



*TOMORROW  
starts here.*

Cisco *live!*



# Managing Policies for a BYOD Network

BRKEWN-2020

Scott Lee-Guard

Systems Engineer, Enterprise Networks

#clmel

Cisco *live!*

# Agenda

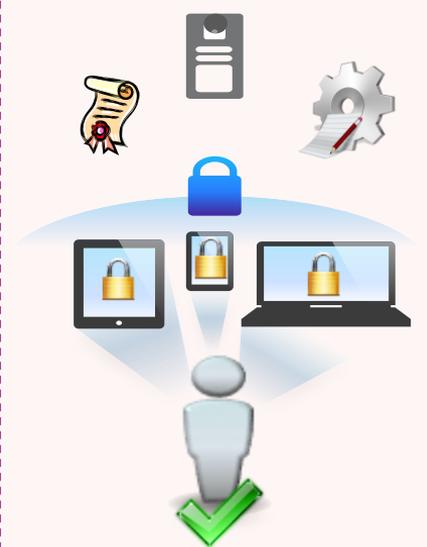
## Managing the BYOD Evolution



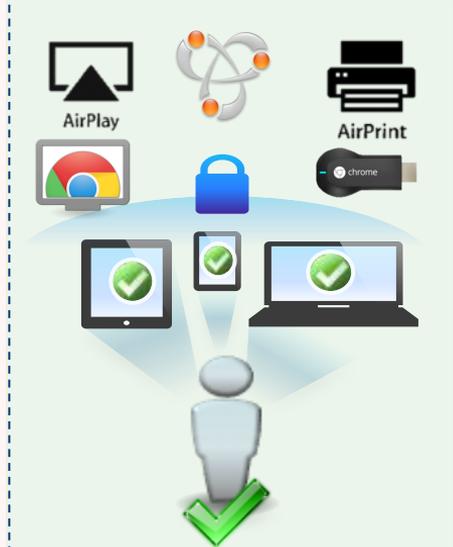
Personal Devices on Network



Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations

# The Need for Managing Devices and Applications

4X

Smartphone connection speeds will grow 4-fold from 2011 to 2016 —Cisco VNI

90%

Mobile video traffic will have annual growth rate of 90% 2011 to 2016 —Cisco VNI

56%

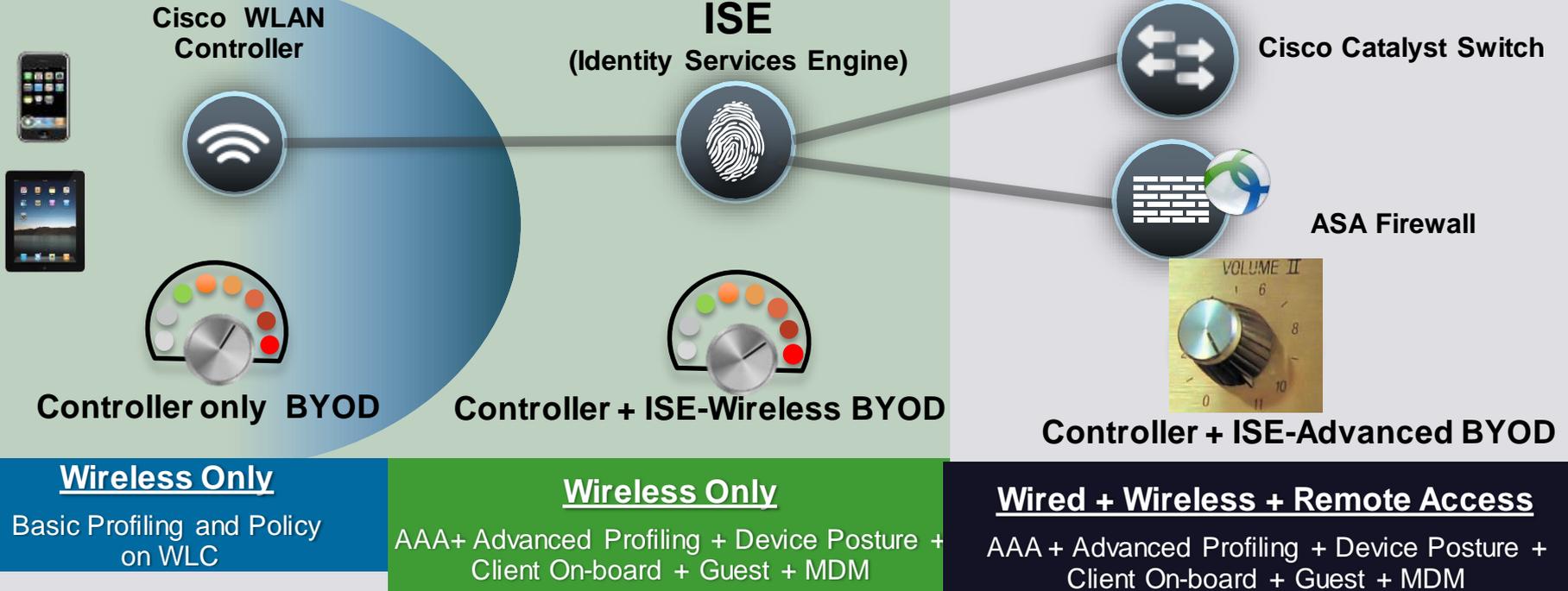
of US information workers spend time working **outside the office** —Forrester

100%

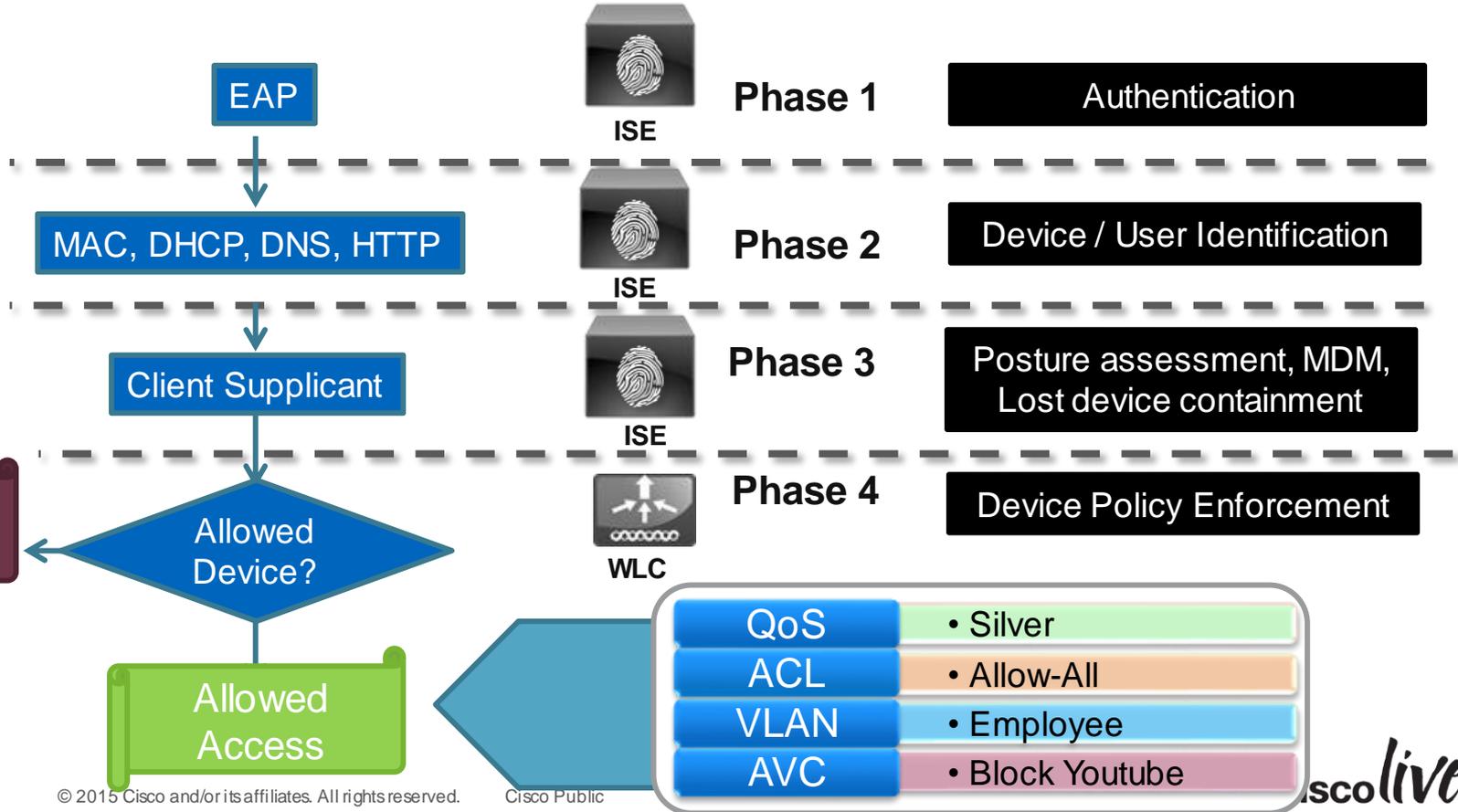
of IT staff is **struggling** to keep up with mobility trends —Gartner

# Spectrum of BYOD Strategies

Different Deployment Requirements for Different Environments



# Cisco BYOD Policy Steps

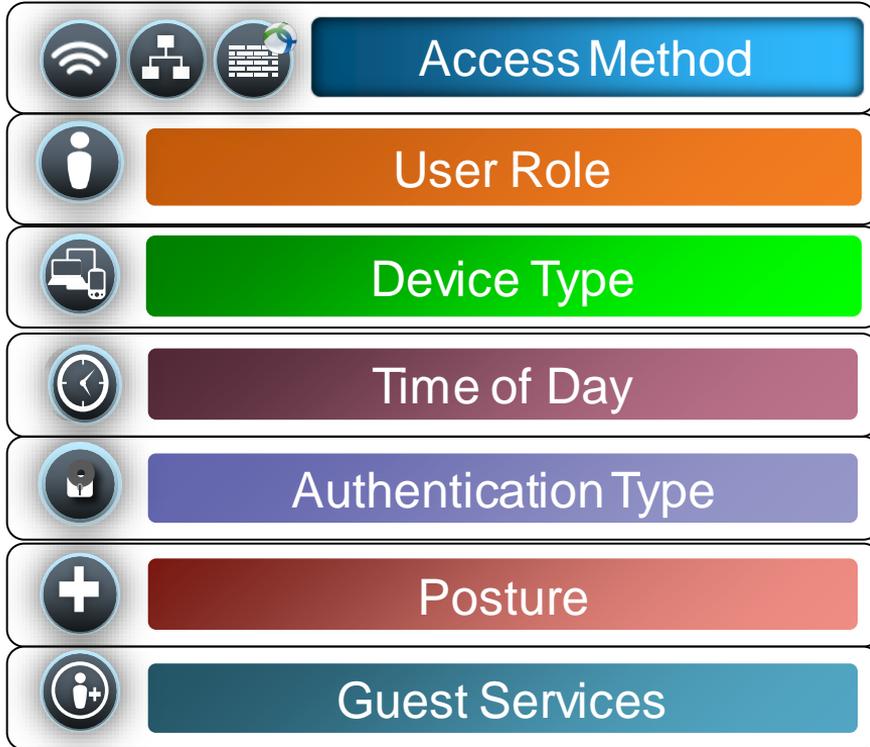


A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several modern buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

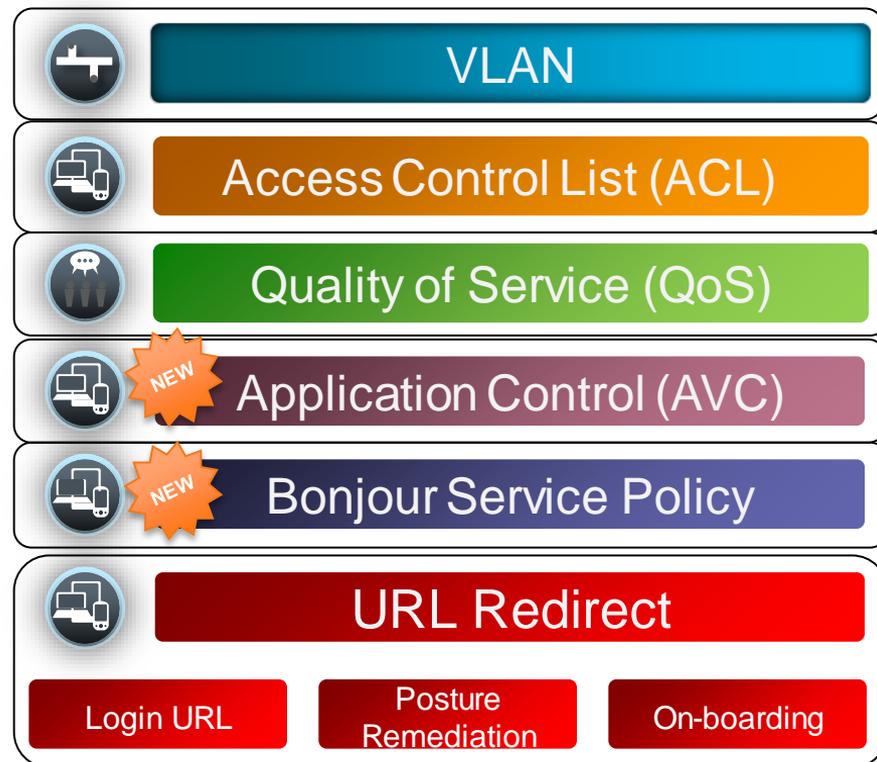
# BYOD Policy Building Blocks: Tools of the Trade

# Building BYOD Policy: Flexible Options

## Inputs: Factors

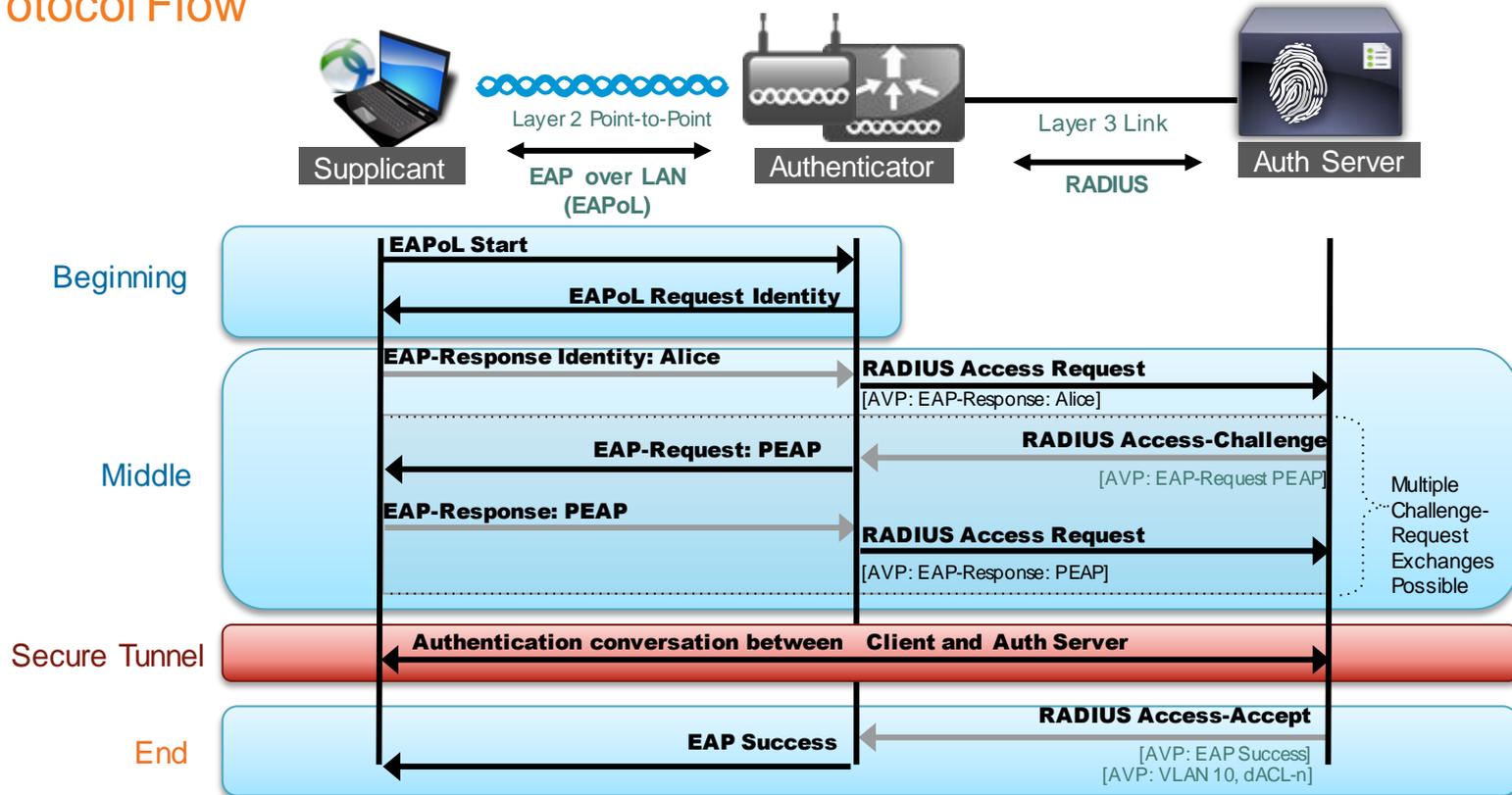


## Results: Enforcement Elements



# Extensible Authentication Protocol (EAP)

## Protocol Flow

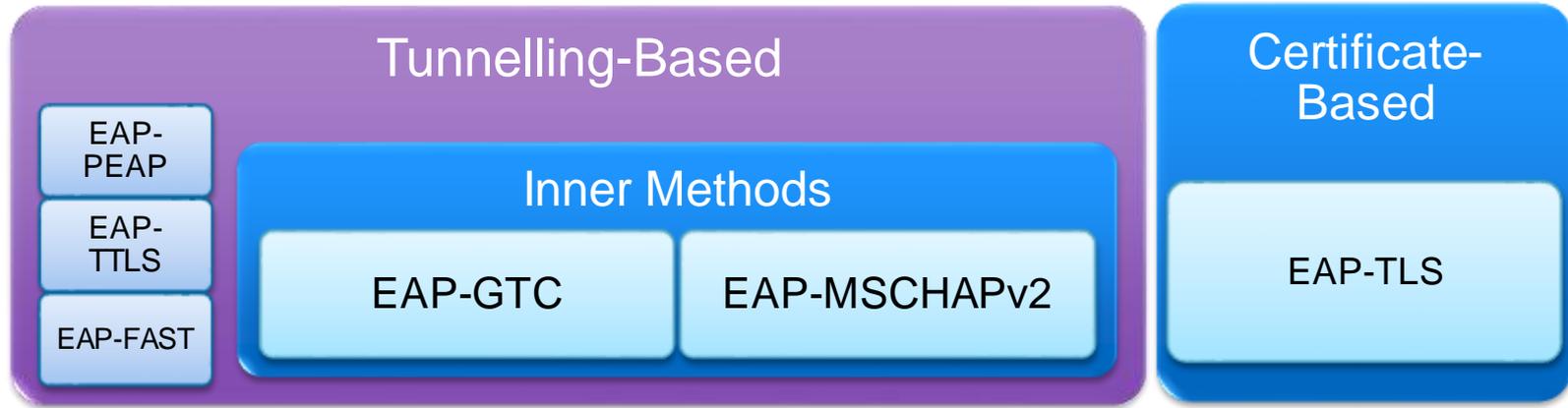


# Why EAP Types?

- 802.1X (EAPoL) is a delivery mechanism
  - Doesn't provide the actual authentication mechanisms
- EAP type defines how the authentication takes place
  - E.g. Transport Layer Security (EAP-TLS) or PEAP
- EAP Type is **negotiated** between Client and RADIUS Server

# EAP Authentication Types

Different Authentication Options Leveraging Different Credentials



- Tunnel-based - Common deployments use a tunnelling protocol combined with an inner EAP type.
  - Provides security for the inner EAP type which may be vulnerable by itself.
- Certificate-based – Mutual authentication of both the server and client.

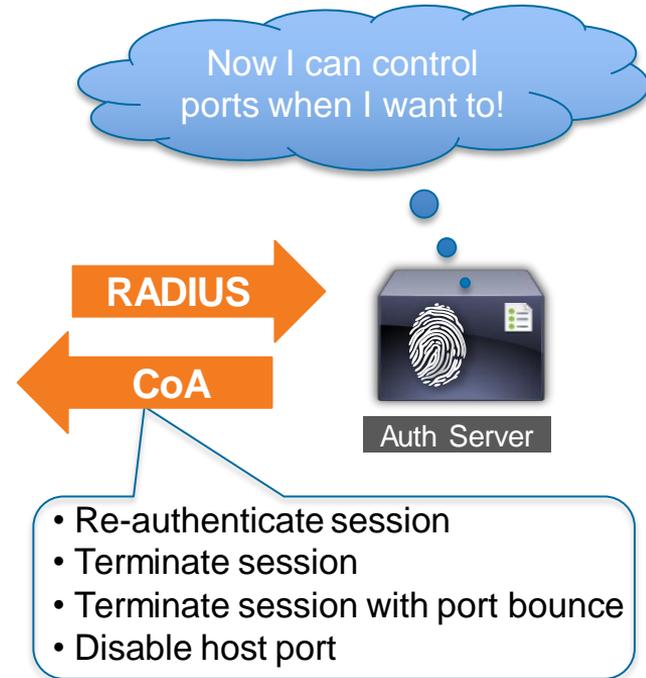
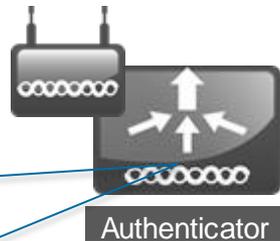
# The RADIUS Protocol

It's initiated by the client to the server, but not CoA...

- RADIUS protocol is initiated by the network devices
- No way to change authorisation from the ISE

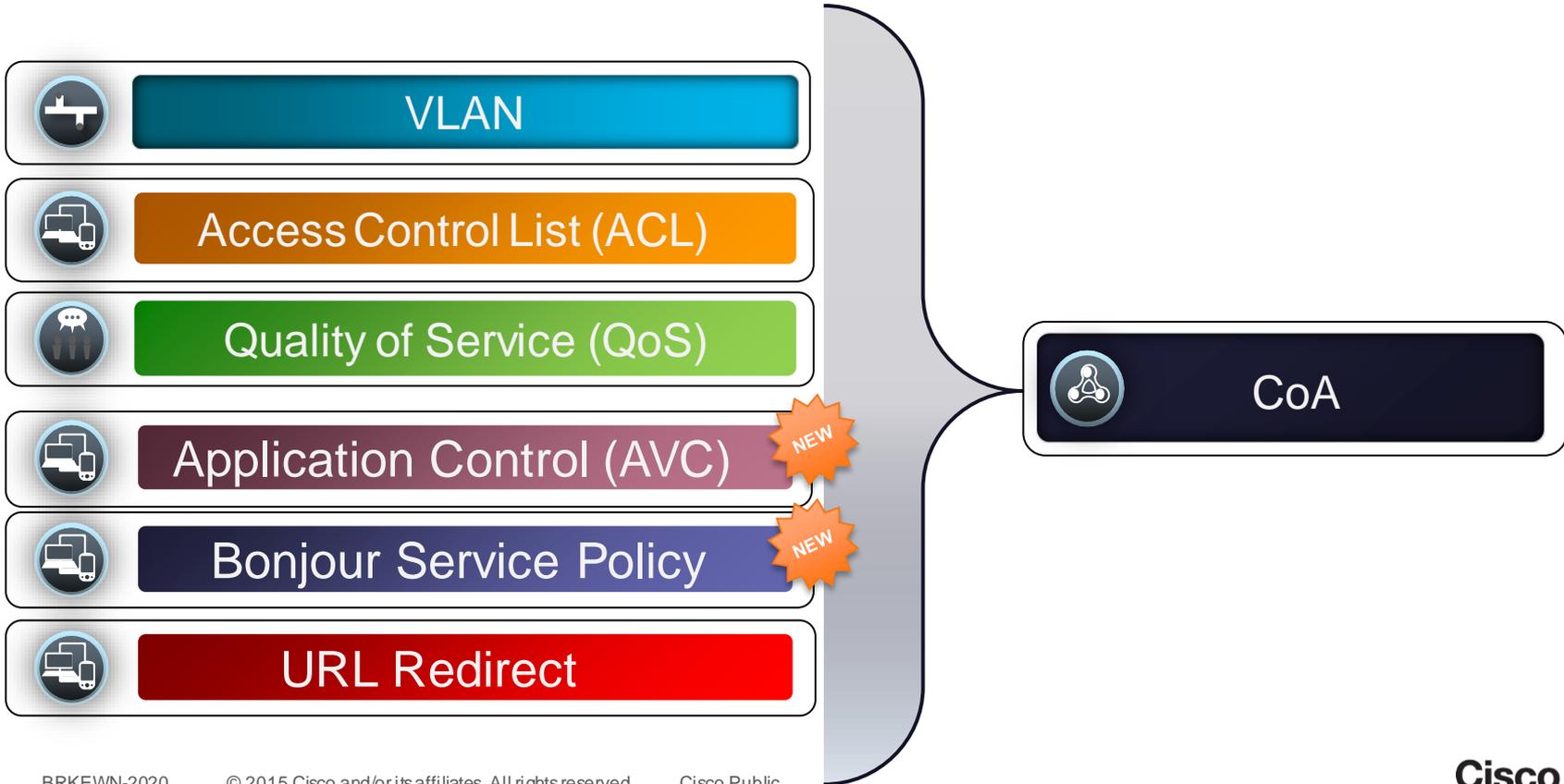
**RADIUS Authentication Servers > Edit**

Server Index	1
Server Address	10.100.7.20
Shared Secret Format	ASCII ▾
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	<input type="checkbox"/> (Designed for FIPS)
Port Number	1812
Server Status	Enabled ▾
Support for RFC 3576	Enabled ▾



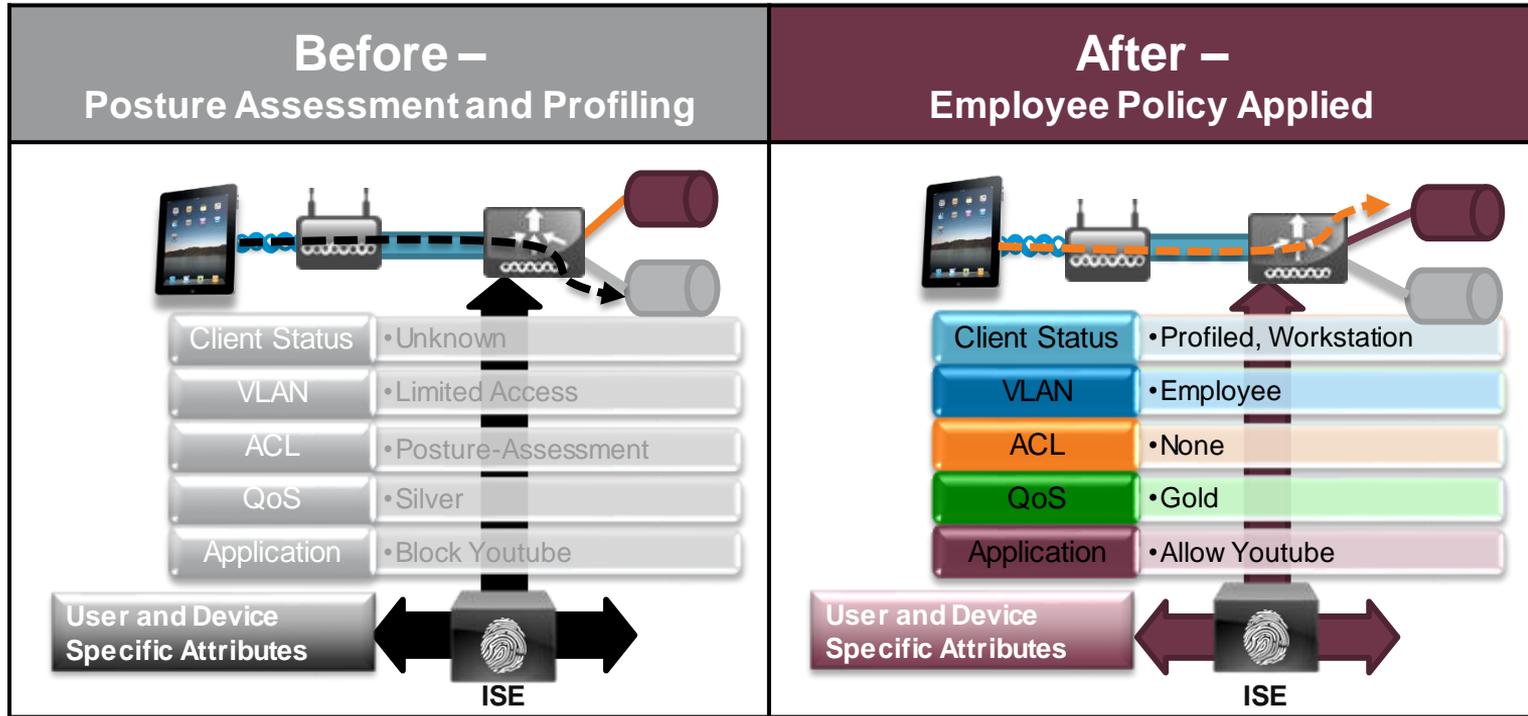
- Now network devices listens to CoA request from ISE

# Per-User Policy Override with CoA



# Change of Authorisation (CoA)

## Changing Connection Policy Attributes Dynamically

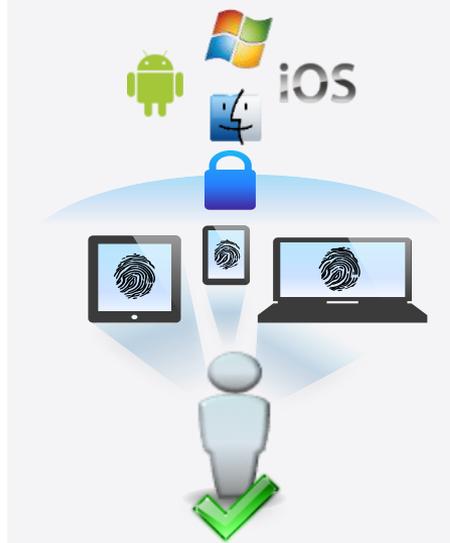


# Agenda

## Managing the BYOD Evolution



Personal Devices on  
Network



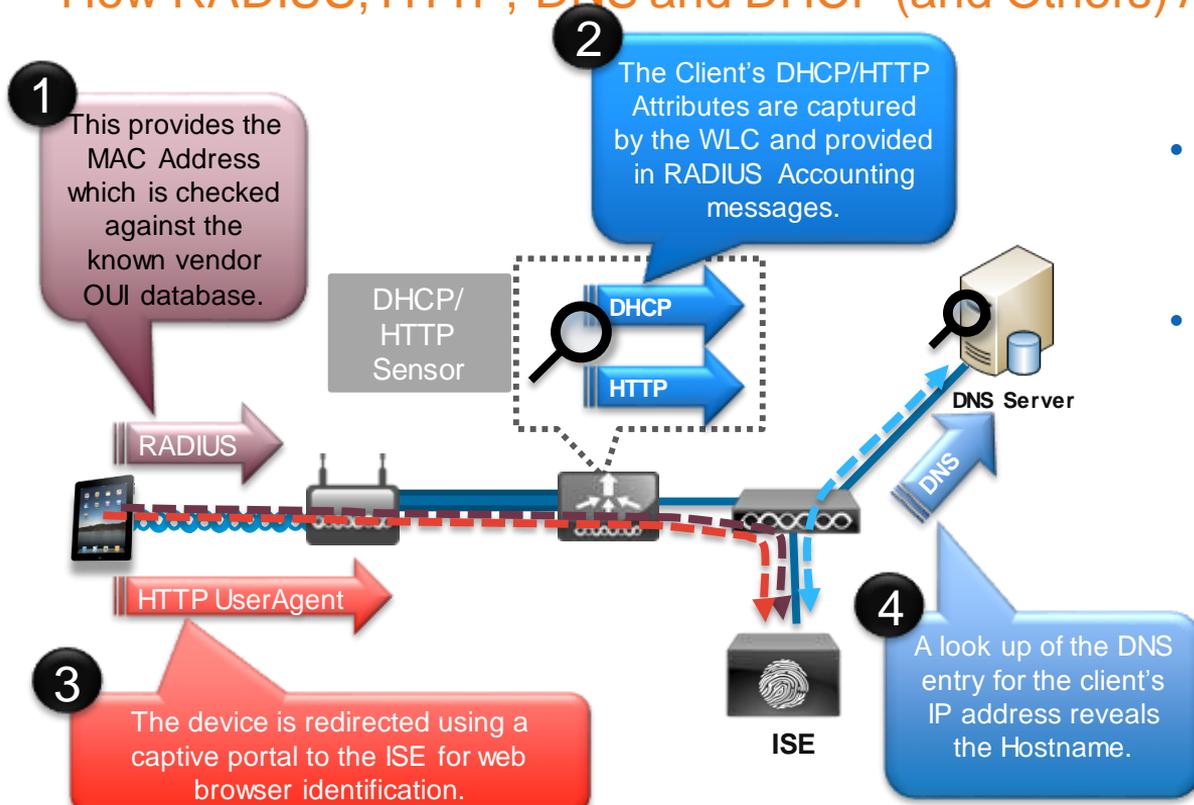
Identification and  
Security Policy  
Enforcement



# Profiling with ISE

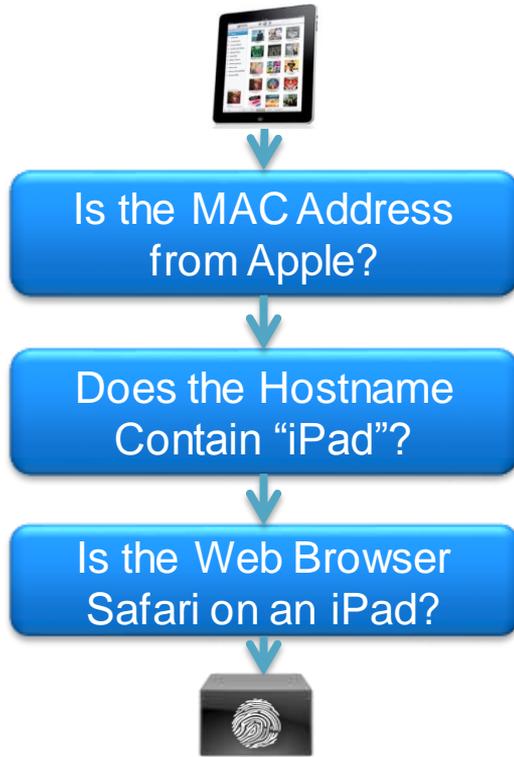
# Client Attributes Used for ISE Profiling

How RADIUS, HTTP, DNS and DHCP (and Others) Are Used to Identify Clients.



- The ISE uses multiple attributes to build a complete picture of the end client's device profile.
- Information is collected from sensors which capture different attributes
  - The ISE can even kick off an NMAP scan of the host IP to determine more details.

# ISE Device Profiling Example - iPad



- Once the device is profiled, it is stored within the ISE for future associations:

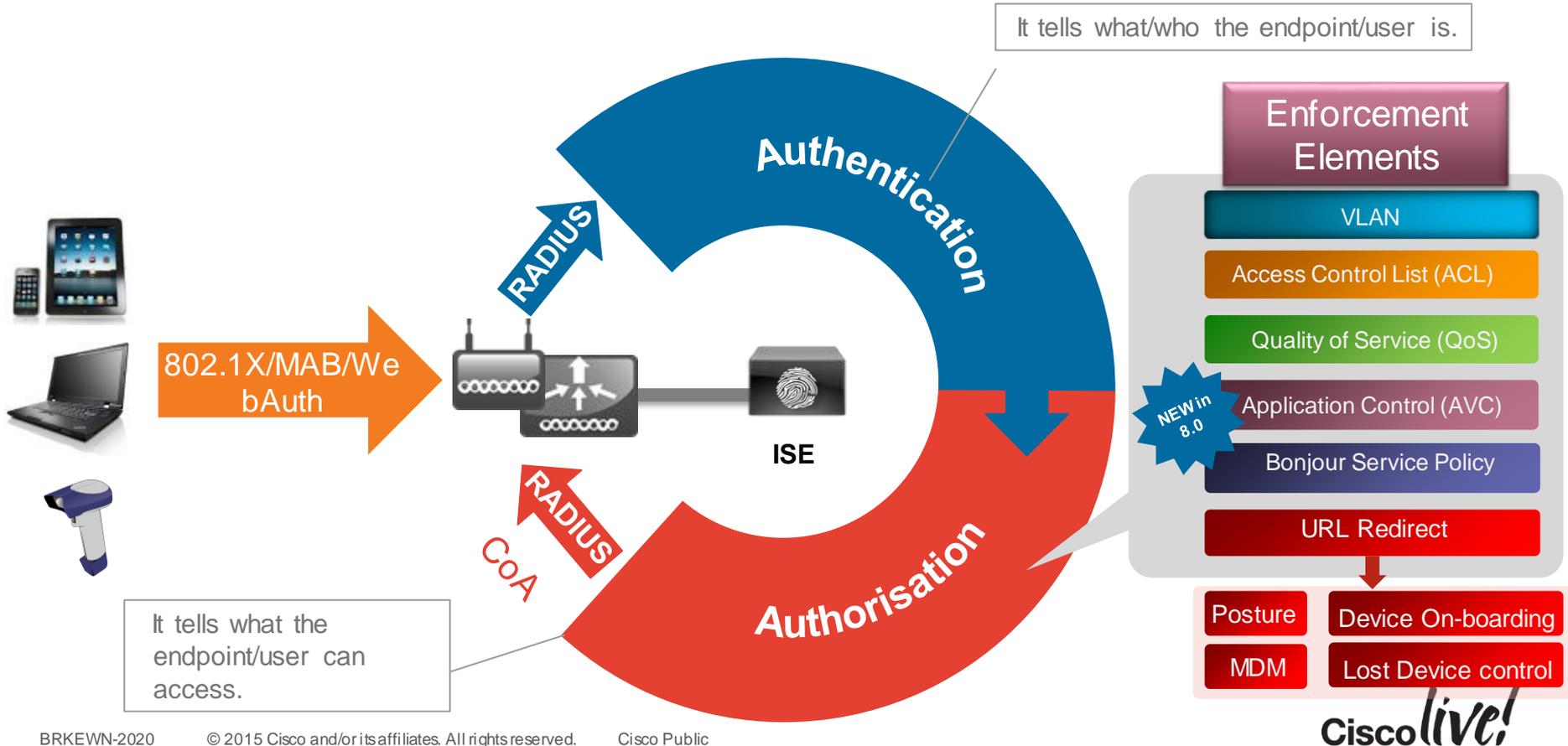
Endpoints	
Endpoint Profile	MAC Address
<input type="checkbox"/> Apple-iPad	D8:A2:5E:32:9D:8D
<input type="checkbox"/> Microsoft-Workstation	00:21:6A:5A:85:3A
<input type="checkbox"/> Microsoft-Workstation	00:24:E8:E7:7B:93
<input type="checkbox"/> Microsoft-Workstation	00:21:6A:5A:86:70
<input type="checkbox"/> Windows7-Workstation	00:23:5E:9D:BC:C9

A large blue arrow points from the 'Apple-iPad' entry in the table back to the 'Apple iPad' box in the diagram below.



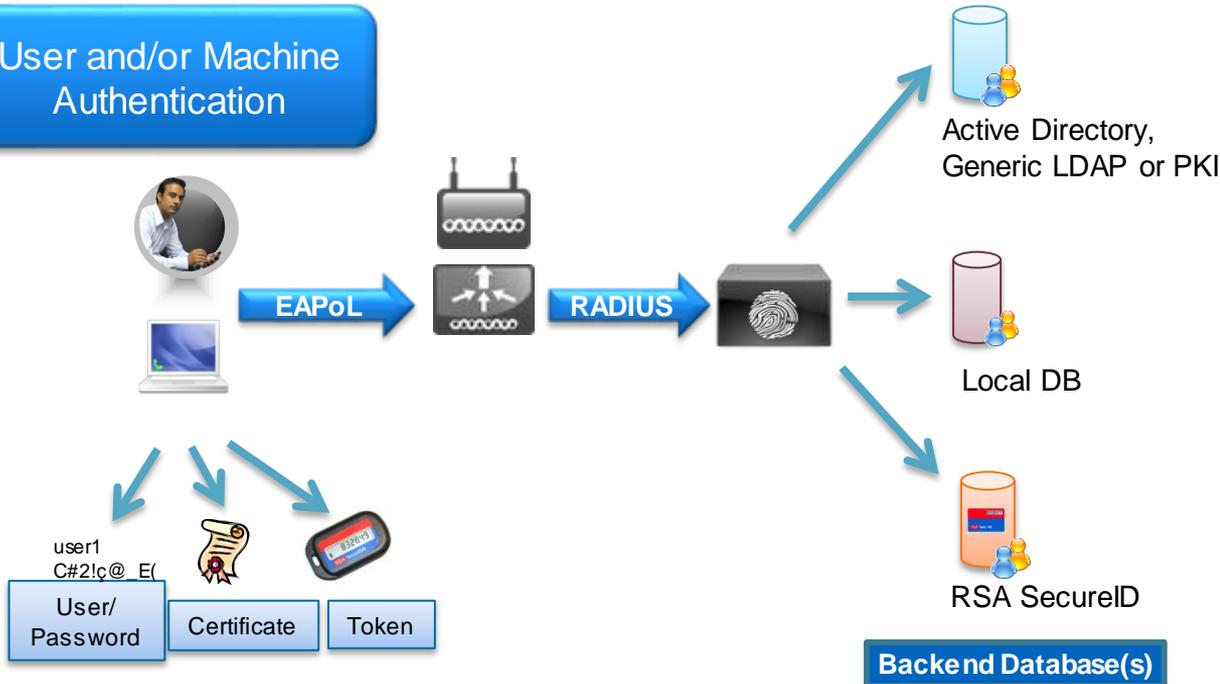
# Defining a Security Policy Within ISE

# Authentication and Authorisation



# ISE Authentication Sources

User and/or Machine Authentication



- Cisco ISE can reference variety of backend identity stores including Active Directory, PKI, LDAP and RSA SecureID.
- The local database can also be used on the ISE itself for small deployments.

# Authentication Rules

**Policy Sets**

Search policy names & descriptions.

**Summary of Policies**  
A list of all your policies

**Global Exceptions**  
Rules across all policy sets

**Authentication Policy**

Status	Name	Conditions	Actions
✓	Dot1x	If Wireless_802.1X	Allow Protocols : DOT1X_ONLY and
✓	Cert_Auth	If EAP-TLS OR EAP-FAST_TLS	use Certificate_CN
✓	Password_Auth	If PEAP-MSCHAPv2 OR EAP-FAST_MSCHAPv2	use AD2008
✓	Default		use DenyAccess
✓	Default Rule (If no match)		Allow Protocols : Default Network Access

**Annotations:**

- If this/these condition(s) is/are matched, then...
- ...optionally check further (sub)rule(s)...
- ...or just use the default rule...
- ...allow this list of authentication protocols, and...
- ...to pick the database for verifying the endpoint/user's identity.

**Buttons:** Save, Reset

# Authorisation Rules and Results

Home | Operations | Policy | Guest Access | Administration

Client Provisioning | TrustSec | Policy Elements

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description	Conditions
✓	Wireless_802_1x	For Wireless dot1x	Wireless_802.1X

► Authentication Policy

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	BYOD_IT	if (MDM_Device)	then VLAN_IT AND SGT_BYOD
✓	BYOD_Marketing	if (Groupe_AD_IT AND ISE_Enregistres)	then VLAN_marketing AND SGT_BYOD
✓	BYOD_Finance	if (Groupe_AD_Marketing AND ISE_Enregistres AND MDM_Conforme)	then VLAN_finance AND SGT_BYOD

## Enforcement Elements

VLAN

Access Control List (ACL)

Quality of Service (QoS)

Application Control (AVC)

Bonjour Service Policy

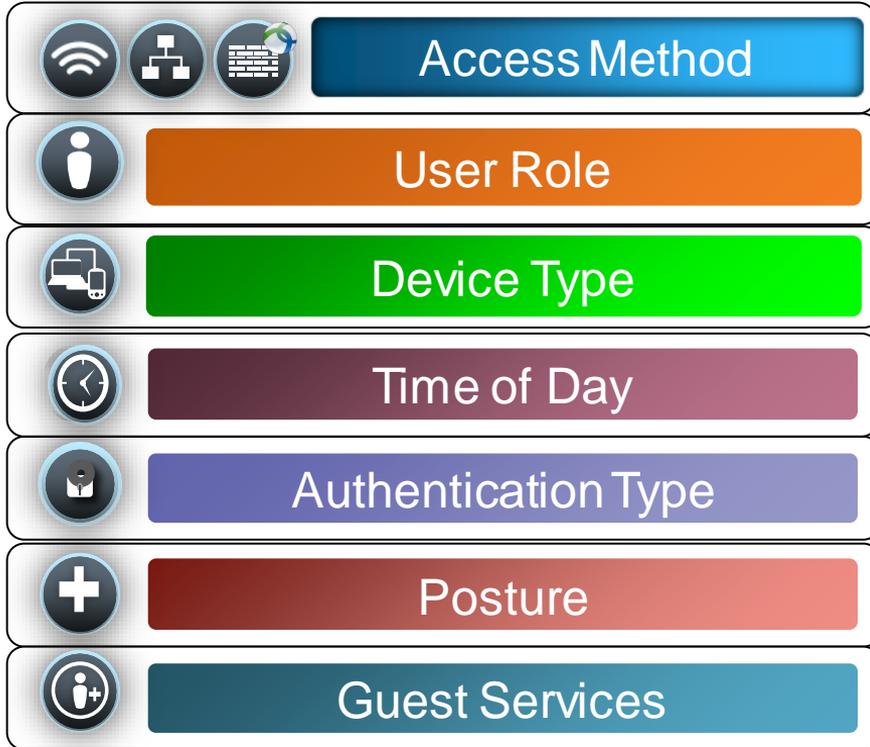
URL Redirect



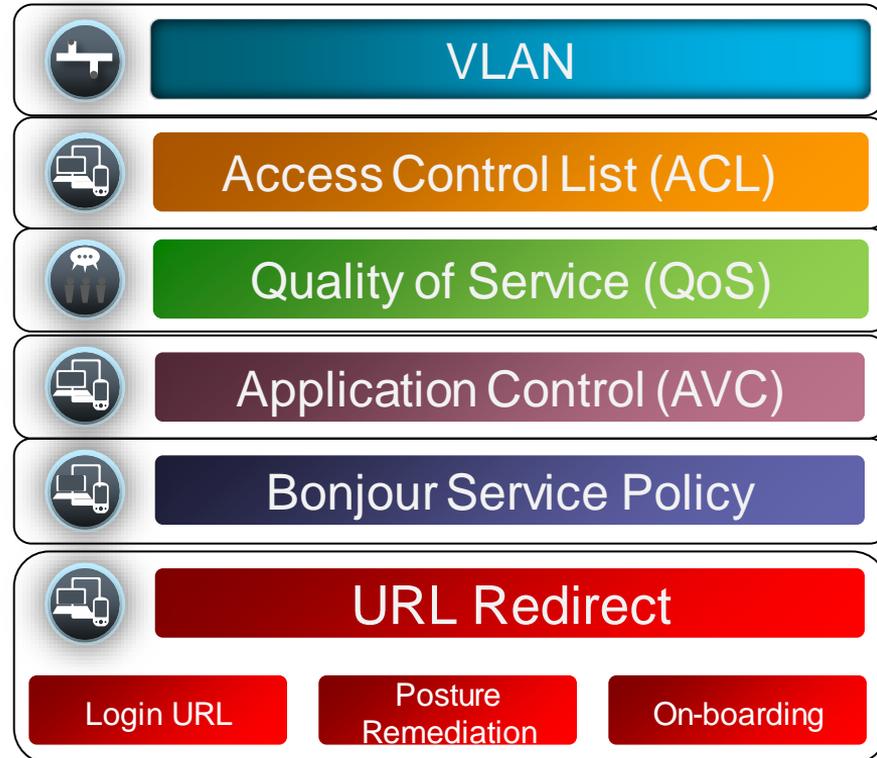
# Native Profiling and Policy on WLC

# Building BYOD Policy: Flexible Options

## Inputs: Factors

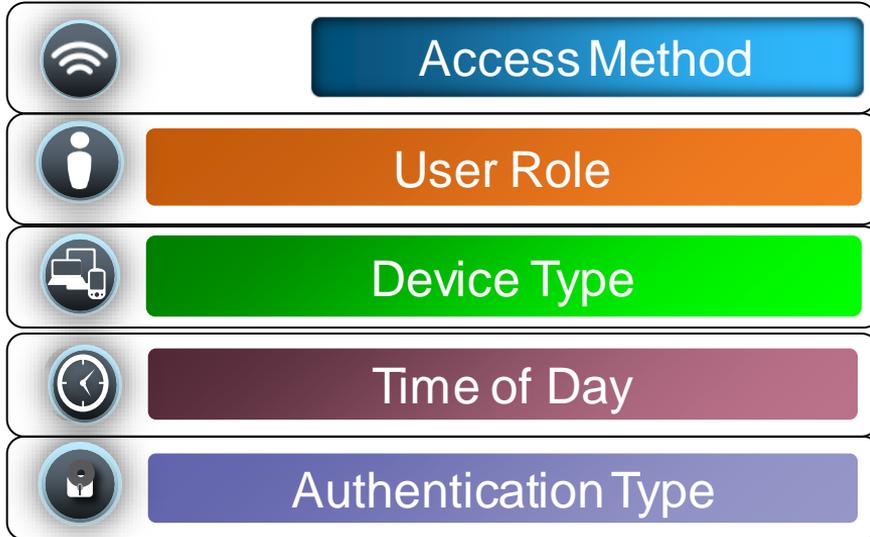


## Results: Enforcement Elements



# Building BYOD Policy: Native WLC Options

## Inputs: Factors



## Results: Enforcement Elements



# Native Device Profiling on WLC



Device Type

Step 1

## Cisco WLC configuration

WLANs > Edit 'AppTest-Cisco'

General Security QoS Policy-Mapping Advanced

### Local Client Profiling

DHCP Profiling   
HTTP Profiling

### DHCP

DHCP Server  Override  
DHCP Addr. Assignment  Required

Enable DHCP and HTTP Profiling on the WLC

Step 2

## Create Device Profiling Policy

MONITOR WLANs CONTROLLER WIRELESS SECURITY

### Policy > Edit

#### Match Criteria

Match Role String Employee  
Match EAP Type none  
Device Type Apple-iPad

Add

## 156 Pre-Defined Device Signatures

### Clients

Entries 1 - 3 of 3

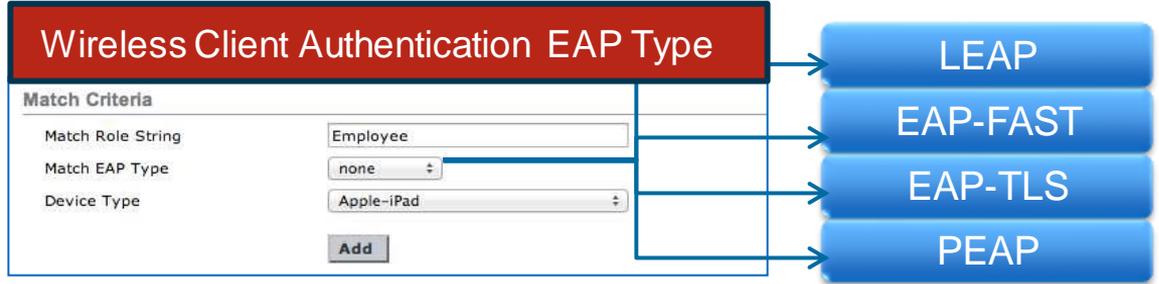
Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	WGB	Device Type
<a href="#">00:27:10:d3:a3:c1</a>	AP2600	Demo-Employee	Demo-Employee	No	Windows7-Works
<a href="#">40:fc:89:75:64:43</a>	AP2600	Demo-Employee	Demo-Employee	No	Android
<a href="#">70:de:e2:0e:ce:01</a>	AP2600	Demo-Employee	Demo-Employee	No	Apple-iPad

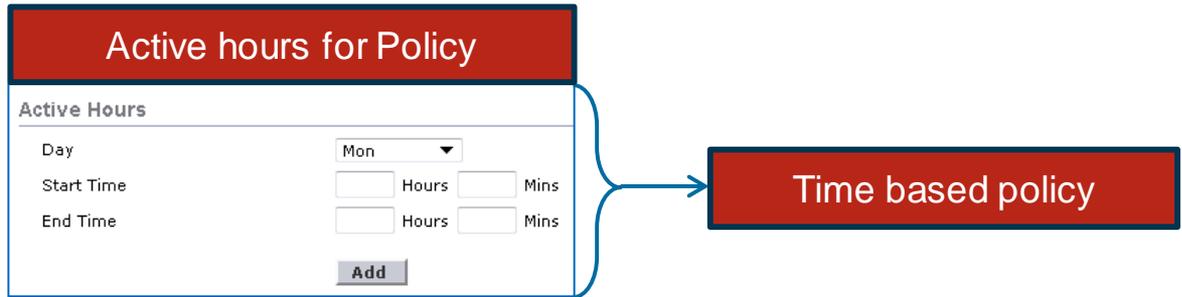
# Native Authentication and Time Policy



Authentication



Time of Day



# Native WLC Policy in Action



## Match Criteria

Match Role String	Employee
Match EAP Type	EAP-TLS

## Device List

Device Type	Android	<b>Add</b>
Apple-iPad		
Microsoft-Surface-Tablet		

## Action

IPv4 ACL	lab-only
VLAN ID	17
Qos Policy	Silver (best effort)
Average Data Rate	0
Average Real time Data Rate	0
Burst Data Rate	0
Burst Real time Data Rate	0
Session Timeout (seconds)	1800
Sleeping Client Timeout (min)	720
Flexconnect ACL	none
AVC Profile	Microsoft Lync
mDNS Profile	AppleTV

## Enforcement Elements

- VLAN
- Access Control List (ACL)
- Quality of Service (QoS)
- Application Control (AVC)
- Bonjour Service Policy

# Apply Native Policy per WLAN / AP Group

## Native Policy per WLAN

WLANs > Edit 'AppTest-Cisco'

General Security QoS Policy-Mapping Advanced

Priority Index (1-16)

Local Policy

Local\_Policy

Add

Priority Index

Local Policy Name

1	iPad-Policy	▼
2	iPhone-Policy	▼
3	Android-Policy	▼
4	MacBook-Policy	▼
5	Windows-Policy	▼

## Native Policy per AP Group

Ap Groups > Edit 'Conference-Room-1'

General WLANs RF Profile APs 802.11u

Add New

WLAN ID	WLAN SSID <sup>2</sup>	Interface/Interface Group(G)	SNMP NAC State
1	AppTest-Cisco	management	Disabled

NAC Enable  
Remove  
Policy-Mapping

AP Group > Policy Mappings

AP Group Name Conference-Room-1

WLAN ID 1

Priority Index (1-16)

Local Policy

Local\_Policy

Add

Priority Index

Local Policy Name

1	iPad-Policy	▼
2	Android-Policy	▼
3	iPhone-Policy	▼
4	MacBook-Policy	▼

Restriction: First Matched Rule Applies

Maximum 16 polices can be created per WLAN / AP Groups and 64 globally

# Required Network Components and Versions



## Cisco Wireless LAN

Feature/Platform	5508 / WiSM2	7500	2500	8500	Converged Access (5760/3850/3650)	440x/WiSM1	210x
OS Version	AireOS 7.2.x onwards			AireOS 7.3.x onwards	IOS XE 3.2.2 onwards		AireOS 7.0.116 onwards
CoA Support	802.1x and L3 Web-auth WLAN					802.1x WLAN only	
Access Point Mode for Profiling and Posture	Local and FlexConnect mode				Local Mode only		
Local Profiling and Policy on WLC	AireOS 7.5 onwards*				IOS XE 3.6.0 onwards		N/A
Extra License	None						

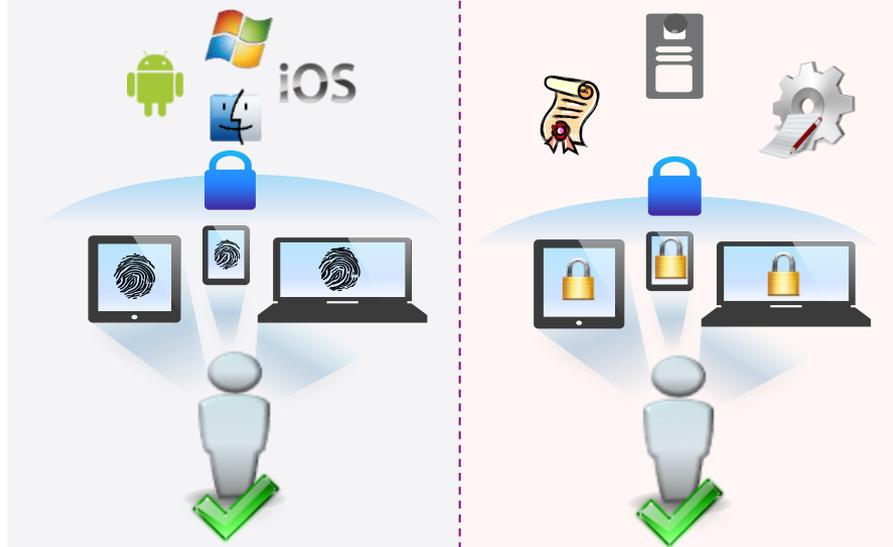
\*FlexConnect mode: No WLC BYOD support for Local Auth on AP

# Agenda

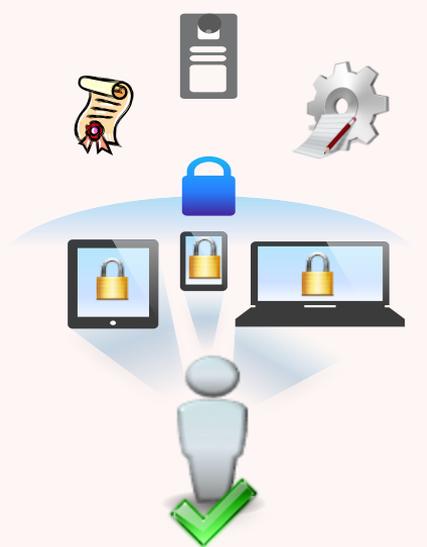
## Managing the BYOD Evolution



Personal Devices on Network



Identification and Security Policy Enforcement



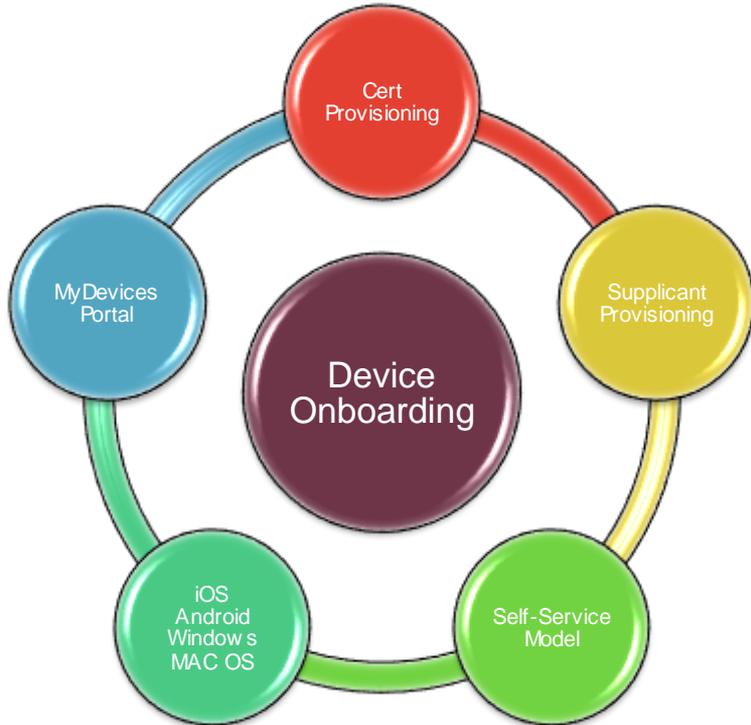
Securely On-Board the Device

A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern cityscape is visible with illuminated buildings and a pedestrian bridge spanning across the street. The overall scene is a blend of urban architecture and dynamic light patterns.

# BYOD Device Provisioning

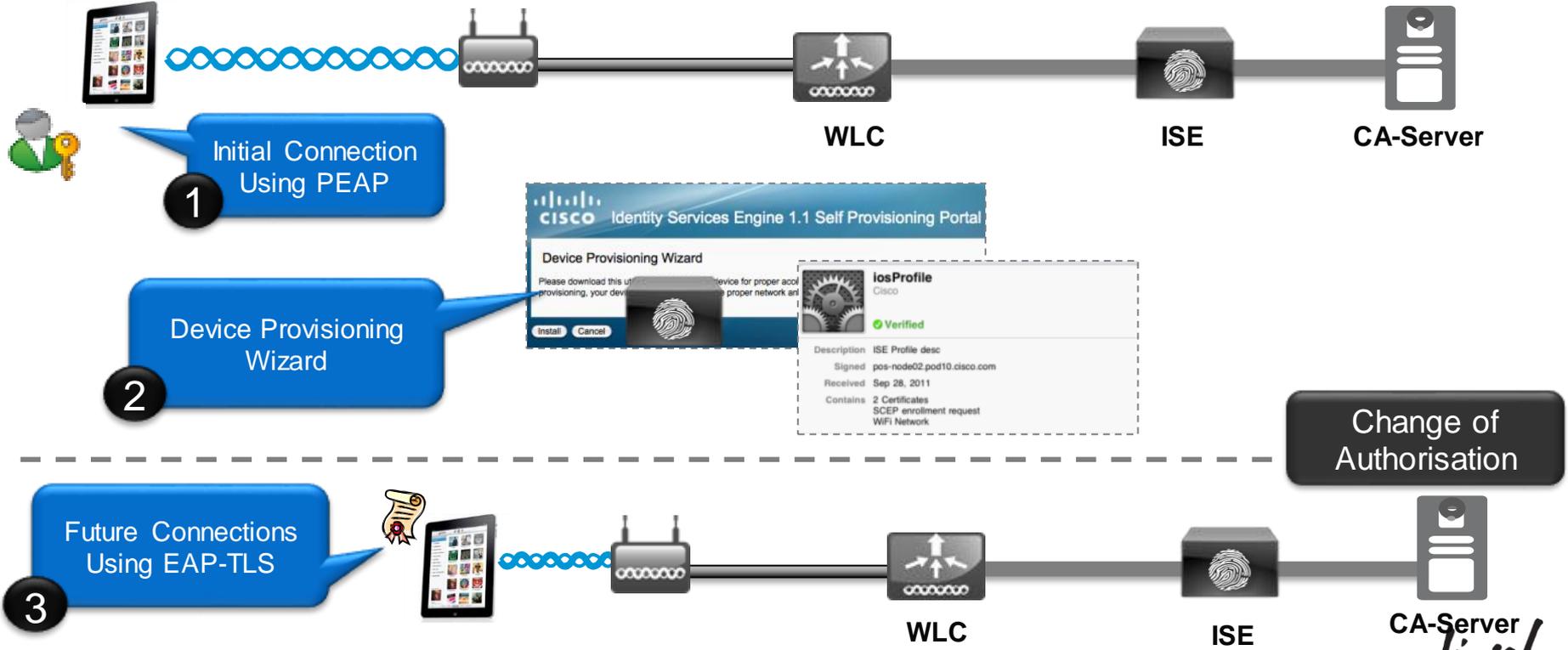
# Simplified On-boarding for BYOD

## Identity Services Engine



- Provision a Certificate for the device.
  - Based on Employee-ID & Device-ID.
- Provision the Native Supplicant for the Device:
  - iOS, Android, Win & Mac OS X
  - Use EAP-TLS or PEAP
- Employees get Self-Service Portal
  - Lost Devices are Blacklisted
- Self-Service Model
  - IT does not need to be in the middle.

# Apple iOS Device Provisioning



# DNS-based ACLs

- For BYOD onboarding use cases, you can set pre-authentication ACLs to determine what sites devices have the permission to visit
- Prior to WLC 7.6, ACLs are IP-based
- With WLC 7.6, ISE can return a URL ACL (url-redirect-acl), with DNS names
  - e.g. play.google.com
- ACL is applied to the client at the AP level
- Works for AP in Local or FlexConnect mode

# MyDevices Portal

## Self-Registration and Self-Blacklisting of BYOD Devices



CiscoLive My Devices Portal

Welcome [Sign Out](#)

### Manage Devices

To add a device, enter the Device ID, which displays on your device as the MAC or Wi-Fi address. It consists of 6 alphanumeric number pairs separated by colons: A1:B2:C3:D4:E5:F6.

\* Device ID:

Description:

### Your Devices

Edit	Reinststate	Lost?	Delete	Full Wipe	Corporate Wipe	PIN Lock
Select	Device ID	Description	State			
<input checked="" type="radio"/>	01:23:45:67:89:AB	Scott's iPhone	<input type="checkbox"/>			
<input type="radio"/>	EF:12:34:56:78:90	Scott's Samsung Note3	<input type="checkbox"/>			



You cannot add this device because you have reached the maximum number of devices.

3

Devices Can be Self-Registered, Up to an Administrator Defined Limit

2

User can Self-Manage Lost/Found/Wipe etc

1

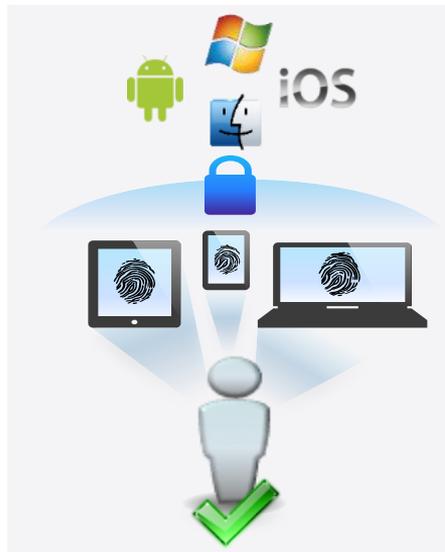
New Devices Can be Added with a Description

# Agenda

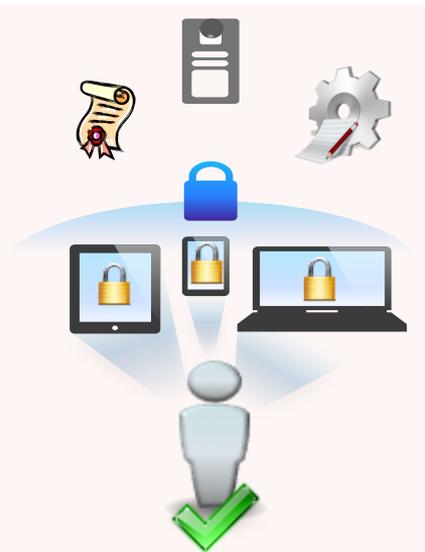
## Managing the BYOD Evolution



Personal Devices on Network



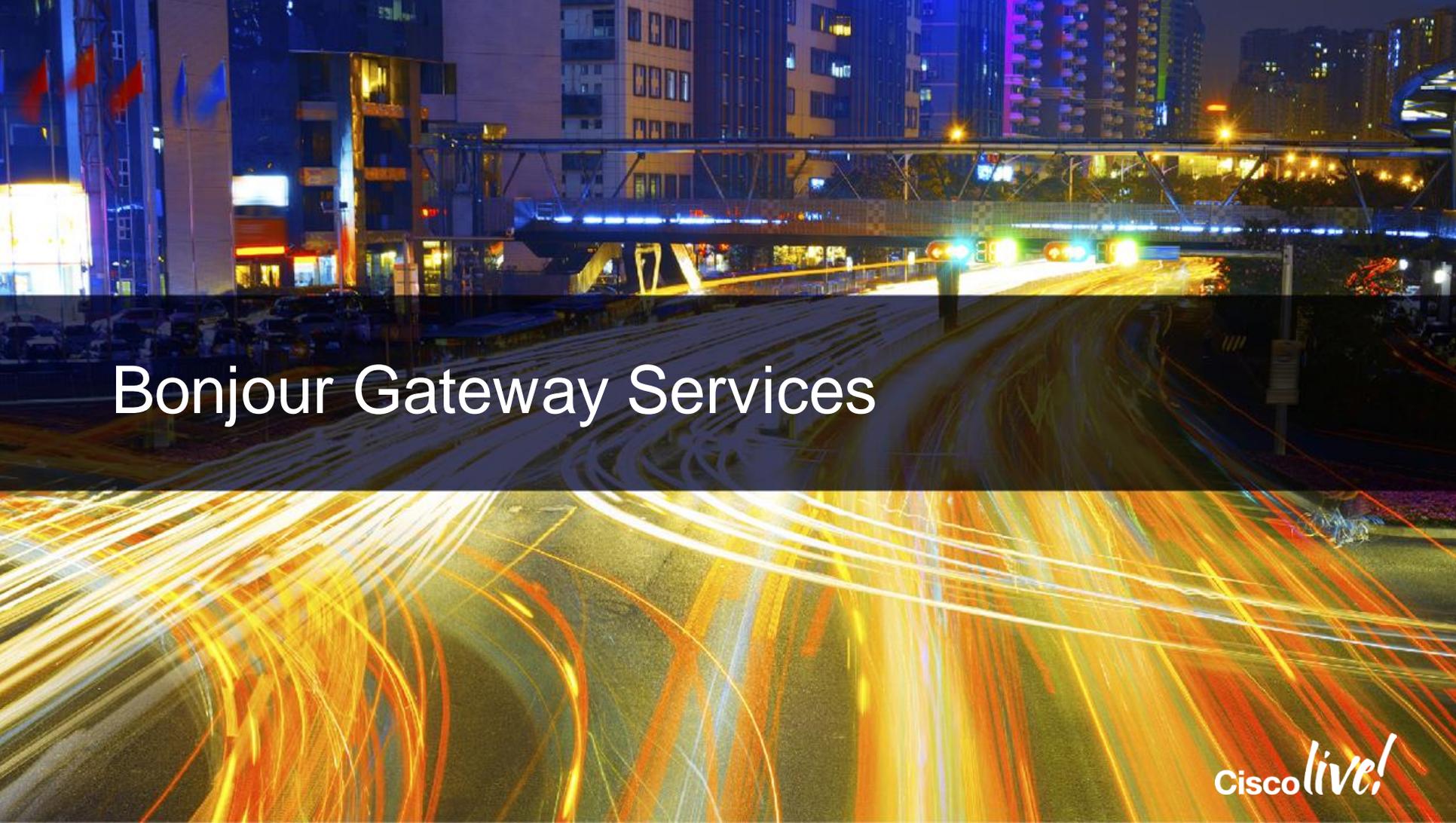
Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations

A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern pedestrian bridge with blue lighting spans across the street. Tall buildings with illuminated windows and balconies line the street, and several flags are visible on the left side. The overall scene is a dynamic and brightly lit urban environment.

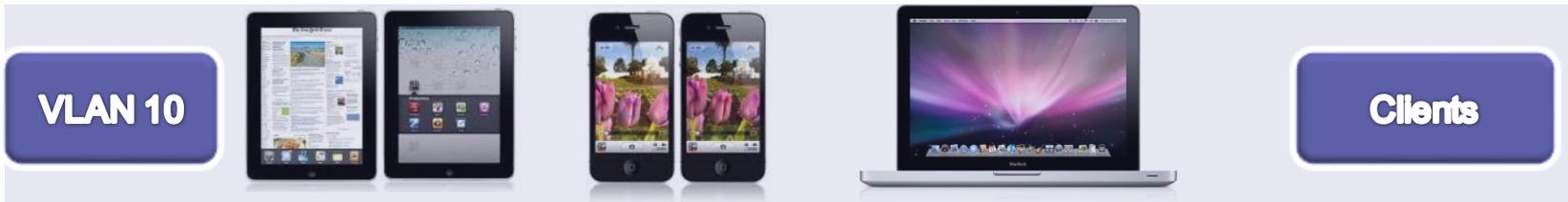
# Bonjour Gateway Services

Cisco *live!*

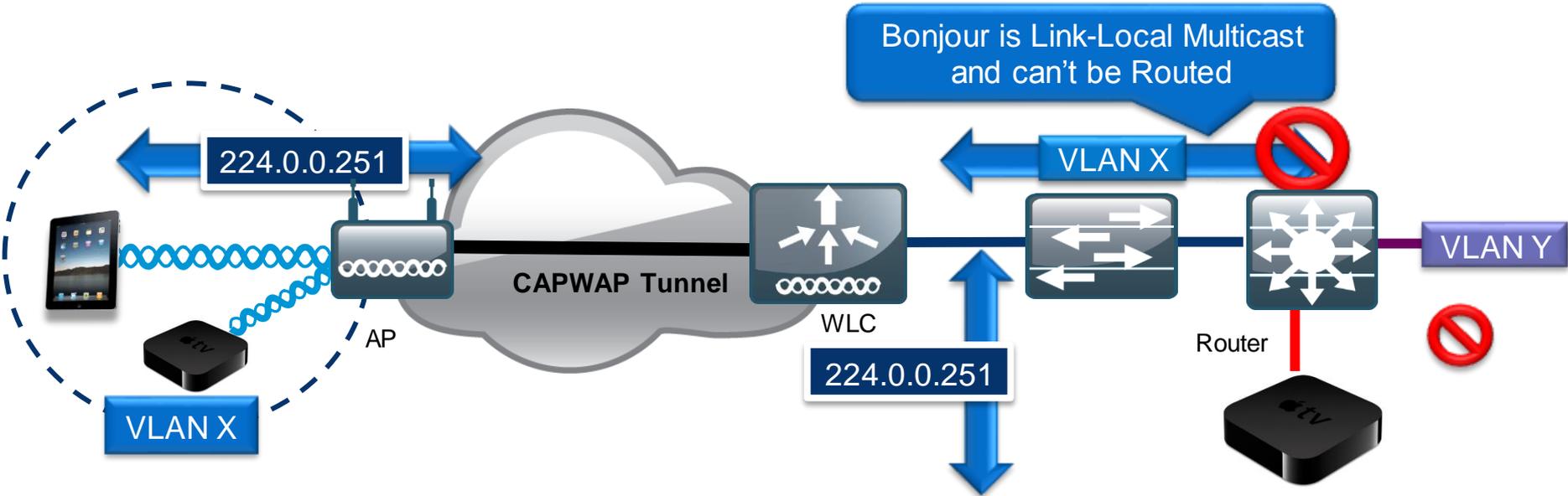
# Bonjour Protocol



- Bonjour Protocol helps apple devices discover services
- Uses mDNS protocol to advertise and discover services
- Link Local: Does not cross subnets



# Bonjour Challenges Across VLAN's

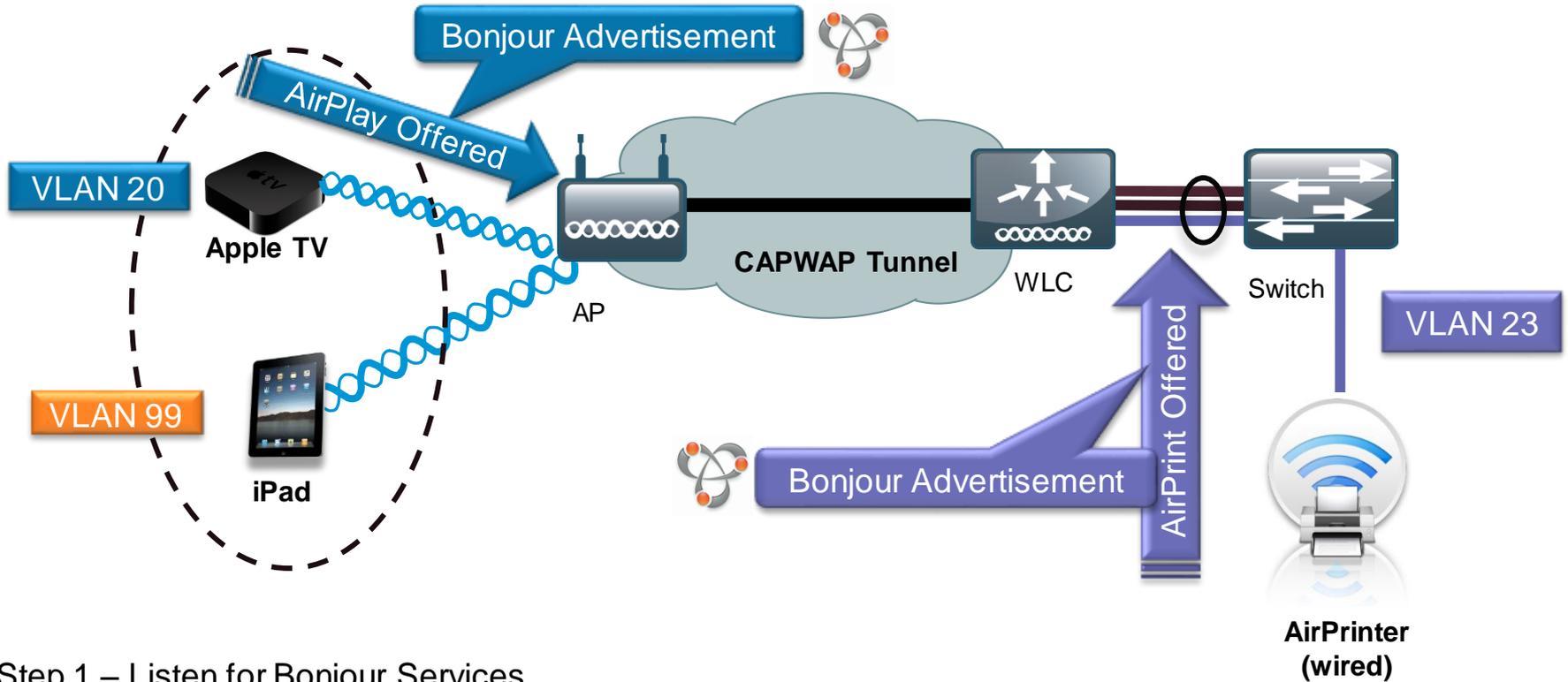


- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:

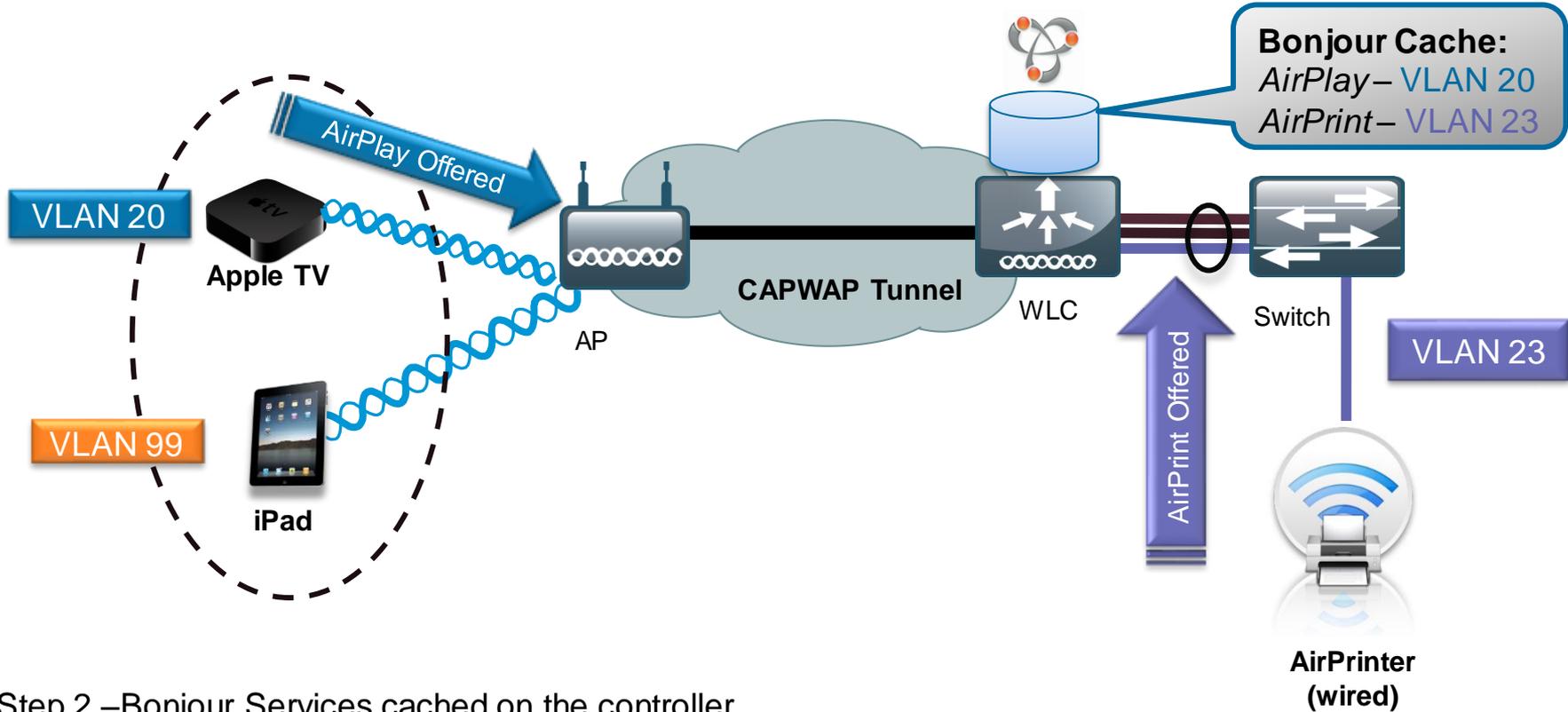
IPv4 Group Address – 224.0.0.251

IPv6 Group Address – FF02::FB

# Bonjour mDNS Gateway on Cisco WLC

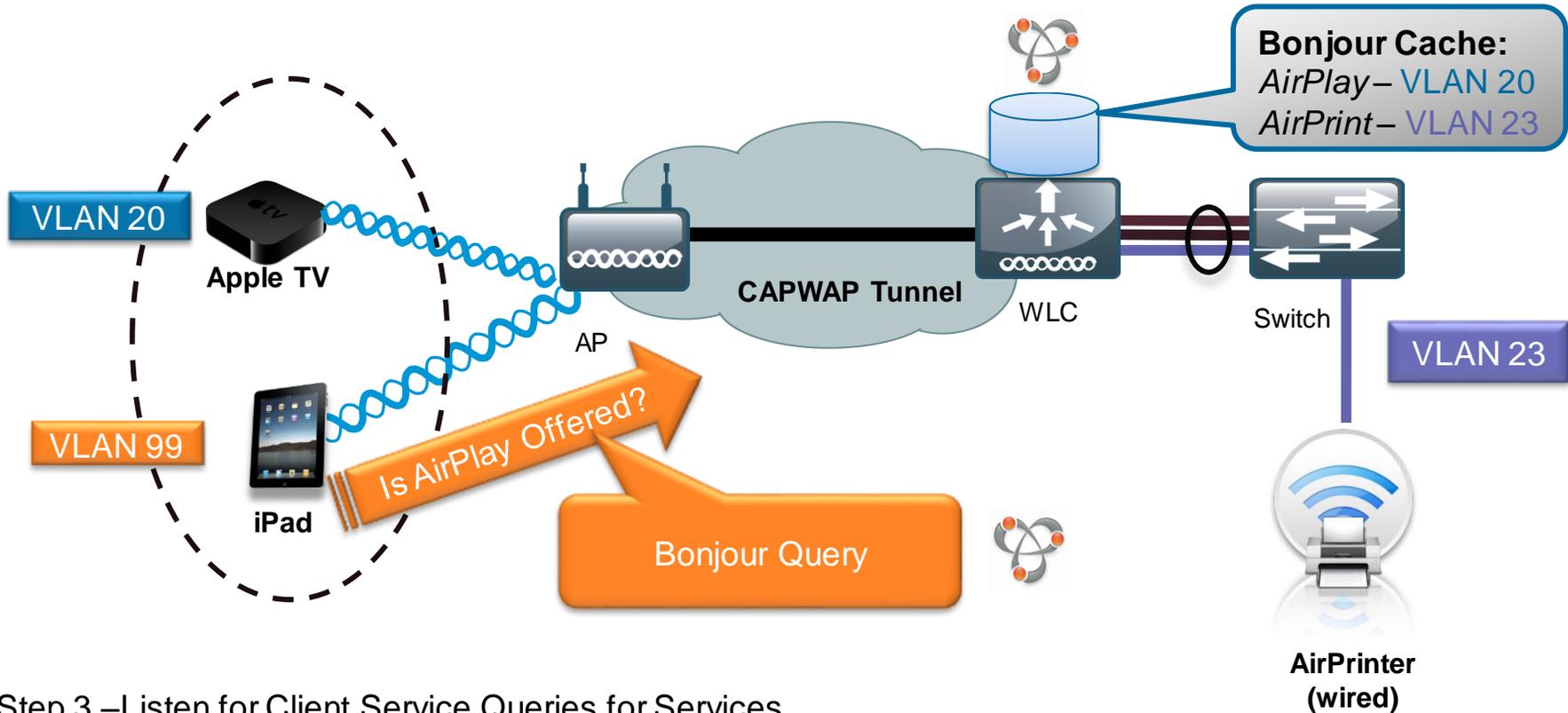


# Bonjour mDNS Gateway on Cisco WLC



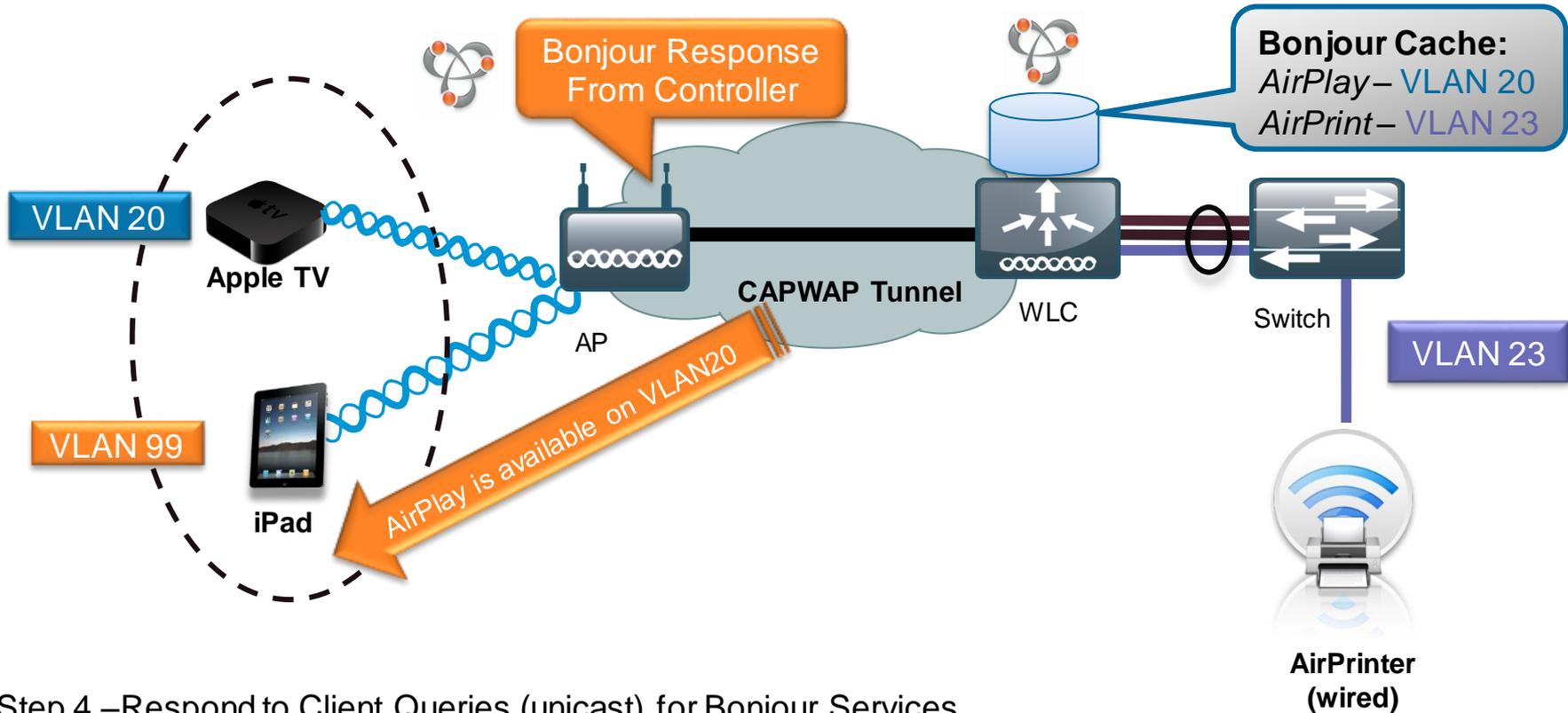
- Step 2 – Bonjour Services cached on the controller

# Bonjour mDNS Gateway on Cisco WLC



- Step 3 –Listen for Client Service Queries for Services

# Bonjour mDNS Gateway on Cisco WLC



- Step 4 – Respond to Client Queries (unicast) for Bonjour Services

# Common Bonjour Services



AirPlay

Airplay Services = 4

Airplay for iOS (*\_airplay.\_tcp*)

Airplay for Mac OSX (*\_appletv-v2.\_tcp*)

Audio for Airplay (*\_roap.\_tcp*)

Remote (*\_touch-able.\_tcp*)



AirPrint

AirPrint Services = 5

Internet Printing protocol (*\_ipp.\_tcp*)

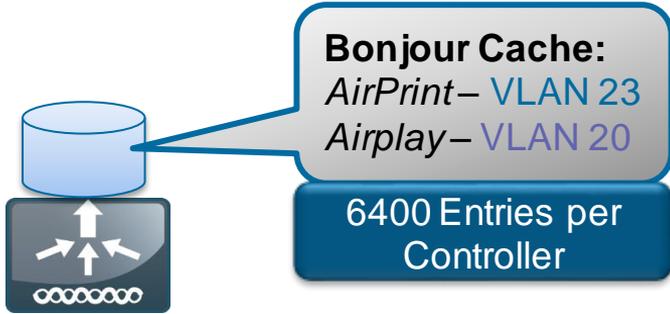
Printer Spool (*\_printer.\_tcp*)

Printer PDL DataStream (*\_pdl-datastream.\_tcp*)

HTTP (*\_http.\_tcp*)

Scanner (*\_scanner.\_tcp*)

# Bonjour Traffic Optimisation



## Reason for Traffic optimisation

Bonjour Service query is cached on Controller

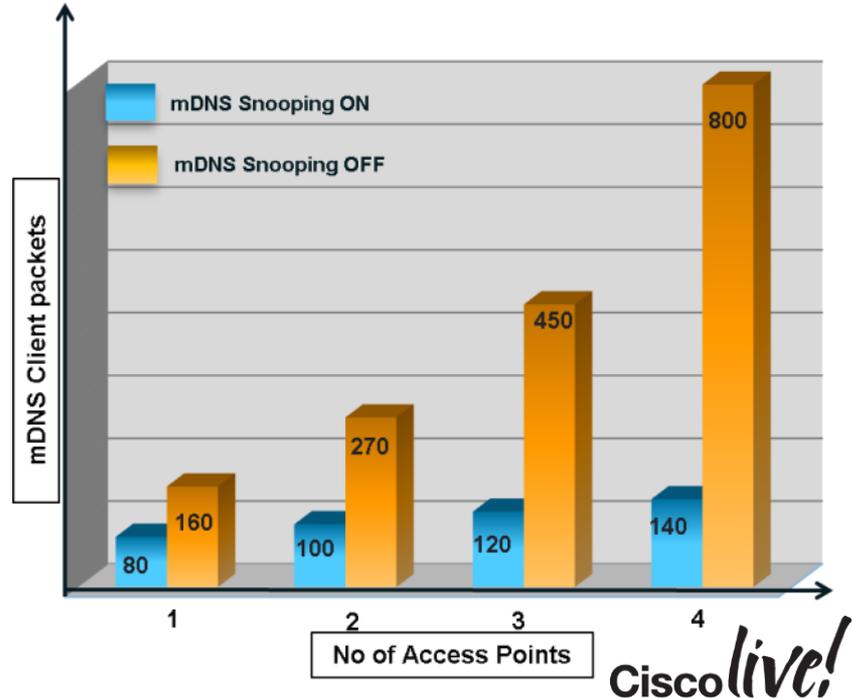
- Not flooded

Bonjour Client Query

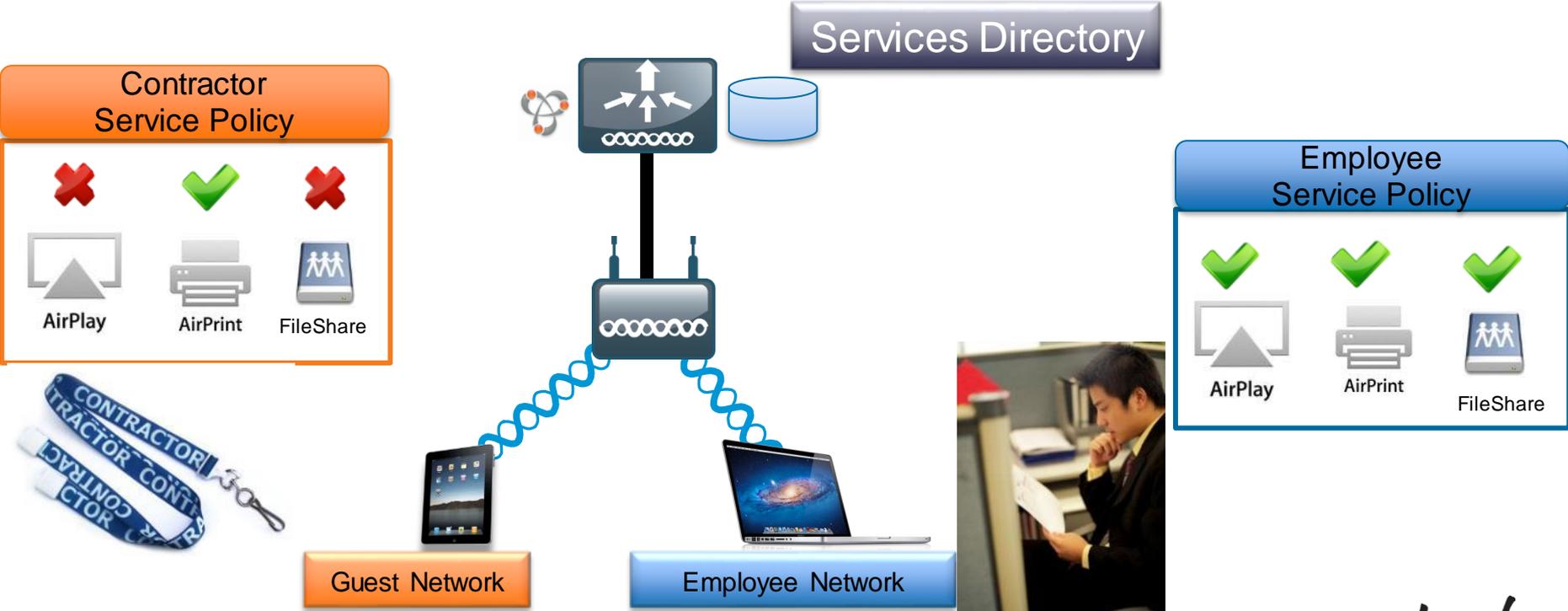
- Unicast Response
- Not flooded

80% less Bonjour Traffic\*

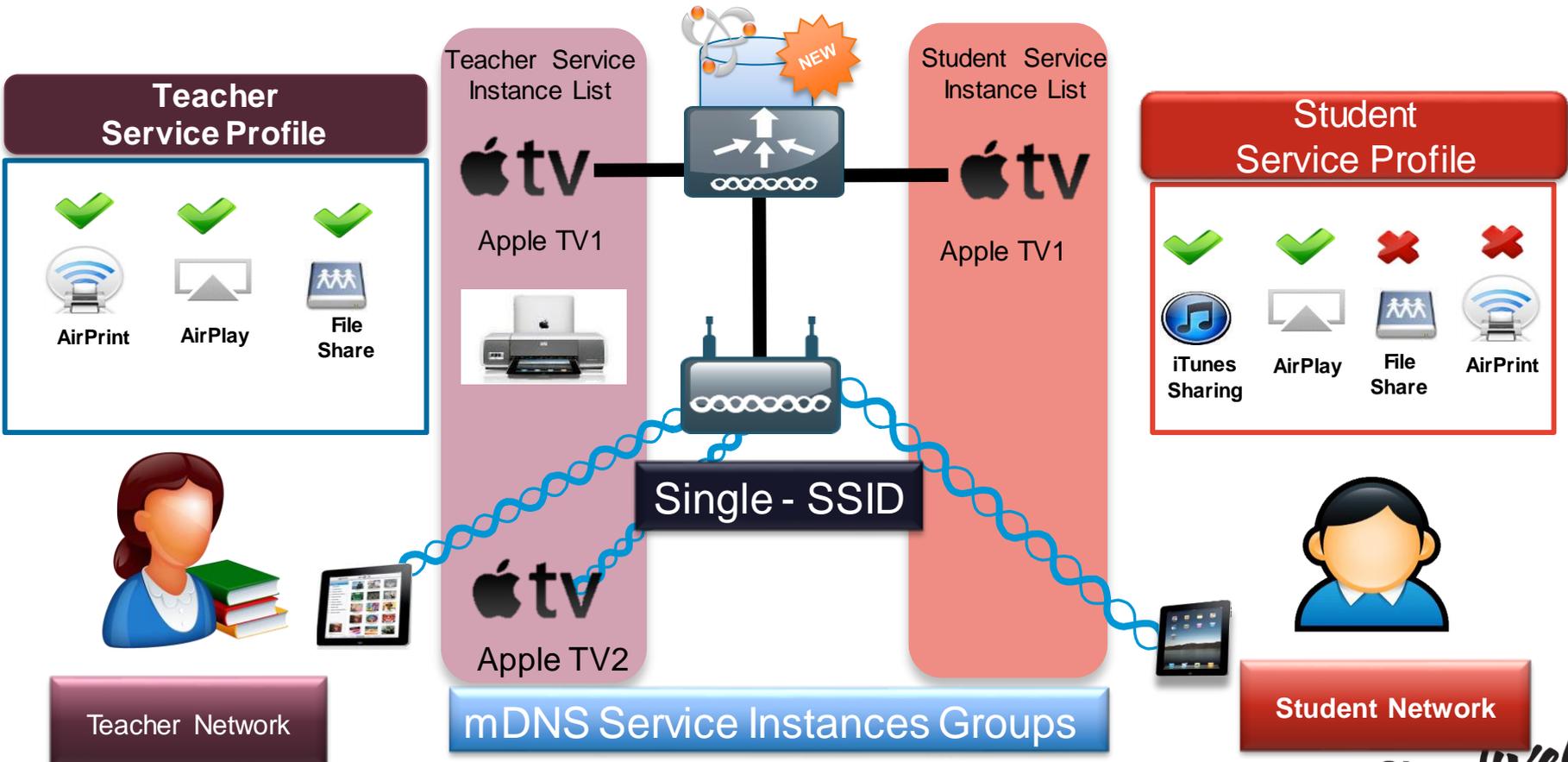
\* For 4 Access Point Deployment



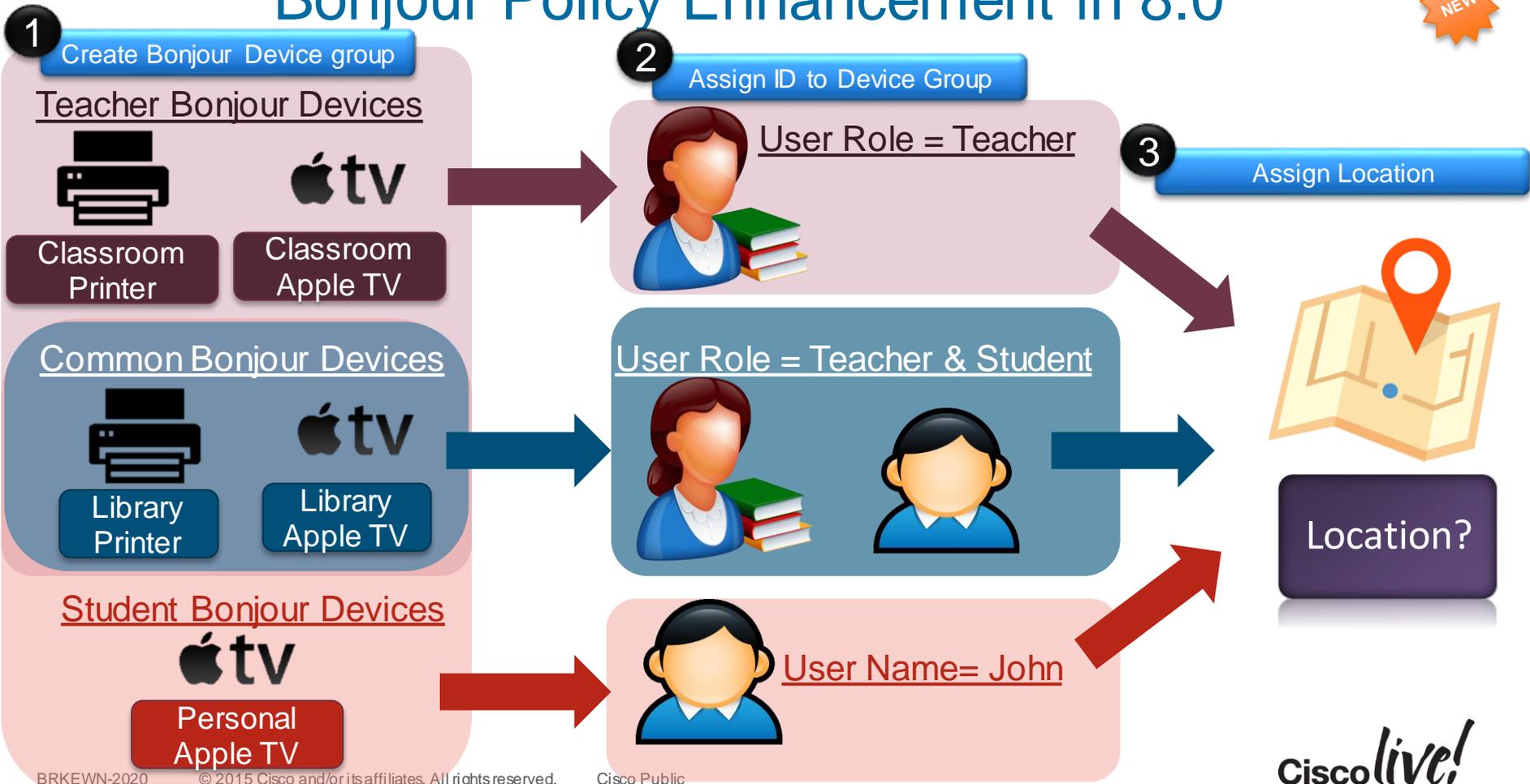
# Filter Services by User Group



# Filter Bonjour Service per Device using v8.0



# Bonjour Policy Enhancement in 8.0



# Bonjour Policy Enhancement in 8.0



Teacher Bonjour  
Devices



Classroom  
Apple TV



User Role = Teacher



Location = Classroom

Teacher can discover Classroom Apple printer from anywhere on the campus



Classroom  
Printer



User Role = Teacher



Location = Any

Location can be AP-Group, AP-Name or AP-Location

# Google ChromeCast With Cisco Wireless

## How Does Google ChromeCast Work?



- ChromeCast Deployment Guide:
  - <http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-6/chromecastDG76/ChromecastDG76.html>

# Summary

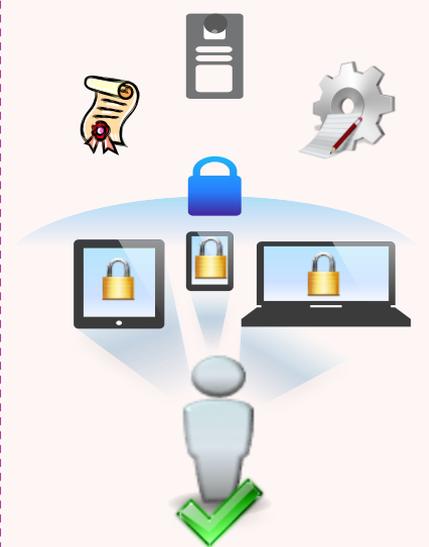
## Managing the BYOD Evolution



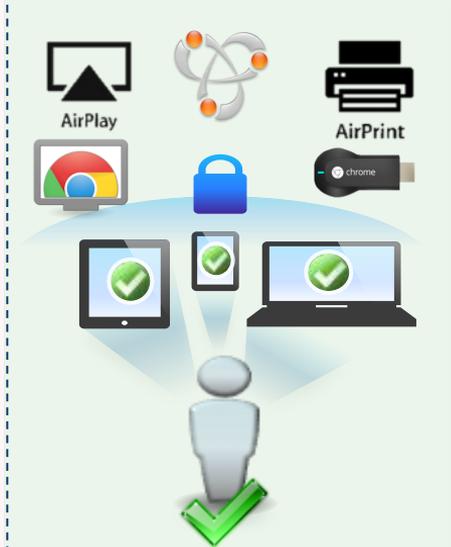
Personal Devices on Network



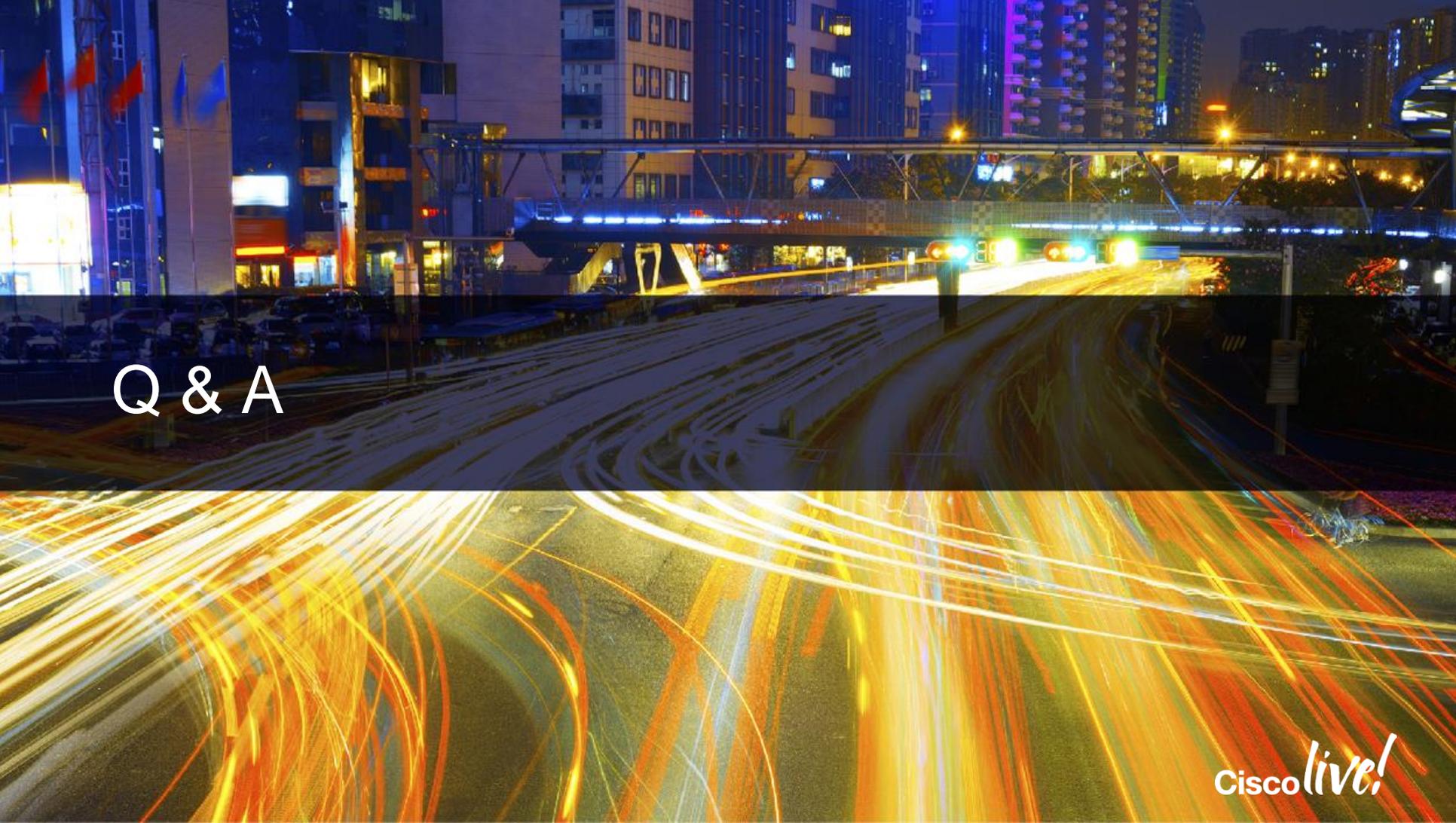
Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations



Q & A

Cisco *live!*

# 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](http://www.CiscoLiveAPAC.com)



Thank you.

Cisco *live!*

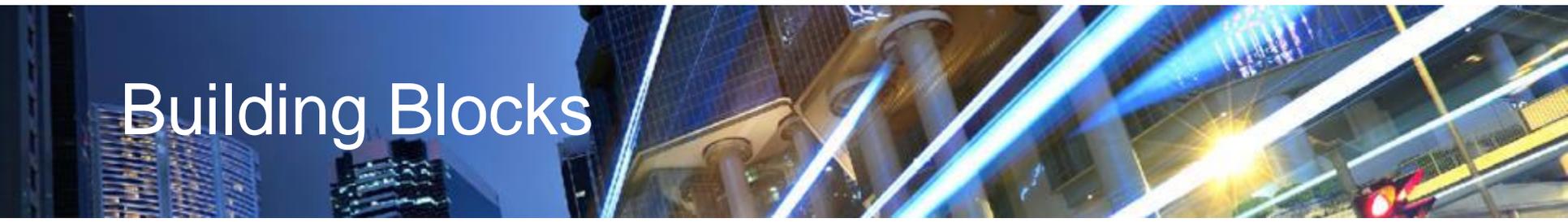


**CISCO**

A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with a glass railing spans across the street. The background features several modern buildings with lit windows and some streetlights. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

Configurations for Your Reference

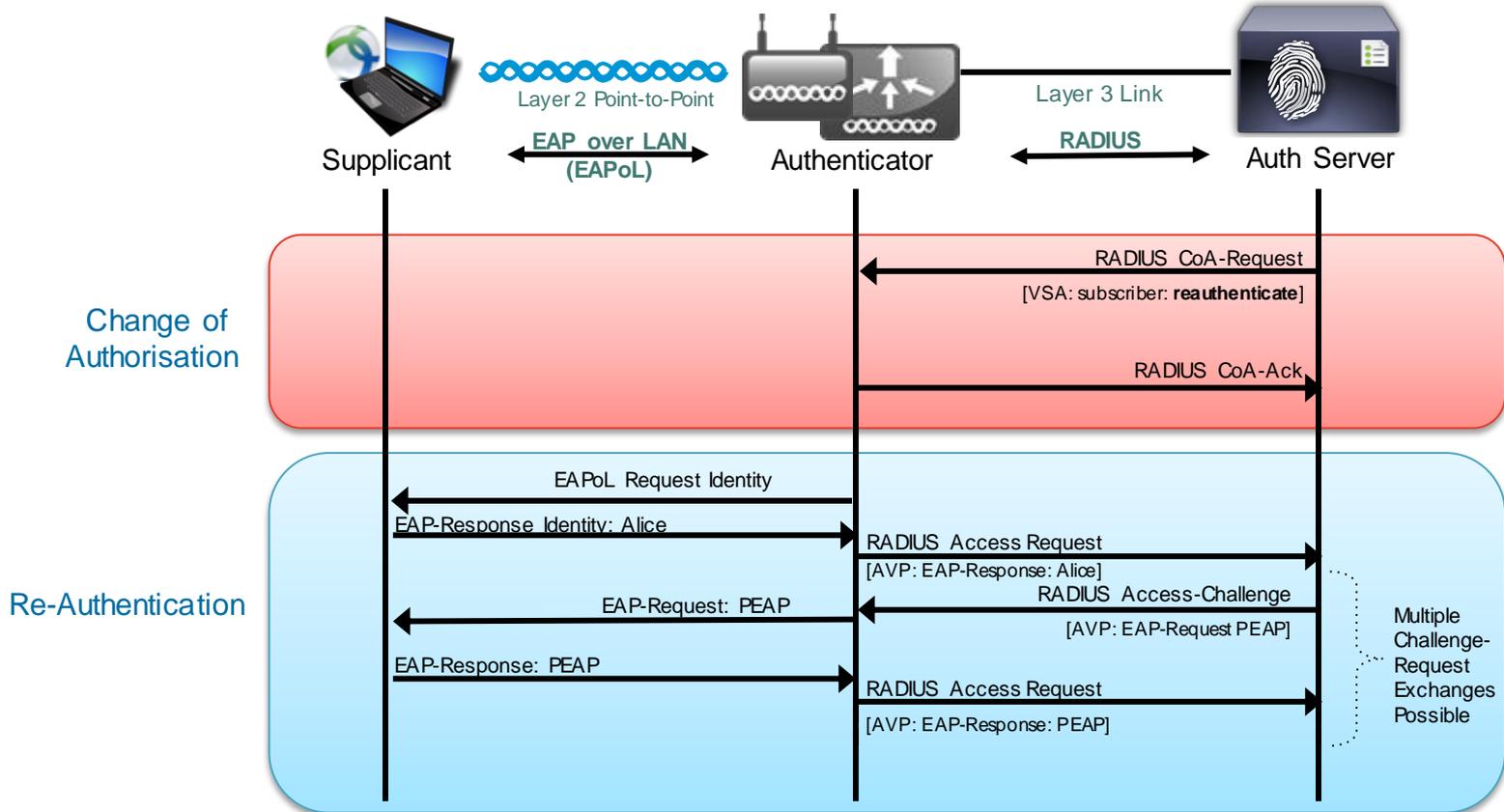
Cisco *live!*



# Building Blocks

# IEEE 802.1X with Change of Authorisation (CoA)

For your reference



# Enable CoA – AAA Override

1  
Allow AAA  
Override to  
Permit ISE to  
Modify User  
Access  
Permissions  
(CoA)

The screenshot shows the 'Advanced' configuration tab for a network device. The 'Allow AAA Override' checkbox is checked and highlighted with a red box. The 'NAC State' dropdown menu is also highlighted with a red box and set to 'Radius NAC'. Other visible settings include 'Coverage Hole Detection' (Enabled), 'Enable Session Timeout' (1800), 'Alronet IE' (Enabled), 'Diagnostic Channel' (Disabled), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Acl' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (Enabled, 60), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (Disabled), 'Wi-Fi Direct Clients Policy' (Disabled), and 'Maximum Allowed Clients Per AP Radio' (200). On the right side, 'DHCP' settings show 'DHCP Server' (Override) and 'DHCP Addr. Assignment' (Required). 'OEAP' settings show 'Split Tunnel (Printers)' (Enabled). 'Management Frame Protection (MFP)' settings show 'MFP Client Protection' (Optional). 'DTIM Period (in beacon intervals)' settings show '802.11a/n (1 - 255)' (1) and '802.11b/g/n (1 - 255)' (1). 'NAC' settings show 'NAC State' (Radius NAC). 'Load Balancing and Band Select' is also visible at the bottom.

2  
Allow AAA  
Override to  
Permit ISE to  
redirect client  
to a specific  
URL

# Converged Access BYOD Config

## Change Of Authorisation (CoA)

**WLAN**  
WLAN > Edit

General Security **Advanced**

Allow AAA Override	<input checked="" type="checkbox"/>
Coverage Hole Detection	<input checked="" type="checkbox"/>
Session Timeout (secs)	<input type="text" value="0"/>
(0 = Session never expires)	
Aironet IE	<input checked="" type="checkbox"/>
Diagnostic Channel	<input type="checkbox"/>
P2P Blocking Action	<input type="text" value="Disabled"/>
Client Exclusion	<input checked="" type="checkbox"/>
Timeout Value(secs)	<input type="text" value="60"/>
Max Allowed Client	<input type="text" value="0"/>

**DHCP**

DHCP Server override	<input type="checkbox"/>
DHCP Address Assignment required	<input type="checkbox"/>
DHCP Option 82	<input type="checkbox"/>
DHCP Option 82 Format	<input type="text" value="None"/>
DHCP Option 82 Ascii Mode	<input type="checkbox"/>
DHCP Option 82 Rid Mode	<input type="checkbox"/>

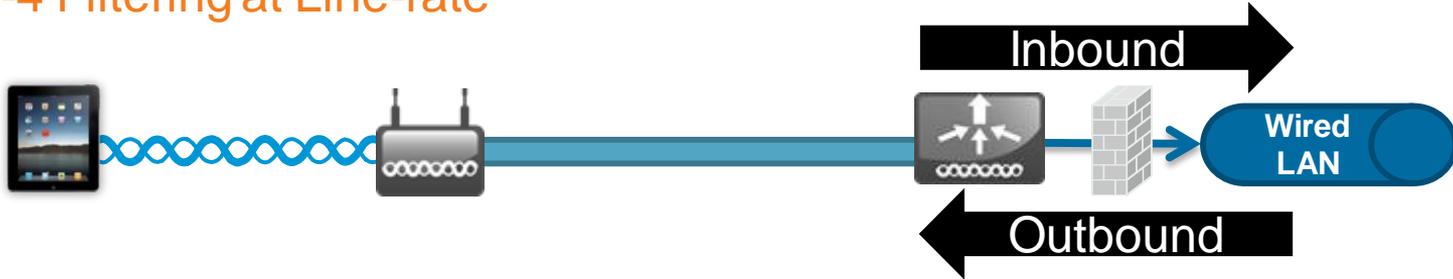
**NAC**

NAC State	<input checked="" type="checkbox"/>
-----------	-------------------------------------

## Network Access Control

# Cisco Wireless LAN Controller ACLs

## Layer 3-4 Filtering at Line-rate



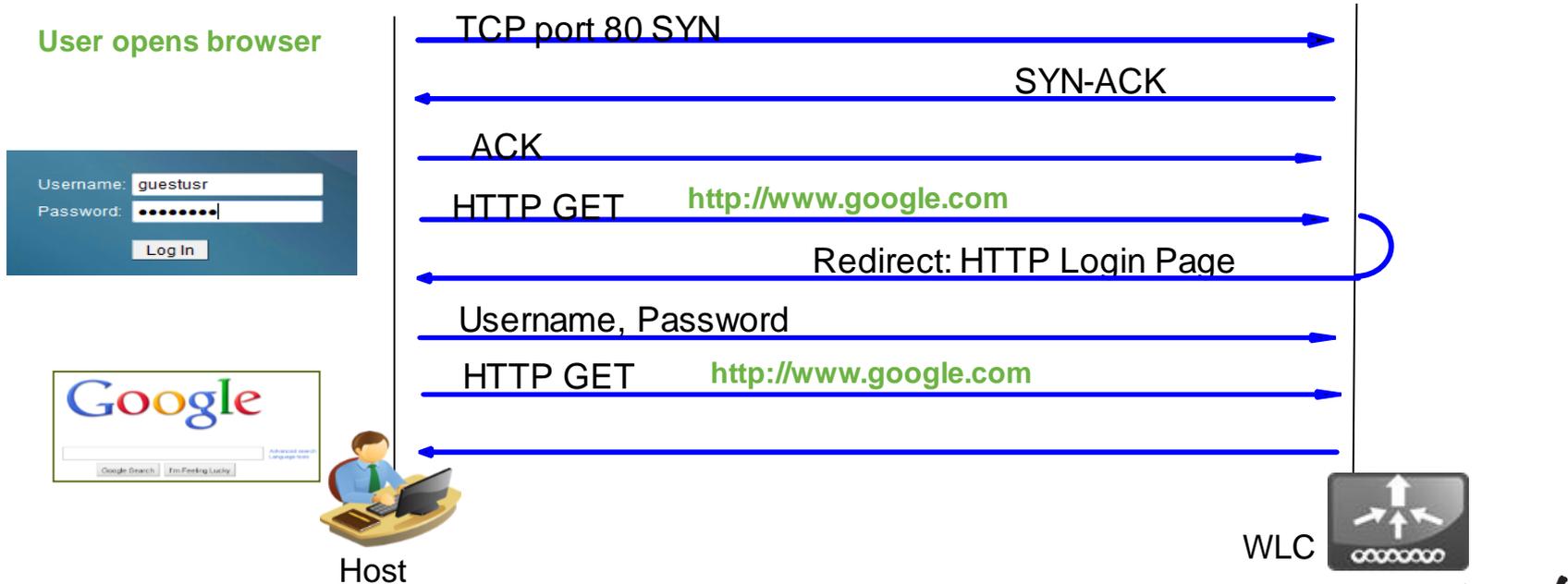
- ACLs provide L3-L4 policy and can be applied per interface or per user.
- Cisco 2500, 5508 and WiSM2 implement hardware, line-rate ACLs.
- Up to 64 rules can be configured per ACL.

Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
Permit	0.0.0.0 / 0.0.0.0	10.10.10.10 / 255.255.255.255	Any	Any	Any	Any	Inbound
Permit	10.10.10.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound

**Implicit Deny All at the End**

# URL Redirection

- Example: TCP Traffic Flow for Login Page



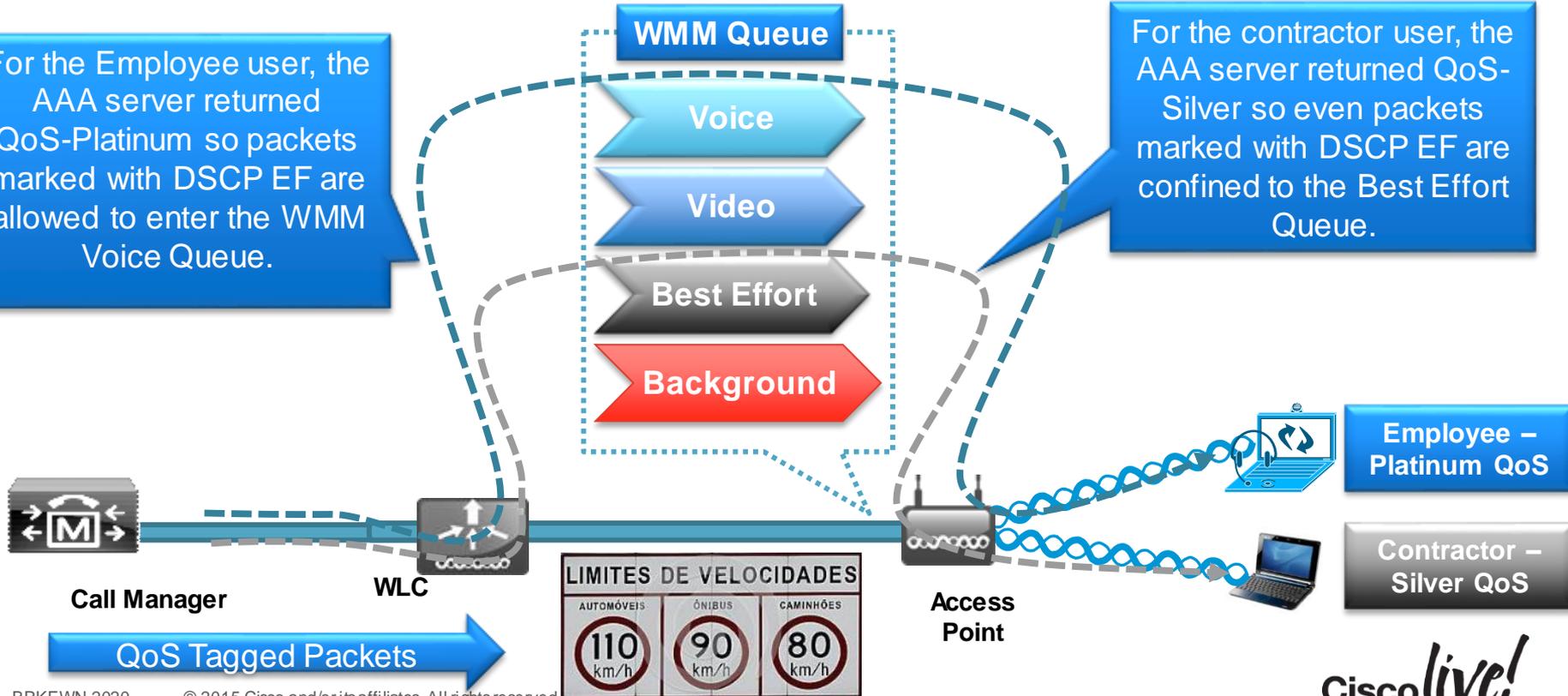
# Cisco Wireless User-Based QoS Capabilities



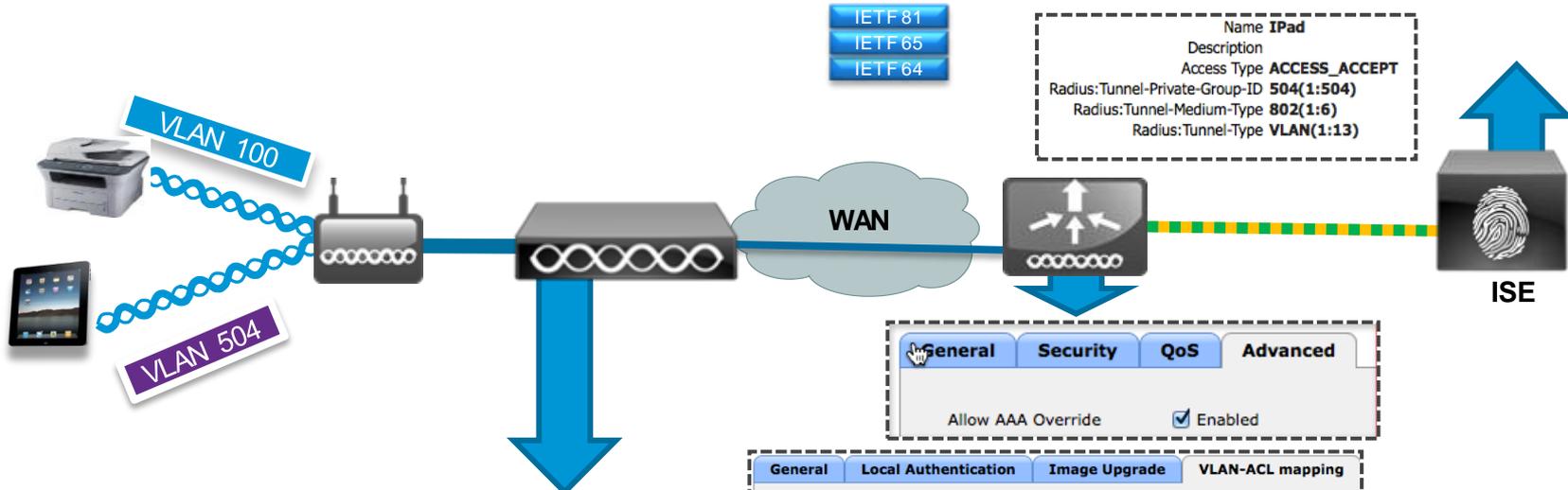
## Allowing Per-User and Per-Devices Limiting of the Maximum QoS Level

For the Employee user, the AAA server returned QoS-Platinum so packets marked with DSCP EF are allowed to enter the WMM Voice Queue.

For the contractor user, the AAA server returned QoS-Silver so even packets marked with DSCP EF are confined to the Best Effort Queue.



# FlexConnect and AAA Override



IETF 81  
IETF 65  
IETF 64

Name **IPad**  
Description  
Access Type **ACCESS\_ACCEPT**  
Radius:Tunnel-Private-Group-ID **504(1:504)**  
Radius:Tunnel-Medium-Type **802(1:6)**  
Radius:Tunnel-Type **VLAN(1:13)**



General Security QoS Advanced  
Allow AAA Override  Enabled

```
interface GigabitEthernet0/37
description AP_1142
switchport access vlan 100
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport trunk allowed vlan 100,502-504
switchport mode trunk
```

General Local Authentication Image Upgrade VLAN-ACL mapping

**VLAN ACL Mapping**

Vlan Id: 0  
Ingress ACL: FlexConnect  
Egress ACL: FlexConnect  
Add

Vlan Id	Ingress ACL	Egress ACL
504	Flex_AAA_Override_ACL	none

Create Sub-Interface on FlexConnect AP and Set the ACL on the VLAN

VLAN for Locally Swit



# Integration of WLC and ISE

# Steps for Integrating the Controller and ISE



## 1. Configure WLAN for 802.1x Authentication

- Configure RADIUS Server on Controller
- Setup WLAN for AAA Override, Profiling and RADIUS NAC

## 2. Configure ISE Profiling

- Enable profiling sensors

## 3. Setup Access Restrictions

- Configure ACLs to filter and control network access.

# Configuring ISE as the Authentication Server and Accounting Server



**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
  - Password Policies
  - Local EAP
  - Priority Order

### RADIUS Authentication Servers > New

< Back    Apply

Server Index (Priority): 3

Server IP Address: 10.10.10.10

Shared Secret Format: ASCII

Shared Secret: [Redacted]

(Designed for FIPS customers and requires a key wrap compliant RADIUS server)

1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: [Redacted]

**1** Enable "RFC 3576" for Support Change of Authorisation

### RADIUS Accounting Servers

MAC Delimiter: Hyphen

Network User	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<a href="#">1</a>	10.10.10.10	1813	Disabled	Enabled <input checked="" type="checkbox"/>

**2** Add to Accounting Servers to Receive Session Statistics

# Configuring the WLAN for Secure Connectivity

## Enabling Secure Authentication and Encryption with WPA2-Enterprise



The screenshot shows the Cisco WLAN configuration page for 'Corporate X'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'WPA+WPA2 Parameters' section shows 'WPA2 Policy' checked and 'WPA2 Encryption' set to 'AES'. The 'Authentication Key Management' section shows '802.1X' checked and 'Enable'. The 'AAA Servers' sub-tab is also visible, showing a table of Radius Servers with columns for Authentication Servers and Accounting Servers.

**1** WPA2 Security with AES Encryption

**2** Assign Radius Server per WLAN

# Setting the WLAN QoS Level for Override

Using WMM, the QoS Level is Based on the Marking of the Packet.



The screenshot shows the Cisco WLAN configuration interface for 'Corporate X'. The 'QoS' tab is selected, and the 'Quality of Service (QoS)' dropdown is set to 'Platinum (voice)'. A blue callout box with a '1' in a black circle points to the dropdown menu, containing the text: 'This Acts As An Upper Limit, or Ceiling for the WLAN's QoS Configuration'.

General	Security	QoS	Policy-Mapping	Advanced
Quality of Service (QoS)		Platinum (voice)		
Application Visibility	<input checked="" type="checkbox"/> Enabled			
AVC Profile	none			
Netflow Monitor	none			

- If WMM is set to Allowed, the Quality of Service configuration serves as a limit for the entire SSID.
- Ensure all controller uplinks, media servers and Access Points have proper Quality of Service trust commands in IOS.

# Configuring the WLAN for ISE Identity-based Networking Cont'd



**1** Allow AAA Override to Permit ISE to Modify User Access Permissions

**2** Enable RADIUS NAC to allow ISE to use Change of Authorisation.

**3** Enable Radius Client Profiling to Send DHCP and HTTP attributes to ISE.

# Configuring the Controller ACL



**CISCO** Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

### Security

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
  - TACACS+
    - LDAP
    - Local Net Users
    - MAC Filtering
    - Disabled Clients
    - User Login Policies
    - AP Policies
    - Password Policies
  - Local EAP
  - Priority Order
  - Certificate
  - Access Control Lists
    - Access Control Lists
    - CPU Access Control Lists
    - FlexConnect ACLs

### Access Control Lists > Edit

**1** This ACL will be referenced by name by the ISE to restrict the user.

**2** Use the ISE server's IP address to allow only traffic to that site.

**General**

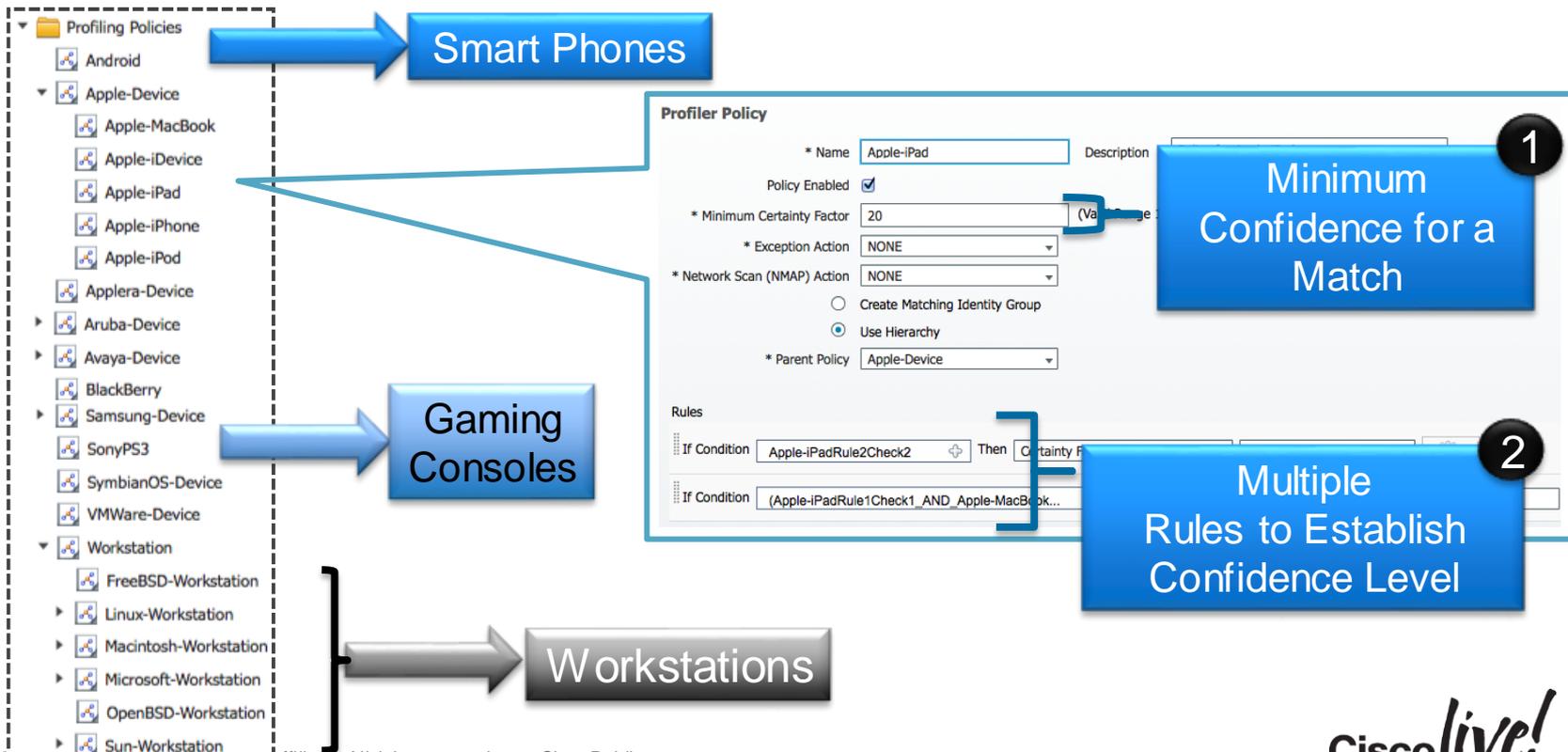
Access List Name: ACL-Web-Redirect

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<a href="#">1</a>	Permit	0.0.0.0 /	10.10.10.10 /	Any	Any	Any	Any	Inbound	0
<a href="#">2</a>	Permit	10.10.10.10 /	0.0.0.0 /	Any	Any	Any	Any	Outbound	0

# ISE Device Profiling Capabilities

Over 200 Built-in Device Policies, Defined Hierarchically by Vendor



# Configuring ISE Profiling Sensors



For your  
reference

NETFLOW

DHCP

Interface: GigabitEthernet 0

Port: 67

Description: DHCP

DHCPSPAN

HTTP

Interface: GigabitEthernet 0

Description: HTTP

RADIUS

Network Scan (NMAP)

Description: NMAP

Manual Scan Subnet:

Run Scan Cancel Scan

[Click to see latest scan results](#)

DNS

- Profiling relies on a multitude of “sensors” to assess the client’s device type.
- Profiling can always be achieved through a span port, more efficient profiling is achieved through sensors which selectively forward attributes.
- For DHCP Profiling:
  - Option A: Use v7.2 MR1 code to send DHCP attributes in RADIUS accounting messages.
  - Option B: Use Cisco IOS “ip helper” addressed to ISE on switches adjacent to the WLC.
- For HTTP Profiling:
  - Use the Web-Authentication redirect to get the HTTP user agent.

# Authentication Policy Sets on ISE



**Identity Services Engine**

Home | Operations | Policy | Guest Access | Administration

Policy Sets | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

### Policy Sets

Search policy names & descriptions.

**Summary of Policies**  
A list of all your policies

- Global Exceptions**  
Rules across entire deployment
- cisco\_live\_policy**  
for cisco live only
- Wireless\_802\_1x\_Milan**  
For Wireless dot1x for AP in Milan
- Wireless\_802\_1x**  
For Wireless dot1x

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description
<input checked="" type="checkbox"/>	Wireless_802_1x	For Wireless dot1x

**Authentication Policy**

**Authorization Policy**

Save Reset

### Authentication Compound Condition Details

Name **Wireless\_802.1X**

**Conditions**

**Radius:Service-Type EQUALS Framed**      **AND**

**Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11**

OK



# Device On-boarding

# Steps for Configuring Device Provisioning



## 1. Configure Integration with External CA Server

- Define SCEP URL and certificates.
- Example – Active Directory, CA Server or Internal DB.

## 2. Define Supplicant Provisioning Profile

- Define what security and EAP type is deployed to end devices.

# Configuring SCEP Integration on the ISE

- The ISE Must Point to the SCEP Server and Have a Valid Certificate Signed by the CA

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar includes Home, Operations, Policy, and Administration. The left sidebar shows 'Certificate Operations' with options like Local Certificates, Certificate Signing Requests, Certificate Authority Certificates, SCEP CA Profiles, and OSCP Services. The main content area is titled 'SEP Certificate Authority Certificates > Windows-2008-CA' and shows an 'Edit Certificate' form. The form fields are: Name (Windows-2008-CA), Description (empty), URL (https://172.20.226.200/certsrv/mscep/mscep.dll), and Certificate Authority (WIN2008-MSCEP-RA). A blue callout bubble with the number '1' points to the URL field, containing the text: 'Configure the SCEP URL Pointing to the Microsoft Windows 2008 Server or other CA'. Below the ISE console, a separate window shows the 'Microsoft Active Directory Certificate Services' web interface. The 'Welcome' message reads: 'Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#). Select a task: [Request a certificate](#)'. A blue callout bubble with the number '2' points to the 'Request a certificate' link, containing the text: 'Request a Certificate for the ISE from the CA Server'. A blue arrow points from the 'Request a certificate' link to a 'Certificate Issued' box on the right. The 'Certificate Issued' box contains the text: 'The certificate you requested was issued to you.' and two radio buttons: 'DER encoded or Base 64 encoded'. Below the radio buttons are two links: 'Download certificate' and 'Download certificate chain'. A blue arrow points from the 'Request a certificate' link to the 'Download certificate' link. The bottom left corner of the slide contains the text 'BRKEWN-2020' and 'Public'. The bottom center contains the page number '79'. The bottom right corner features the 'Cisco live!' logo.

# Configuring Certificates on the ISE

- Certificates are Used for HTTPS and EAP Connections

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Operations, Policy, and Administration. Under Administration, there are tabs for System, Identity Management, Network Resources, and Web Portal Management. The Certificates tab is selected, showing sub-tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Admin Access, and Settings. The main content area is titled 'Local Certificates' and contains a table of certificates. A blue callout bubble with a '1' points to the table.

<input type="checkbox"/>	Friendly Name	Protocol	Issued To	Issued By
<input type="checkbox"/>	Default self-signed server certificate		ise.corpdemo.net	ise.corpdemo.net
<input type="checkbox"/>	ise.corpdemo.net#Go Daddy Secure Certification A...	HTTPS	ise.corpdemo.net	Go Daddy Secure Certif...
<input type="checkbox"/>	ise.corpdemo.net#corpdemo-AD-CA#00002	EAP	ise.corpdemo.net	corpdemo-AD-CA

1 The Web Server Certificate Can Be The Same, or Different than the EAP/RADIUS Certificate

2

Use the Certificate from Your CA Server for EAP Authentication

# Configuring the Web-Authentication Redirect ACL



For your reference

- The ACL is Used in HTTP Profiling as Well as Posture and Client Provisioning.

**1** This ACL will be referenced by name by the ISE to restrict the user.

**2** Use the ISE server's IP address to allow only traffic to that site.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<a href="#">1</a>	Permit	0.0.0.0 /	10.10.10.10 /	Any	Any	Any	Any	Inbound	0
<a href="#">2</a>	Permit	10.10.10.10 /	0.0.0.0 /	Any	Any	Any	Any	Outbound	0

# Defining the Supplicant Provisioning Authorisation Profile



**Authorization Profile**

\* Name: BYOD\_CP

Description: Client Provisioning

\* Access Type: ACCESS\_ACCEPT

**Common Tasks**

- DACL Name
- VLAN
- Voice Domain Permission
- Web Authentication: Supplicant Provisioning
- Auto Smart Port
- Filter-ID

ACL: ACL\_WEBAUTH\_REDIRECT

**Advanced Attributes Settings**

Select an item =

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = url-redirect-aci=ACL\_WEBAUTH\_REDIRECT  
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionId&action=nsip

**1** Configure Redirect ACL On WLC

Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
Permit	0.0.0.0 / 0.0.0.0	10.10.10.10 / 255.255.255.255	/ Any	Any	Any	Any	Inbound
Permit	10.10.10.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	/ Any	Any	Any	Any	Outbound

**2** Choose "Supplicant Provisioning" for the Redirect Portal



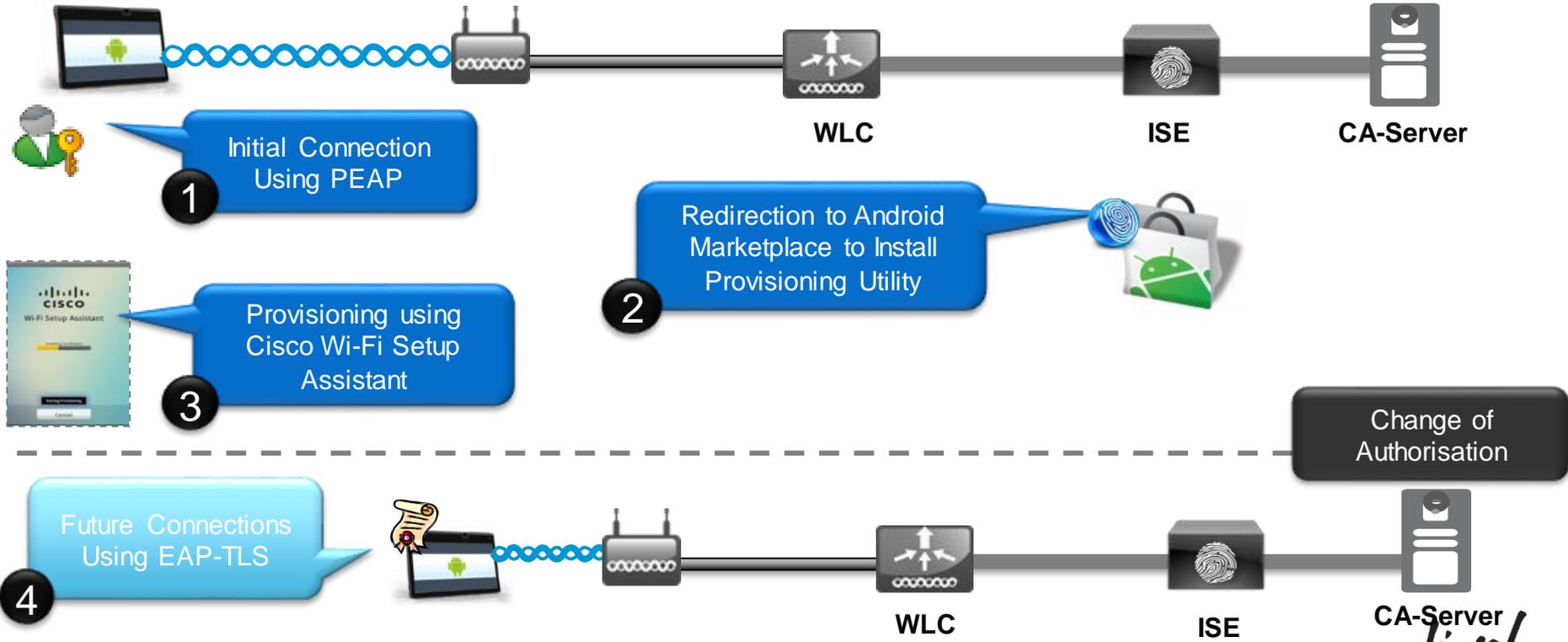
# Apple Captive Network Assistant (CNA)

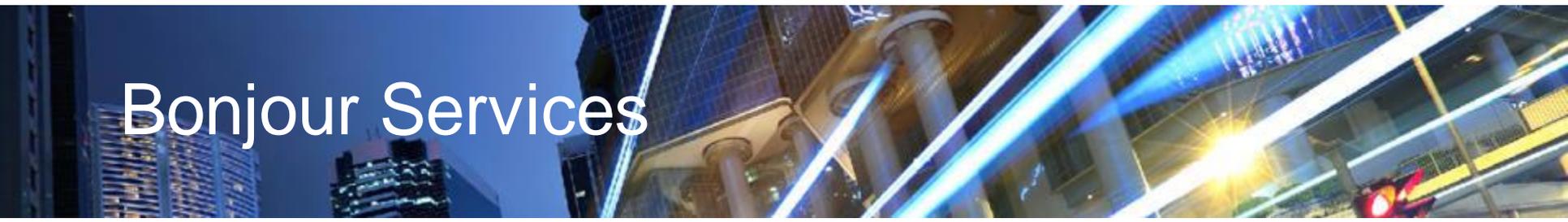


- Prior to iOS7, Apple iOS and current Mac OS X attempt to discover public Internet access using a crafted URL:
  - <http://www.apple.com/library/test/success.html>
- Captive Portal Bypass feature added in WLC 7.2
  - config network web-auth captive-bypass enable
- Starting in iOS7, multiple domains are tested to verify Internet access
- Solution:
  - ISE 1.2 Patch 2
  - WLC 7.4.121.0 or 7.6.100.0

# Android Device Provisioning

For your reference





# Bonjour Services

Cisco *live!*

# Steps for Bonjour Configuration

## Bonjour Profile

- Steps to configure mDNS profile
- Steps to Apply the mDNS profile per interface.

## Location specific Bonjour Service

- Steps to enable location specific services on controller

## Remote VLAN Bonjour Service

- Steps to discover Bonjour service on remote VLAN by enabling mDNS AP

# Bonjour Gateway Services Filter



**Controller**

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Redundancy
- Internal DHCP Server
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- IPv6
- mDNS
  - General
  - Profiles
  - Domain Names
- Advanced

**mDNS**

## Enable mDNS Globally / Add Services

**Global Configuration**

mDNS Global Snooping

Query Interval (10-120)

**Master Services Database**

Select Service

Query Status

Service Name	Service String	
<a href="#">AFP</a>	__afpovertcp._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">AirPrint-PDL</a>	__pdl-datastream._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">AirPrint-Spool</a>	__printer._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">AirPrint-ipp</a>	__ipp._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">AirTunes</a>	__raop._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">Airplay-Mac</a>	__appletv-v2._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">Airplay-iOS</a>	__airplay._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">AppleRemoteDesktop</a>	__net-assistant._udp.local.	<input checked="" type="checkbox"/>
<a href="#">AppleTV-Remote</a>	__touch-able._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">HTTP</a>	__http._tcp.local.	<input checked="" type="checkbox"/>
<a href="#">Scanner</a>	__scanner._tcp.local.	<input checked="" type="checkbox"/>



**Controller**

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Redundancy
- Internal DHCP Server
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- IPv6
- mDNS
  - General
  - Profiles
  - Domain Names
- Advanced

## mDNS Profile > Edit

Profile Name	Corporate-Employees
Profile Id	3
Service Count	12
No. of Interfaces Attached	1
No. of Interface Groups Attached	0
No. of Wlans Attached	1

**mDNS Profile for Employee**

## Services List

Service Name

Service Name	
AFP	<input checked="" type="checkbox"/>
AirPrint-PDL	<input checked="" type="checkbox"/>
AirPrint-Spool	<input checked="" type="checkbox"/>
AirPrint-ipp	<input checked="" type="checkbox"/>
AirTunes	<input checked="" type="checkbox"/>
Airplay-Mac	<input checked="" type="checkbox"/>
Airplay-iOS	<input checked="" type="checkbox"/>

**Max. of 64 services can be enabled**



# Applying the Bonjour Gateway Profile



## WLAN

WLANs > Edit 'AppTest-Cisco'

General Security QoS Policy-Mapping Advanced

### mDNS

mDNS Snooping  Enabled

mDNS Profile Corporate-Employees ▼

## VLAN

Interfaces > Edit

### General Information

Interface Name contractor

### mDNS

mDNS Profile Contractors ▼

Controlling Bonjour Gateway Profile per Interface

# Bonjour: Steps Configuring LSS service from CLI



1. Once the basic Bonjour gateway setup is configured the LSS can be enabled by accessing the WLC CLI, LSS is disabled by default on the WLC

```
(Cisco Controller) >show mdns service summary
Number of Services..... 7

Service-Name          LSS   Origin   No SP   Service-string
-----
AirPrint              No    All      1      _ipp._tcp.local.
AirTunes              No    All      2      _raop._tcp.local.
AppleTV               No    All      2      _airplay._tcp.local.
HP_Photosmart_Printer_1 No    All      0      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2 No    All      1      _cups._sub._ipp._tcp.local.
Printer               No    All      0      _printer._tcp.local.
Scanner               No    All      0      _scanner._tcp.local.
```

2. Configure LSS services from CLI:

**(WLC) >config mdns service lss <enable / disable> <service\_name/all>**

```
(Cisco Controller) >config mdns service lss enable all

(Cisco Controller) >show mdns service summary
Number of Services..... 7

Service-Name          LSS   Origin   No SP   Service-string
-----
AirPrint              Yes    All      1      _ipp._tcp.local.
AirTunes              Yes    All      2      _raop._tcp.local.
AppleTV               Yes    All      2      _airplay._tcp.local.
HP_Photosmart_Printer_1 Yes    All      0      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2 Yes    All      1      _cups._sub._ipp._tcp.local.
Printer               Yes    All      0      _printer._tcp.local.
Scanner               Yes    All      0      _scanner._tcp.local.
```



## 1. Configure switch port for mDNS-AP in trunk mode or Access Mode

```
interface GigabitEthernet1/0/17
switchport trunk encapsulation dot1q
switchport trunk native vlan 70
switchport trunk allowed vlan 70,71
switchport mode trunk
```

## 2. Configure mDNS-AP **Trunk Mode** or **Access Mode**:

**(WLC)> config mdns ap enable/disable <APName/all> vlan <vlan-id>**

**(WLC) >config mdns ap vlan add/delete <vlanid> <AP Name>**

**(WLC)> config mdns ap enable/disable <APName/all> - no VLAN Config in Access Mode**

```
(Cisco Controller) >config mdns ap enable AP6073.5caa.030b vlan 71
```

Requested state is already set on the AP.

```
(Cisco Controller) >show mdns ap summary
```

Number of mDNS APs..... 1

AP Name	Ethernet MAC	Number of Vlans	VlanIden
AP6073.5caa.030b	60:73:5c:aa:03:0b	1	70

```
(Cisco Controller) >config mdns ap vlan add 71 AP6073.5caa.030b
```

```
(Cisco Controller) >show mdns ap summary
```

Number of mDNS APs..... 1

AP Name	Ethernet MAC	Number of Vlans	VlanIdentifiers
AP6073.5caa.030b	60:73:5c:aa:03:0b	2	70,71

# Bonjour Policy Configuration



## 1. Enable mDNS policy on the controller from GUI or CLI

```
(Cisco Controller) >config mdns policy ?
disable      Enable / Disable mDNS access policy.
enable       Enable / Disable mDNS access policy.
service-group Configures mDNS service-group.

(Cisco Controller) >config mdns policy enable
```

**Controller**

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Redundancy
- Internal DHCP Server
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- IPv6
- mDNS**
  - General
  - Profiles
  - Domain Names
  - mDNS Browser
  - mDNS Policies

**mDNS**

**Global Configuration**

- mDNS Global Snooping
- mDNS Policy
- Query Interval (10-120)  (mins)

**Master Services Database**

Select Service:

Query Status

LSS Status

Origin:

Service Name	Service String	Query Status	LSS Status	Origin
<a href="#">AirTunes</a>	_raop._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Airplay</a>	_airplay._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">HP_Photosmart_Printer_1</a>	_universal._sub._ipp._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL

# Bonjour Policy Configuration

## 2. Create mDNS Service Group

```
(Cisco Controller) >config mdns policy service-group create ?
```

```
<service-group-name> Enter a mDNS service-group name.
```

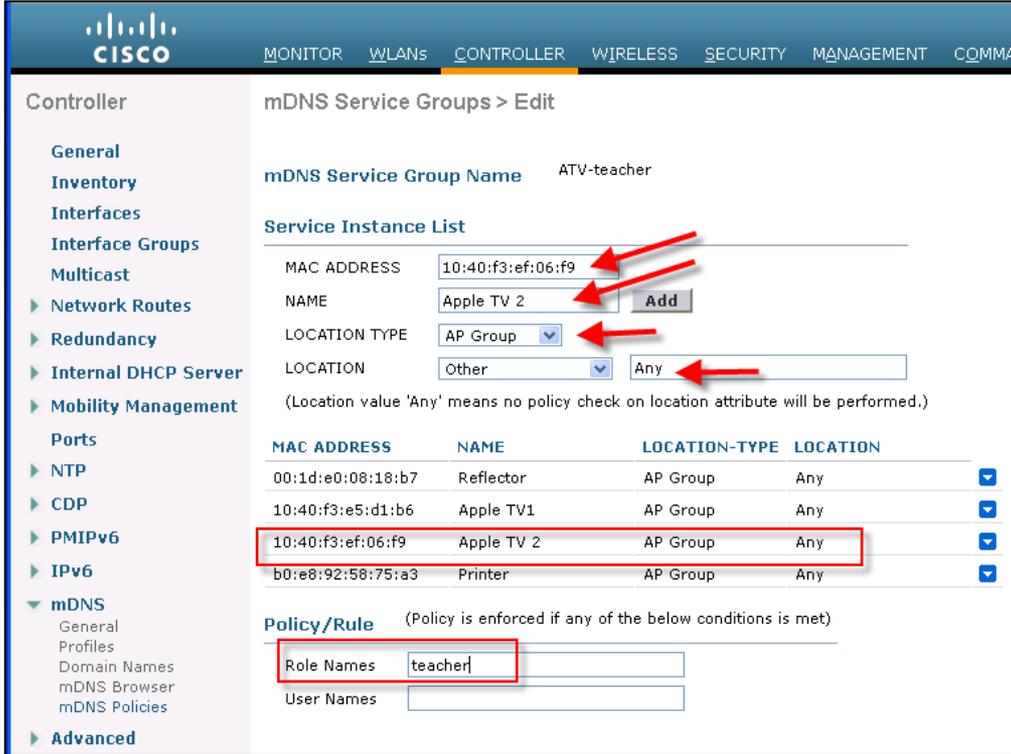
```
(Cisco Controller) >config mdns policy service-group create
```

The screenshot shows the Cisco Controller GUI with the 'CONTROLLER' tab selected. The left sidebar lists various configuration categories, with 'mDNS' expanded to show 'mDNS Policies'. The main content area displays 'mDNS Service Groups' with a table of existing groups. A red arrow points from the 'ATV-teacher' link in the table to the 'Enter a mDNS service-group name' prompt in the terminal window on the left.

mDNS Service Group Name	Description	Origin
<a href="#">ATV-student1</a>	Apple services for Student1	WLC
<a href="#">ATV-teacher</a>	Apple TV services for teachers	WLC
<a href="#">Guest Service</a>	Services for Guests	WLC
<a href="#">default-mdns-policy</a>	Default Access Policy created by WLC	WLC

# Bonjour Policy Configuration

## 3. Configure Service Instances in the mDNS group, and role



**Controller** | mDNS Service Groups > Edit

mDNS Service Group Name: ATV-teacher

**Service Instance List**

MAC ADDRESS	NAME	LOCATION TYPE	LOCATION
00:1d:e0:08:18:b7	Reflector	AP Group	Any
10:40:f3:e5:d1:b6	Apple TV1	AP Group	Any
10:40:f3:ef:06:f9	Apple TV 2	AP Group	Any
b0:e8:92:58:75:a3	Printer	AP Group	Any

**Policy/Rule** (Policy is enforced if any of the below conditions is met)

Role Names: teacher

LOCATION TYPE: AP Group

LOCATION: AP Group

(Location value 'Any' means no policy check)

LOCATION-TYPE	LOCATION
AP Group	Any
AP Group	Any
AP Location	same
AP Name	AP3700_TME_lab

LOCATION: Other

(Location value 'Any' means no policy check)

MAC ADDRESS: 00:1d:e0:08:18:b7



**CISCO**