CISCO

*TOMORROW*
*starts here.*

Cisco live!

# Securing Wireless LANs

BRKEWN-2664

Will Blake

Consulting Systems Engineer

#clmel

# Agenda

- Define terms and approach
- Enterprise WLANs – Threats, Vulnerabilities and Mitigation strategies
- External threats – Detection, Identification and Remediation
- Conclusion

# What does “secure” really mean?

# Dictionary Definition

1. Free from danger or attack
2. Free from risk of loss; safe
3. Free from risk of being intercepted or listened to by unauthorised persons
4. Reliable; Dependable
5. Assured; Certain

thefreedictionary.com
http://www.thefreedictionary.com/secure

# 3 Key Elements

1. Confidentiality
2. Integrity
3. Availability

Maybe some others:

Accountability, Auditability, Authenticity, Non-repudiation, Privacy, etc.

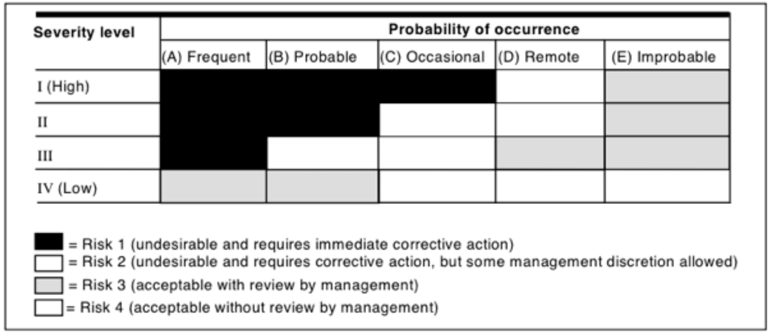
# How much security is enough?

1
2
3
4
5
6
7
8
9
0
OK

# Need to Assess Risk

## Risk Assessment Process

1. Identify threats and vulnerabilities
2. Assess consequence if they were to occur
3. Determine likelihood of occurrence
4. Calculate risk
5. For any unacceptable risk, identify mitigation/control options
6. Re-assess risk following application of controls



| Severity level | Probability of occurrence | | | | |
|---|---|---|---|---|---|
| | (A) Frequent | (B) Probable | (C) Occasional | (D) Remote | (E) Improbable |
| I (High) | ■ | ■ | ■ | □ | ▨ |
| II | ■ | ■ | □ | □ | ▨ |
| III | ■ | □ | □ | ▨ | ▨ |
| IV (Low) | ▨ | ▨ | □ | □ | □ |

■ = Risk 1 (undesirable and requires immediate corrective action)
□ = Risk 2 (undesirable and requires corrective action, but some management discretion allowed)
▨ = Risk 3 (acceptable with review by management)
□= Risk 4 (acceptable without review by management)

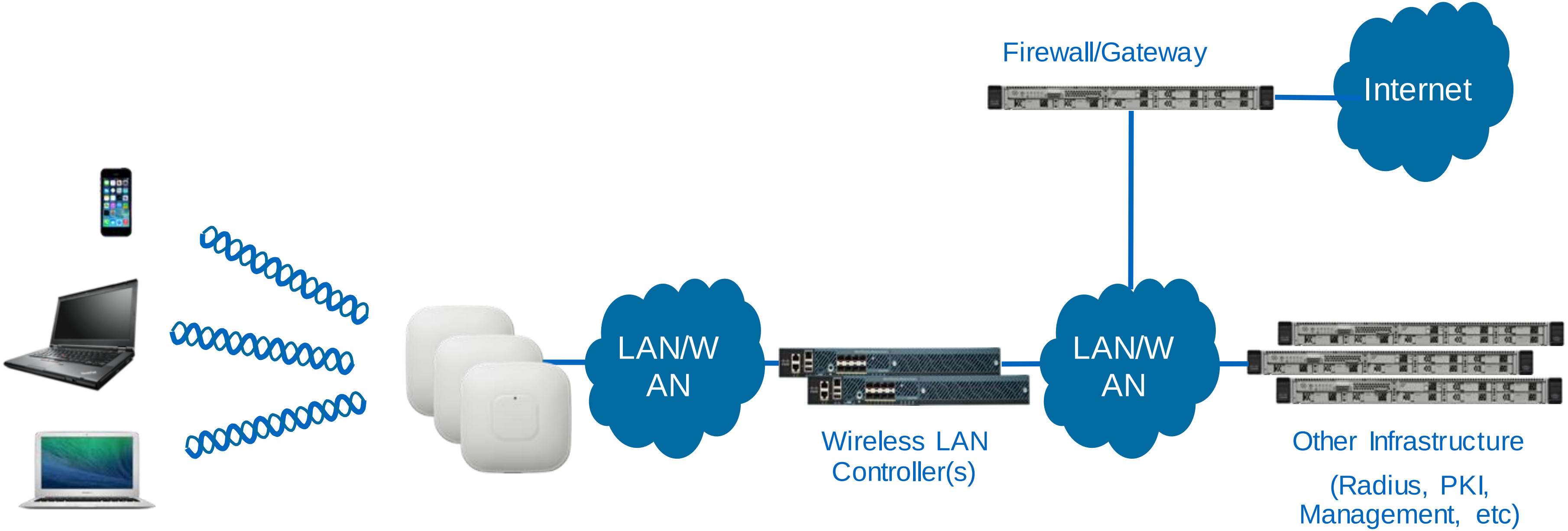
**NEEDS TO BE PERFORMED EARLY IN THE DESIGN PROCESS**

# Risk Mitigation

## Some thoughts

- The only vector that can be changed is “likelihood of occurrence”
- Common approaches:
  - Add time
  - Make compromise more difficult
- Need to consider cost and usability
- Technology is not always the answer
- Management support is mandatory

# A Typical Enterprise Network



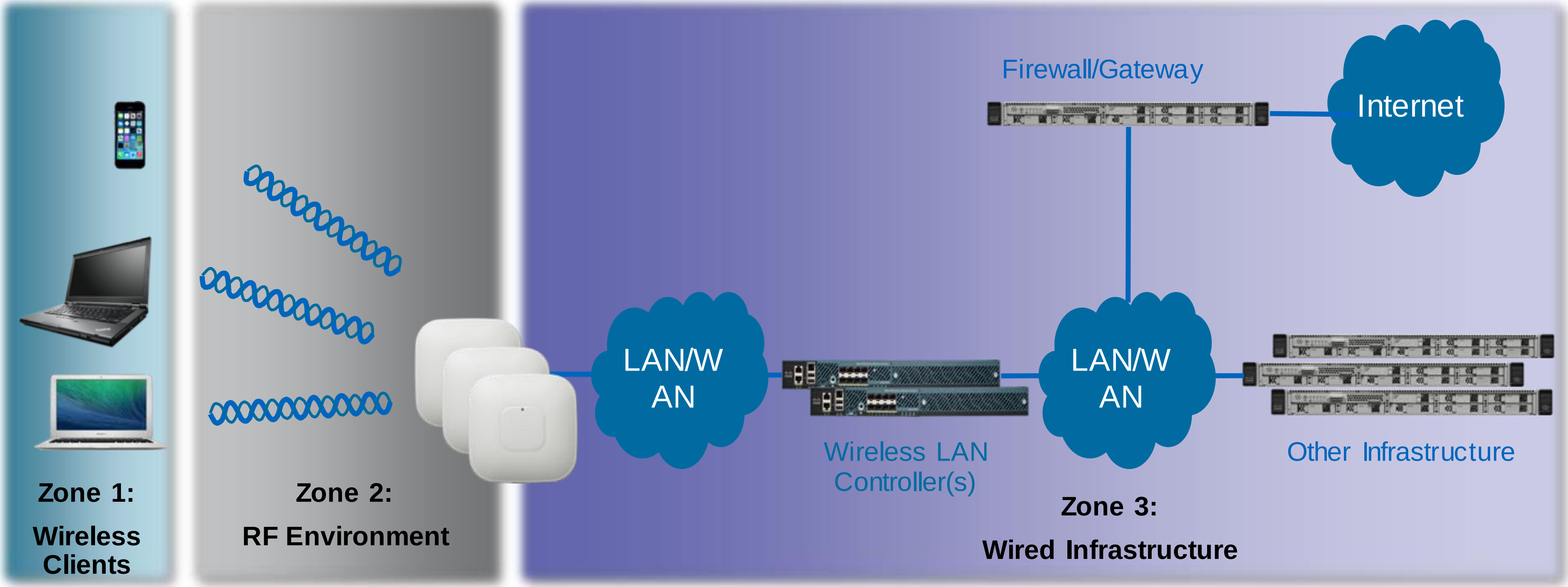
# Wireless Threats and Vulnerabilities

- Wireless propagates beyond the traditional physical boundaries of the wired network
  - Attack could originate from outside traditional enterprise boundaries
    - Passive scanning attacks
    - Active spoofing attacks
    - Active jamming or DoS attacks

- Rogue APs can be a source of different vulnerabilities
  - Honeypot APs
  - Unsecured backdoor access

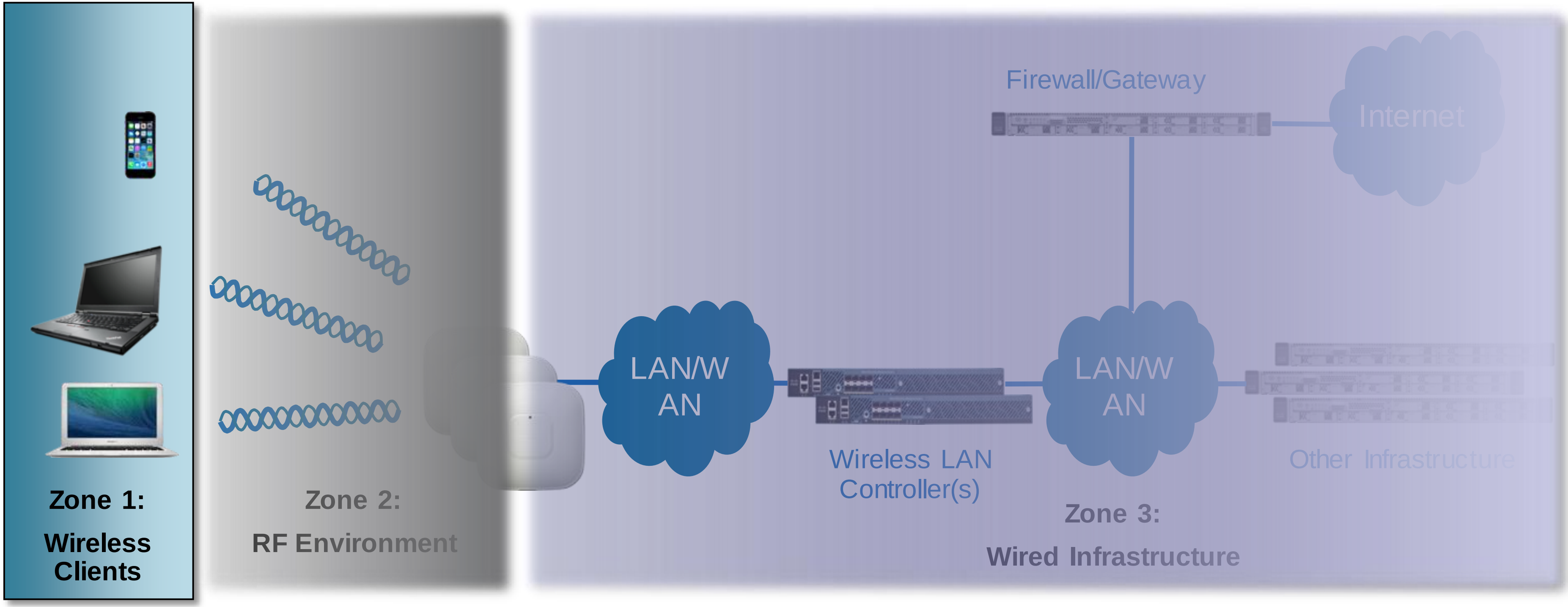
- Wireless Clients themselves can introduce vulnerabilities as well
  - Bridge wireless to wired network
  - Unsecured Hot-Spot usage
  - Data Seepage

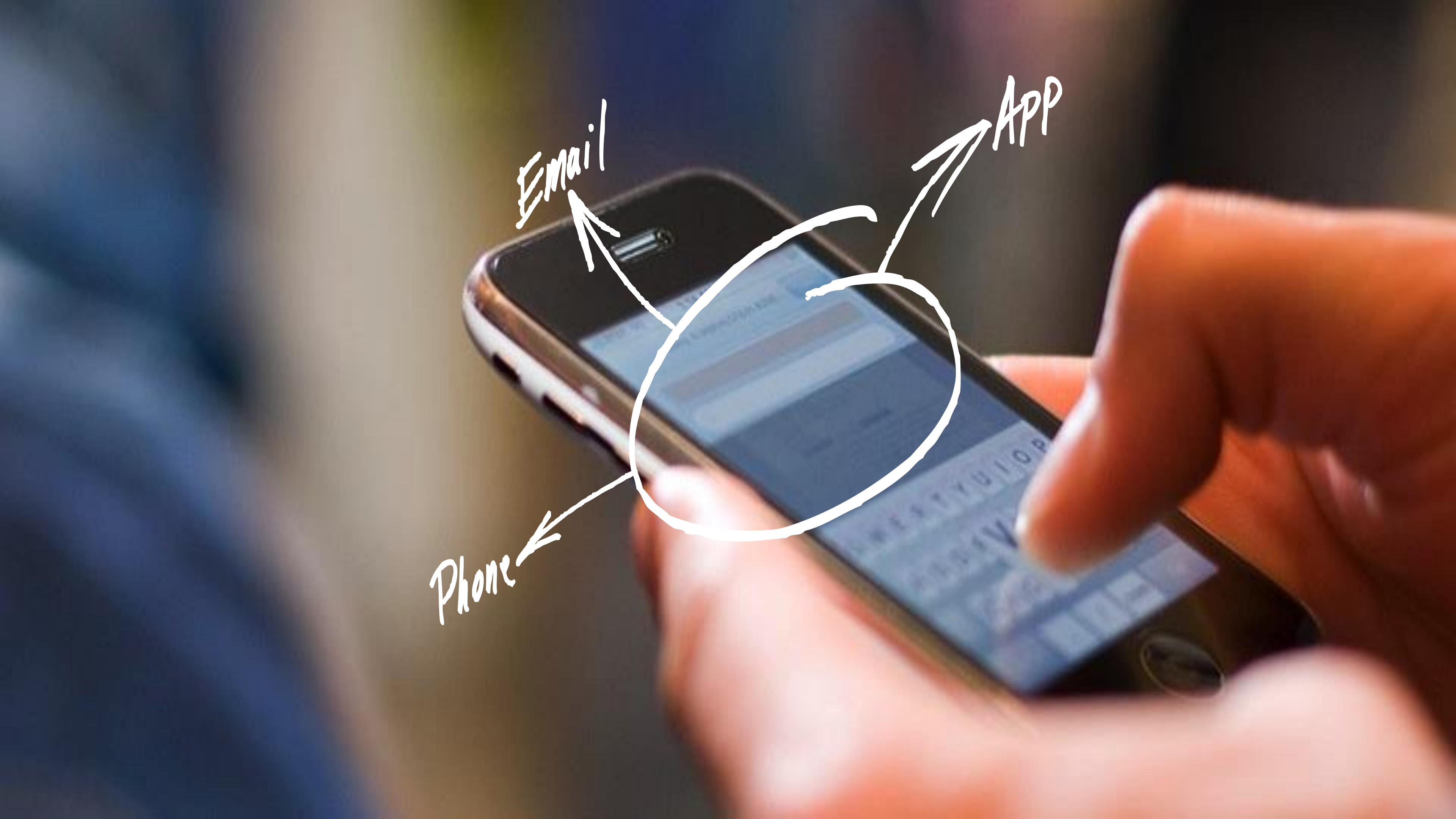
# Assessing Risk



# Wireless Clients

# Assessing Risk – Wireless Clients




Email
App
Phone

# Wireless Client Considerations

## Some thoughts

- What user groups?
  - Guests?  Do they need to be treated differently
- How many devices?  What kind?
  - Do they all represent the same level of risk?  Probably not
- Usage patterns
  - Are they different to usage of wired devices?  Probably yes
- Access locations
  - Are wireless clients accessing the network from new locations?  Quite likely

# Wireless Clients - Risks, Threats and Vulnerabilities

## Analysed through the CIA lens

- Confidentiality
  - What data is stored on the device?
  - Is it appropriately secured?
  - Who has/could have access? Directly? Indirectly?
- Integrity
  - Need to ensure that data isn't altered without authorisation
  - Also want to ensure the integrity of your network
- Availability
  - Vital to ensure that the right person has the right access to the right information at the right time from the right device

# Mitigation

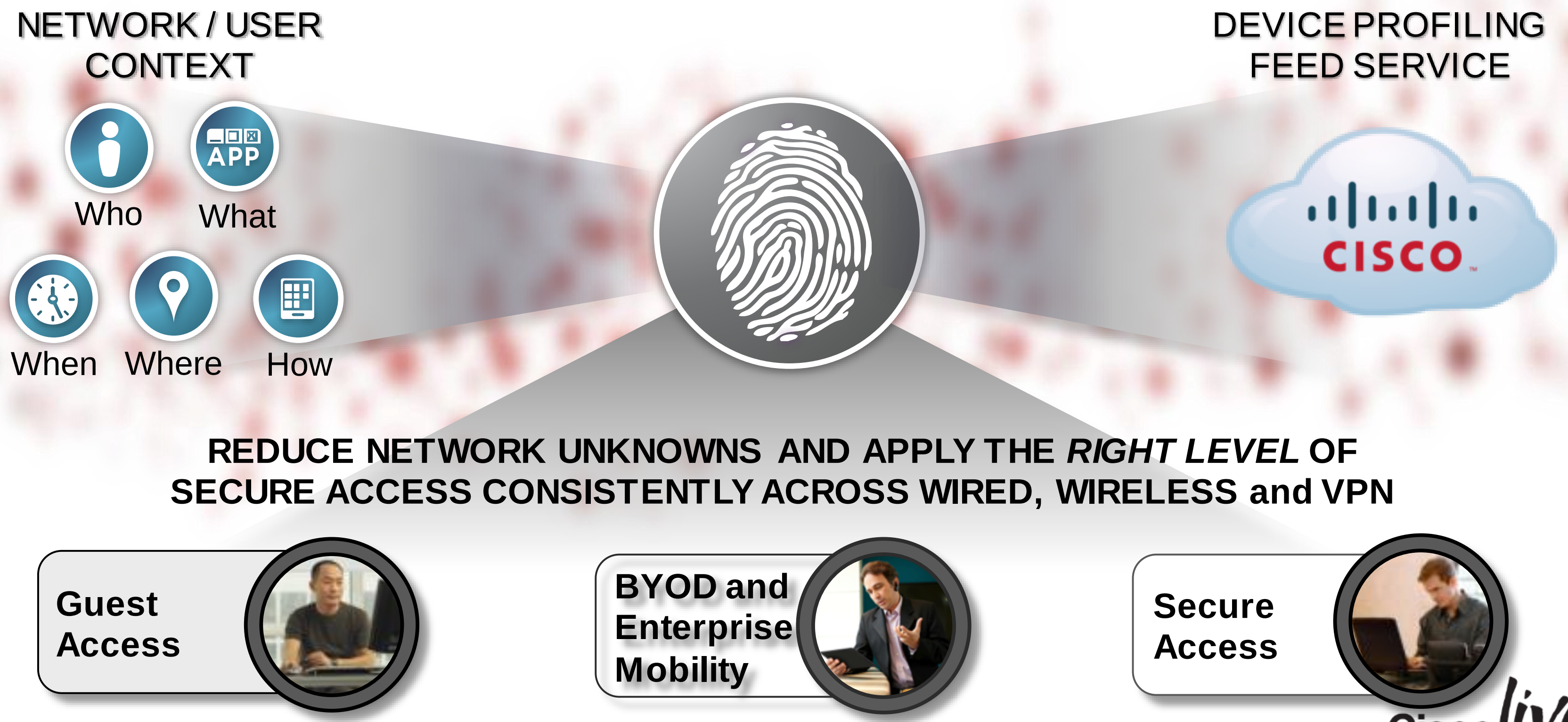
## Identity and device management

- Who is trying to connect to the network?
- What type of device is it? What is it’s current state?
- What time of day is it?
- Where is it connecting from? Wired? Wireless? VPN?
- Based on all of the above, how much do I trust this device?

What access should the user and device combination have to the network and other corporate resources?

# Cisco Identity Services Engine

## Delivering Visibility, Context, and Control to Secure Network Access



NETWORK / USER CONTEXT

Who What

When Where How

DEVICE PROFILING FEED SERVICE

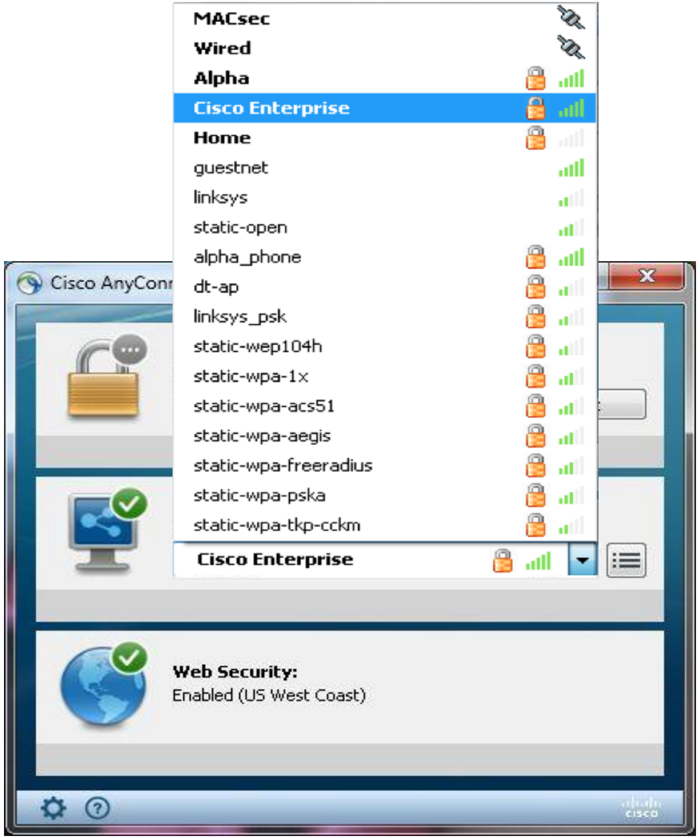
REDUCE NETWORK UNKNOWNS AND APPLY THE *RIGHT LEVEL* OF SECURE ACCESS CONSISTENTLY ACROSS WIRED, WIRELESS and VPN

**Guest Access**

**BYOD and Enterprise Mobility**

**Secure Access**

# AnyConnect

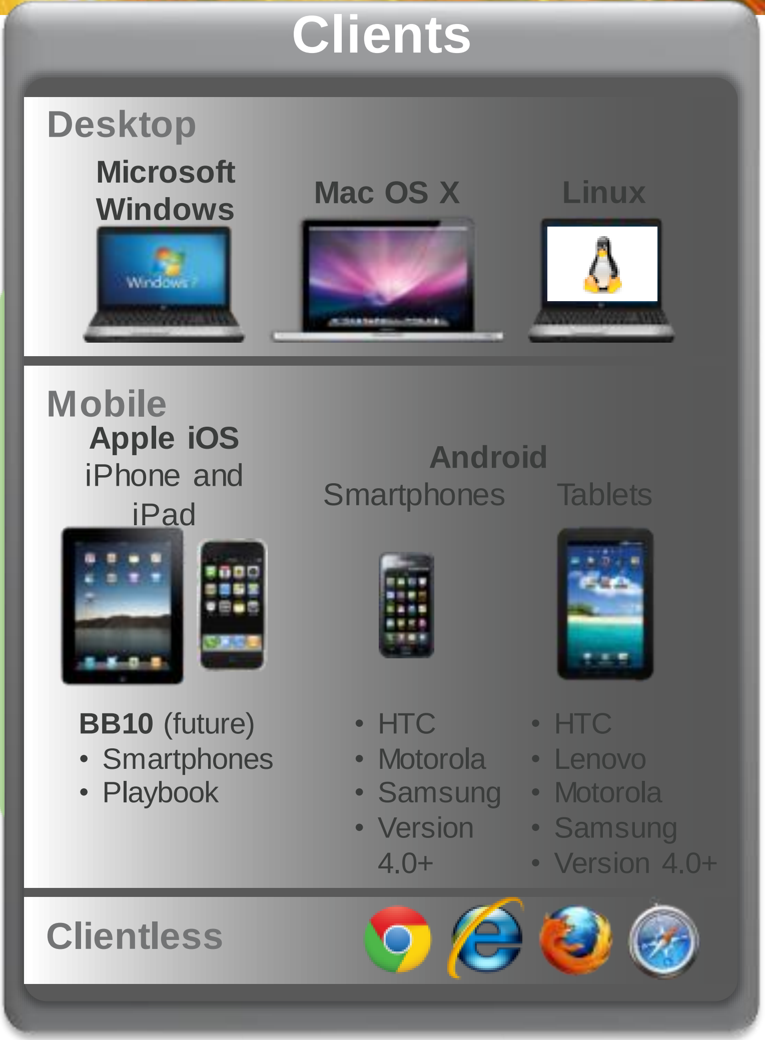


Cisco AnyConn

MACsec
Wired
Alpha
Cisco Enterprise
Home
guestnet
linksys
static-open
alpha_phone
dt-ap
linksys_psk
static-wep104h
static-wpa-1x
static-wpa-acs51
static-wpa-aegis
static-wpa-freeradius
static-wpa-pska
static-wpa-tkp-cckm

Cisco Enterprise

**Web Security:**
Enabled (US West Coast)



## Clients

### Desktop

**Microsoft Windows**

**Mac OS X**

**Linux**

### Mobile

**Apple iOS**
iPhone and iPad

**BB10** (future)
- Smartphones
- Playbook

**Android**

Smartphones
- HTC
- Motorola
- Samsung
- Version 4.0+

Tablets
- HTC
- Lenovo
- Motorola
- Samsung
- Version 4.0+

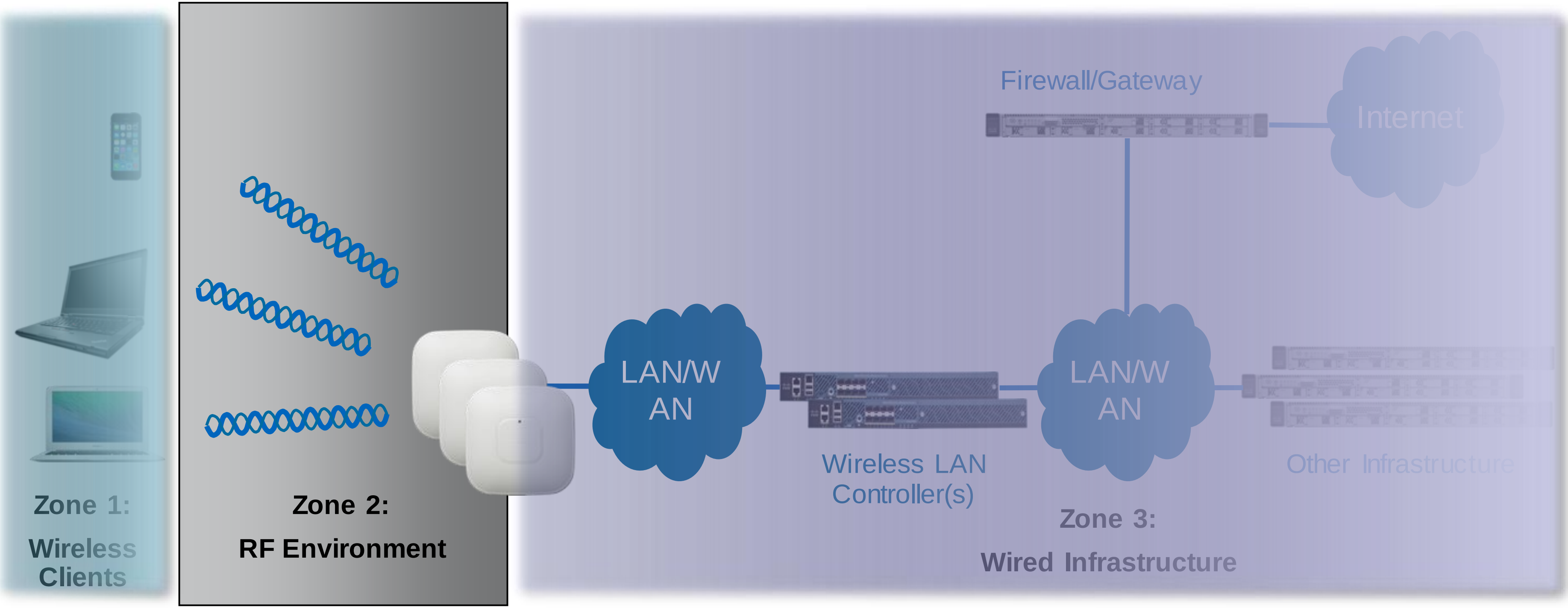
### Clientless

# Risk Assessment – Mobile Devices

| RISK | MITIGATION |
|---|---|
| Unauthorised access to data viewed on mobile device | **AnyConnect** – control network access<br>**ISE** – granular access controls once connected |
| Mobile device lost or stolen | **ISE** – revoke network access<br>**MDM** – remote wipe |
| Unauthorised data stored on mobile device | **ISE** – granular network access controls<br>*Additional mitigation may be necessary (depending on corporate security policy) |
| Unauthorised mobile device used to access and/or compromise the wireless network | **Various controls** – (ISE, network infrastructure, AAA, WIPS, Layer 4 – 7 controls, ACLs, etc.) |
| Mobile device used to created an unauthorised "hotspot" or bridge to the corporate network | **AnyConnect** – control active network interfaces on mobile device<br>**Wired 802.1x** – manage wired access |

# Securing the RF Environment

# Assessing Risk – RF Transmission

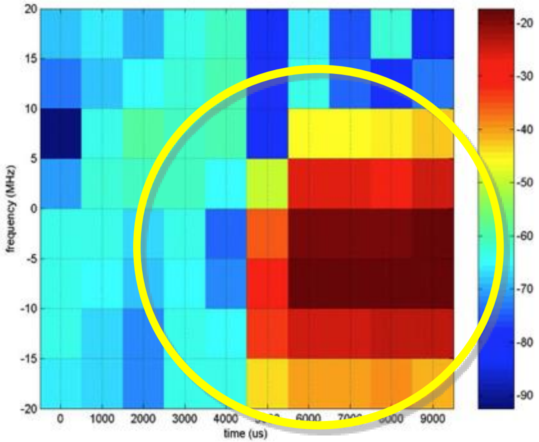


# RF Risks, Threats and Vulnerabilities

- Confidentiality
  - Ensure that any intercepted data is not readable
  - Ensure that only authorised users and devices are able to access the network
- Integrity
  - ensure that transmitted data and management traffic is not altered in transit
- Availability
  - deal with RF interference, both intentional and accidental

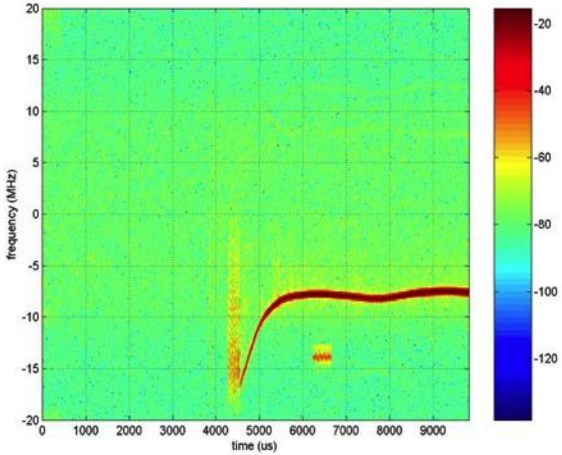
# Radio Frequency (RF) Availability

## Spectrum Intelligence Solution - Cisco CleanAir



CleanAir
Hardware based Solution

32 times WiFi chip's visibility
Accurate classification
Multiple device recognition



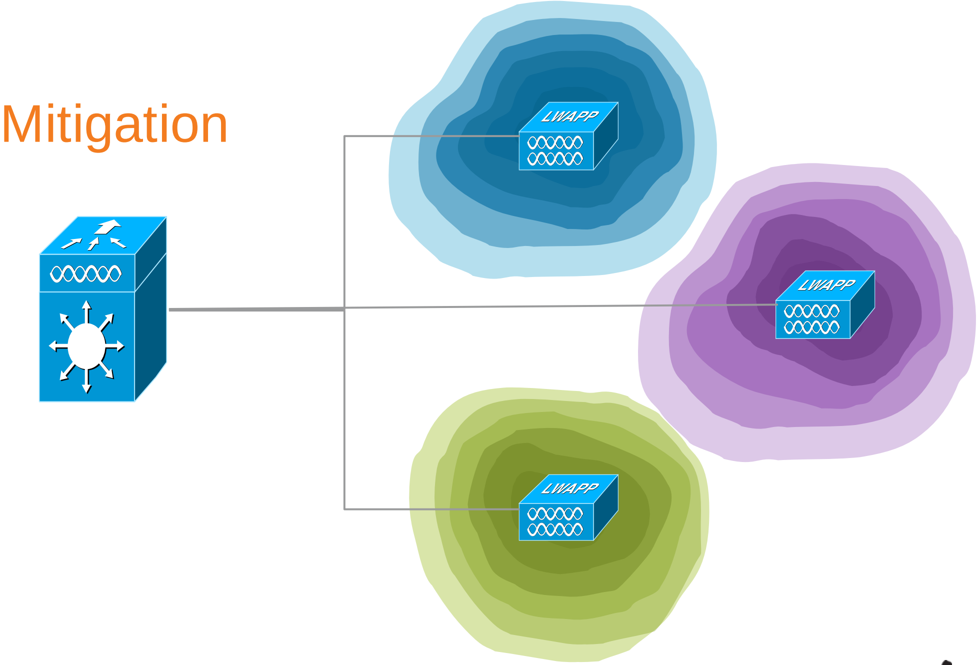
- Spectrum intelligence solution designed to proactively manage the challenges of a shared spectrum
- Assess impact to Wi-Fi performance; proactively change channels when needed
- CleanAir Radio ASIC: Only ASIC based solution can reliably detect interference sources
- TURN IT ON!

For more info: http://www.cisco.com/en/US/netsol/ns1070

# Radio Resource Management

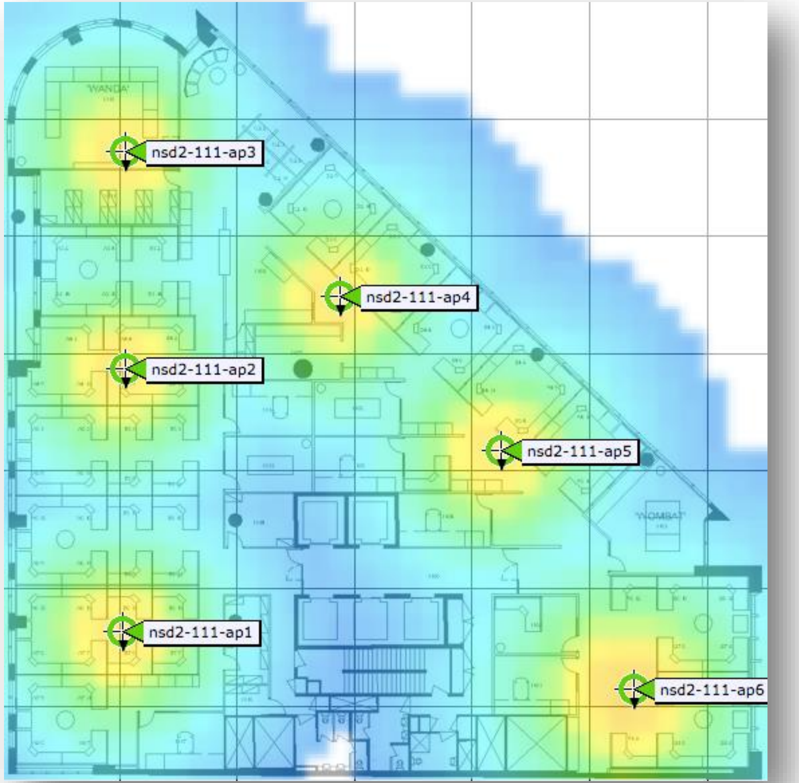
1. Dynamic Channel Assignment
2. Transmit Power Control
3. Coverage Hole Detection and Mitigation

- What It Does
  - Dynamically balances infrastructure and mitigate changes
  - Monitor and maintain coverage for all clients
  - Provide the optimal throughput under changing conditions



# Radio Frequency (RF) Emanation

- All Cisco AP's use variable power radios
- There will ALWAYS* be some RF leakage
- With a decent antenna your wireless data transmission can be intercepted from some distance away

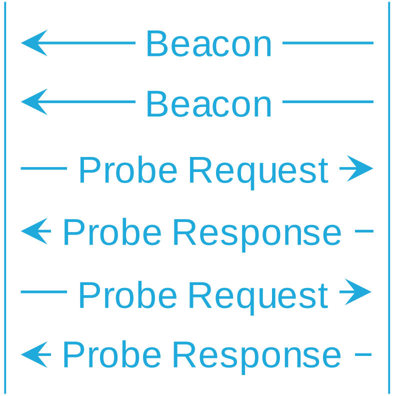


# Wireless Encryption

| | |
|---|---|
| WPA | • A snapshot of the 802.11i Standard<br>• Commonly used with TKIP encryption |
| WPA2 | • Final version of 802.11i<br>• Commonly used with AES encryption |
| Authentication Mechanisms | • Personal (PSK – Pre-Shared Key)<br>• Enterprise (802.1X/EAP) |

# 802.11 Fundamentals

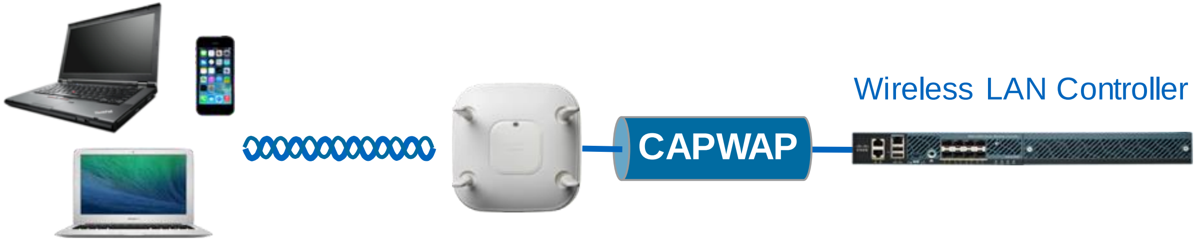
## Beacons and Probes

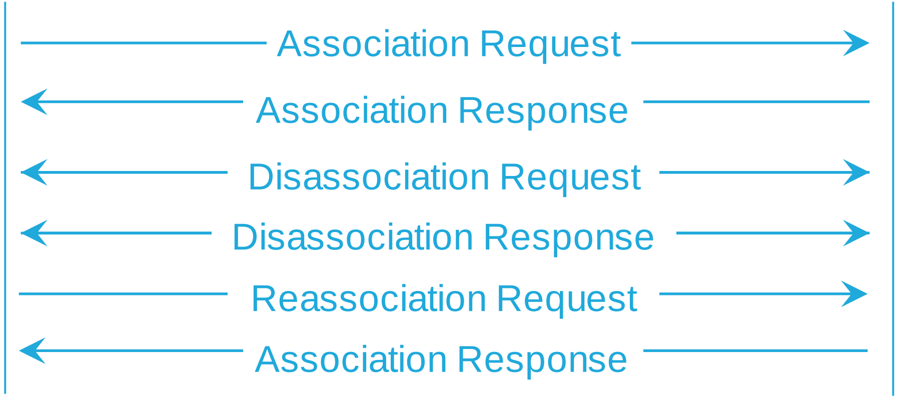


| | |
|---|---|
| ← Beacon — | SSID = blizzard, Security = WPA2-Enterprise |
| ← Beacon — | SSID = ciscolive, Security = WPA2-Personal |
| — Probe Request → | SSID = blizzard |
| ← Probe Response – | SSID = blizzard, Security = WPA2-Enterprise |
| — Probe Request → | SSID = ciscolive |
| ← Probe Response – | SSID = ciscolive, Security = WPA2-Personal |

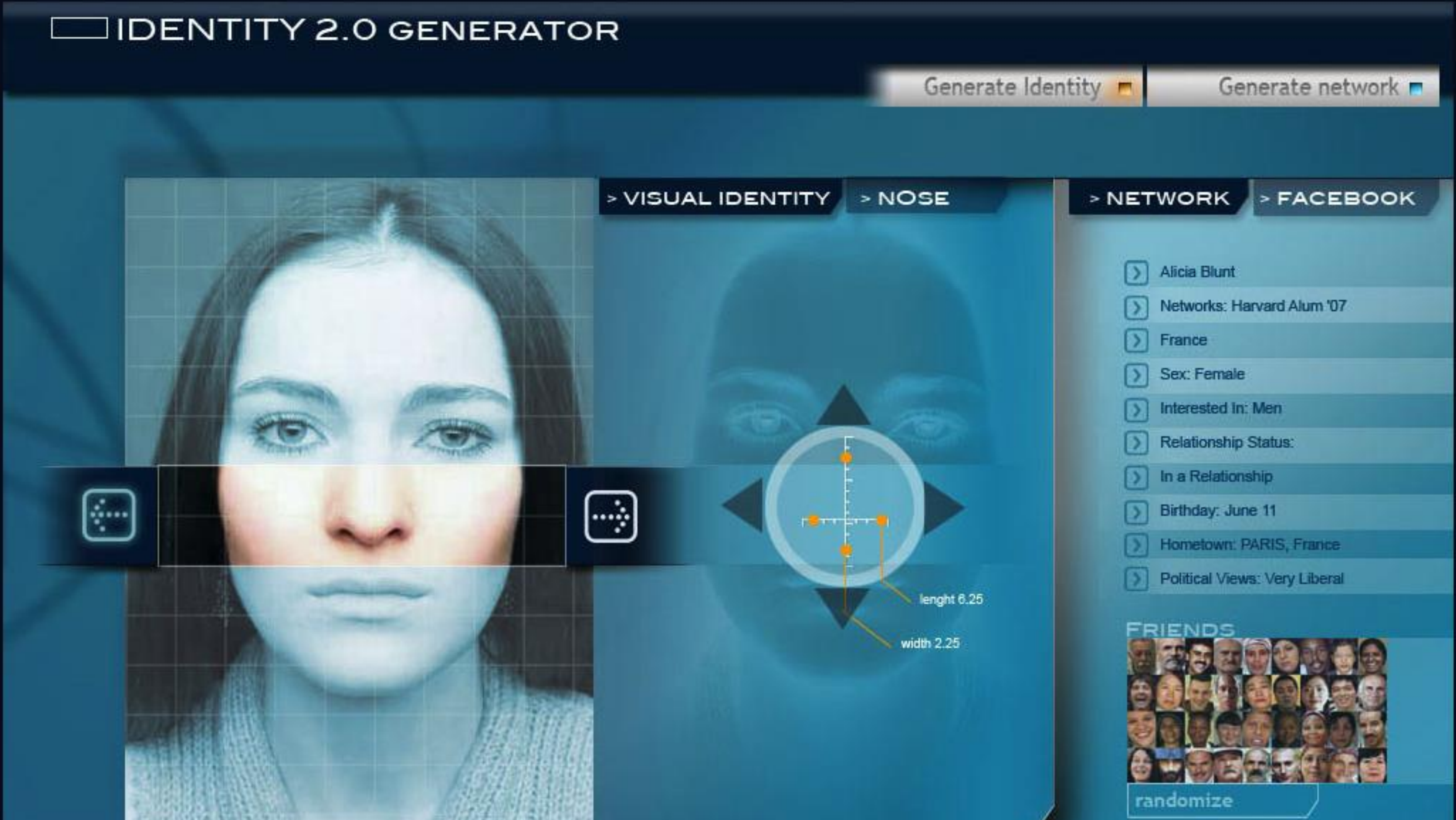
# 802.11 Fundamentals

## Association





| | |
|---|---|
| Association Request → | SSID = blizzard |
| ← Association Response | SSID = blizzard, Security = WPA2-Enterprise |
| ← Disassociation Request → | SSID = blizzard |
| ← Disassociation Response → | SSID = blizzard |
| Reassociation Request → | SSID = blizzard |
| ← Association Response | SSID = blizzard, Security = WPA2-Enterprise |



Alicia Blunt

Networks: Harvard Alum '07

France

Sex: Female

Interested In: Men

Relationship Status:

In a Relationship

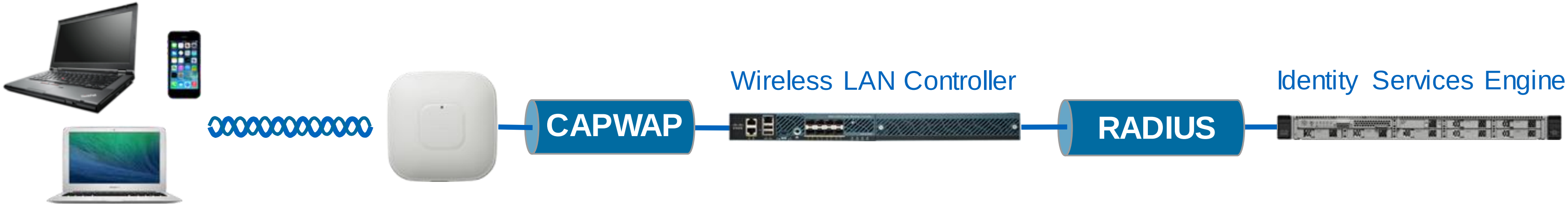
Birthday: June 11

Hometown: PARIS, France

Political Views: Very Liberal

# 802.11 Fundamentals

## Authentication



Wireless LAN Controller

Identity Services Engine

CAPWAP

RADIUS

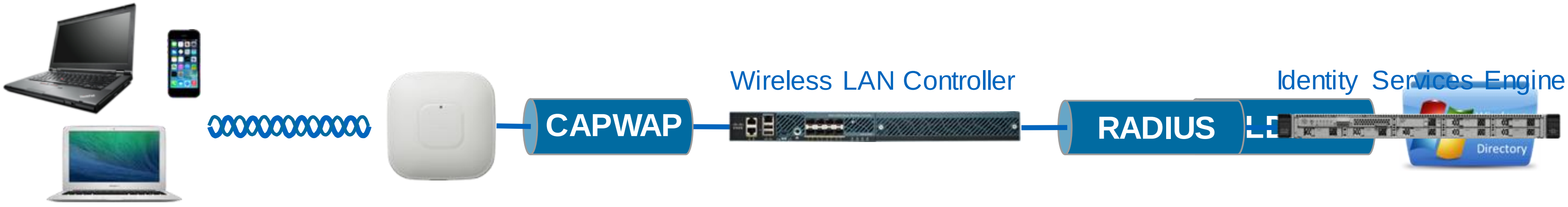
Supplicant

Authenticator

Authentication Server

# 802.11 Fundamentals

## Authentication



Wireless LAN Controller

Identity Services Engine

Supplicant

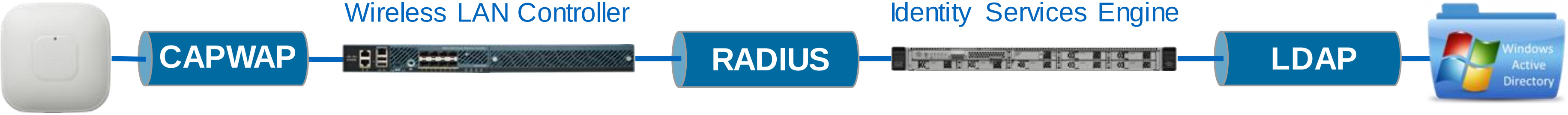
Authenticator

Authentication Server

Credential Server

# 802.11 Fundamentals

## Authentication



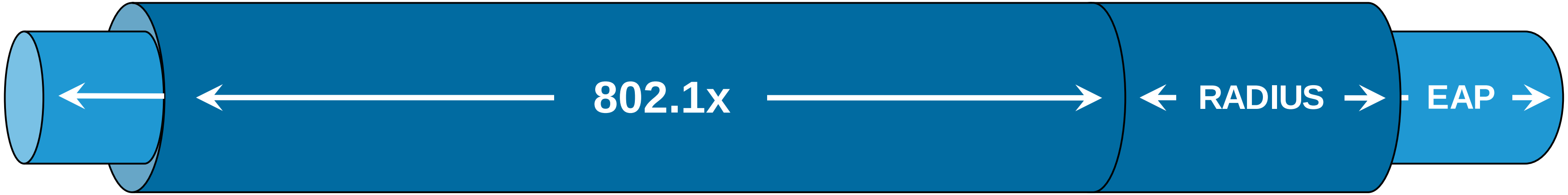
Wireless LAN Controller

Identity Services Engine

Authenticator

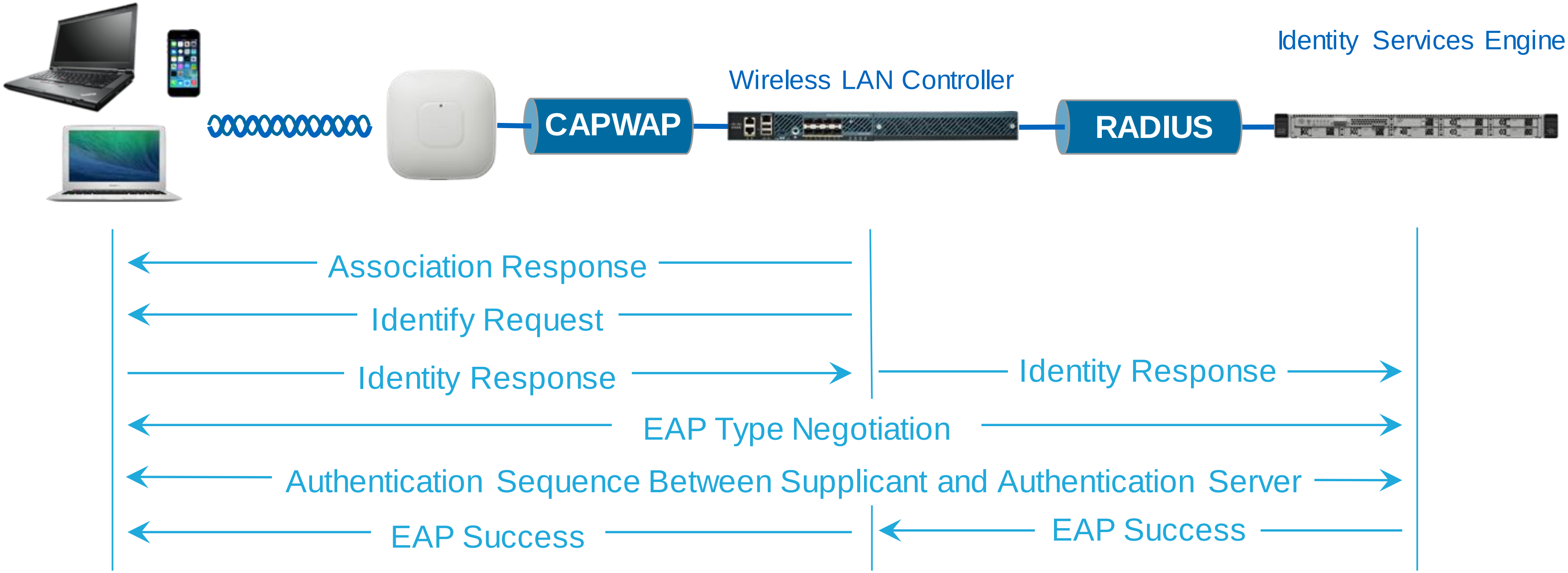
Authentication Server

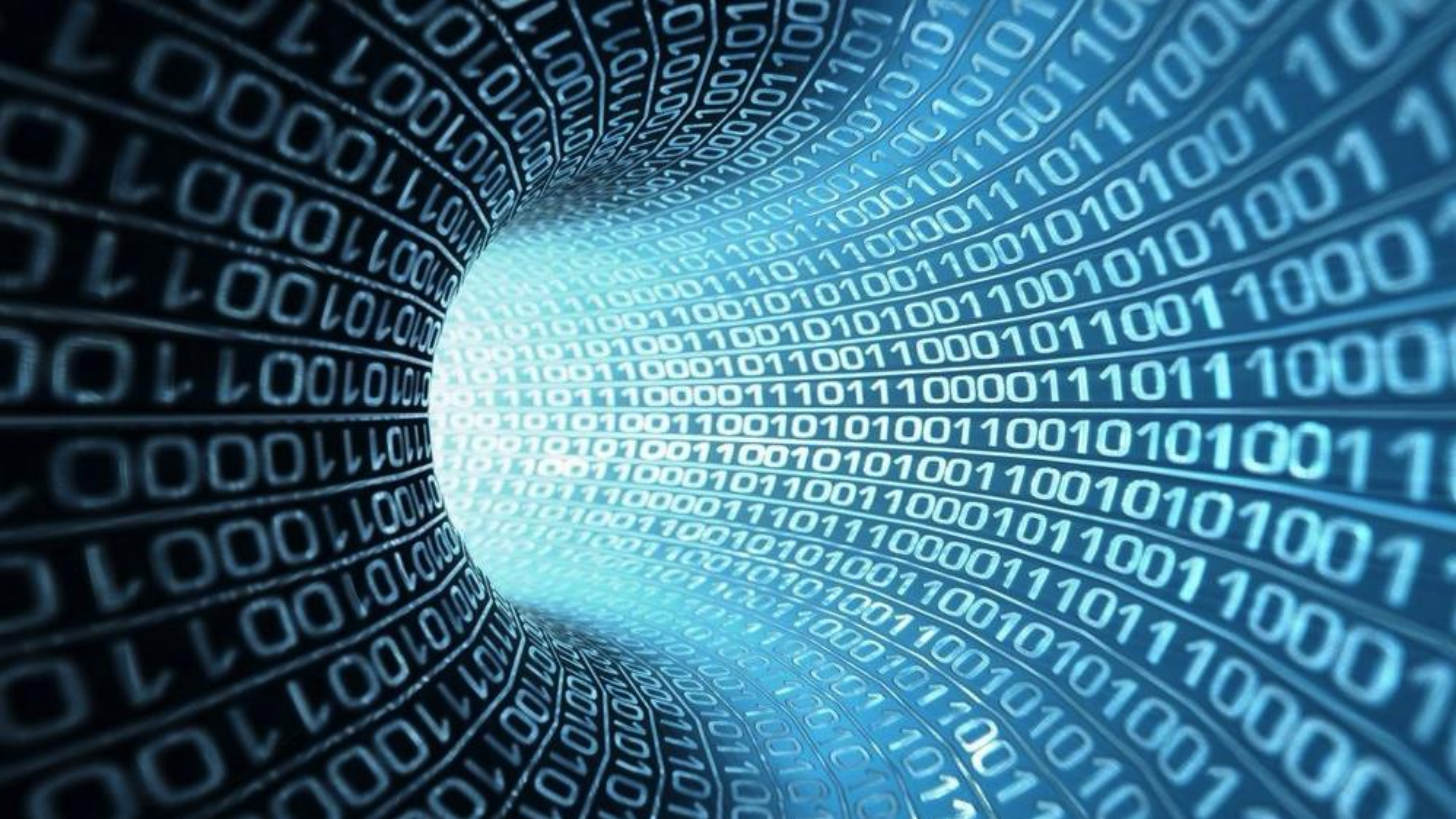
Credential Server



# 802.11 Fundamentals

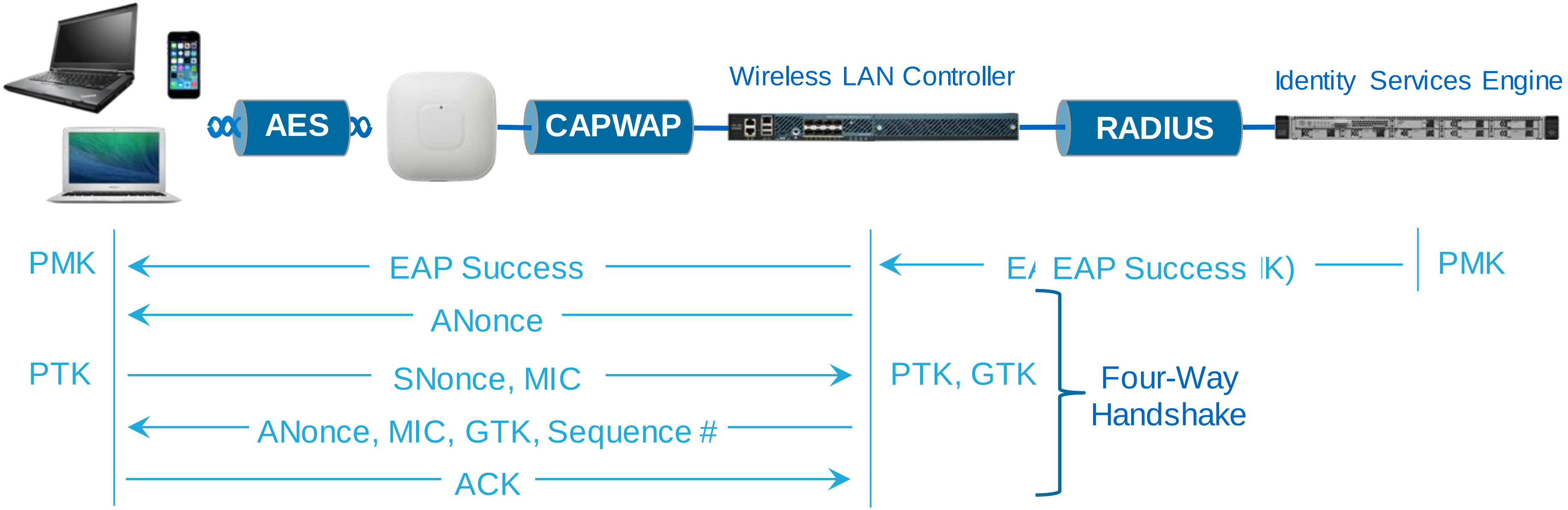
## Authentication





# 802.11 Fundamentals

## Encryption



PTK = SHA(PMK + ANonce + SNonce + AP MAC + STA MAC)

# Secure Fast Roaming

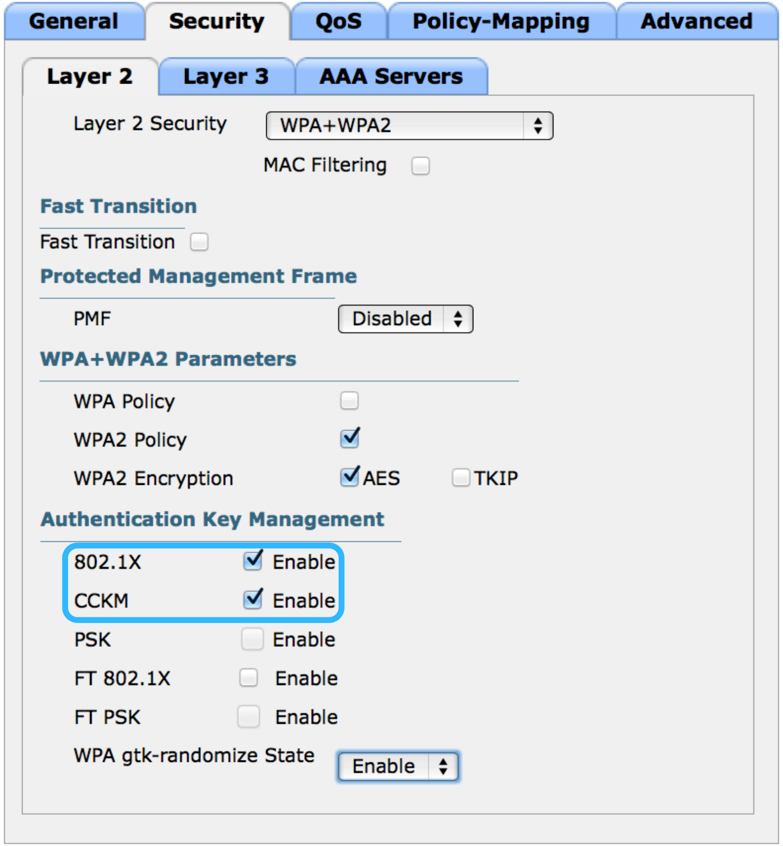
## Challenges

- Client channel scanning and AP selection
- Re-authentication of client device and re-keying

# Secure Fast Roaming

## Cisco Compatible Extensions

- Client channel scanning and AP selection
  - Improved via Cisco Compatible Extensions (CCX) Neighbour Lists
- Re-authentication of client device and re-keying
  - Cisco Centralised Key Management (CCKM)
- In *highly controlled test environments*, CCKM roam times measure 5-8ms
- Available in CCX enabled clients



Layer 2 Security: WPA+WPA2

MAC Filtering □

**Fast Transition**

Fast Transition □

**Protected Management Frame**

PMF: Disabled

**WPA+WPA2 Parameters**

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

**Authentication Key Management**

802.1X ☑ Enable

CCKM ☑ Enable

PSK □ Enable

FT 802.1X □ Enable

FT PSK □ Enable

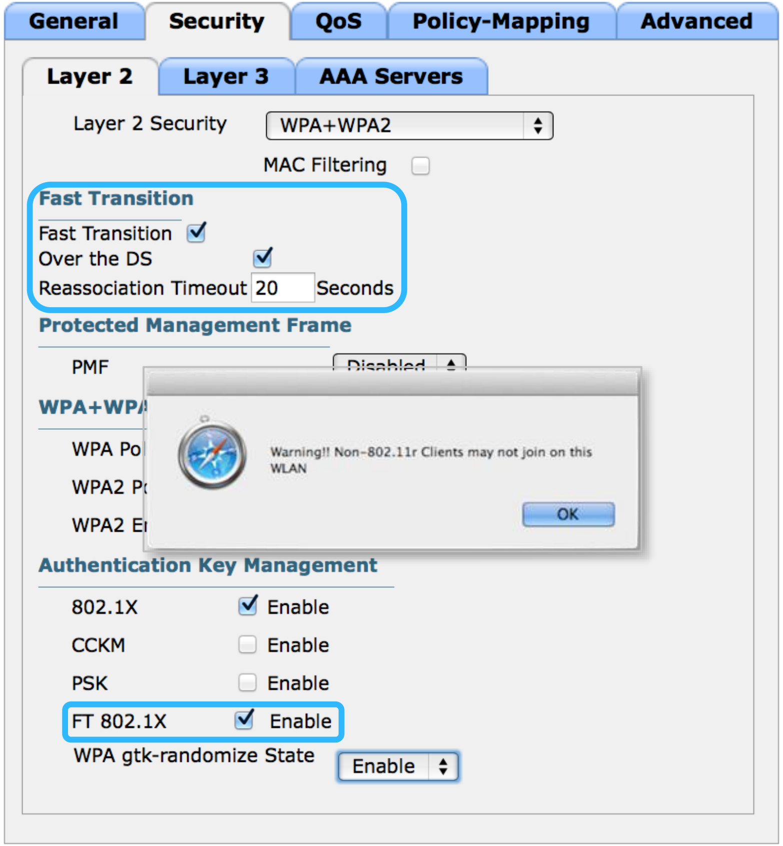
WPA gtk-randomize State: Enable

Compatible

# Secure Fast Roaming

## Voice-Enterprise and 802.11k and 802.11r

- Client channel scanning and AP selection
  - Improved via 802.11k Neighbour Lists
- Re-authentication of client device and re-keying
  - 802.11r based on CCKM
- Available in Voice-Enterprise certified clients
  - Due to changes to 802.11 management frames, older client drivers may not understand the 11r response frame



Layer 2 Security: WPA+WPA2

MAC Filtering ☐

**Fast Transition**

Fast Transition ☑

Over the DS ☑

Reassociation Timeout 20 Seconds

**Protected Management Frame**

PMF Disabled

**WPA+WPA**

WPA Po

WPA2 Po

WPA2 En

Warning!! Non-802.11r Clients may not join on this WLAN

OK

**Authentication Key Management**

802.1X ☑ Enable

CCKM ☐ Enable

PSK ☐ Enable

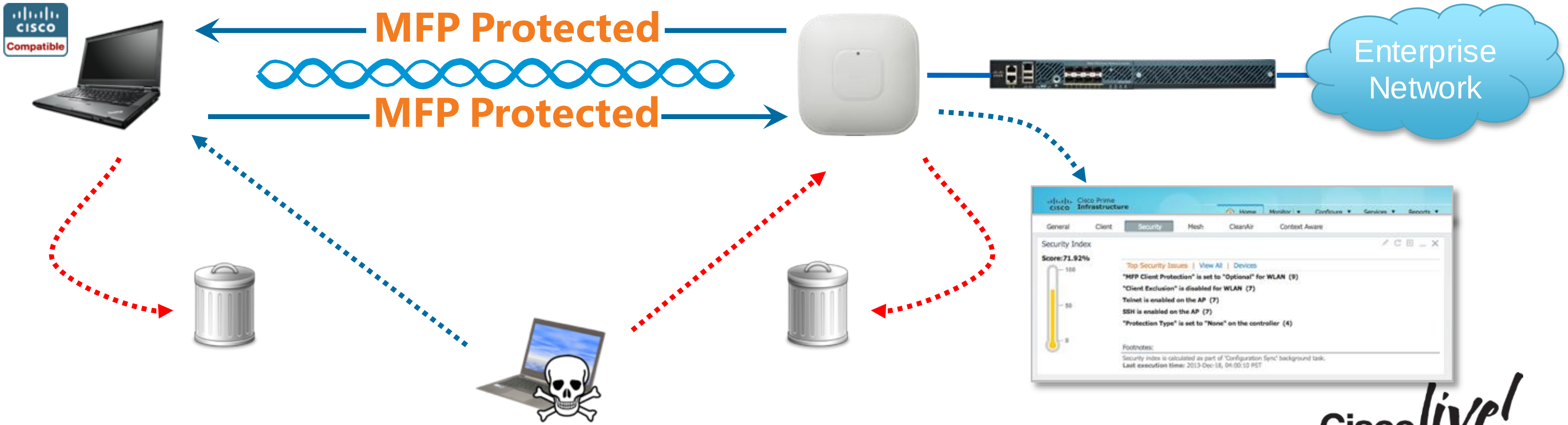
FT 802.1X ☑ Enable

WPA gtk-randomize State Enable

35
30
25
20
15

# Management Frame Protection

- Infrastructure Management Frame Protection
  - Detection
- Client Management Frame Protection
  - Prevention



Cisco Prime Infrastructure

Security Index

Score:71.92%

Top Security Issues | View All | Devices

"MFP Client Protection" is set to "Optional" for WLAN (9)

"Client Exclusion" is disabled for WLAN (7)

Telnet is enabled on the AP (7)

SSH is enabled on the AP (7)

"Protection Type" is set to "None" on the controller (4)

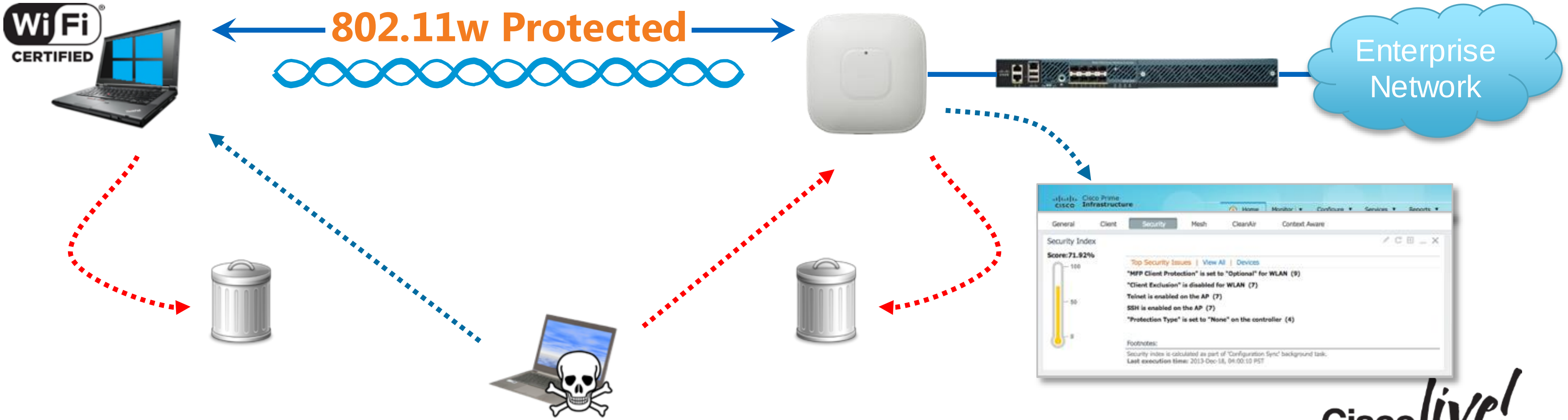
Footnotes:

Security index is calculated as part of 'Configuration Sync' background task.
Last execution time: 2013-Dec-18, 04:00:10 PST

# Management Frame Protection

## 802.11w and Protected Management Frames

- Unicast Management Frames
  - Confidentiality and Integrity Protection
- Multicast Management Frames
  - Integrity Protection



Security Index

Score:71.92%

Top Security Issues | View All | Devices

"MFP Client Protection" is set to "Optional" for WLAN (9)

"Client Exclusion" is disabled for WLAN (7)

Telnet is enabled on the AP (7)

SSH is enabled on the AP (7)

"Protection Type" is set to "None" on the controller (4)

Footnotes:

Security index is calculated as part of 'Configuration Sync' background task.

Last execution time: 2013-Dec-18, 04:00:10 PST

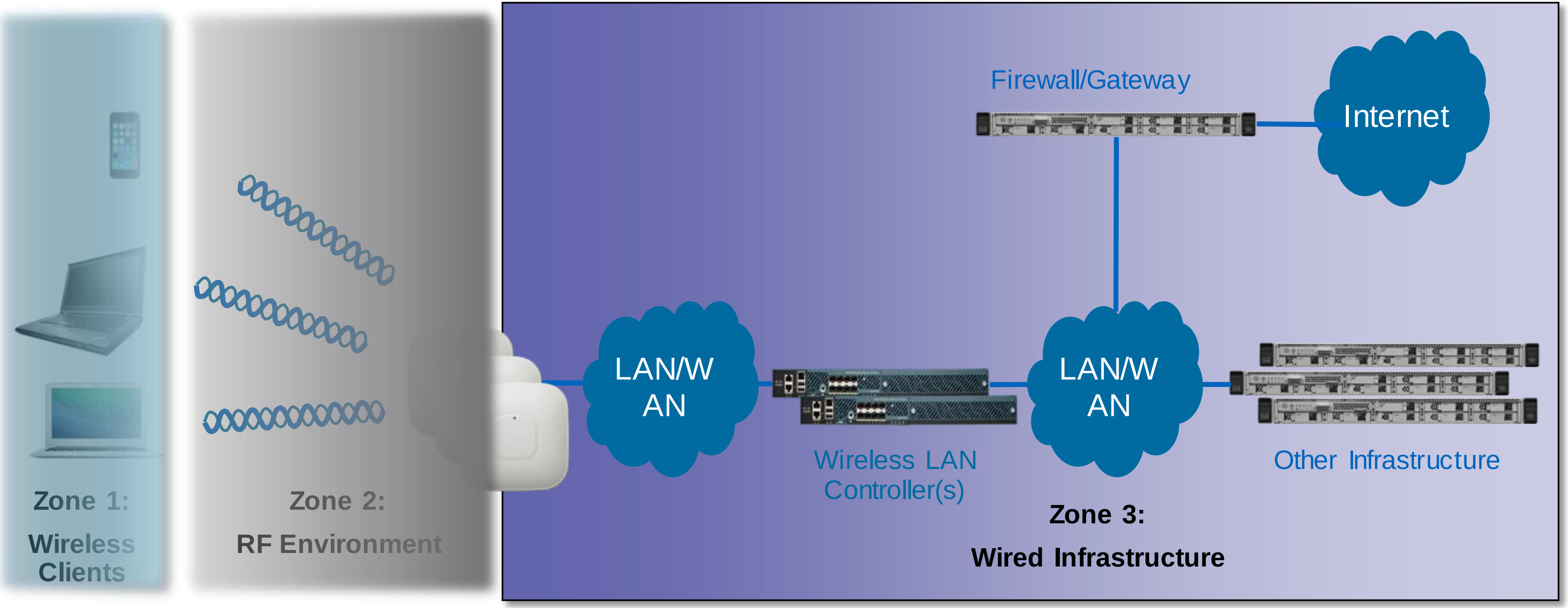
# Risk Assessment

## RF environment

| RISK | MITIGATION |
|---|---|
| Data transmitted over the wireless infrastructure can be intercepted and read | WPA2 uses AES encryption to protect all transmitted data |
| Wireless control traffic is altered in transit | Management Frame Protection ensures the integrity of all control traffic |
| An attacker attempts to compromise the network via spoofed control traffic | Management Frame Protection ensures the integrity of all control traffic |
| Availability of the wireless network compromised by RF interference, either accidental or malicious | CleanAir automatically detects, classifies and mitigates interference |
| An attacker attempts to masquerade as a legitimate corporate WLAN | Management Frame Protection (and WIPS – covered later) |

# Wired Infrastructure

# Implications of wireless infrastructure on the existing wired network

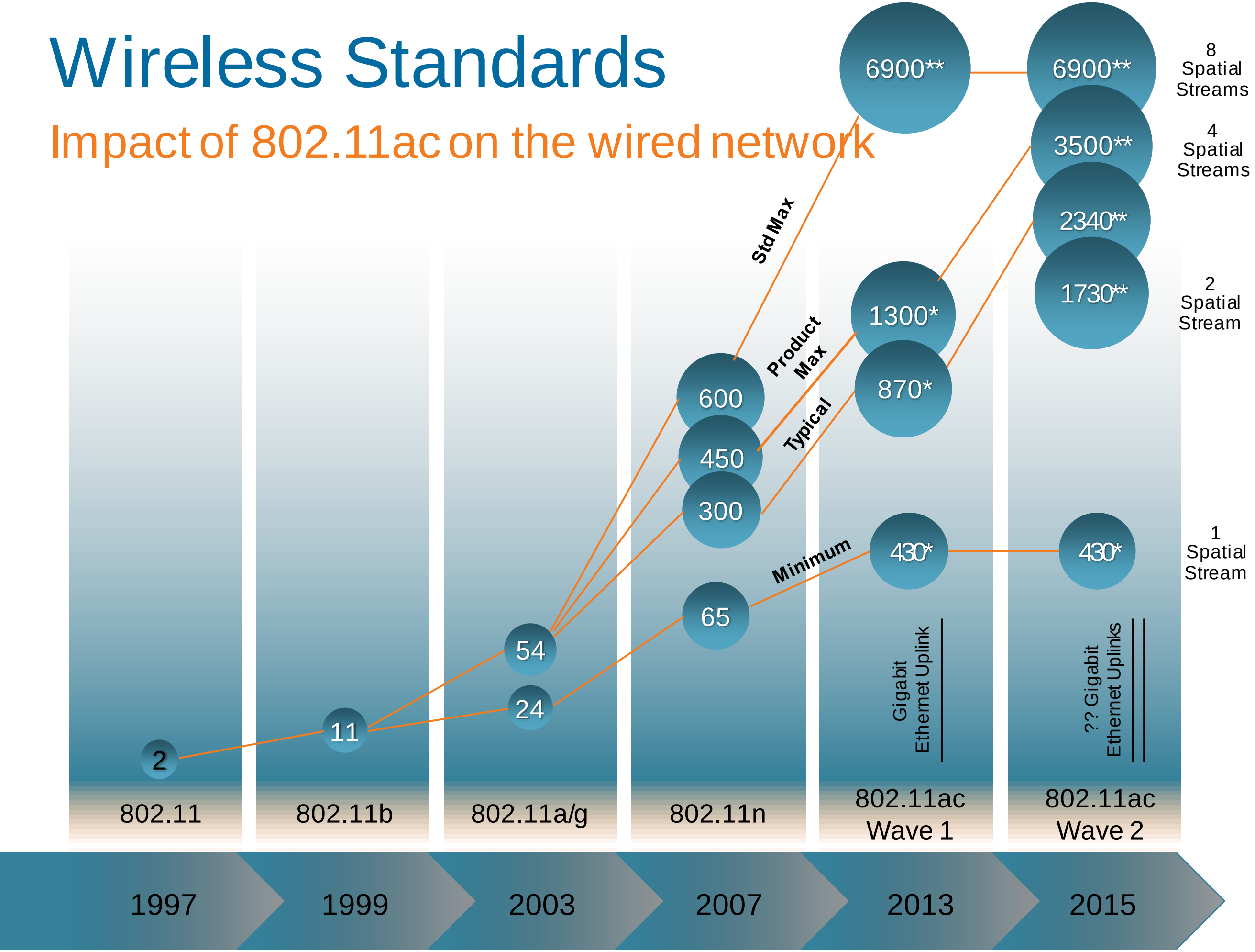


# Risks, Threats and Vulnerabilities

- Is the wired network already trusted?
  - Risks should (in theory) already have been identified and treated if necessary
- Introduction of a wireless network may change the current risk profile
  - Change to network boundary
  - Change to traffic flows
  - Possible change to user/device population(s)
- What controls are currently in place that can be re-used?
  - Directory services
  - PKI
  - Etc.
- Availability
  - Wired must be at least as reliable as wireless

# Wireless Standards

## Impact of 802.11ac on the wired network



| | |
|---|---|
| 4SS | Desktops |
| 3SS | Desktops / Laptops |
| 2SS | Laptops / Tablets |
| 1SS | Tablets / Smartphones |

● = Connect Rates (Mbps)

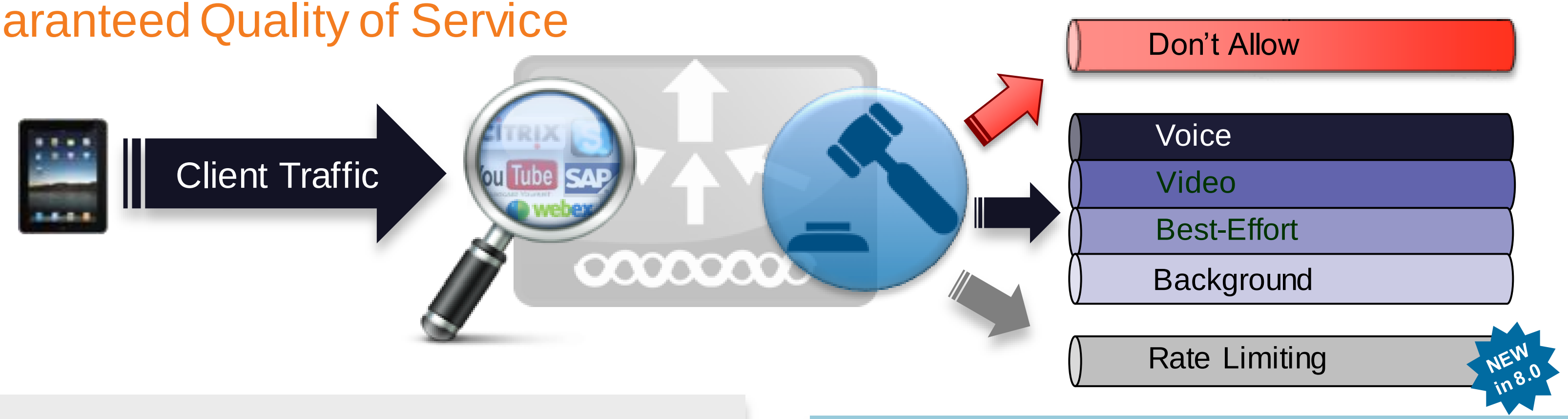
SS = Spatial Streams

*Assuming 80 MHz channel is available and suitable

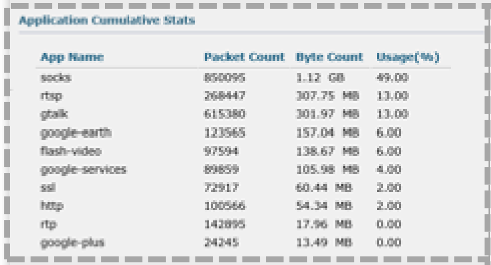
**Assuming 160 MHz channel is available and suitable

# Application Visibility and Control

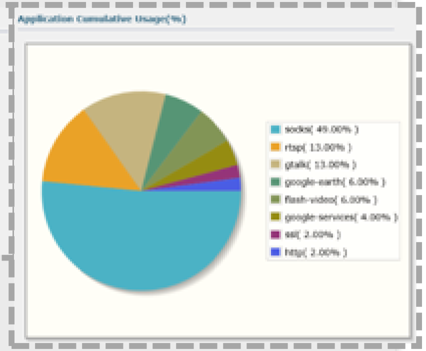
## Guaranteed Quality of Service



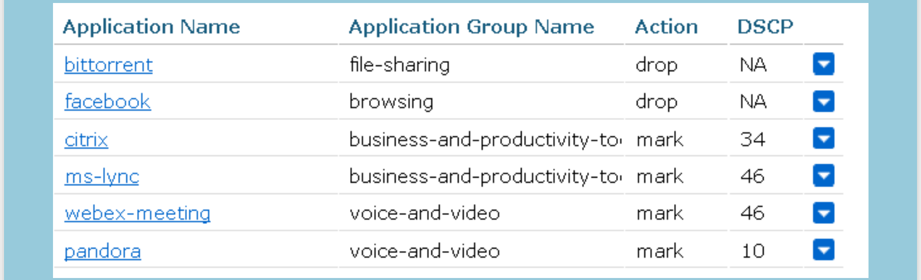
## Identify Applications using NBAR2


Application Cumulative Stats

| App Name | Packet Count | Byte Count | Usage(%) |
|---|---|---|---|
| socks | 850095 | 1.12 GB | 49.00 |
| rtsp | 268447 | 307.75 MB | 13.00 |
| gtalk | 615380 | 301.97 MB | 13.00 |
| google-earth | 123565 | 157.04 MB | 6.00 |
| flash-video | 97594 | 138.67 MB | 6.00 |
| google-services | 89859 | 105.98 MB | 4.00 |
| ssl | 72917 | 60.44 MB | 2.00 |
| http | 100566 | 54.34 MB | 2.00 |
| rtp | 142895 | 17.96 MB | 0.00 |
| google-plus | 24245 | 13.49 MB | 0.00 |



## Control Application Behaviour



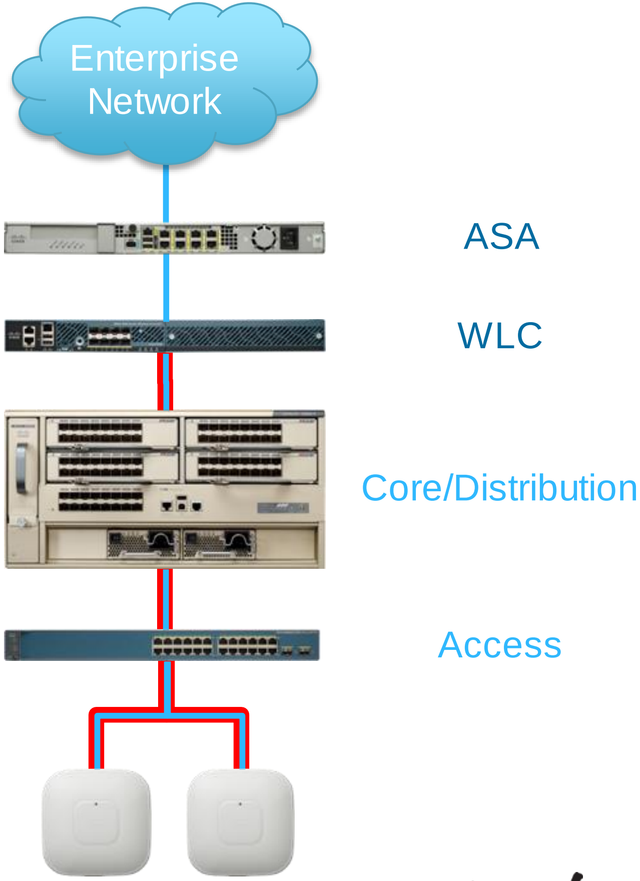
| Application Name | Application Group Name | Action | DSCP | |
|---|---|---|---|---|
| bittorrent | file-sharing | drop | NA | ▾ |
| facebook | browsing | drop | NA | ▾ |
| citrix | business-and-productivity-to | mark | 34 | ▾ |
| ms-lync | business-and-productivity-to | mark | 46 | ▾ |
| webex-meeting | voice-and-video | mark | 46 | ▾ |
| pandora | voice-and-video | mark | 10 | ▾ |

# Network Design Implications

## Centralised Wireless Deployment

- WLC acts as a chokepoint
- ASA provides policy enforcement and threat detection on wireless traffic before bridging onto the Enterprise network

- Wireless traffic tunneled to the network core
- Wireless traffic treated differently to wired traffic



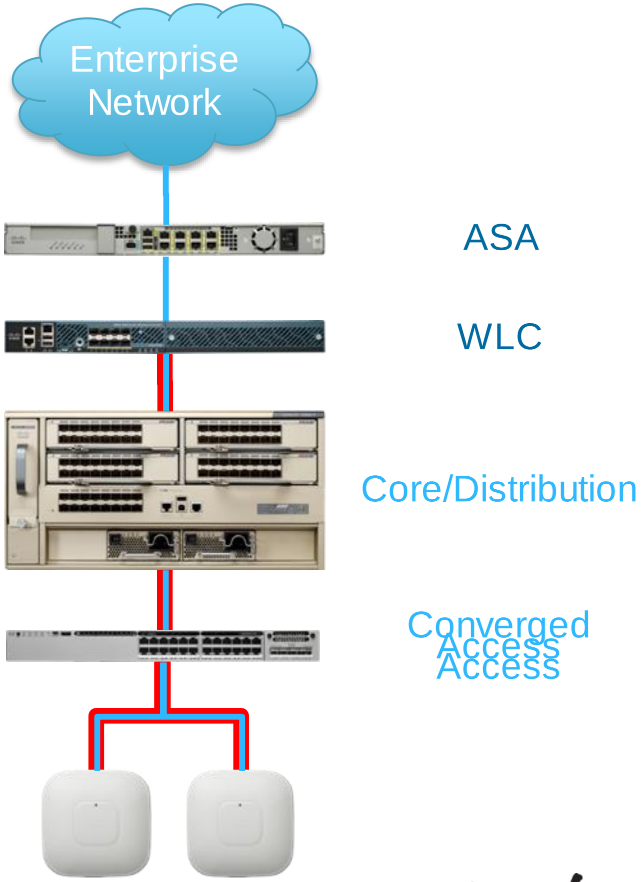
# Network Design Implications

## Converged Access Deployment

- Wireless traffic bridged at the access layer
- Wireless traffic treated the same as wired traffic

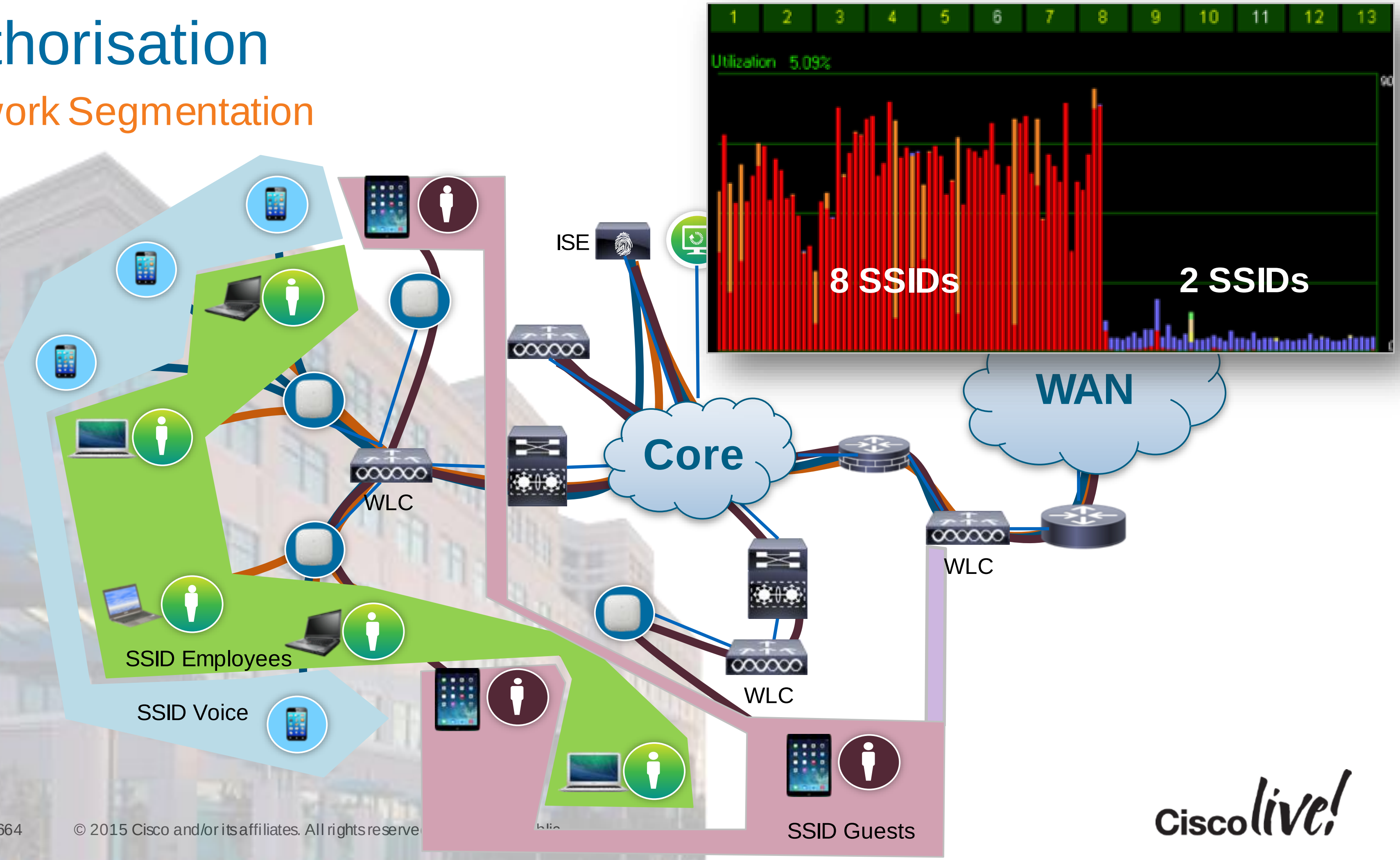
- Wireless
  - wIPS
    - Rogue AP Detection
      - Containment
      - Switch Port Tracing
    - WSSI support pending
  - ACLs
    - Airespace
    - Downloadable
    - SGACL

- Wired
  - Security Features
    - Storm Control
    - Protected Ports
    - IP Source Guard
    - IPv6 First Hop Security
  - Application Visibility
    - Flexible Netflow
    - Wireshark
  - EEM



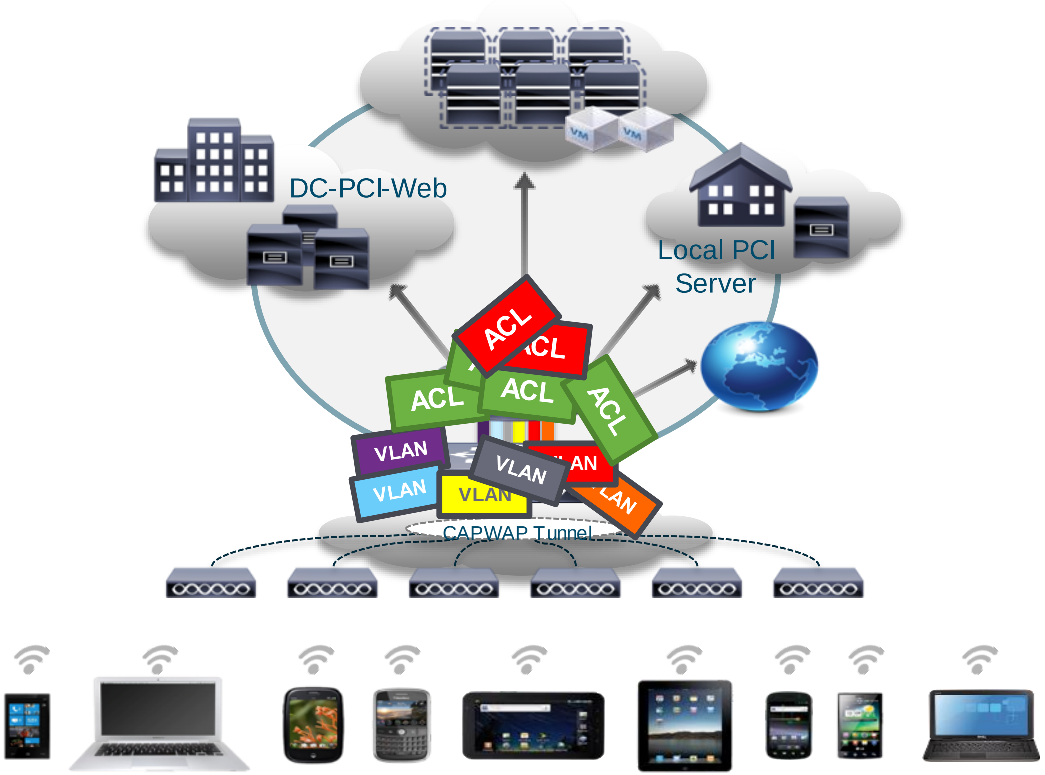
# Authorisation

## Network Segmentation



# The Trouble with VLANs and ACLs - Scalability

- Granular authorisation to corporate assets is vital
- VLAN Segmentation and static ACLs are a common approach to network segmentation
- Current solution relies on named ACLs (64 ACL max) or static policy (ACL) on other network devices



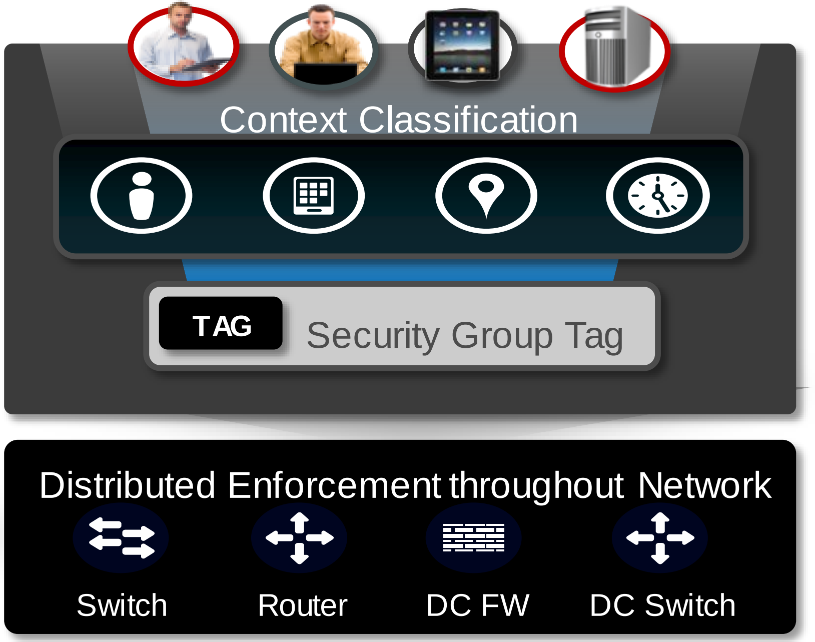
# TrustSec

## A better way?

TrustSec lets you define policy in meaningful business terms

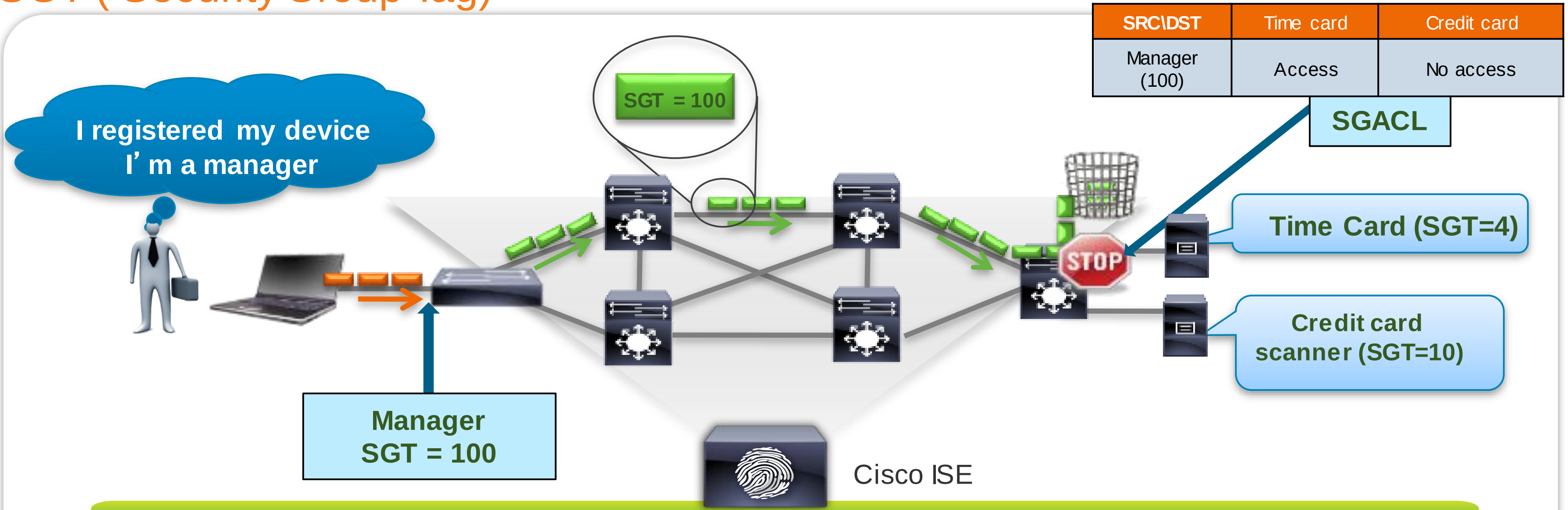
Business Policy

| Destination<br>Source | HR Database | Prod HRMS | Storage |
|---|---|---|---|
| Exec BYOD | X | X | X |
| Exec PC | X | ✓ | X |
| Prod HRMS | ✓ | ✓ | X |
| HR Database | ✓ | ✓ | ✓ |



# Trustsec SGA (Security Group Access)

## SGT ( Security Group Tag)



| SRC\DST | Time card | Credit card |
|---|---|---|
| Manager (100) | Access | No access |

## Security Group Based Access Control

- ISE maps tags (SGT) with user identity
- ISE Authorisation policy pushes SGT to ingress NAD ( switch/WLC)
- ISE Authorisation policy pushes ACL (SGACL) to egress NAD (ASA or Nexus)

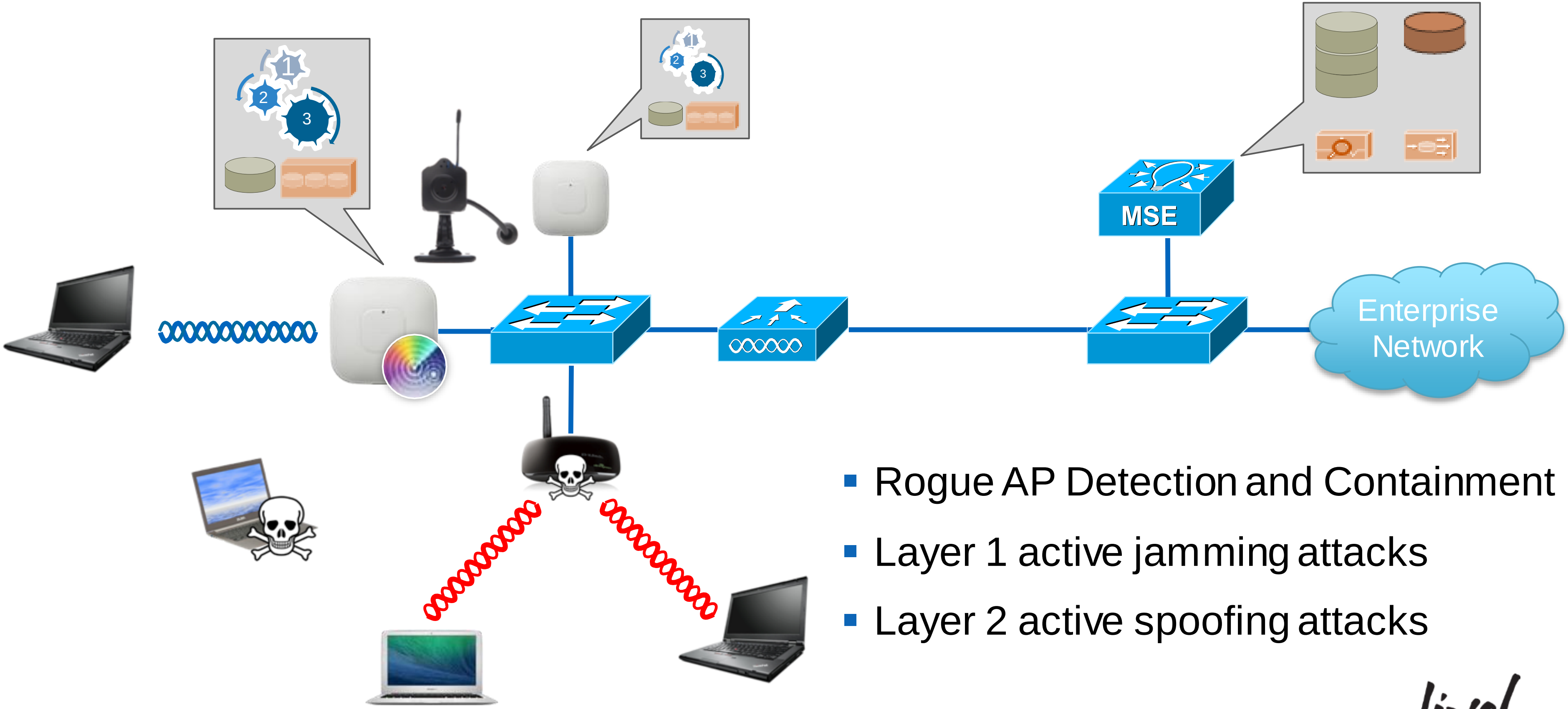
# Risk Assessment

## Wired infrastructure

| RISK | MITIGATION |
|---|---|
| Introduction of wireless network compromises the security of the existing wired network | This risk assessment ☺ |
| Wireless user/device obtains unauthorised access to corporate network resources | Trustsec security group tags (SGT) or VLAN/ACL used for network segmentation |
| Wireless network users overload current wired network capacity | Assessment of current wired network capacity and remediation if necessary |

# Advanced Security Capabilities

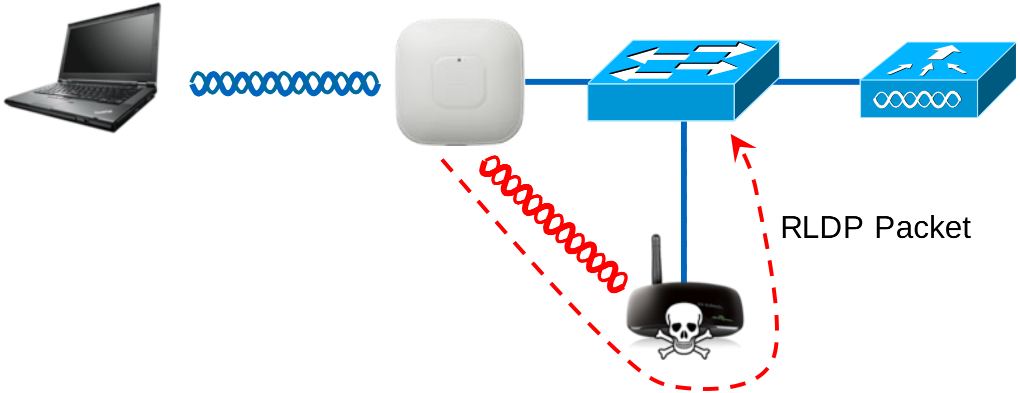
# Advanced Security Capabilities



- Rogue AP Detection and Containment
- Layer 1 active jamming attacks
- Layer 2 active spoofing attacks

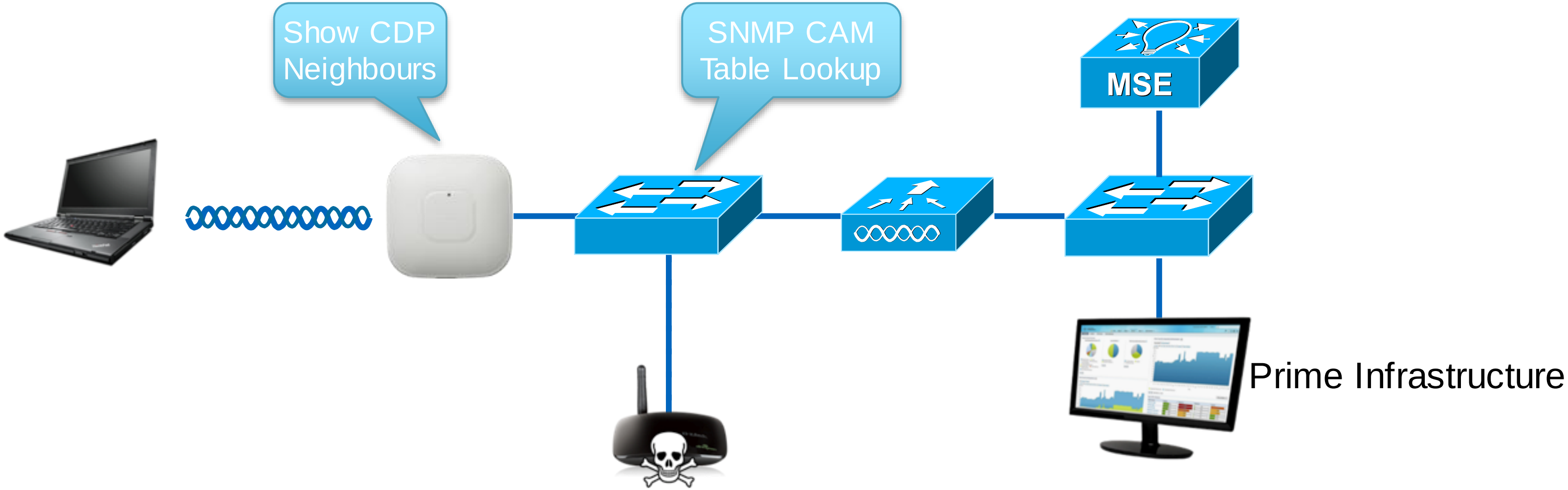
# Rogue AP Detection

## Rogue Location Discovery Protocol

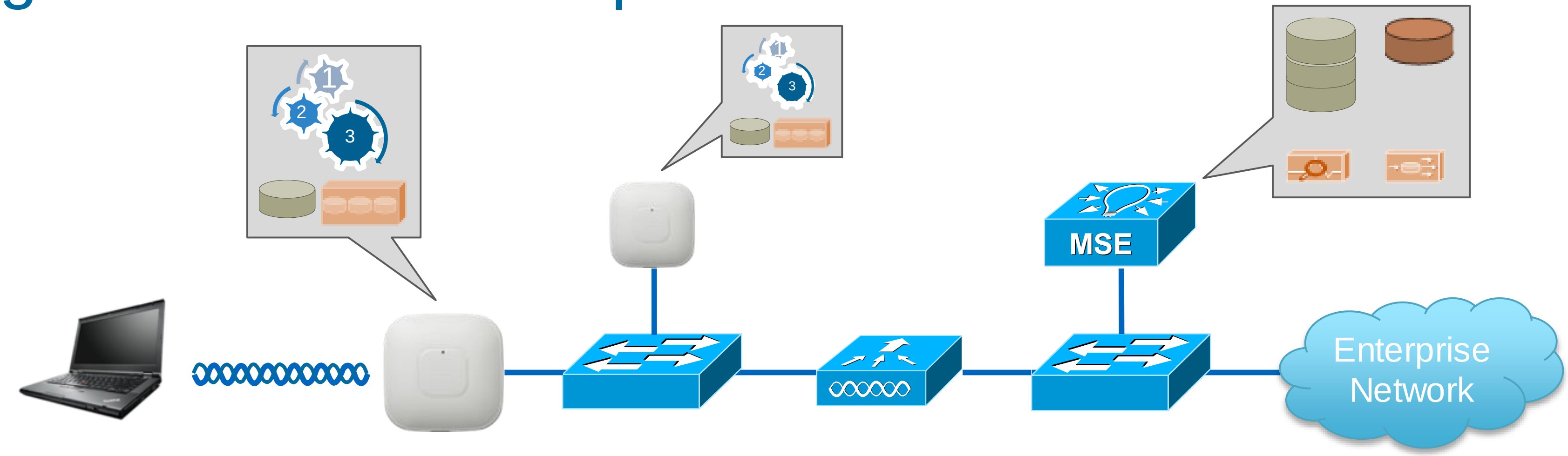


# Rogue AP Detection

## Switch Port Tracing



# Integrated IDS and Adaptive wIPS



- Monitor Mode AP / WLC Integrated IDS
  - Rogue AP and Client Detection
  - 17 Common Attack Signatures
- Enhanced Local Mode
  - Enables Client Serving APs to periodically go off-channel for IDS scanning

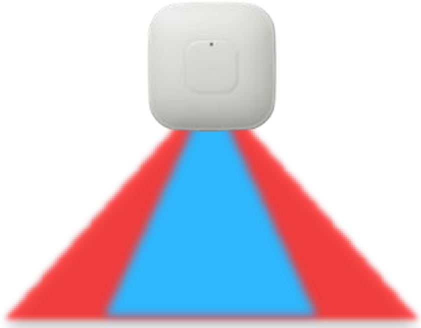
- Adaptive wIPS
  - Alarm Aggregation, Consolidation and False Positive Reduction
  - Enhanced DoS Attack Behaviour Analysis
  - Coordinated Rogue Containment
  - Anomaly Detection
  - Forensic, Blacklisting, Auto Containment, and Auto Immunity responses

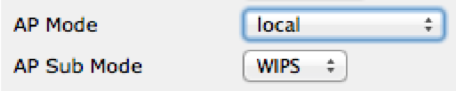
# Wireless Security and Spectrum Intelligence

## Deployment Modes

### Enhanced Local Mode

Data, wIPS & CleanAir





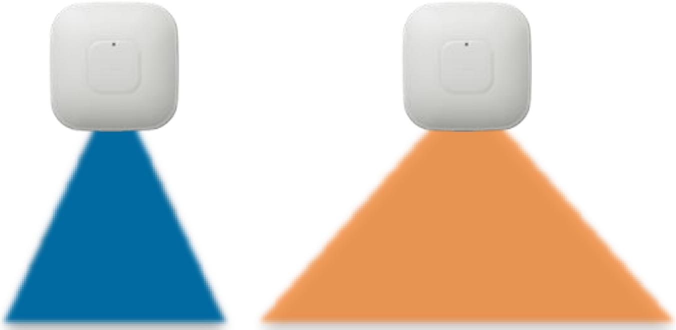
AP Mode: local

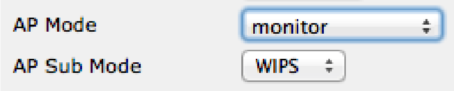
AP Sub Mode: WIPS

### Monitor Mode

Data

wIPS & CleanAir



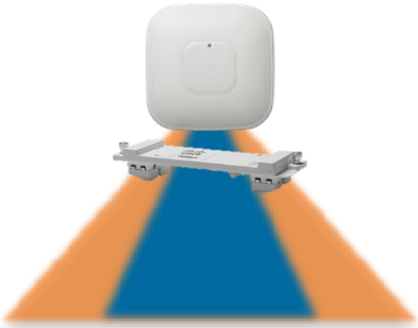


AP Mode: monitor

AP Sub Mode: WIPS

### AP3600/3700 with WSSI

Data, wIPS & CleanAir



▲ Data with wIPS & CleanAir "On Channel"

▲ Best Effort wIPS coverage "Off Channel"

▲ Data with CleanAir "On Channel"

▲ wIPS & CleanAir "All Channels"

# Wireless Security and Spectrum Intelligence

## Off Channel Scanning

Enhanced
Local Mode

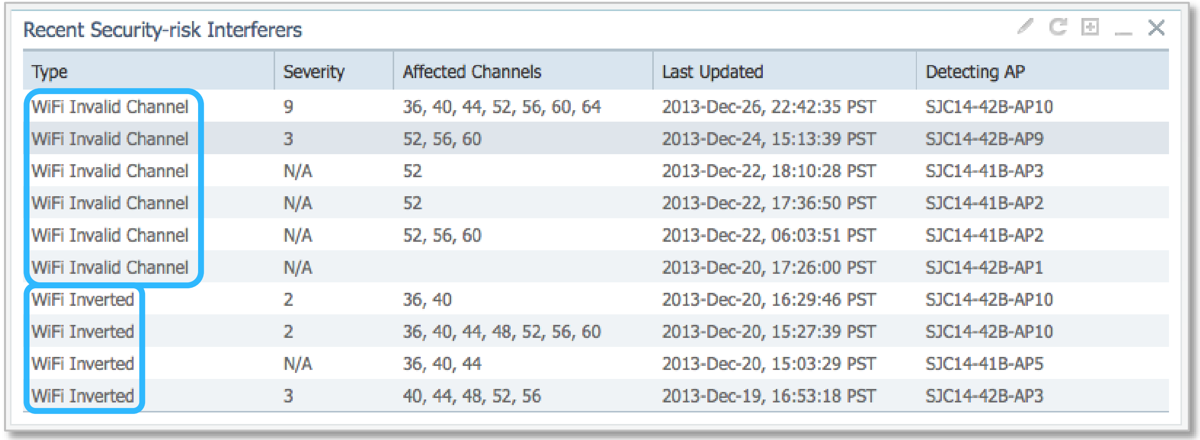
Monitor Mode

Local Mode with
WSSI Module

- Dwell time
  - ELM: 50ms per-channel
  - MM: 1.2s per channel
- Monitor Mode
  - 1 Monitor Mode AP : 5 Local Mode
- WSSI Module
  - 1:5 Clean Air
  - 2:5 wIPS

# Wireless Security and Spectrum Intelligence

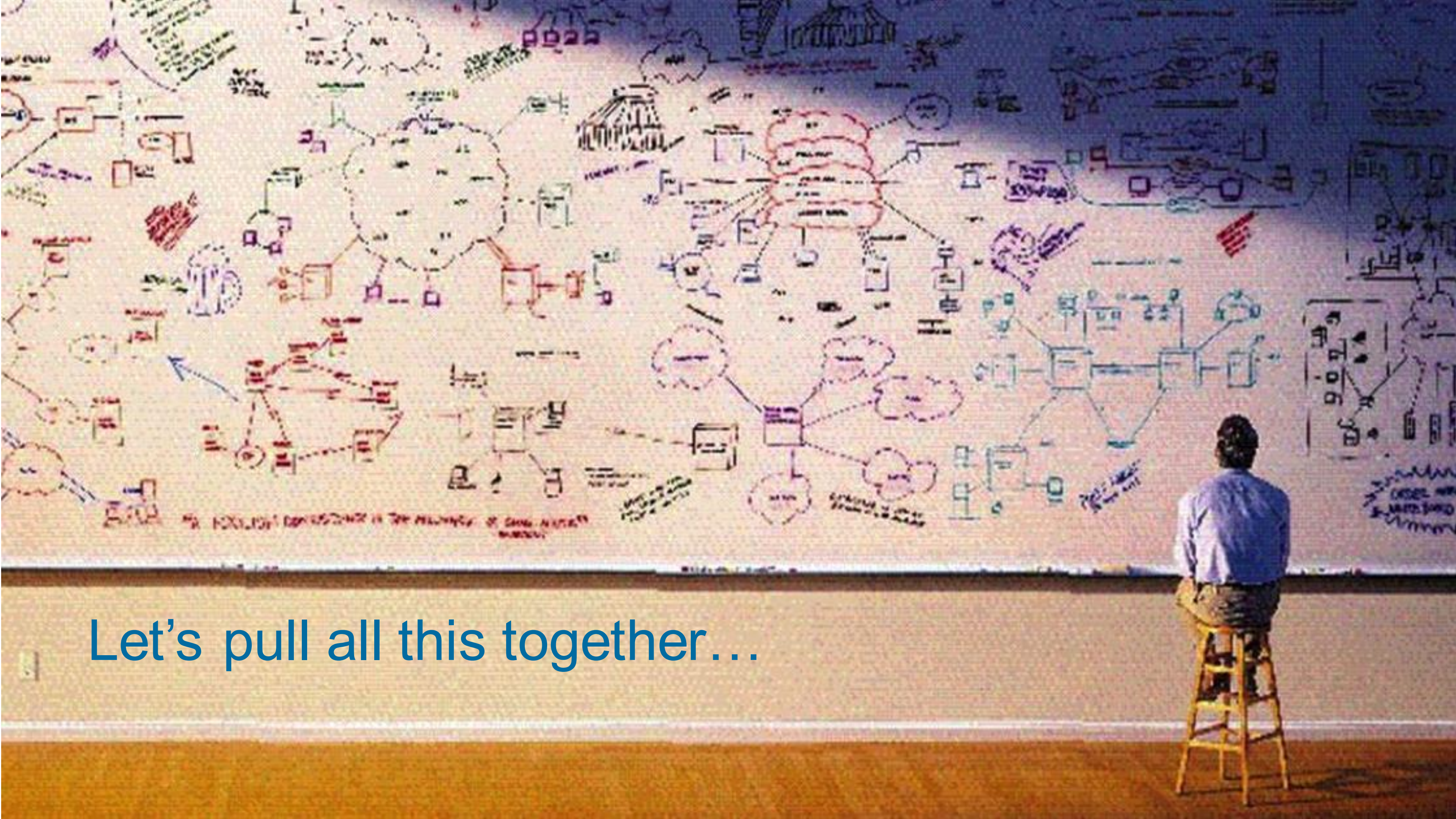
## CleanAir Integration



Recent Security-risk Interferers

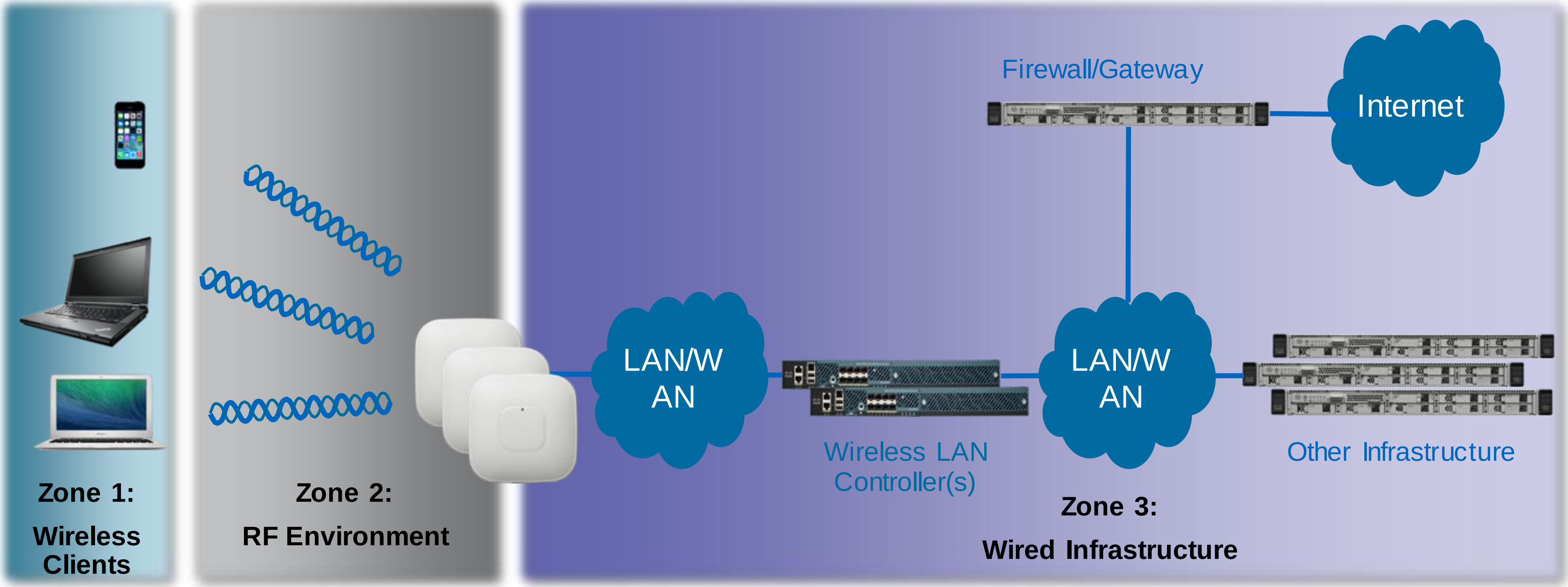
| Type | Severity | Affected Channels | Last Updated | Detecting AP |
|---|---|---|---|---|
| WiFi Invalid Channel | 9 | 36, 40, 44, 52, 56, 60, 64 | 2013-Dec-26, 22:42:35 PST | SJC14-42B-AP10 |
| WiFi Invalid Channel | 3 | 52, 56, 60 | 2013-Dec-24, 15:13:39 PST | SJC14-42B-AP9 |
| WiFi Invalid Channel | N/A | 52 | 2013-Dec-22, 18:10:28 PST | SJC14-41B-AP3 |
| WiFi Invalid Channel | N/A | 52 | 2013-Dec-22, 17:36:50 PST | SJC14-41B-AP2 |
| WiFi Invalid Channel | N/A | 52, 56, 60 | 2013-Dec-22, 06:03:51 PST | SJC14-41B-AP2 |
| WiFi Invalid Channel | N/A | | 2013-Dec-20, 17:26:00 PST | SJC14-42B-AP1 |
| WiFi Inverted | 2 | 36, 40 | 2013-Dec-20, 16:29:46 PST | SJC14-42B-AP10 |
| WiFi Inverted | 2 | 36, 40, 44, 48, 52, 56, 60 | 2013-Dec-20, 15:27:39 PST | SJC14-42B-AP10 |
| WiFi Inverted | N/A | 36, 40, 44 | 2013-Dec-20, 15:03:29 PST | SJC14-41B-AP5 |
| WiFi Inverted | 3 | 40, 44, 48, 52, 56 | 2013-Dec-19, 16:53:18 PST | SJC14-42B-AP3 |

- Detection and location of RF layer DoS attacks
- Non-standard channel threat detection
- Detection and mitigation of non-Wi-Fi device interference



Let’s pull all this together…

# Assessing Risk End-to-end



# Risk Assessment

| RISK | MITIGATION |
|---|---|
| Unauthorised access to data viewed on mobile device | **AnyConnect** – control network access<br>**ISE** – granular access controls once connected |
| Mobile device lost or stolen | **ISE** – revoke network access<br>**MDM** – remote wipe |
| Unauthorised data stored on mobile device | **ISE** – granular network access controls<br>*Additional mitigation may be necessary (depending on corporate security policy) |
| Unauthorised mobile device used to access and/or compromise the wireless network | **Various controls** – (ISE, network infrastructure, AAA, WIPS, Layer 4 – 7 controls, ACLs, etc.) |
| Mobile device used to created an unauthorised "hotspot" or bridge to the corporate network | **AnyConnect** – control active network interfaces on mobile device |

# Risk Assessment

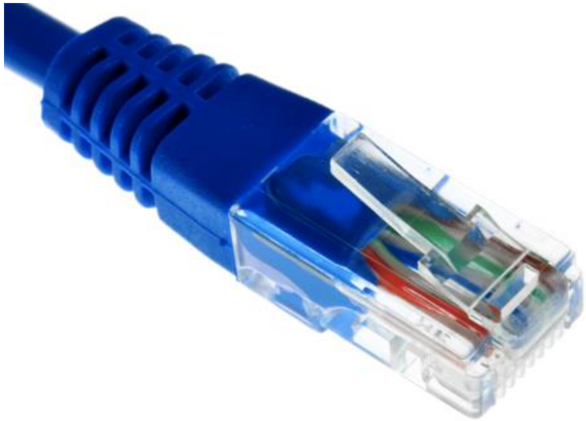
| RISK | MITIGATION |
|---|---|
| Data transmitted over the wireless infrastructure can be intercepted and read | WPA2 uses AES encryption to protect all transmitted data |
| Wireless control traffic is altered in transit | Management Frame Protection ensures the integrity of all control traffic |
| An attacker attempts to compromise the network via spoofed control traffic | Management Frame Protection ensures the integrity of all control traffic |
| Availability of the wireless network compromised by RF interference, either accidental or malicious | CleanAir automatically detects, classifies and mitigates interference |
| An attacker attempts to masquerade as a legitimate corporate WLAN | Management Frame Protection (and WIPS – covered later) |

# Risk Assessment

| RISK | MITIGATION |
|---|---|
| Introduction of wireless network compromises the security of the existing wired network | This risk assessment ☺ |
| Wireless user/device obtains unauthorised access to corporate network resources | Trustsec security group tags (SGT) or VLAN/ACL used for network segmentation |
| Wireless network users overload current wired network capacity | Assessment of current wired network capacity and remediation if necessary |

# A Parting Thought

## Which is more secure?



OR

# Q & A

# Complete Your Online Session Evaluation

**Give us your feedback and receive a Cisco Live 2015 T-Shirt!**

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

**Learn online with Cisco Live!**
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

# Thank you.

cisco