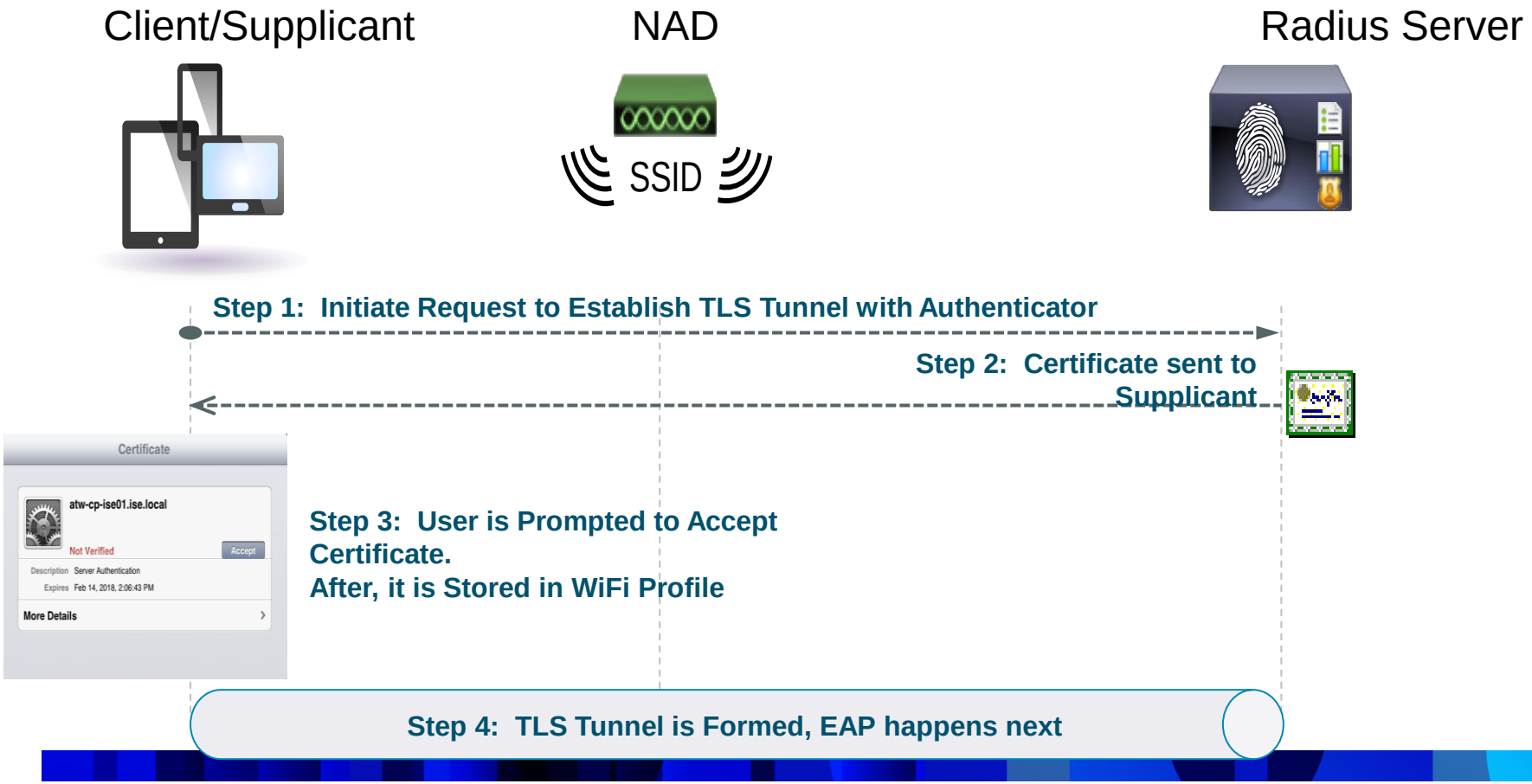

Miercom

# Clients Misbehave!

- Example education customer:
  - 6,000 Endpoints (all BYOD style)
  - 9M Auth Failures in 24 hours
  - Many Different Failure Scenarios – all related to clients dropping TLS (both PEAP & EAP-TLS). Untrusted Certificate Failures
  - Large number of BYOD devices – many models from many vendors
  - Error: No response received during 120 seconds on last EAP message sent to the client – This means the supplicant just ignored the Policy Server/WLC
  - These devices authenticate at 10 times the rate as Windows/MACOSX desktop/laptop – this has engineering implications: radius & dhcp infrastructure

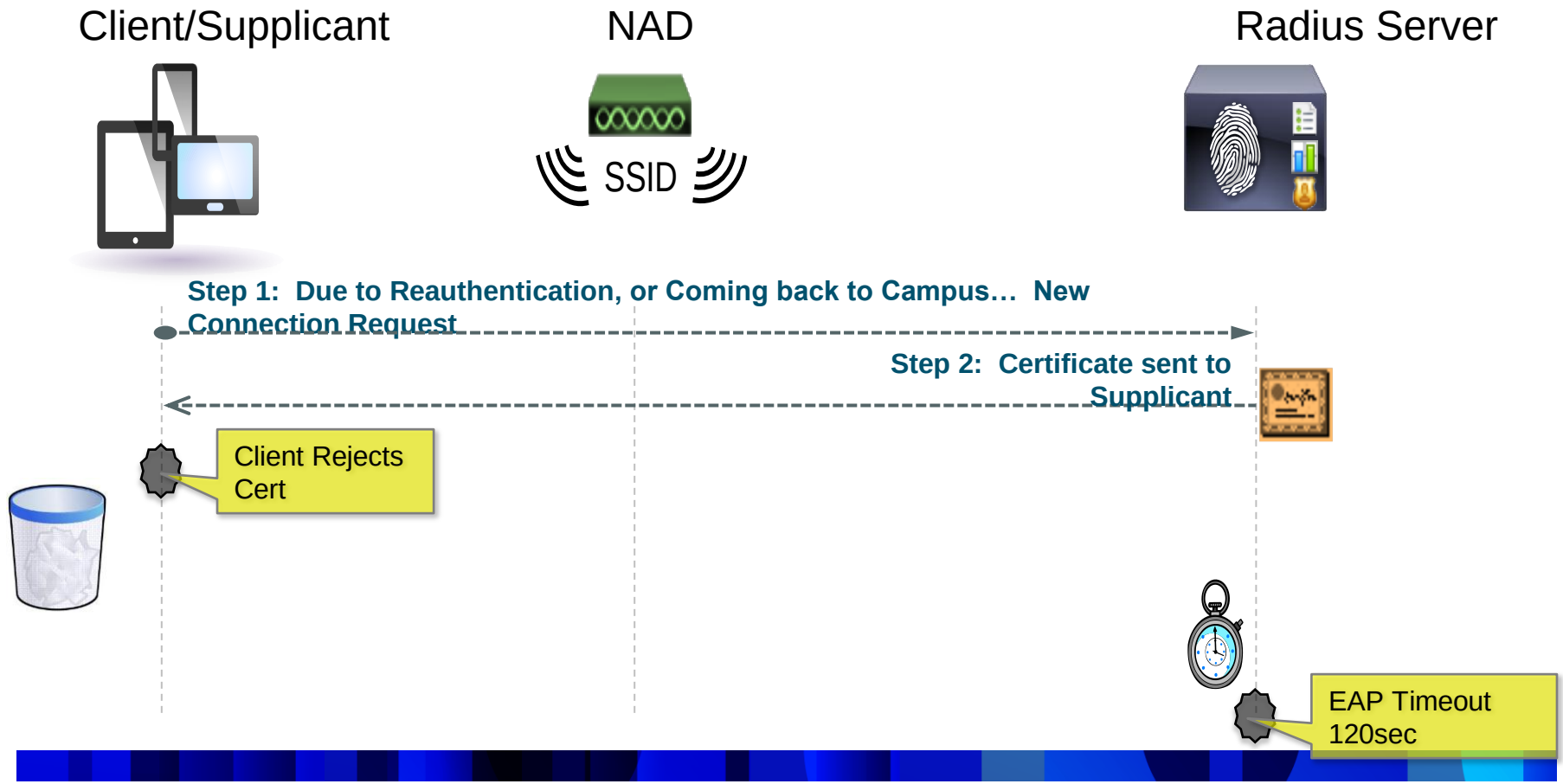
# Example: Join Network (PEAP / MSChapV2)

- Client sets up a PEAP connection:
  - MAY not trust the Certificate on the Server, like going to a https:// site where the certificate is not trusted.
  - Is a ONE-WAY trust (Client trust server) not bi-directional trust.

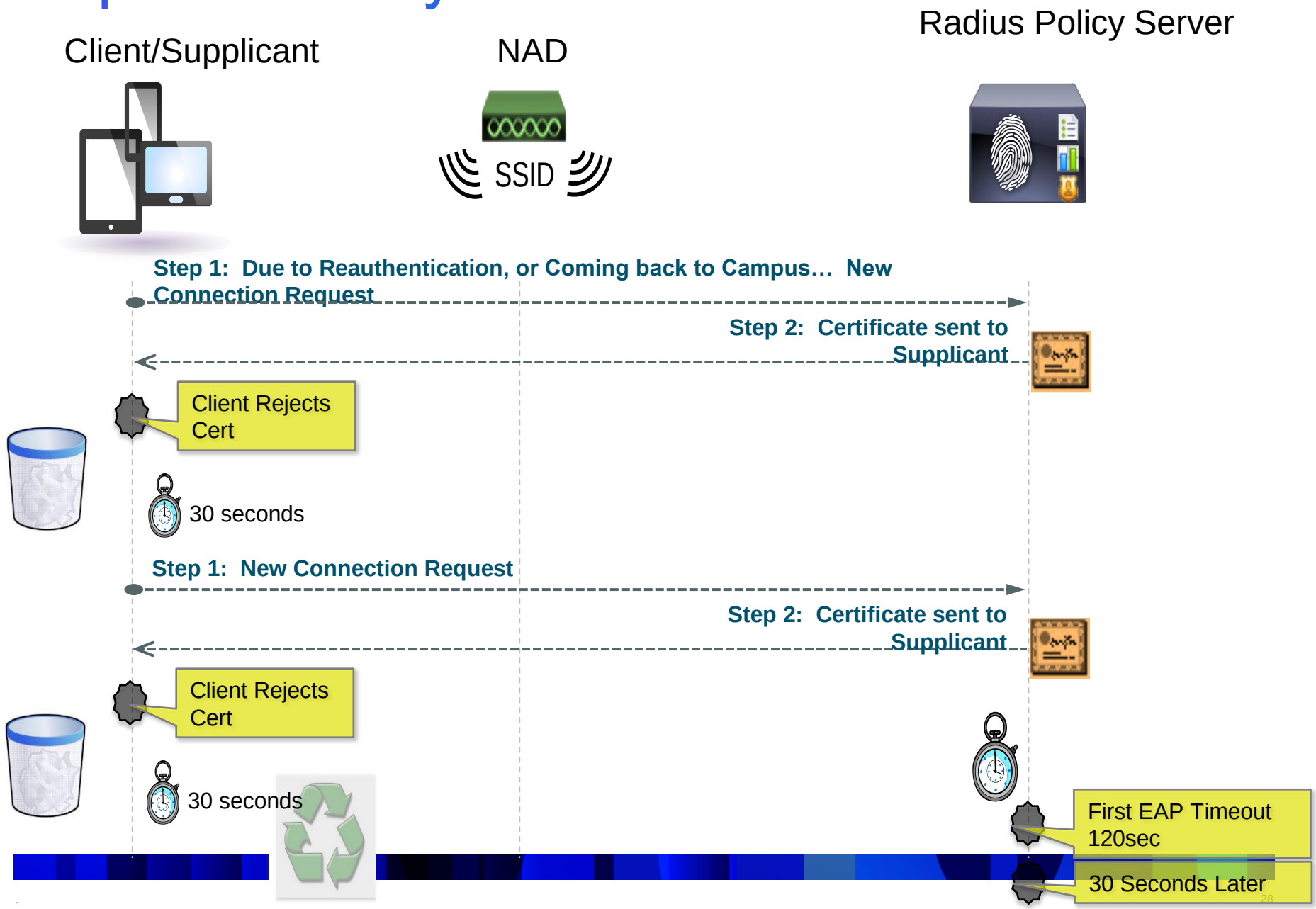


# Let’s break this!

- Client has cert saved in WiFi profile:
  - Let’s Change the Cert on the Radius Policy Server
  - Supplicant SHOULD prompt to accept new cert, most do not. This is the problem: many say nothing.



# Repeats Every 30 Seconds



# Observed Results

- Androids:
  - CIUS (Android 2.2.2)
  - Galaxy Tab 10.1 (4.0.4)
  - Galaxy Tab2 7 (4.1.1)
  - Google Nexus 7 (4.2.2)

All Just Accepted New Cert & Kept working.
- BAD Behavior on Supplicant, Security Vulnerability…

Google: [M#1225844005]

- iOS:
  - iPod Touch (3.1.3) - Reject Cert, Retry 30 Seconds
  - iPhone 4 (4.2.1) - Reject Cert, Retry 30 Seconds
  - iPhone 4 (6.0.0) - Dropped Network, Prompted to Accept Cert on Reconnect
  - iPad 2 (6.0.1) - Dropped Network, Prompted to Accept Cert on Reconnect
  - iPhone 5 (6.1.0) - Dropped Network, Prompted to Accept Cert on Reconnect
- Windows RT
  - MS Surface Tablet - Reject Cert, Retry 30 Seconds – But Prompted User

# What Breaks?

- TLS Certificates are used in:
  1. Most EAP Methods including EAP-TLS, PEAP, EAP-FAST
  2. Web Portals: Admin Portal, Guest Portal, Sponsored Guest Portal, Device On-Boarding Portal, MyDevices Portal
- When can this break?
  1. The Certificate on the Policy Server Changes
  2. The Policy Server dies and another takes over
  3. A Wireless client roams to another WLC on a separate Policy Server
- Apple iOS: device stores trusted certs in the profile. It does <u>not</u> follow the ios keychain where the signing root is trusted. It will not trust the new certificate even if the root CA is trusted (it is the root CA of the old cert and the new one) . User must accept the new certificate in this scenario.

# The Solution: Wildcard Certificates on all Radius Policy Servers

There are three options:

1. Use a wildcard in the Subject Common Name (CN) (*policyserver.company.local)

   Problem: All Native Microsoft Supplicants (incl. Windows Mobile) do not support this:

   http://technet.microsoft.com/en-US/cc730460

Solution: Put the wildcard values in the Subject Alternative Name (SAN) extension called dNSName

2. Leave the CN Blank + Wildcard in SAN

   Works with most private Certificate Authorities (incl. MS AD CA)

   Problem: The Majority of public CAs do not allow a cert with a blank CN value

# Recommended Wildcard Solution

3. Use a common generic hostname for all policy servers for the CN in the subject and use both this generic hostname and a wildcard value in two SAN dNSName entries:

   CN = aaa.policyservers.company.local

   SAN dNSName = aaa.policyservers.company.local

   SAN dNSName = *.policyservers.company.local

Public CAs (examples – Comodo.com and SSL.com) support these as certificate request types = unified communications certificate

# RFC 2818 and RFC 6125

tools.ietf.org ▸ html ▸ rfc6125

**1.5. Overview of Recommendations**

To orient the reader, this section provides an informational overview of the recommendations contained in this document.

For the primary audience of application protocol designers, this document provides recommended procedures for the representation and verification of application service identity within PKIX certificates used in the context of TLS.

For the secondary audiences, in essence this document encourages certification authorities, application service providers, and application client developers to coalesce on the following practices:

- o Move away from including and checking strings that look like domain names in the subject's Common Name.

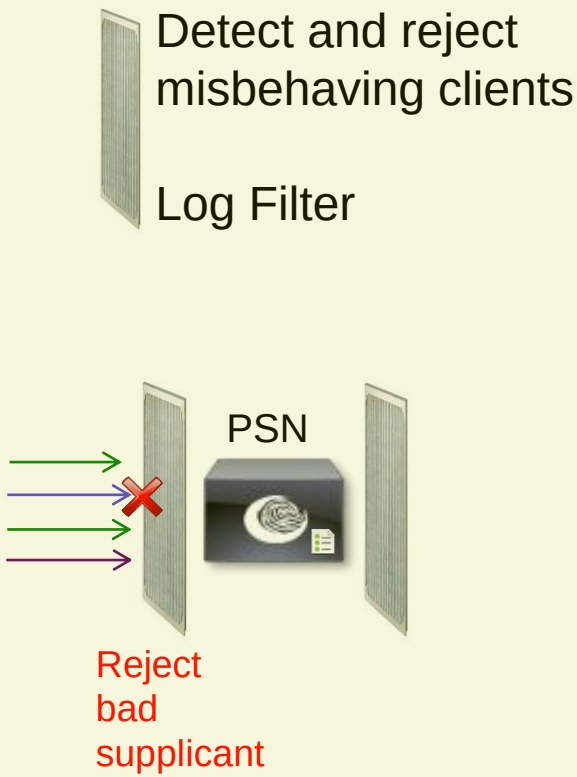
- o Move toward including and checking DNS domain names via the subjectAlternativeName extension designed for that purpose: dNSName.

# Policy Node Noise Suppression and Smarter Logging

## Filter Noise and Provide Better Feedback on Authentication Issues

- Filters
- Misconfigured Client Dynamic Detection and Suppression
- Accounting Flood Suppression
- Detect Slow Authentications
- Enhanced Handling for EAP sessions dropped by supplicant or NAS

**Filtering at Receiving Chain**



# Mobile Device Management (MDM) Vendors

# Mobile Device Management Vendors

## Limit the Risk From Mobile Devices

- New Requirement:

  We need to secure access to mobile devices that connect to corporate network and prevent potential loss of company data

- New Requirement:

  Require all employee mobile devices to be registered and comply with corporate policies before accessing network including:

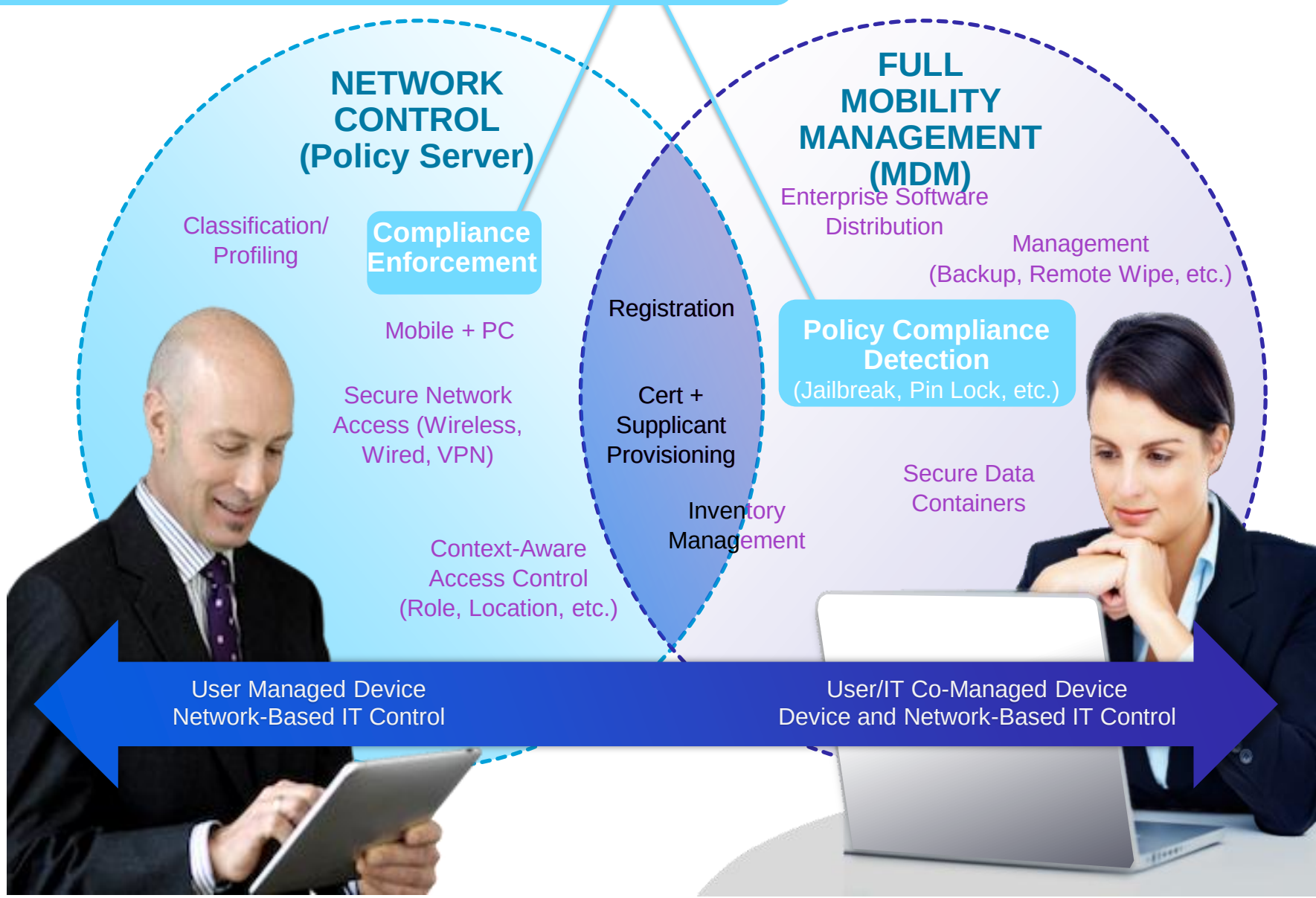
  – Pin Locked and Not Jail Broken

  – Wipe Corporate Data if Policy Broken

- New Term: Mobile Device Management (MDM)

Extends "posture" assessment and remediation to mobile devices

# Policy Server+ MDM



# Policy Server – MDM Integration

- REST API between Policy Server and MDM Console
- Integrate an MDM Vendor into the Policy Server (often OEM)

- Trend: Policy Server Vendor own MDM-Lite agent built into an existing agent

# Radius Change of Authorization (COA)

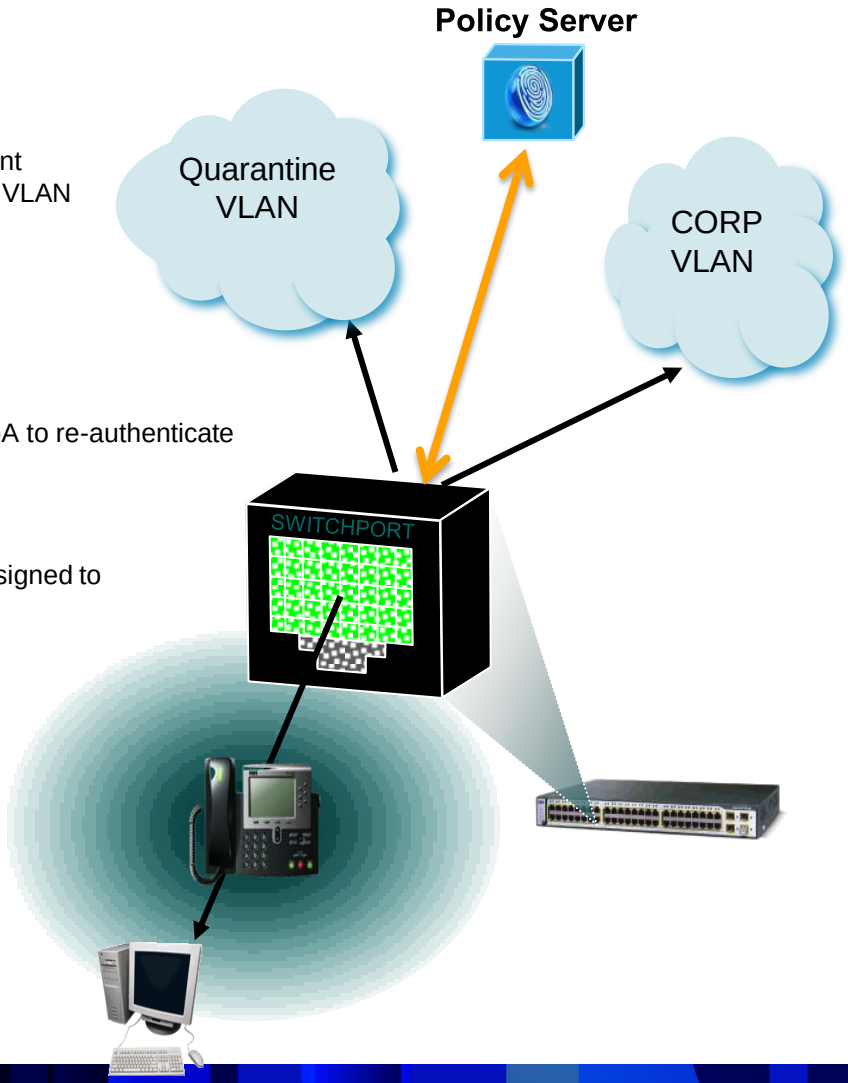
# Making this Work Well

## Radius Change of Authorization (CoA)

- Changes traditional radius from a one-way (NAD to server only) to a two-way highway
- CoA allows an enforcement device (switchport, wireless controller, VPN device) to change the VLAN/ACL/Redirection for a device/user without having to start the entire process all over again.
- Without it:  Manually remove the user from the network & then have the entire AAA process begin again.
  - Example: disassociate wireless device & have to join wireless again.
- RFC 3576 and 5176

# RADIUS Change of Authorization (CoA)

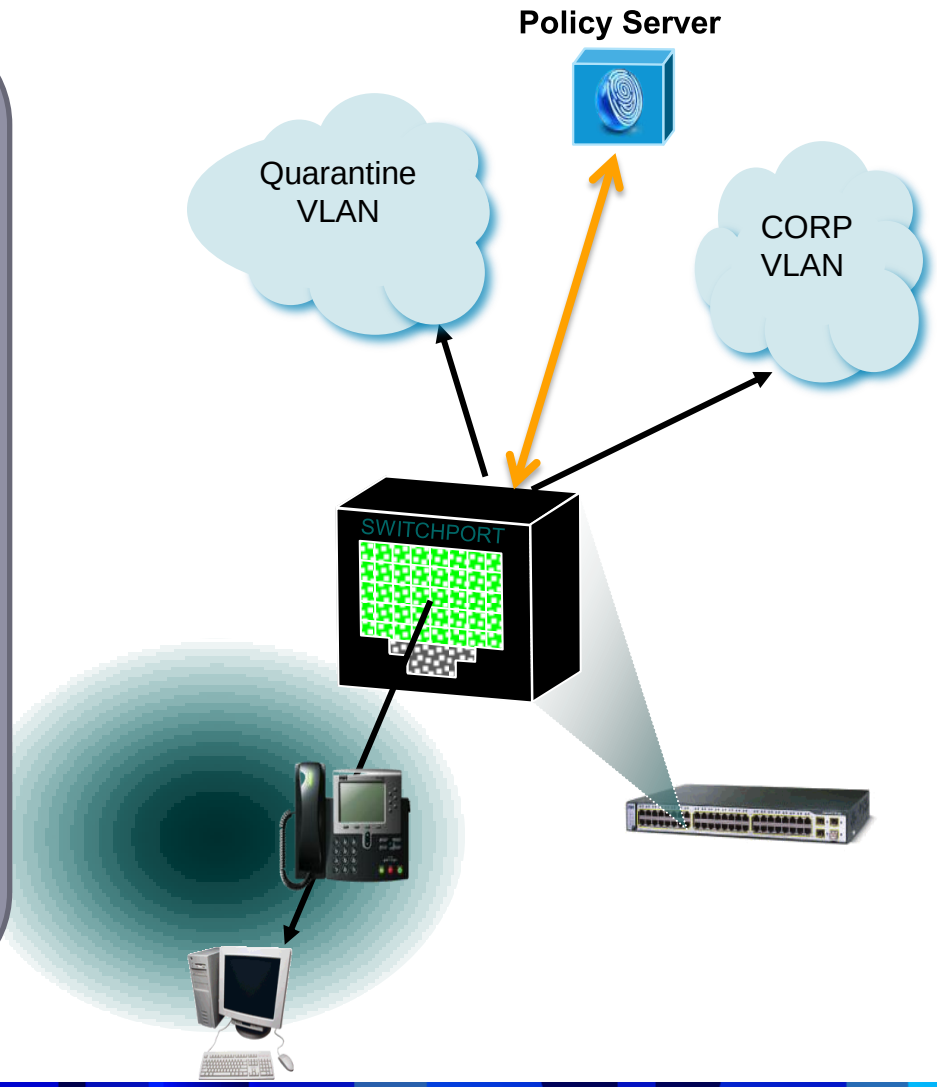
1. Endpoint fails Posture Assessment and gets assigned to Quarantine VLAN
2. Endpoint remediates itself and is reported: Posture=Compliant
3. Policy Server issues RADIUS CoA to re-authenticate
4. Client is re-authenticated and assigned to CORP VLAN



# RADIUS Change of Authorization (CoA)

## Dynamic session control from a Policy server

- Re-authenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port
- Session Query
  - For Active Services
  - For Complete Identity
  - Service Specific
- Service Activate
- Service De-activate
- Service Query



# Radius COA Inter-Vendor Interoperability – still immature

## Radius Change of Authorization (CoA)

- Port mismatches – RFC calls out port 3799
- Different vendors implement different message-types. Only Disconnect Message mandatory (cause user experience to suffer)
- A shared session-id between the policy server and the Network Access Device (NAD) is required to keep sync – not in the RFC
- URL Redirection at NAD not in RFC
- RFC 3576: http://tools.ietf.org/html/rfc3576
- RFC 5176: http://tools.ietf.org/html/rfc5176