
TOMORROW
starts here.
CISCO
Cisco live!

Managing Policies for a BYOD Network

BRKEWN-2020

Scott Lee-Guard

Systems Engineer, Enterprise Networks

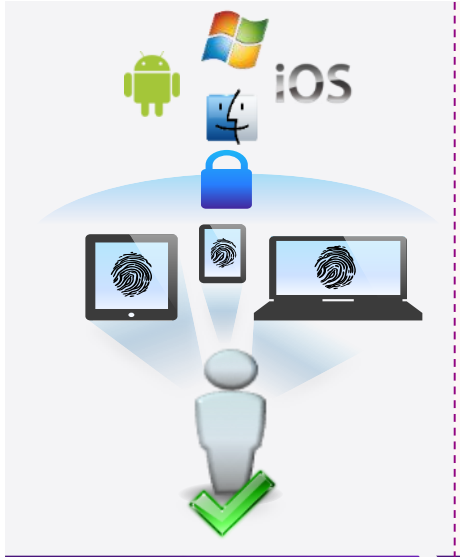
#clmel

Cisco live!

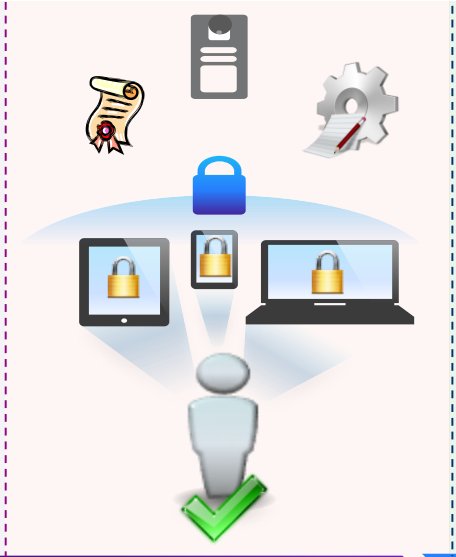
Agenda

Managing the BYOD Evolution

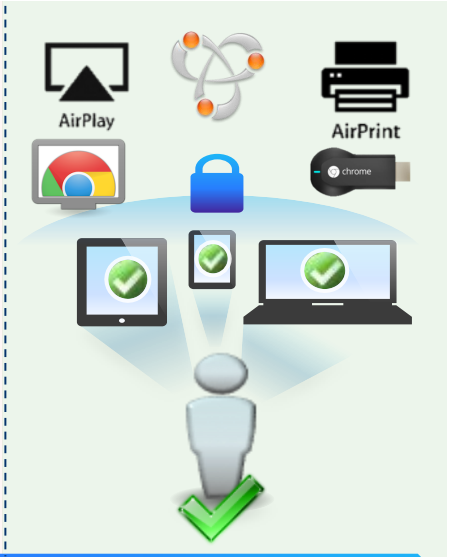
Personal Devices on Network



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 WLAN Controller

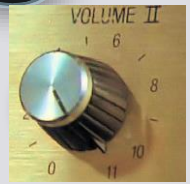
Controller only BYOD

ISE (Identity Services Engine)

Controller + ISE-Wireless BYOD

Cisco Catalyst Switch

ASA Firewall



Controller + ISE-Advanced BYOD

Wireless Only

Basic Profiling and Policy on WLC

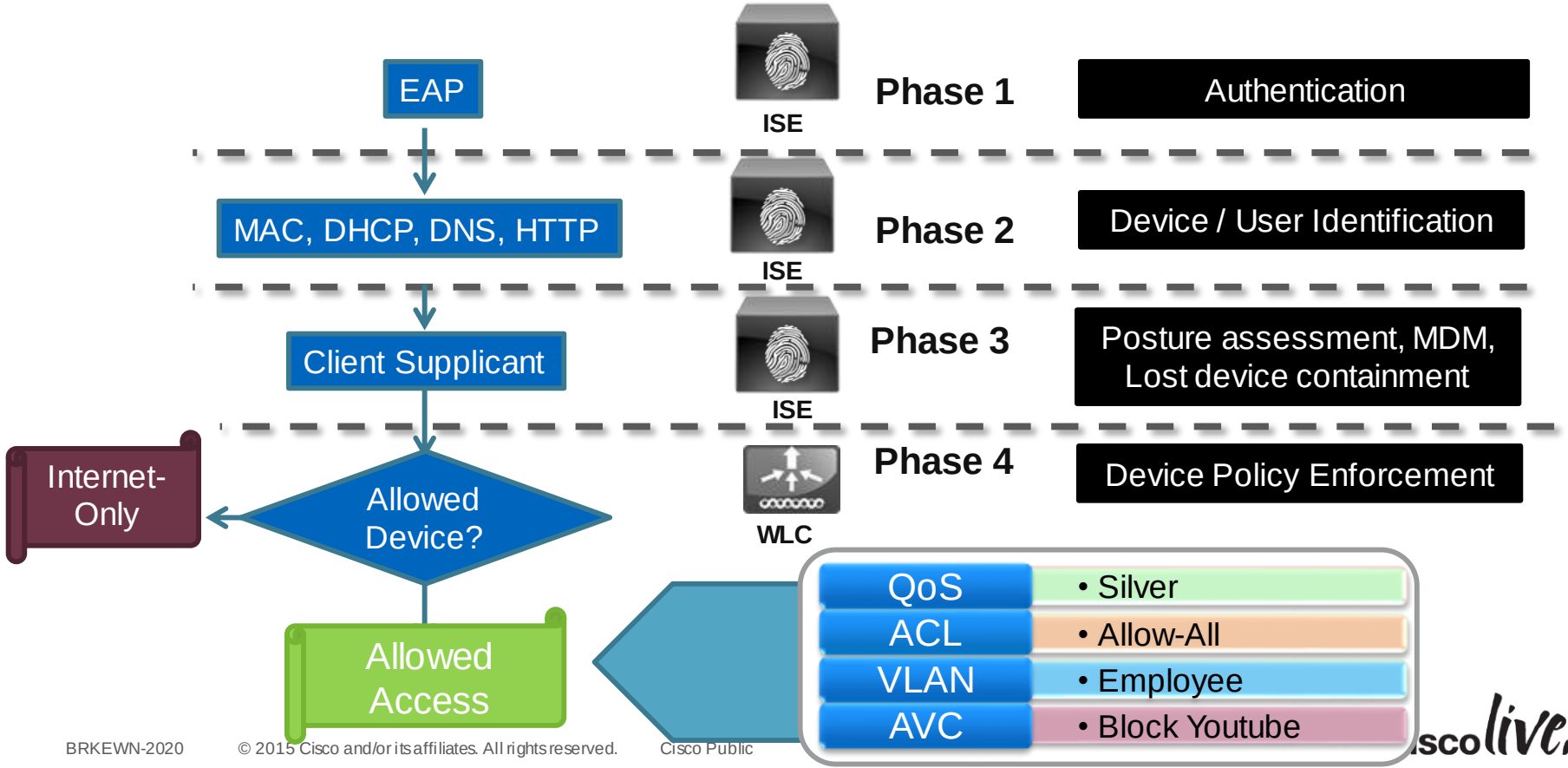
Wireless Only

AAA+ Advanced Profiling + Device Posture + Client On-board + Guest + MDM

Wired + Wireless + Remote Access

AAA + Advanced Profiling + Device Posture + Client On-board + Guest + MDM

Cisco BYOD Policy Steps

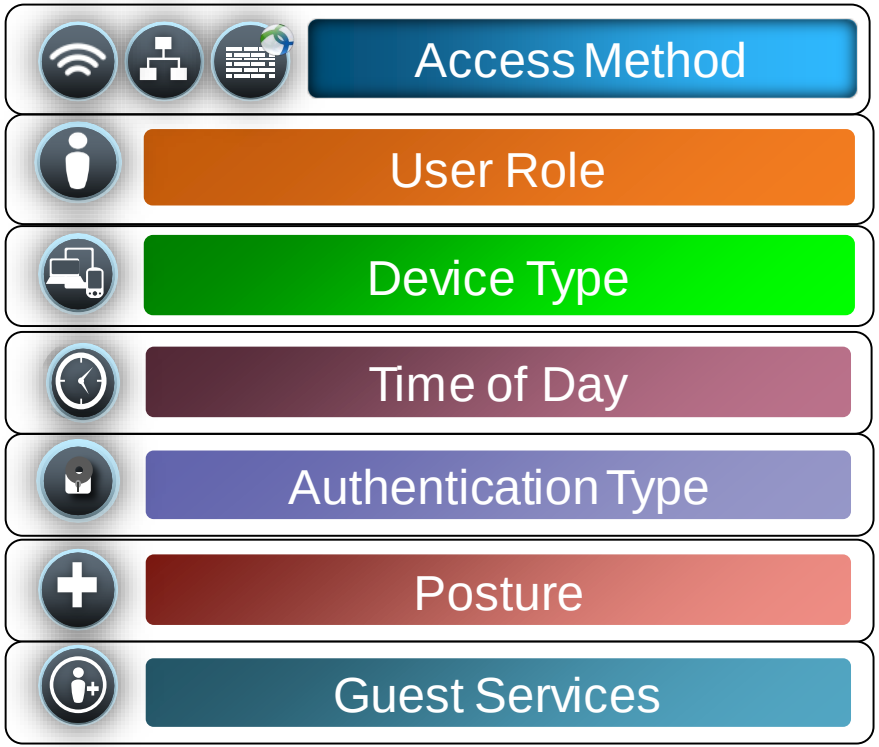


BYOD Policy Building Blocks: Tools of the Trade

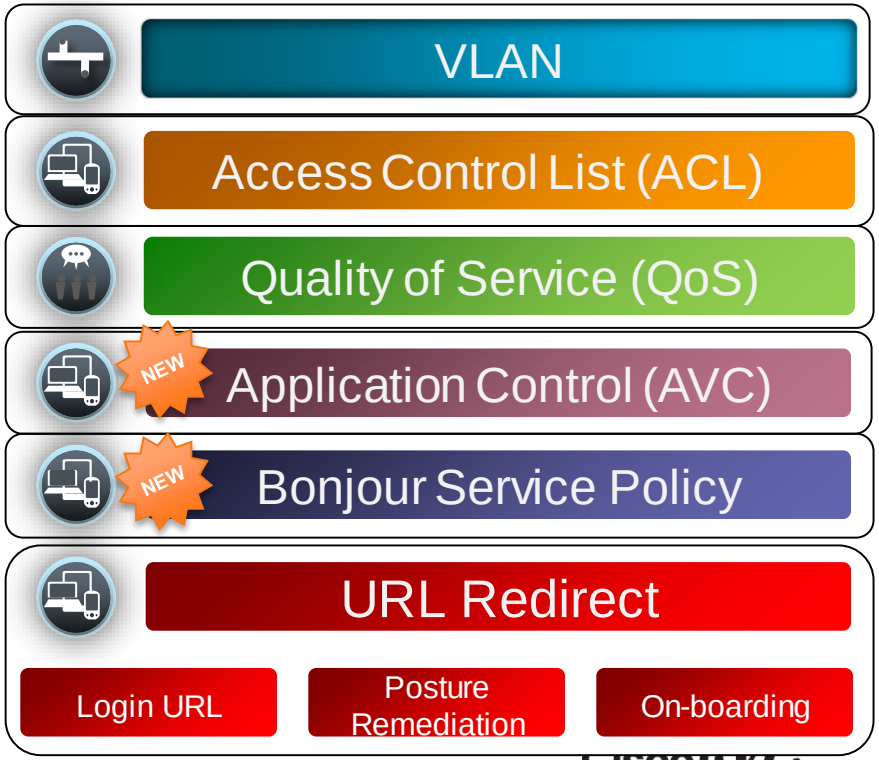
Cisco live!

Building BYOD Policy: Flexible Options

Inputs: Factors

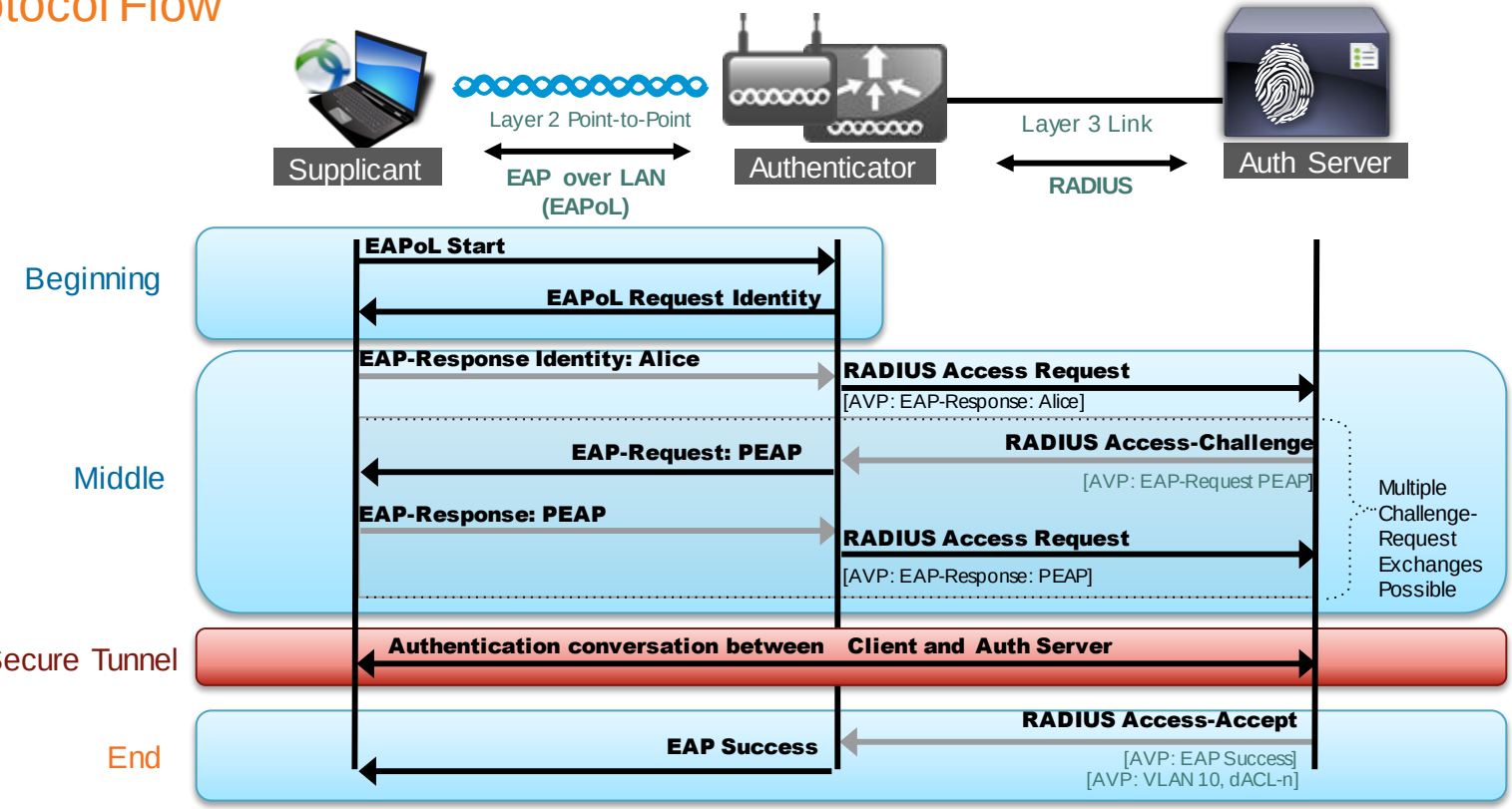


Results: Enforcement Elements



Extensible Authentication Protocol (EAP)

Protocol Flow

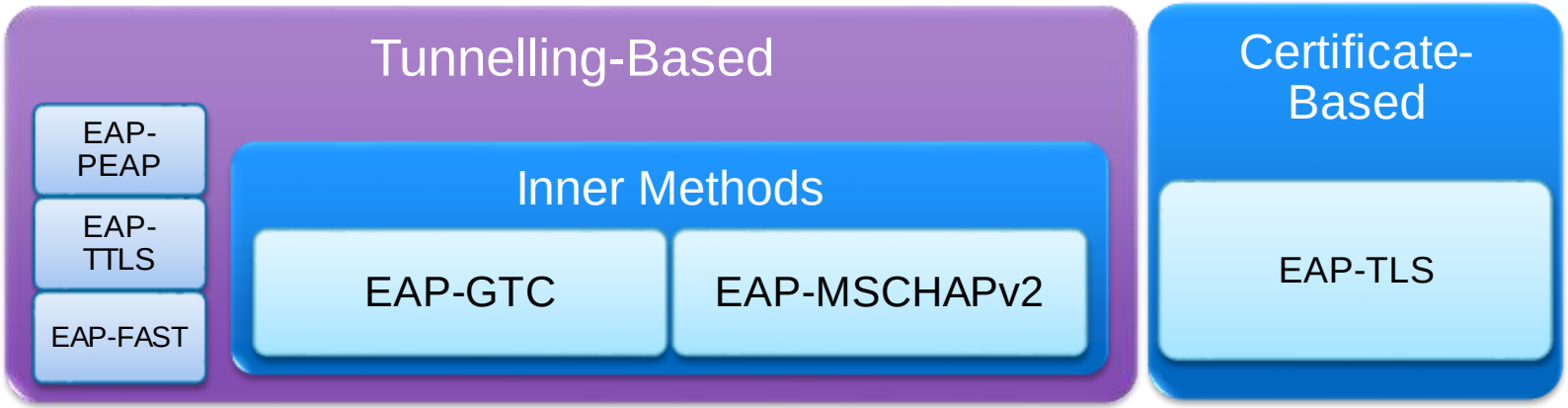


Why EAP Types?

- 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

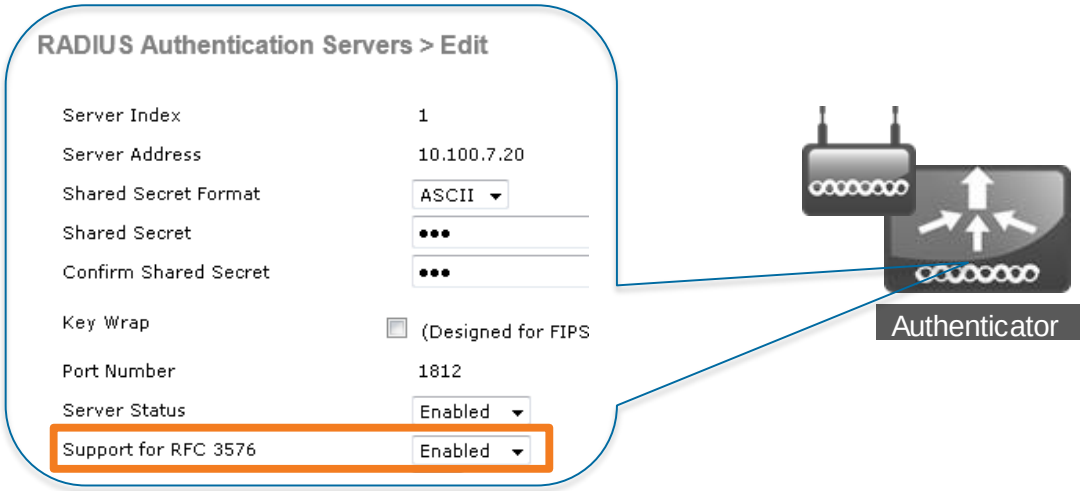


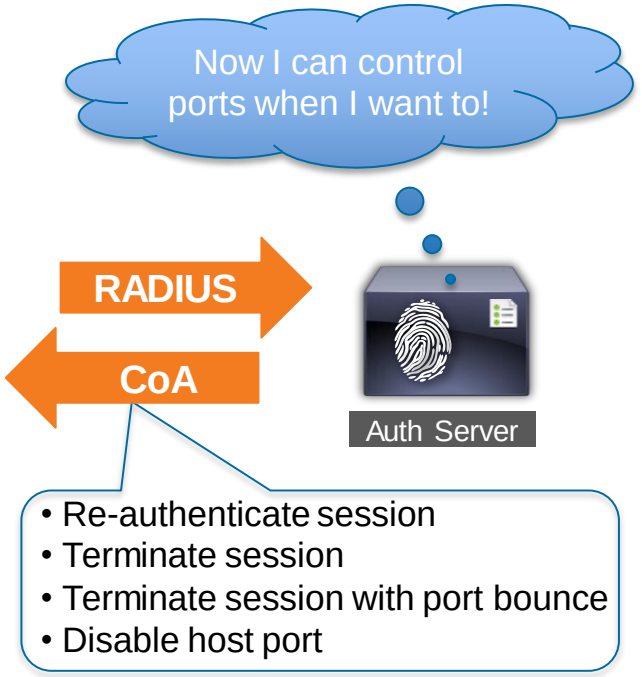
- Tunnel-based - Common deployments use a tunnelling protocol combined with an inner EAP type.
  - Provides security for the inner EAP type which may be vulnerable by itself.
- Certificate-based – Mutual authentication of both the server and client.

The RADIUS Protocol

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

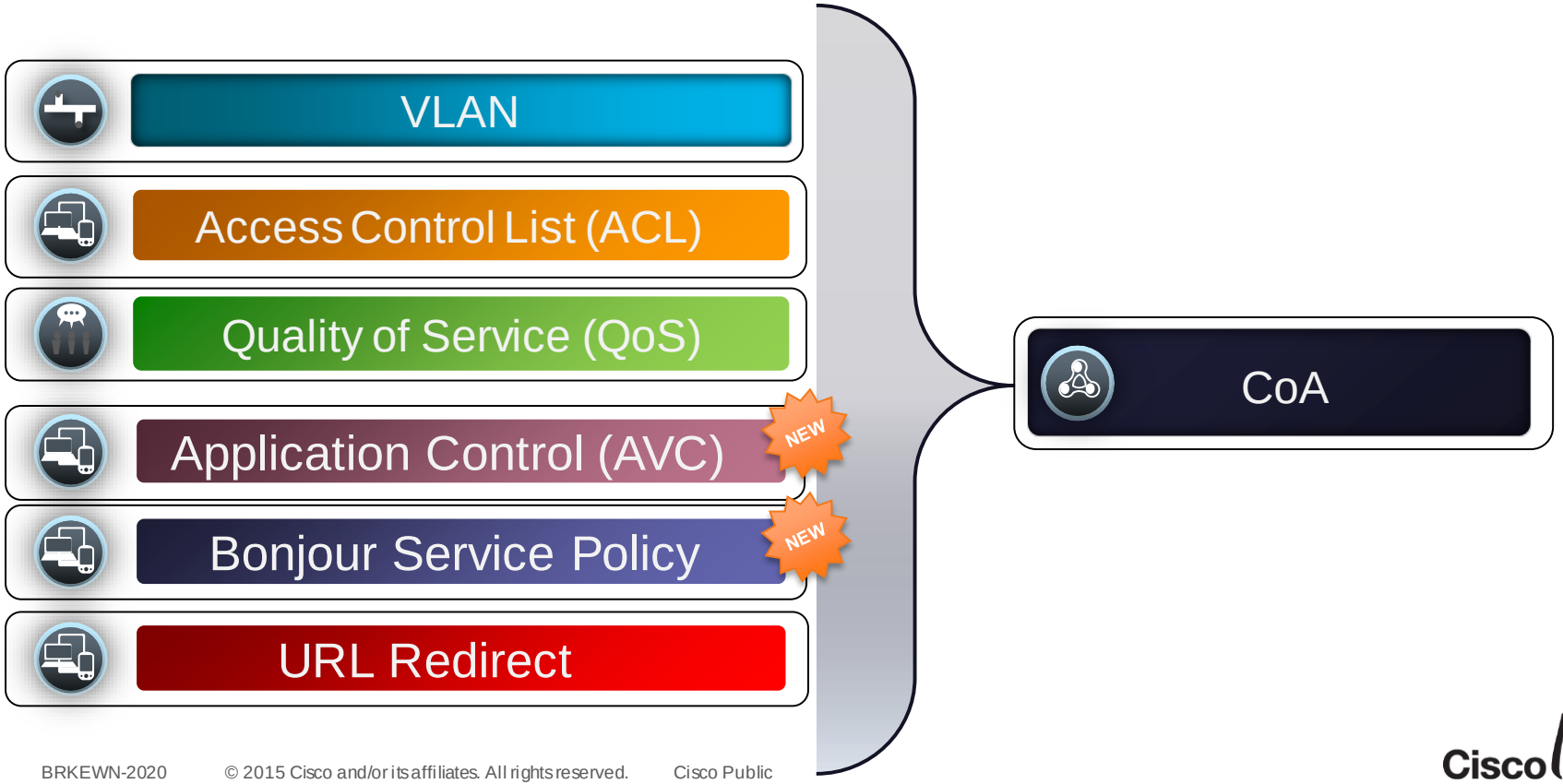
- RADIUS protocol is initiated by the network devices
- No way to change authorisation from the ISE





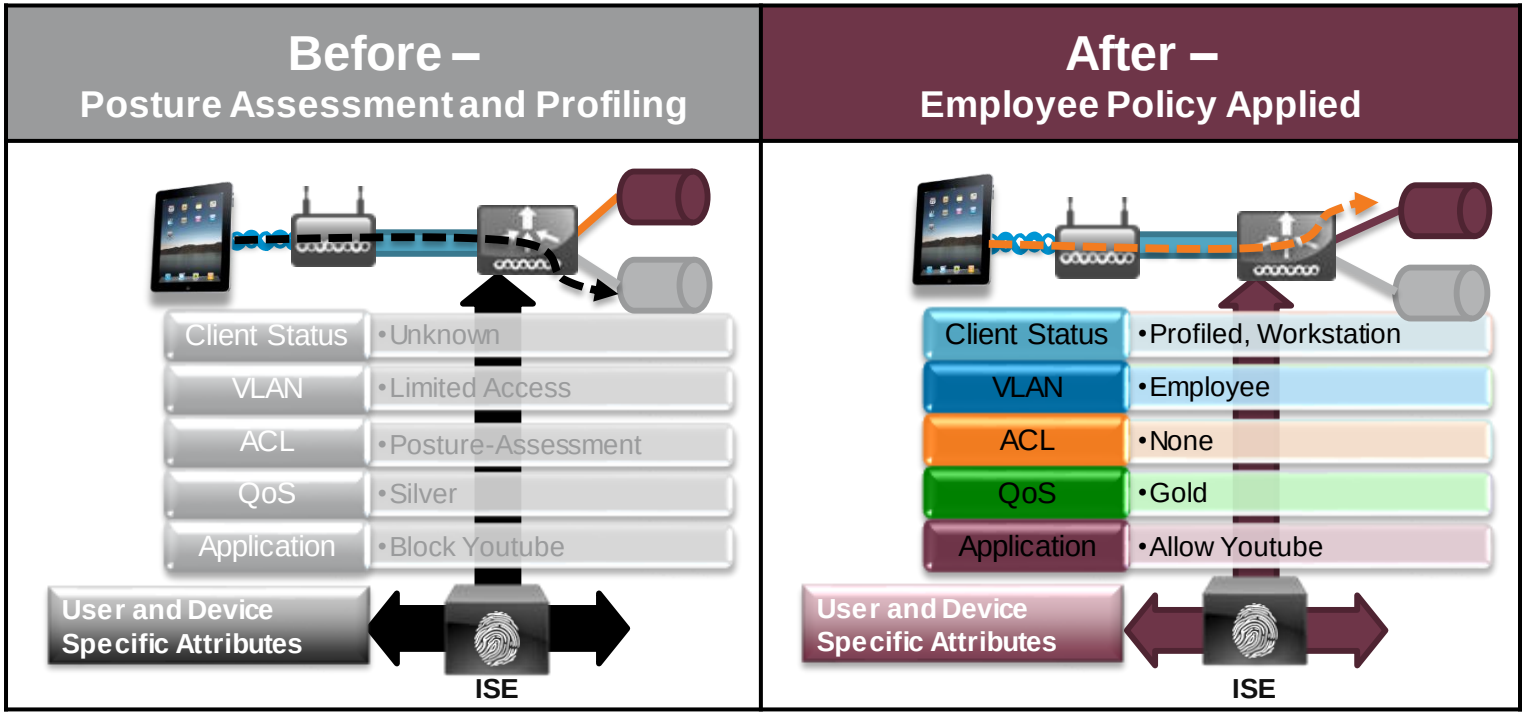
- Now network devices listens to CoA request from ISE

Per-User Policy Override with CoA



Change of Authorisation (CoA)

Changing Connection Policy Attributes Dynamically



Agenda

Managing the BYOD Evolution

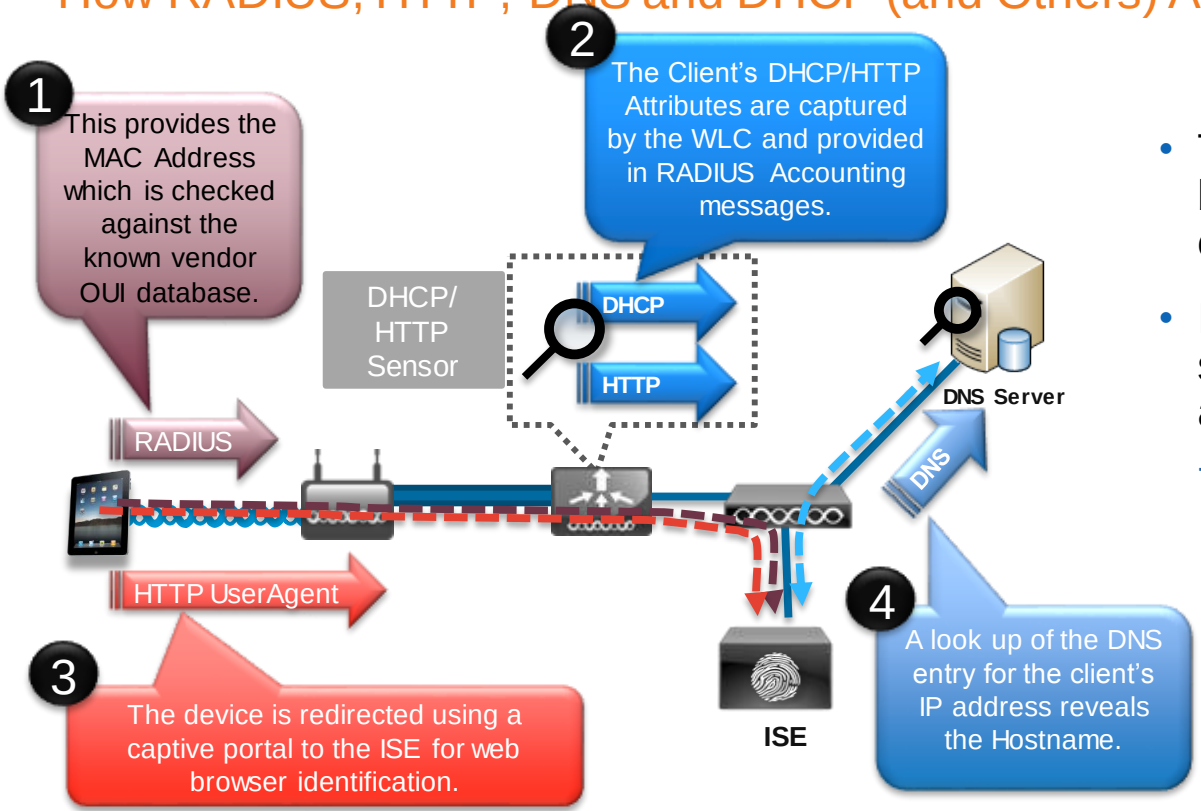
Personal Devices on Network

Identification and Security Policy Enforcement


Profiling with ISE
Cisco live!

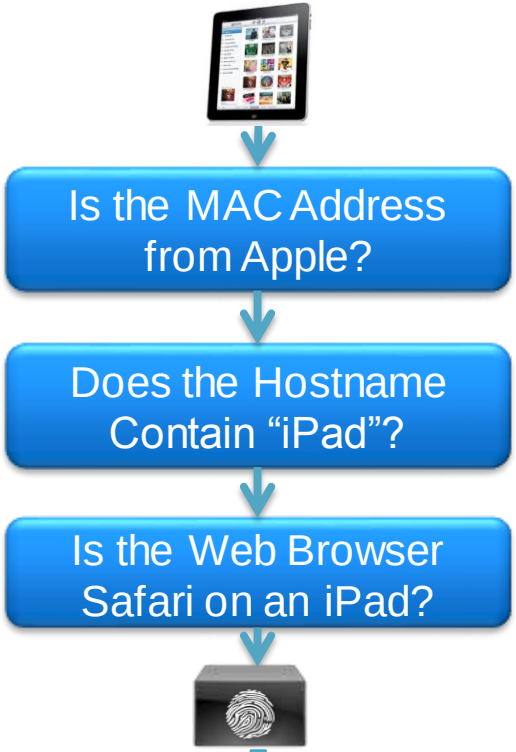
Client Attributes Used for ISE Profiling

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

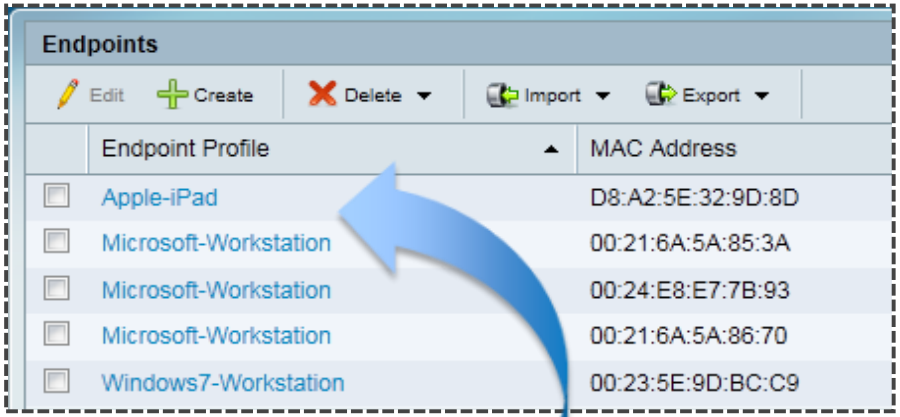


- The ISE uses multiple attributes to build a complete picture of the end client's device profile.
- Information is collected from sensors which capture different attributes
  - The ISE can even kick off an NMAP scan of the host IP to determine more details.

ISE Device Profiling Example - iPad



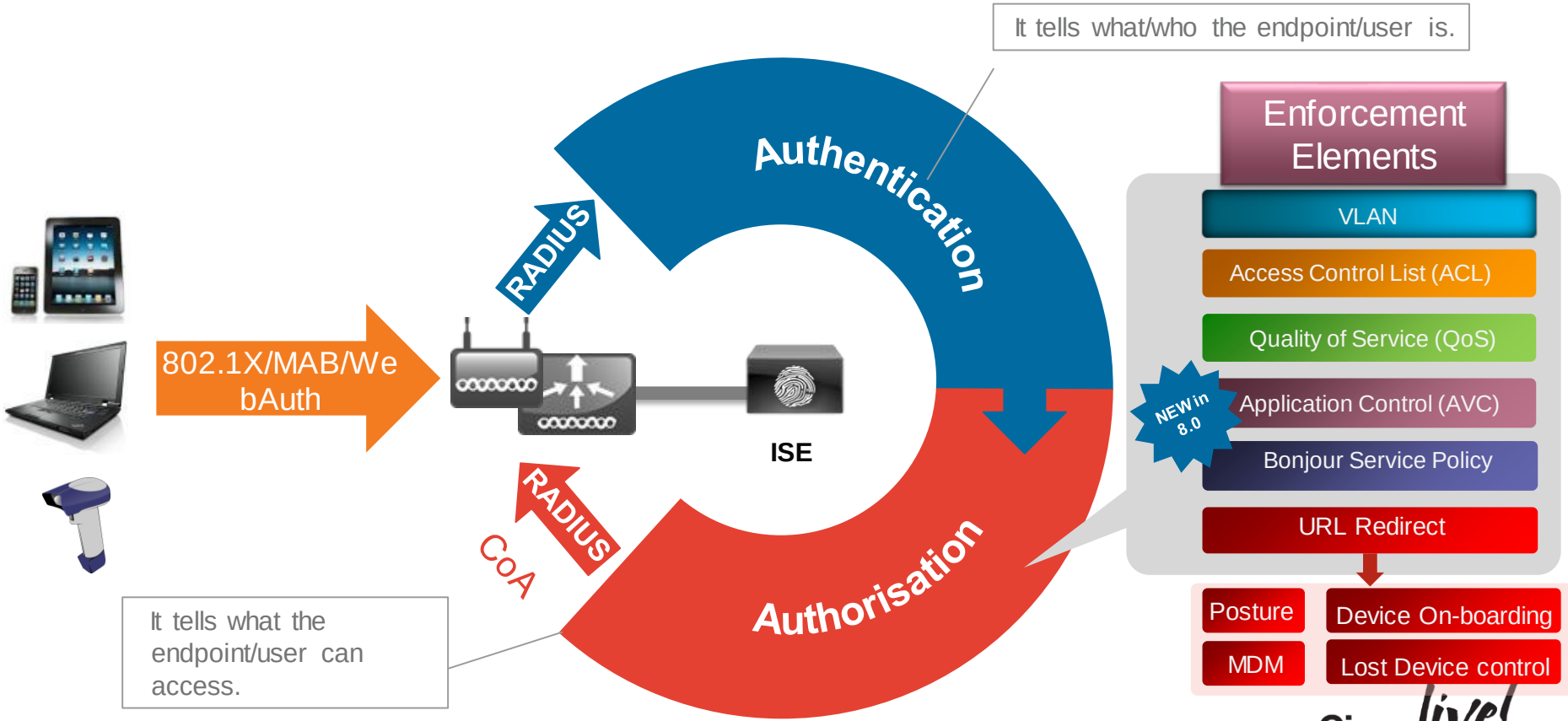
- Once the device is profiled, it is stored within the ISE for future associations:



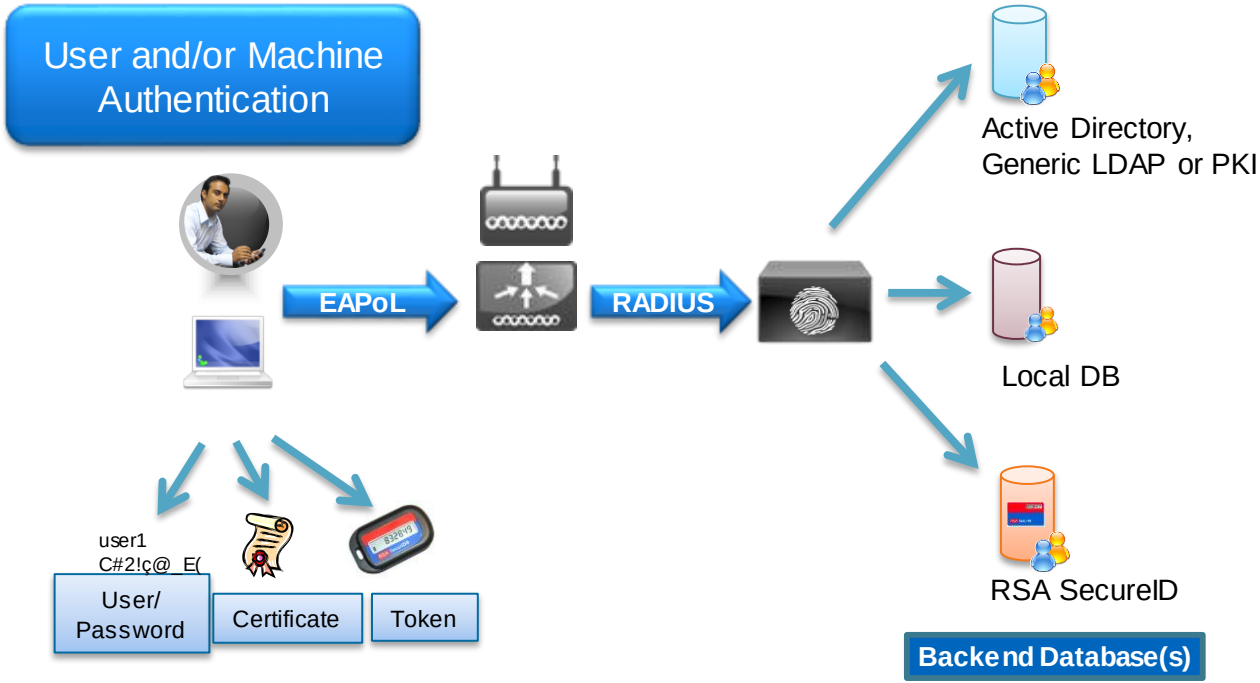
Defining a Security Policy Within ISE

Cisco live!

Authentication and Authorisation

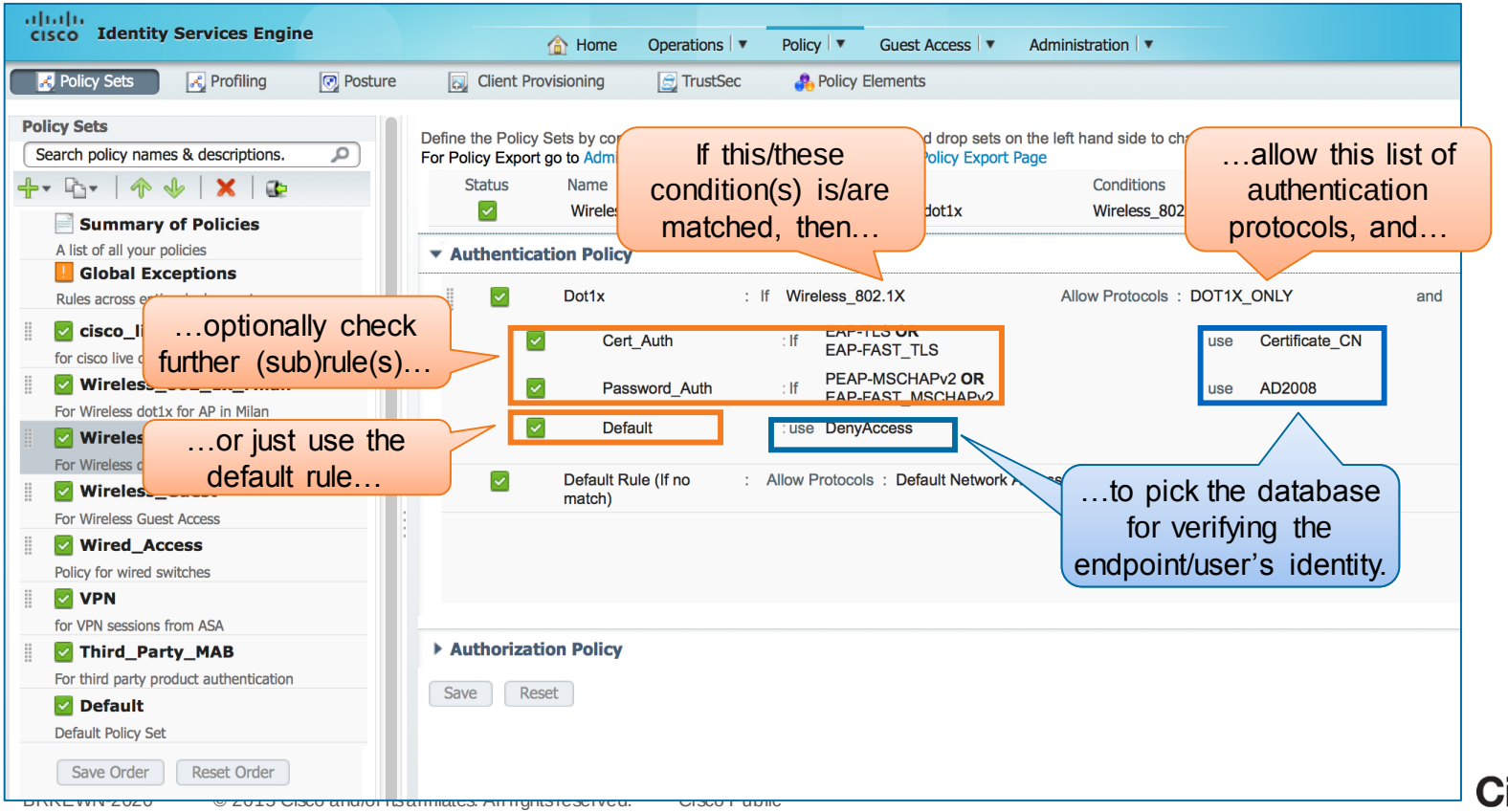


ISE Authentication Sources

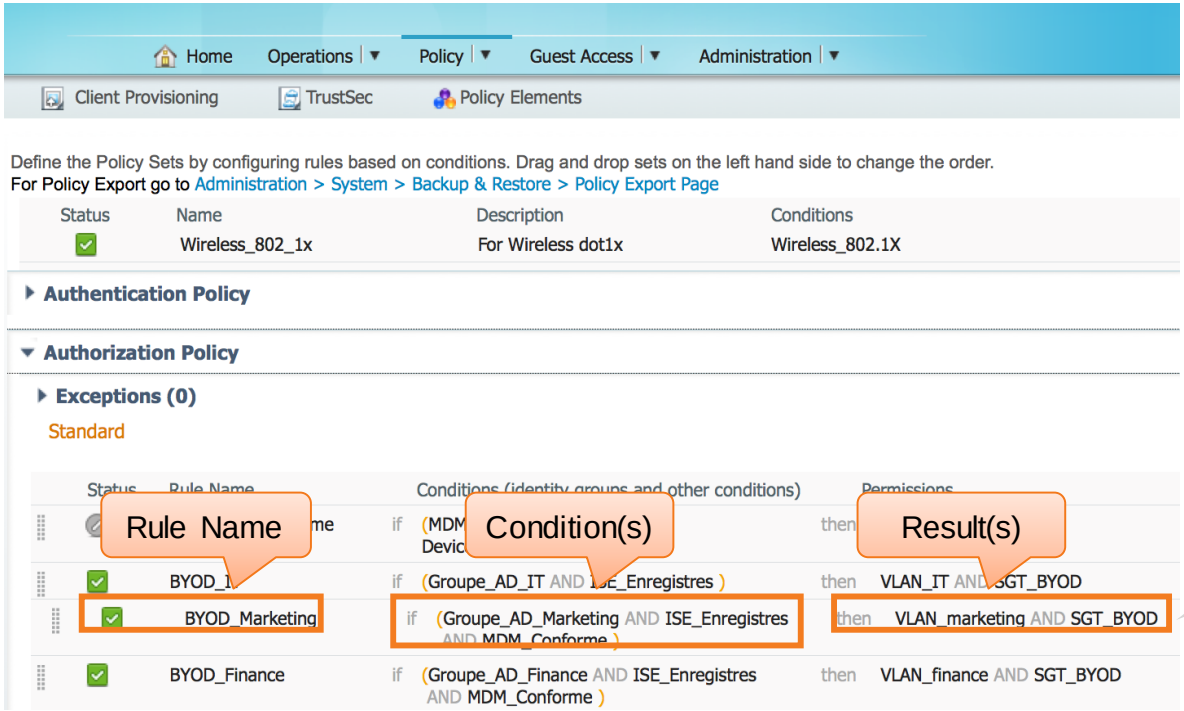


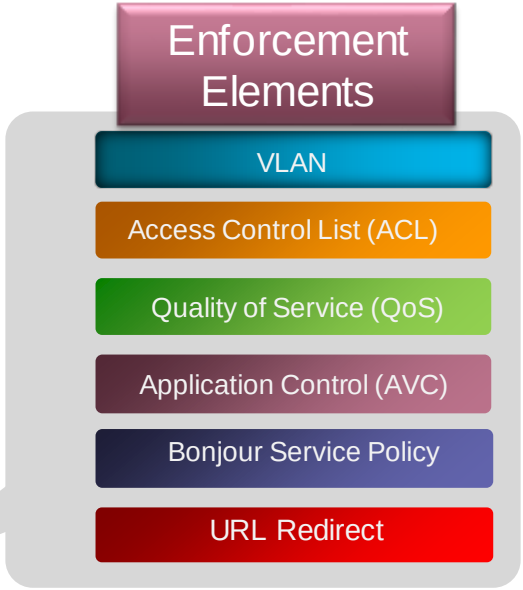
- Cisco ISE can reference variety of backend identity stores including Active Directory, PKI, LDAP and RSA SecureID.
- The local database can also be used on the ISE itself for small deployments.

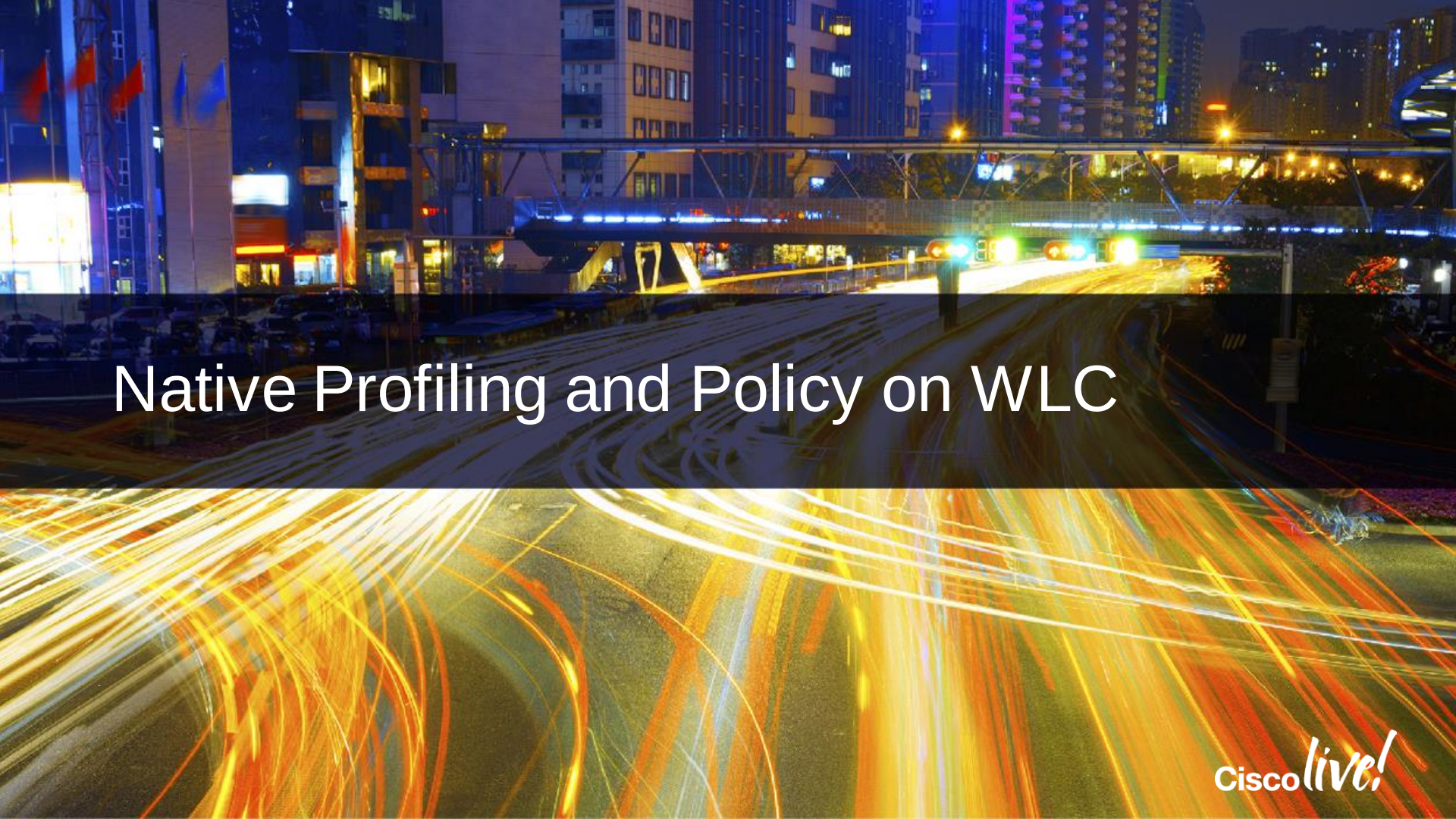
Authentication Rules



Authorisation Rules and Results





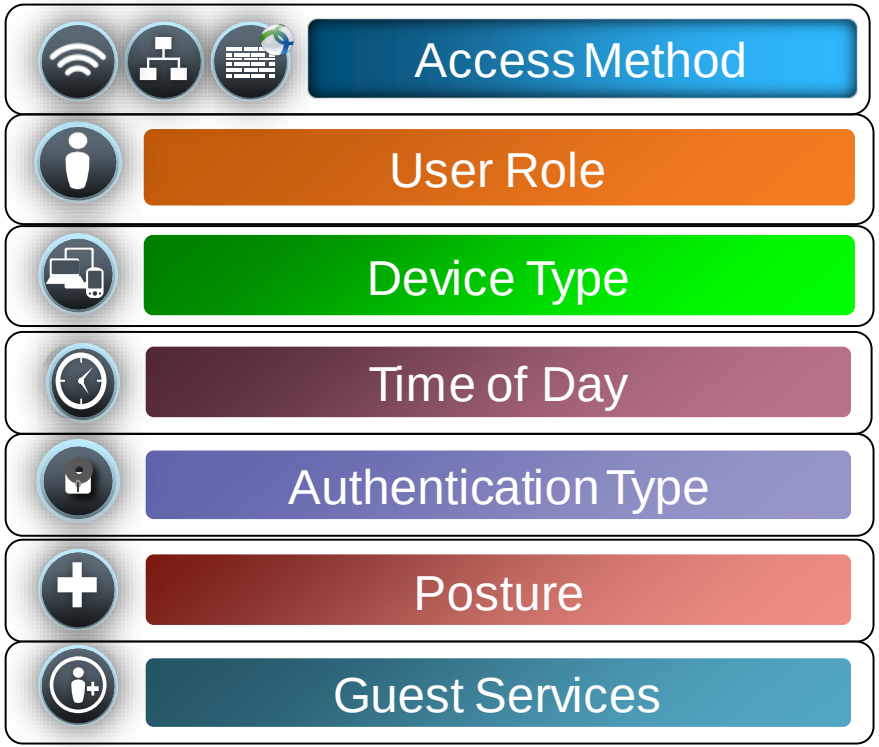


Native Profiling and Policy on WLC

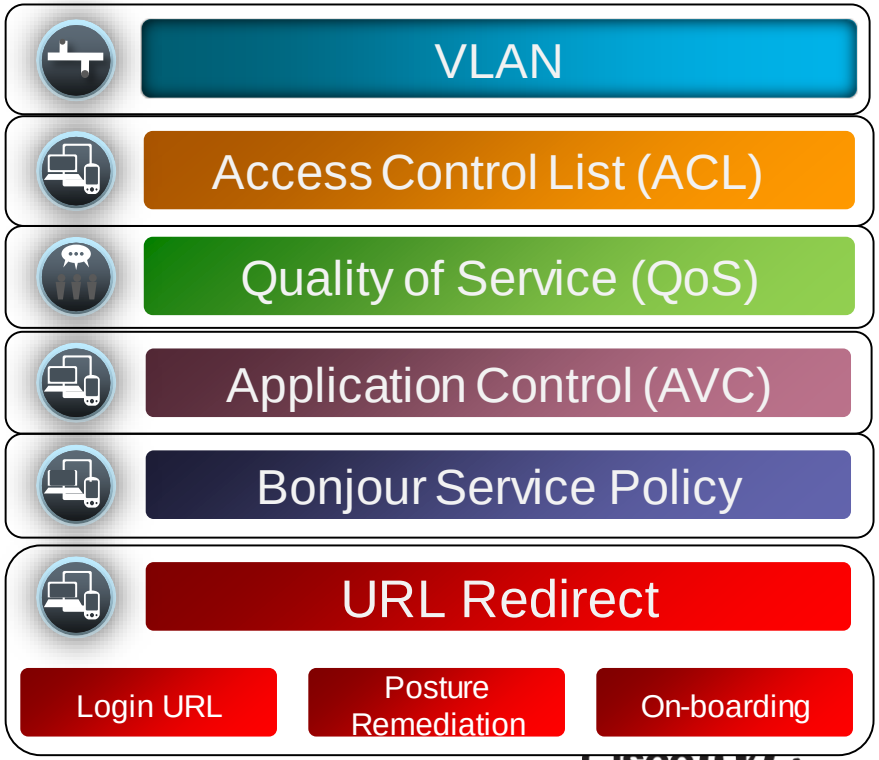
Cisco live!

Building BYOD Policy: Flexible Options

Inputs: Factors

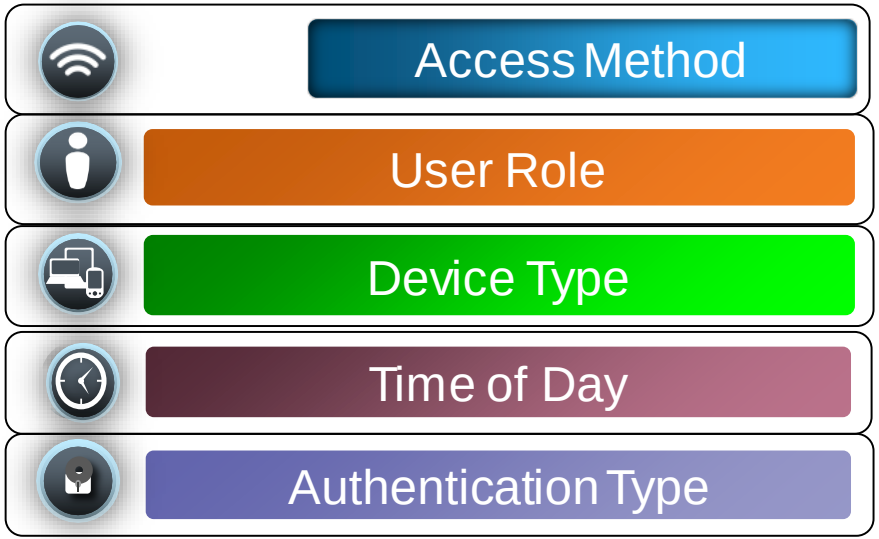


Results: Enforcement Elements

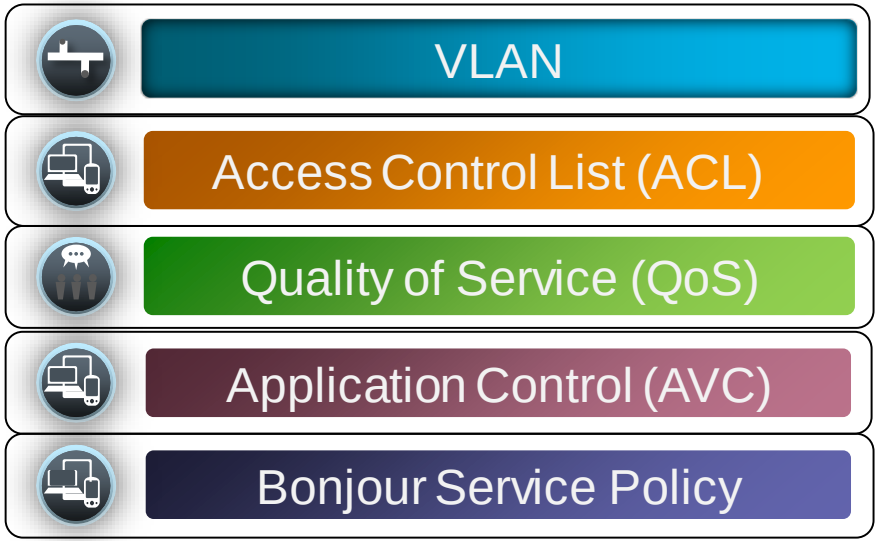


Building BYOD Policy: Native WLC Options

Inputs: Factors



Results: Enforcement Elements



Native Device Profiling on WLC

Device Type

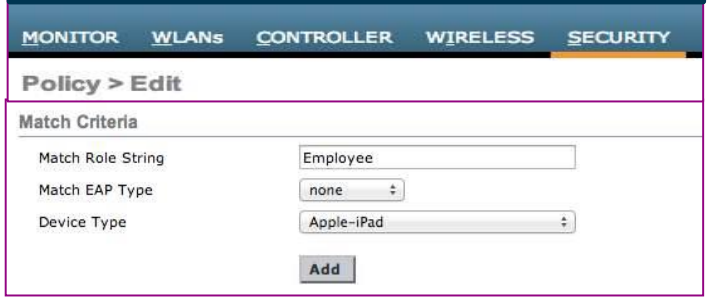
Step 1

Cisco WLC configuration

Enable DHCP and HTTP Profiling on the WLC

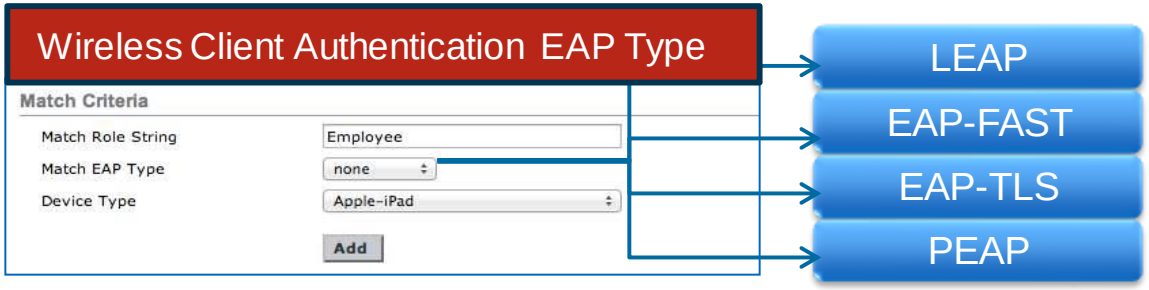
Step 2

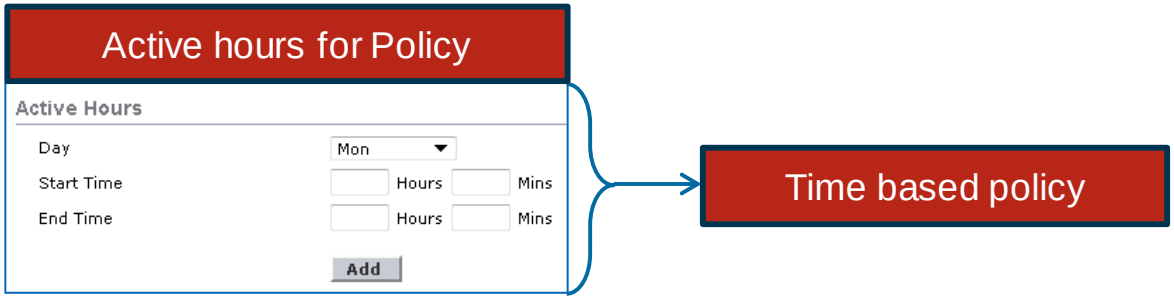
Create Device Profiling Policy



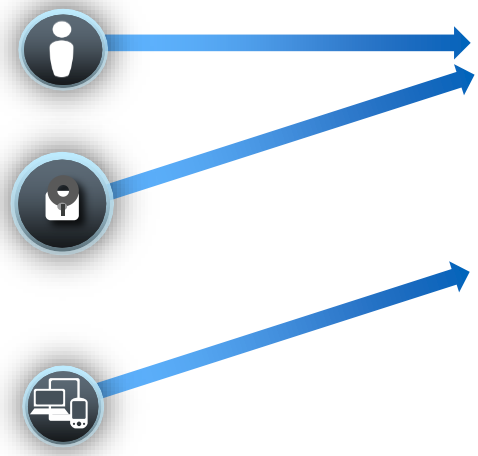
156 Pre-Defined Device Signatures

Native Authentication and Time Policy





Native WLC Policy in Action



Match Criteria

Match Role String	Employee
Match EAP Type	EAP-TLS

Device List

Device Type	Android (Add)
	Apple-iPad
	Microsoft-Surface-Tablet

Action

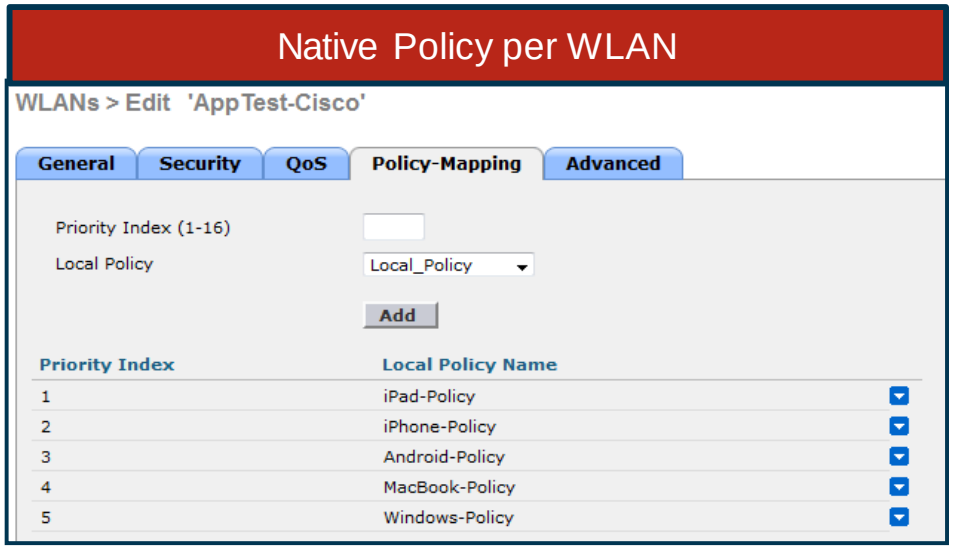
IPv4 ACL	lab-only
VLAN ID	17
Qos Policy	Silver (best effort)
Average Data Rate	0
Average Real time Data Rate	0
Burst Data Rate	0
Burst Real time Data Rate	0
Session Timeout (seconds)	1800
Sleeping Client Timeout (min)	720
Flexconnect ACL	none
AVC Profile	Microsoft Lync
mDNS Profile	AppleTV

Enforcement Elements

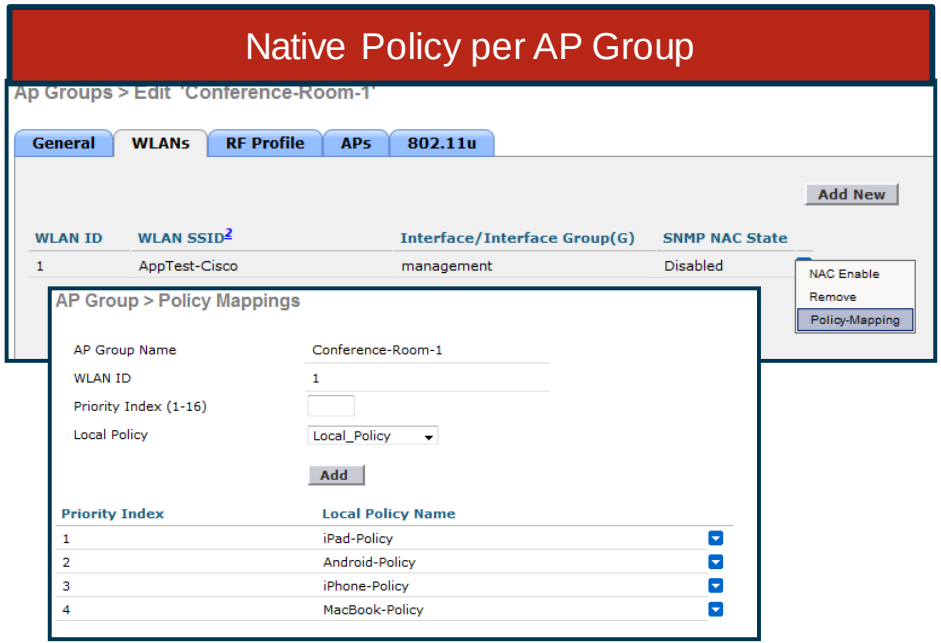
- VLAN
- Access Control List (ACL)
- Quality of Service (QoS)
- Application Control (AVC)
- Bonjour Service Policy

Apply Native Policy per WLAN / AP Group

Native Policy per WLAN



Native Policy per AP Group



Restriction: First Matched Rule Applies

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

Required Network Components and Versions

For your reference

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						

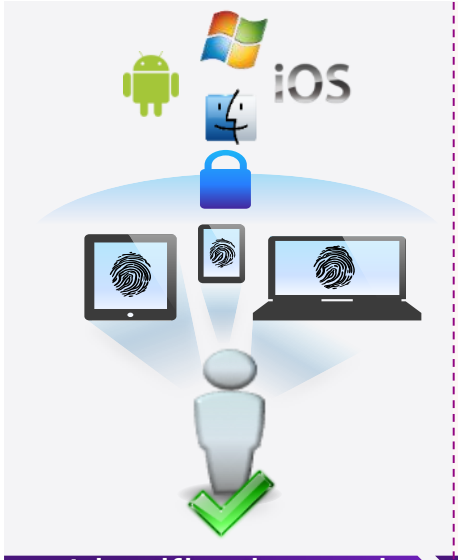
*FlexConnect mode: No WLC BYOD support for Local Auth on AP

Cisco live!

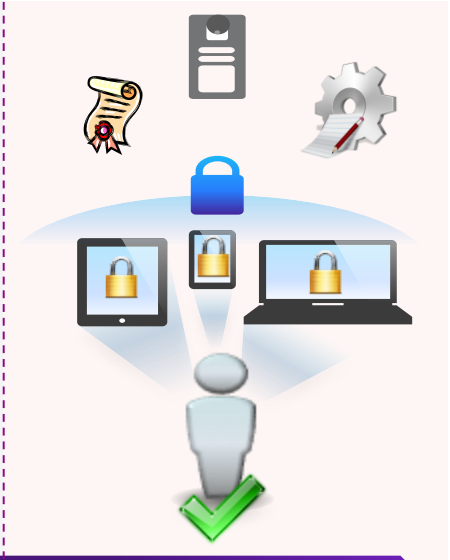
Agenda

Managing the BYOD Evolution

Personal Devices on Network



Identification and Security Policy Enforcement



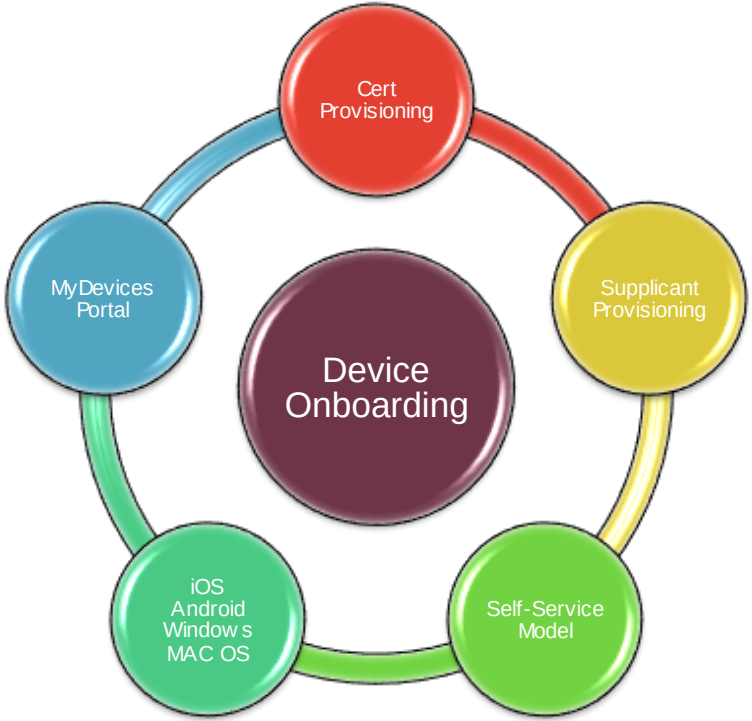
Securely On-Board the Device

BYOD Device Provisioning

Cisco live!

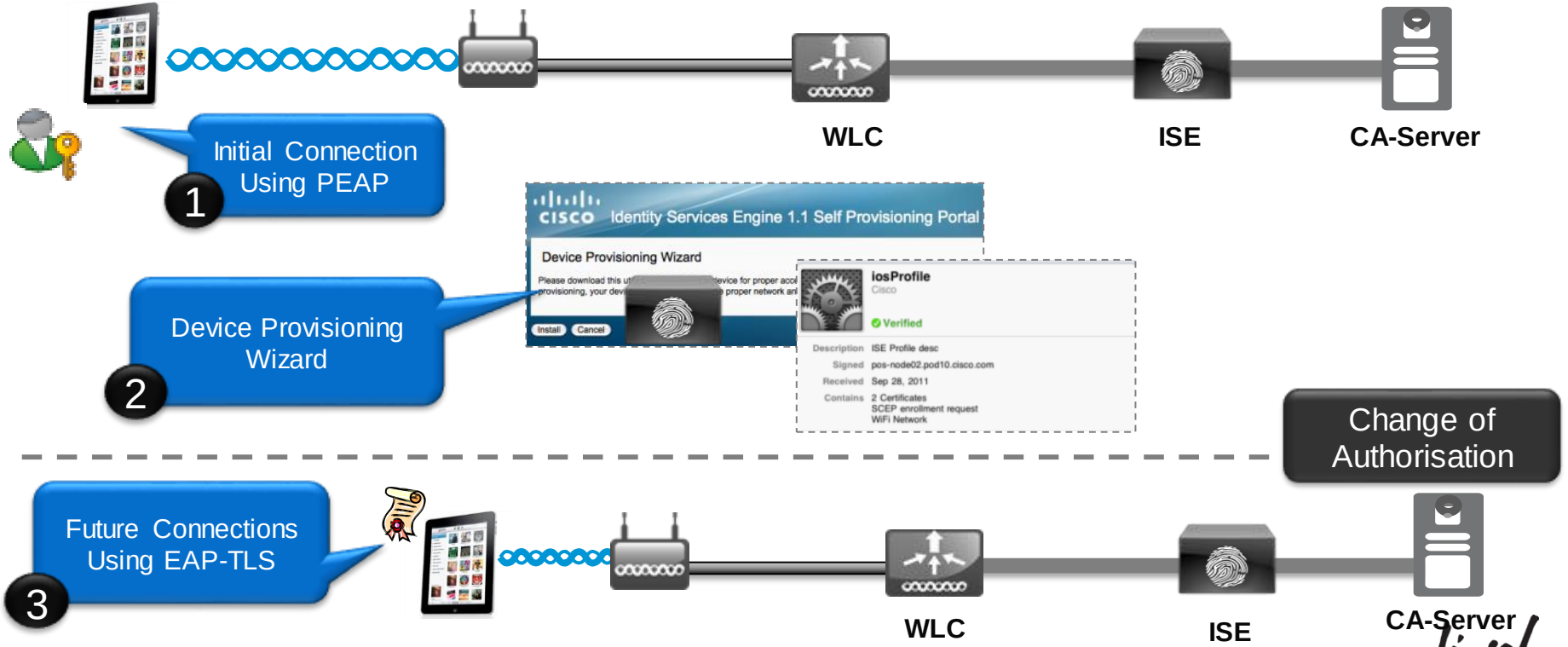
Simplified On-boarding for BYOD

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

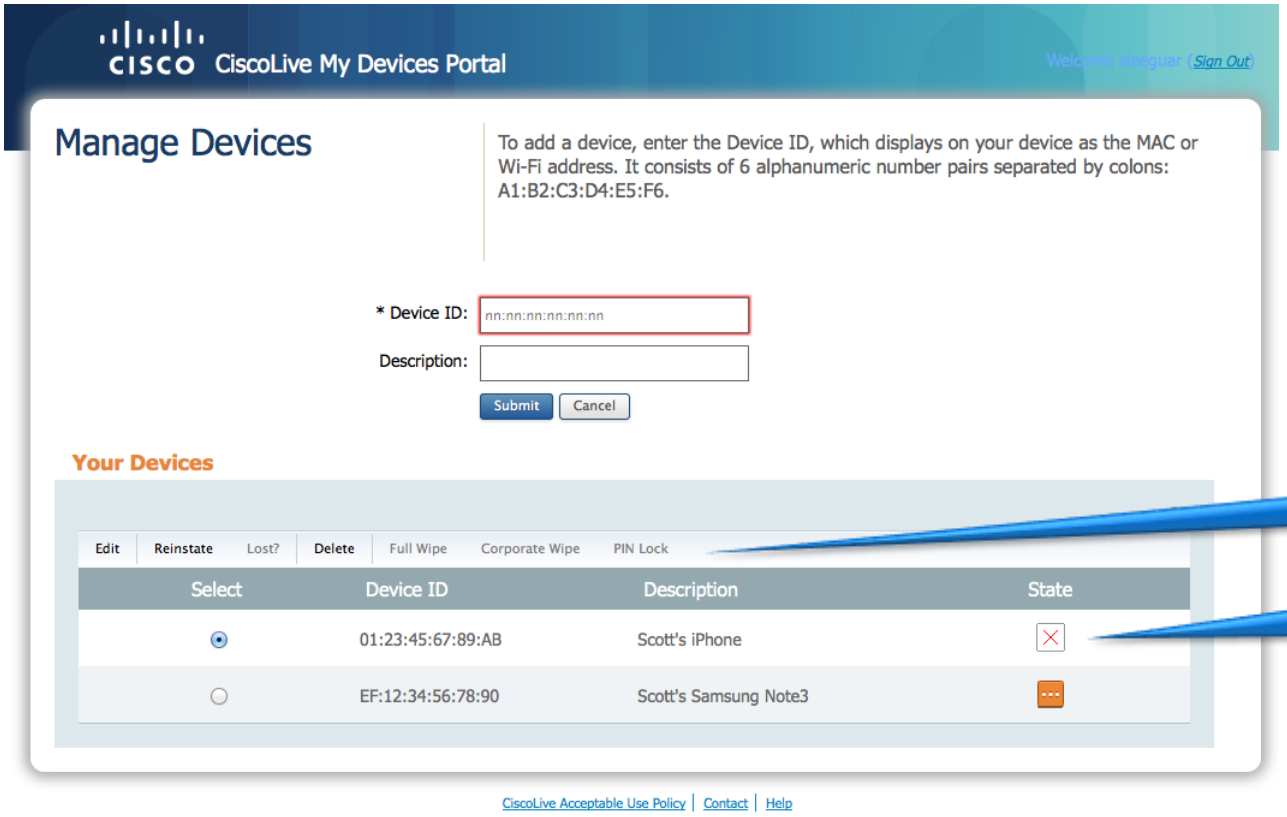


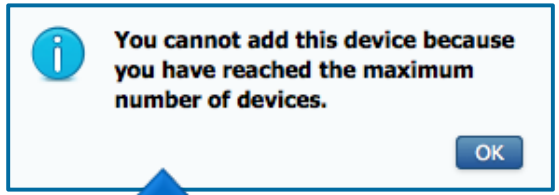
DNS-based ACLs

- 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





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

2 User can Self-Manage Lost/Found/Wipe etc

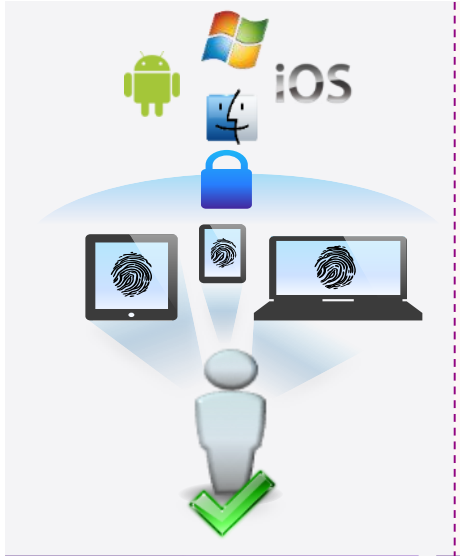
1 New Devices Can be Added with a Description

Cisco live!

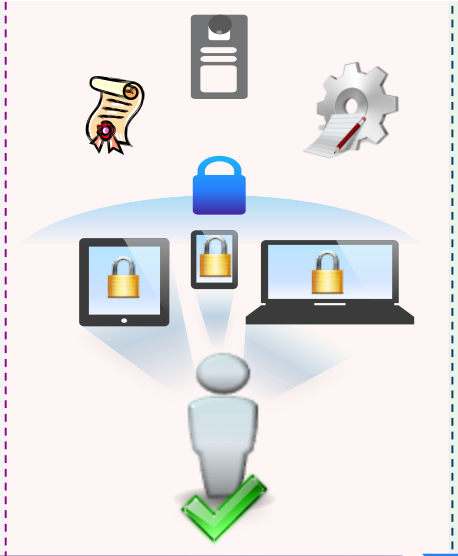
Agenda

Managing the BYOD Evolution

Personal Devices on Network



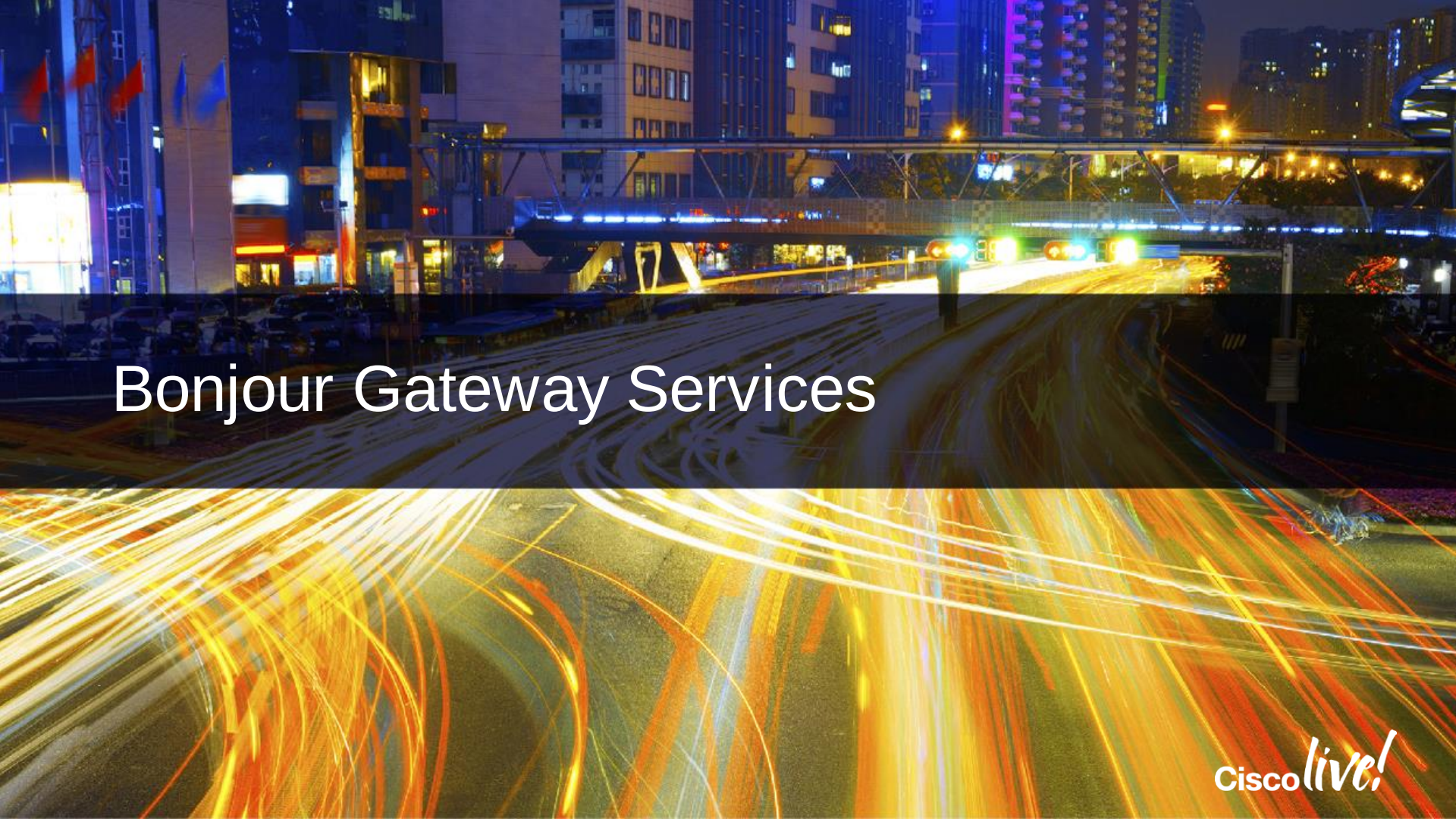
Identification and Security Policy Enforcement



Securely On-Board the Device

Simplified Bonjour Operations

Cisco live!

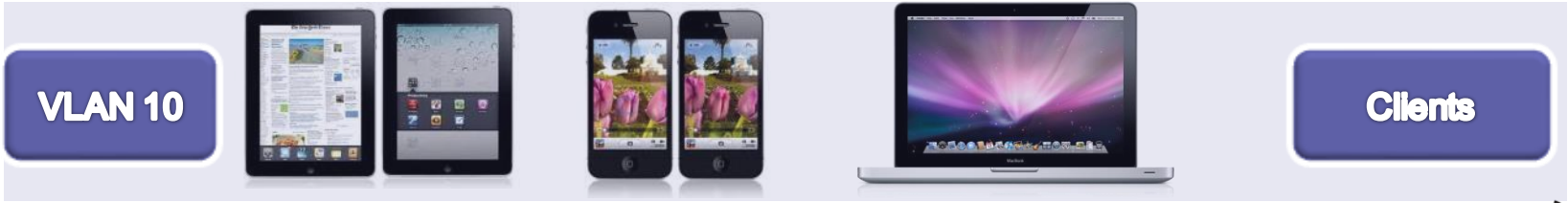


Bonjour Gateway Services

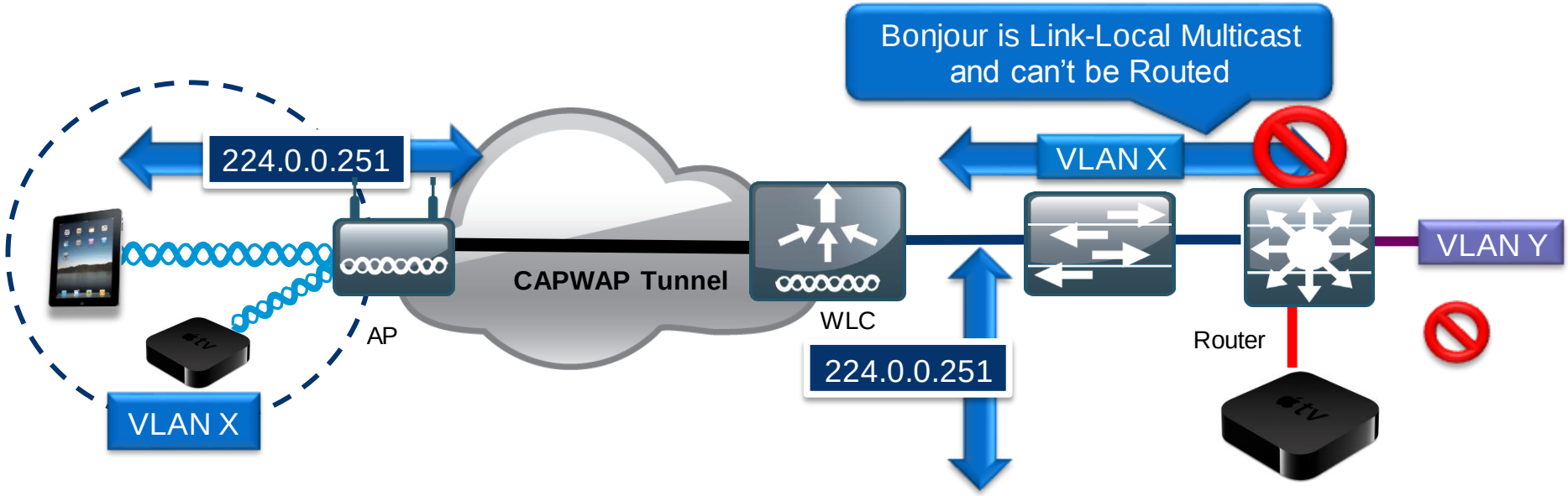
Cisco live!

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

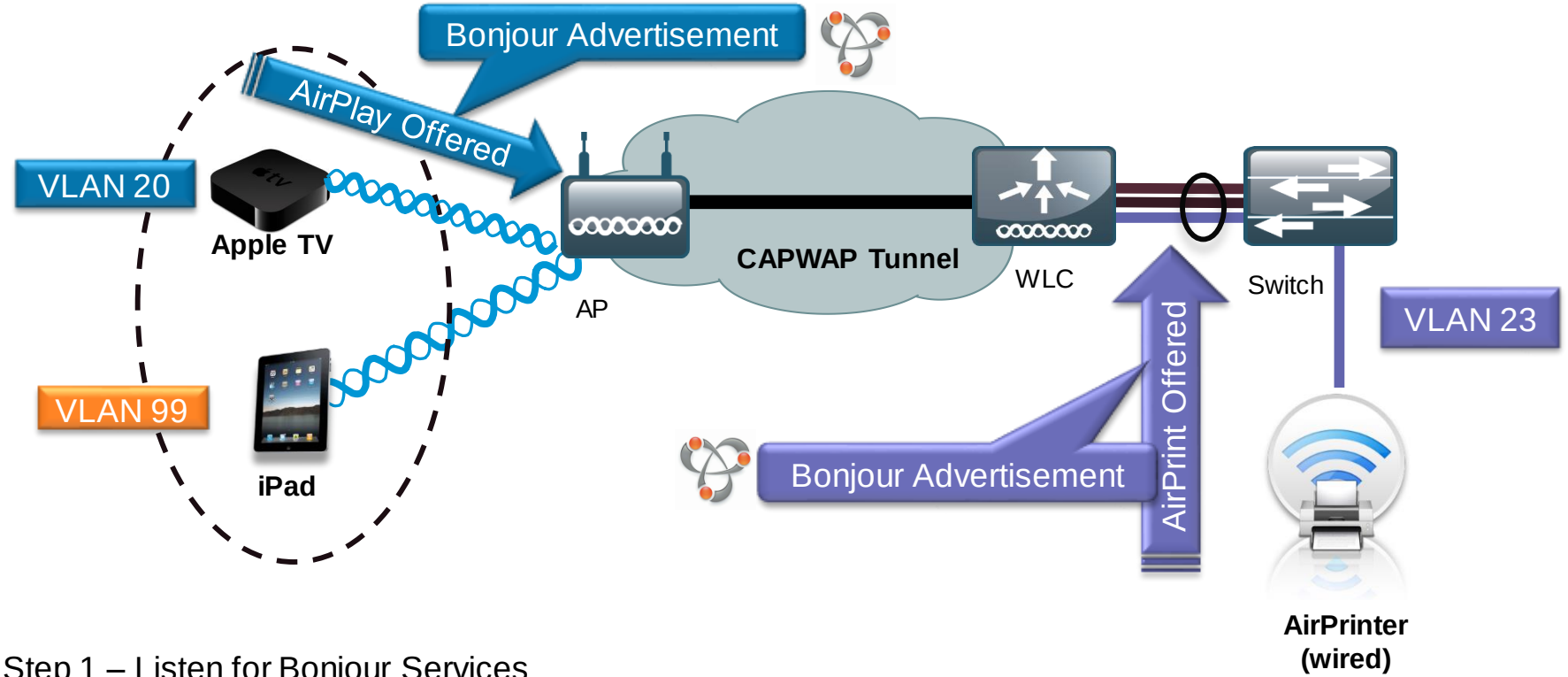


- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:

  IPv4 Group Address – 224.0.0.251

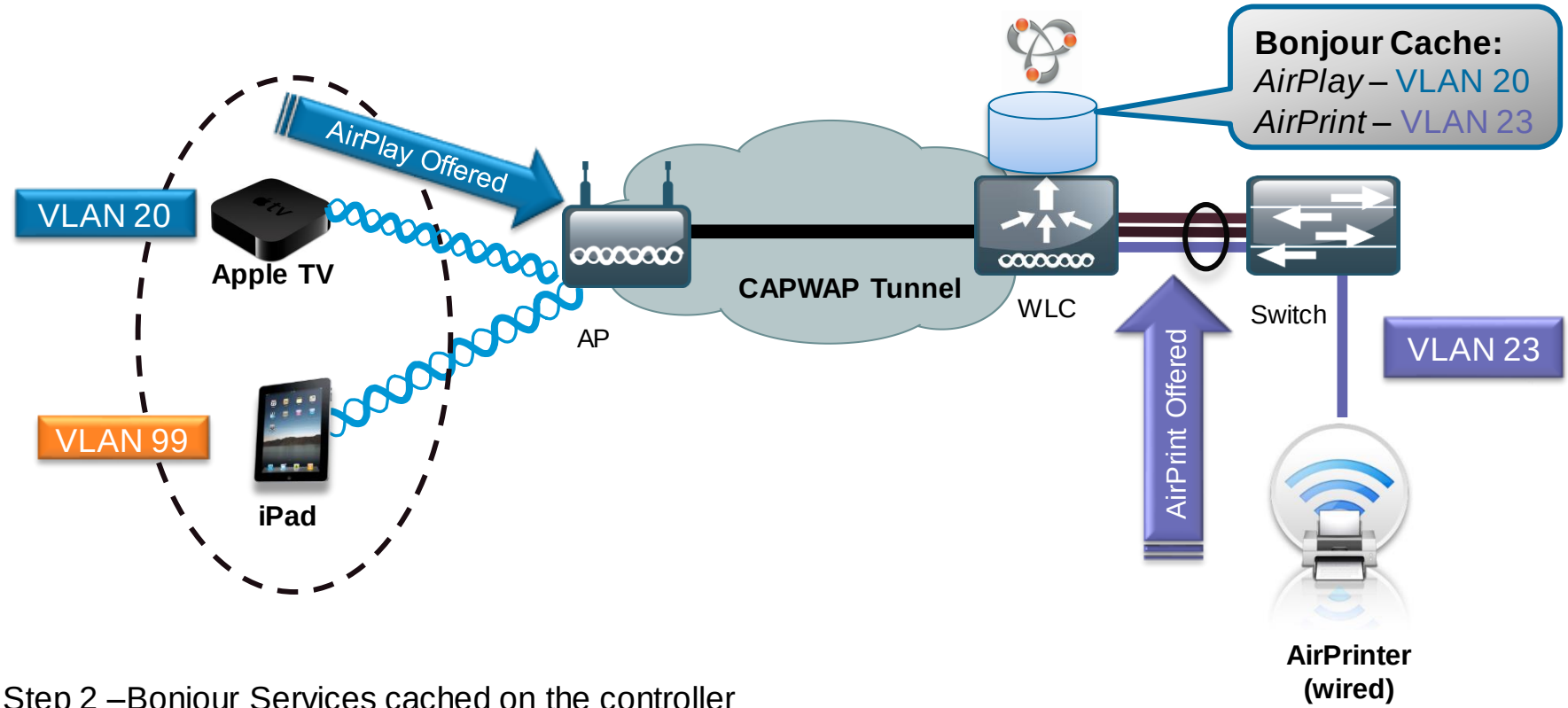
  IPv6 Group Address – FF02::FB

Bonjour mDNS Gateway on Cisco WLC



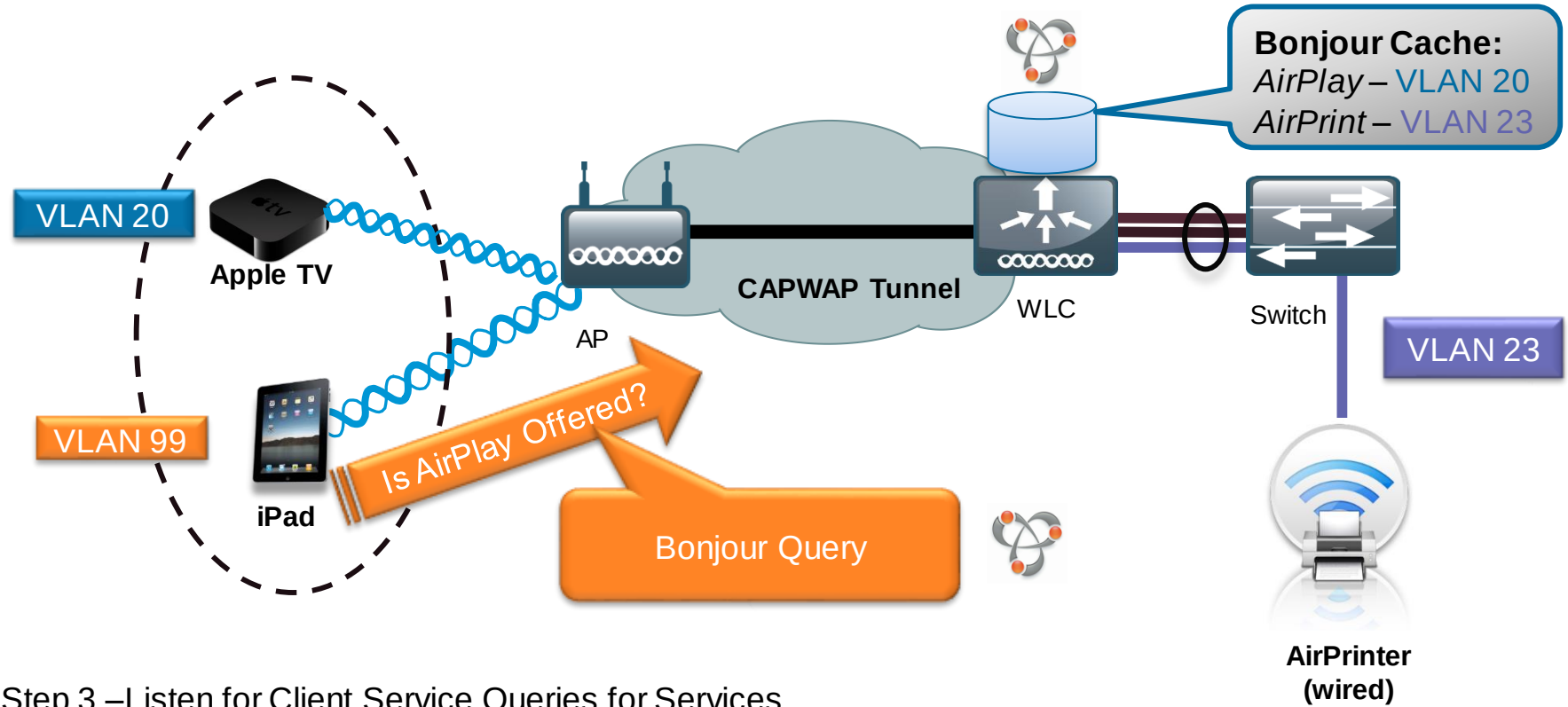
- Step 1 – Listen for Bonjour Services

Bonjour mDNS Gateway on Cisco WLC



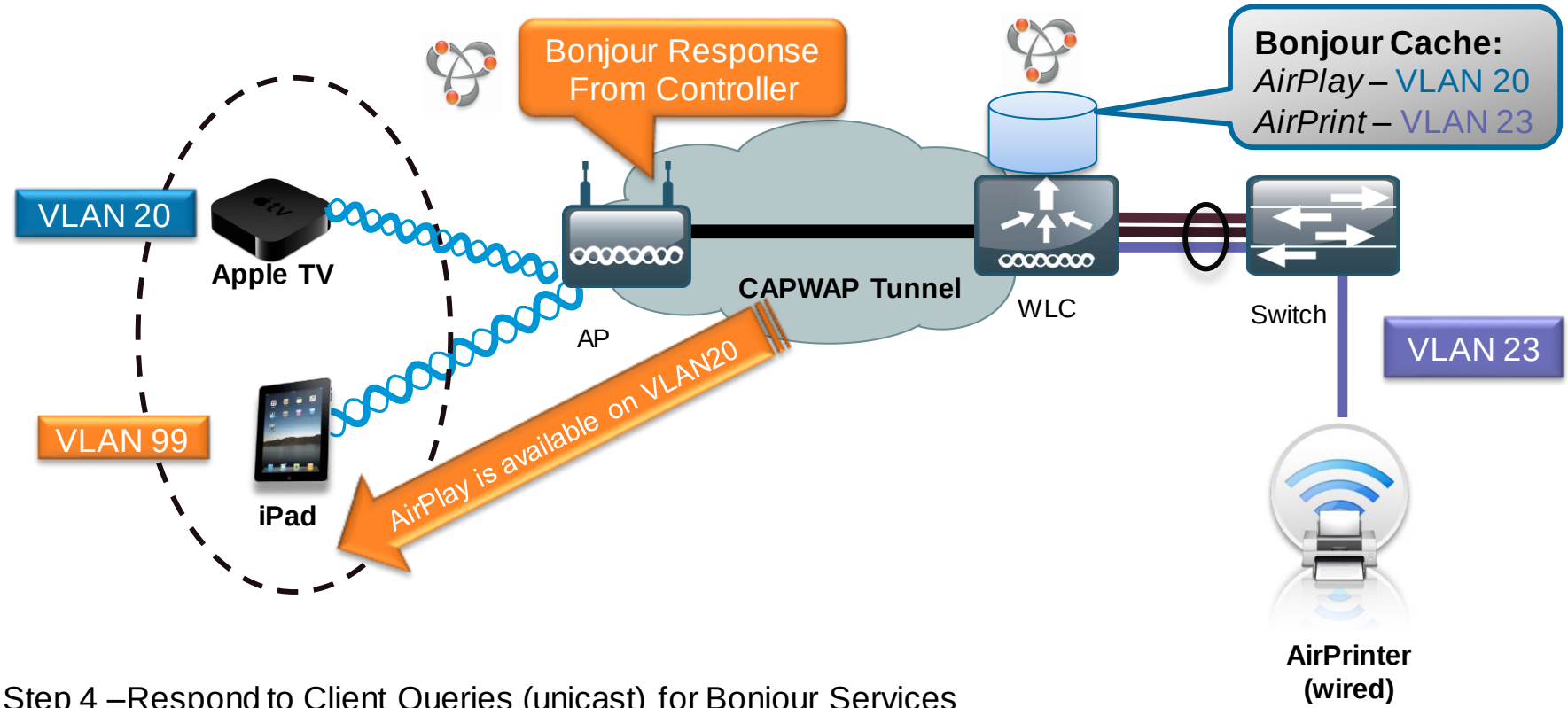
- Step 2 –Bonjour Services cached on the controller

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

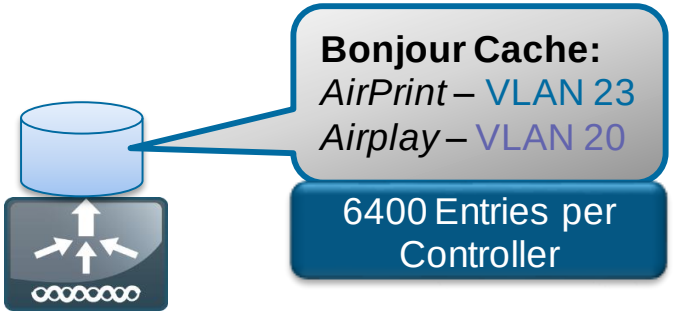
Airplay Services = 4

- Airplay for iOS *(_airplay._tcp)*
- Airplay for Mac OSX *(_appletv-v2._tcp)*
- Audio for Airplay *(_roap._tcp)*
- Remote *(_touch-able._tcp)*

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

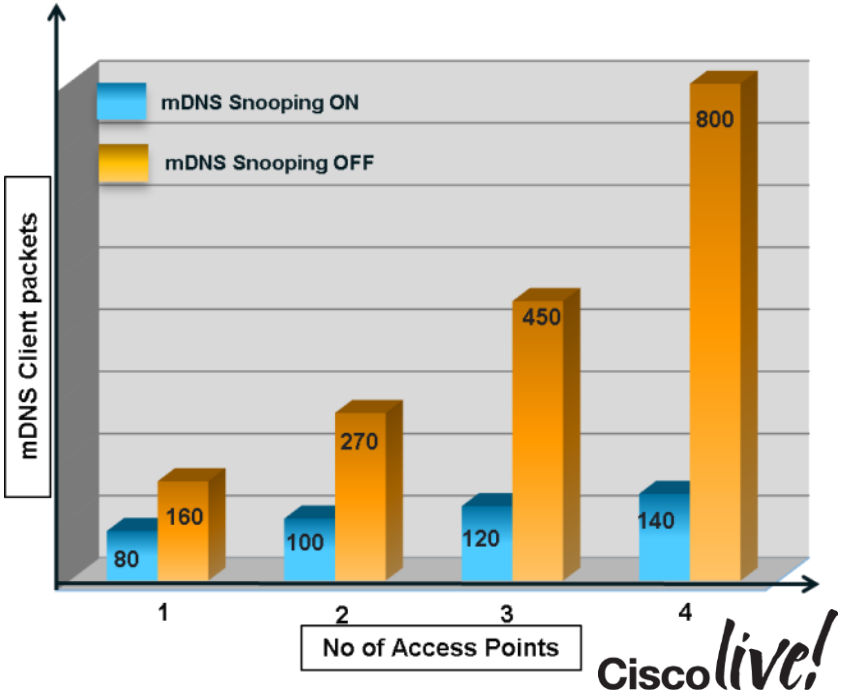
- Not flooded

Bonjour Client Query

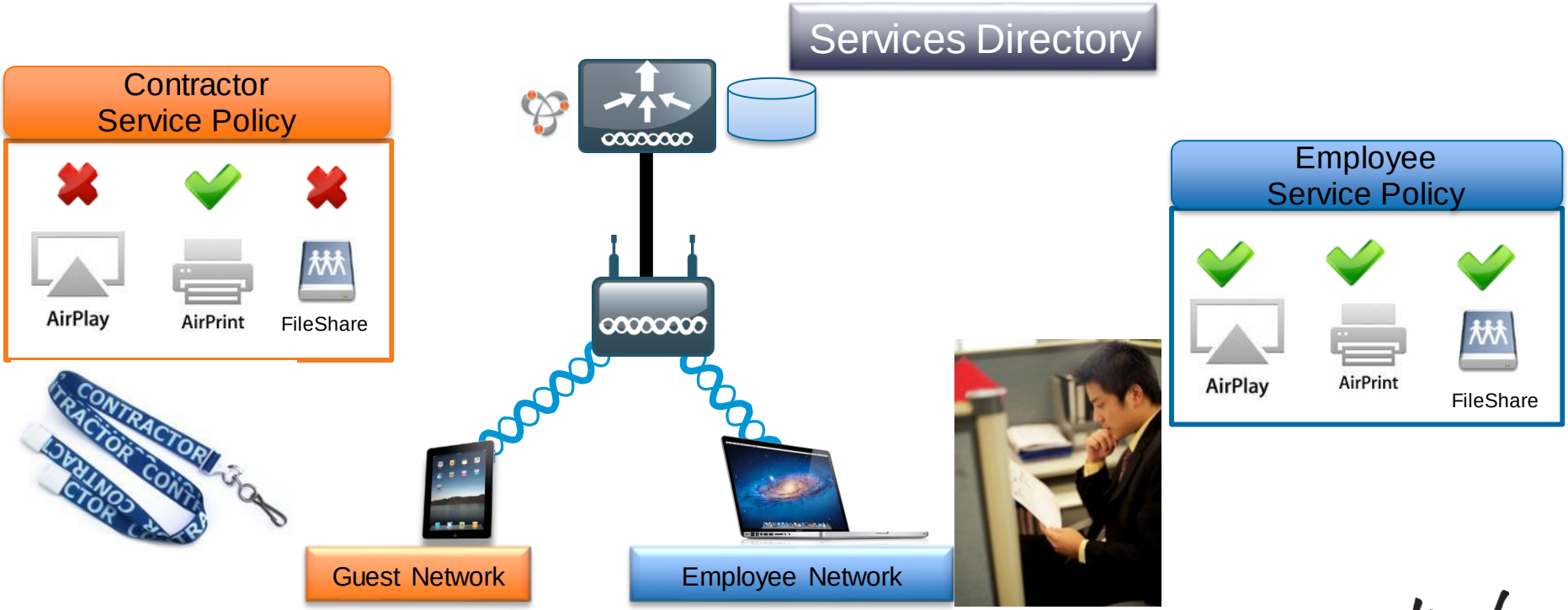
- Unicast Response
- Not flooded

80% less Bonjour Traffic*

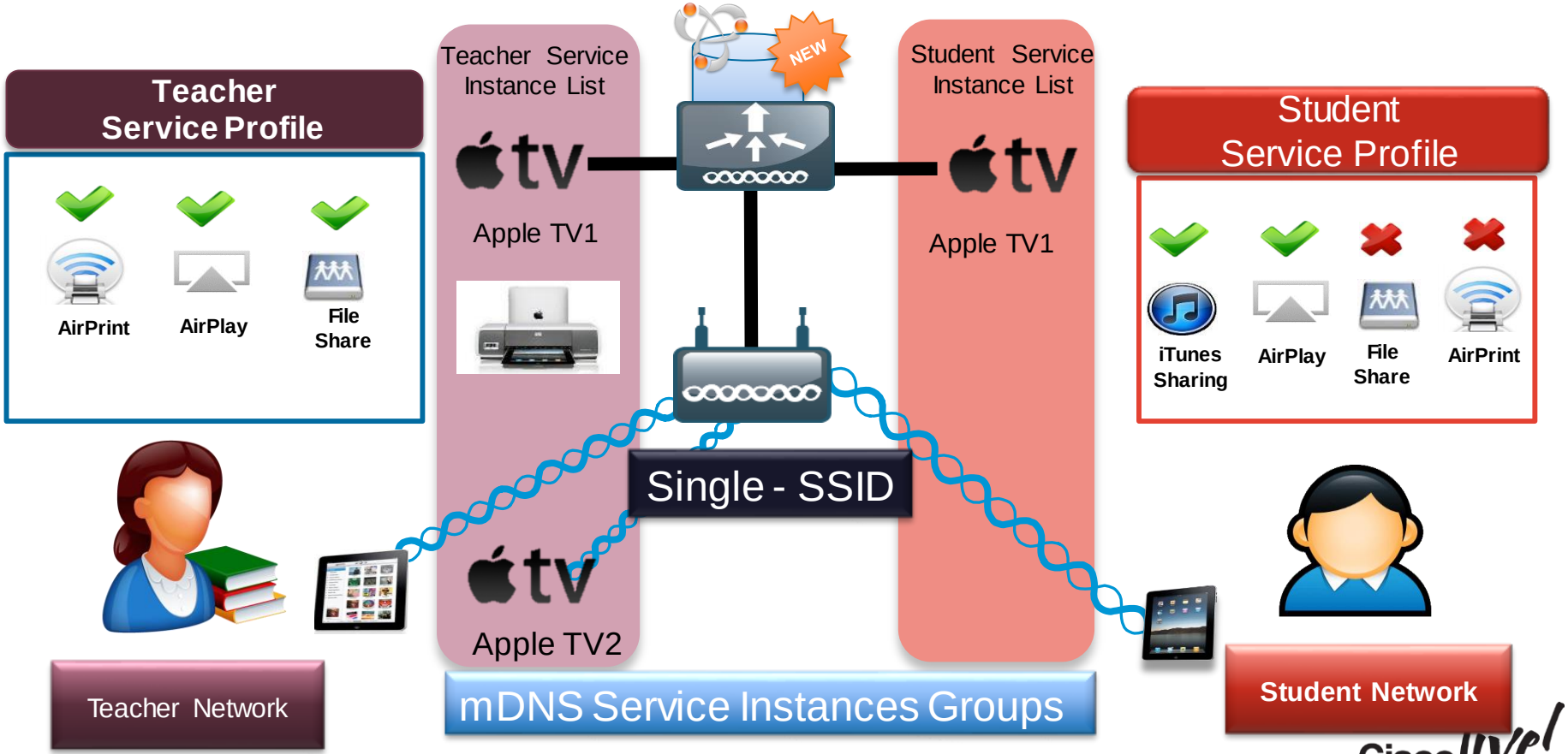
* For 4 Access Point Deployment



Filter Services by User Group



Filter Bonjour Service per Device using v8.0



Bonjour Policy Enhancement in 8.0

NEW

1 Create Bonjour Device group

Teacher Bonjour Devices

Classroom Printer

Classroom Apple TV

Common Bonjour Devices

Library Printer

Library Apple TV

Student Bonjour Devices

Personal Apple TV

2 Assign ID to Device Group

User Role = Teacher

User Role = Teacher & Student

User Name= John

3 Assign Location

Location?

Cisco live!

Bonjour Policy Enhancement in 8.0

NEW

Teacher Bonjour Devices

Classroom Apple TV

Teacher can discover Classroom Apple TV **only** when present in classroom

User Role = Teacher

Location = ClassRoom

Classroom Printer

Teacher can discover Classroom Apple printer from anywhere on the campus

User Role = Teacher

Location = Any

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

Google ChromeCast With Cisco Wireless

How Does Google ChomeCast Work?

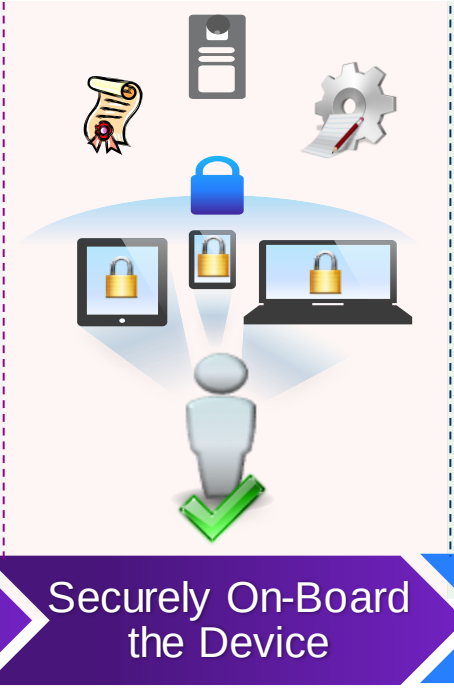
- ChromeCast Deployment Guide:
  - http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-6/chromecastDG76/ChromecastDG76.html

Summary

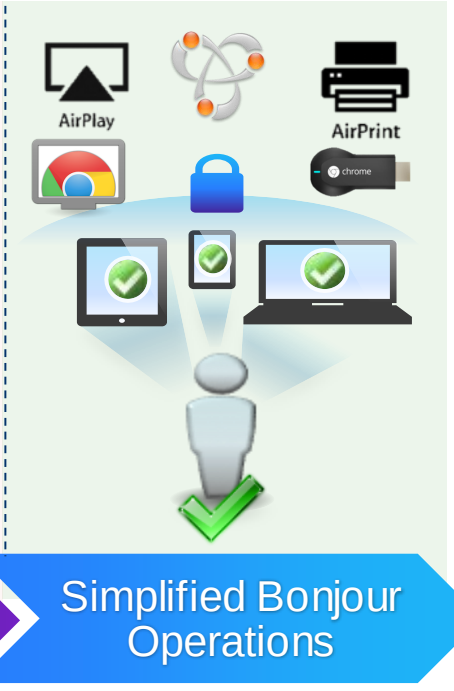
Managing the BYOD Evolution

Personal Devices on Network

Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations

Cisco live!


Q & A
Cisco live!

Complete Your Online Session Evaluation

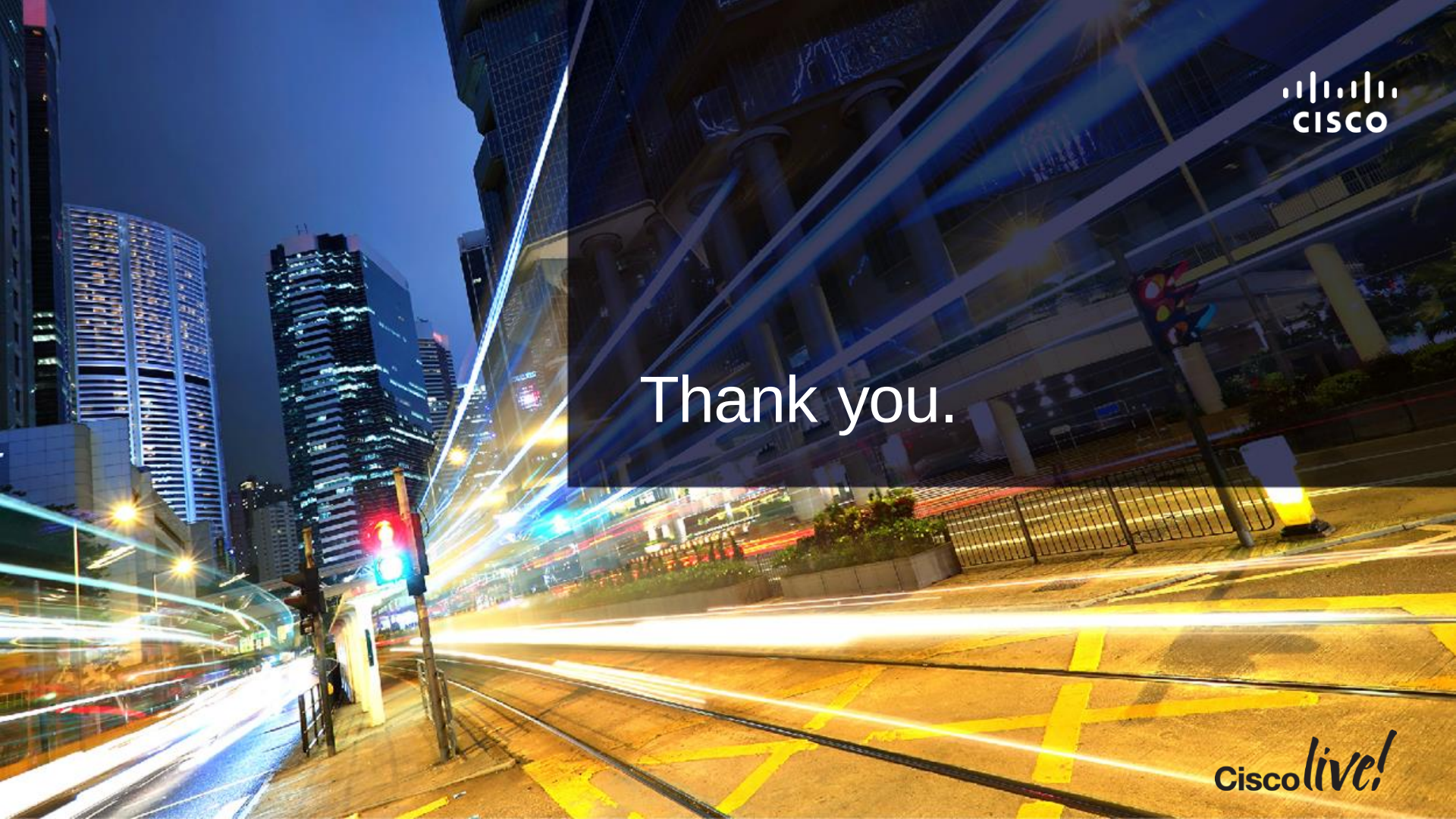
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

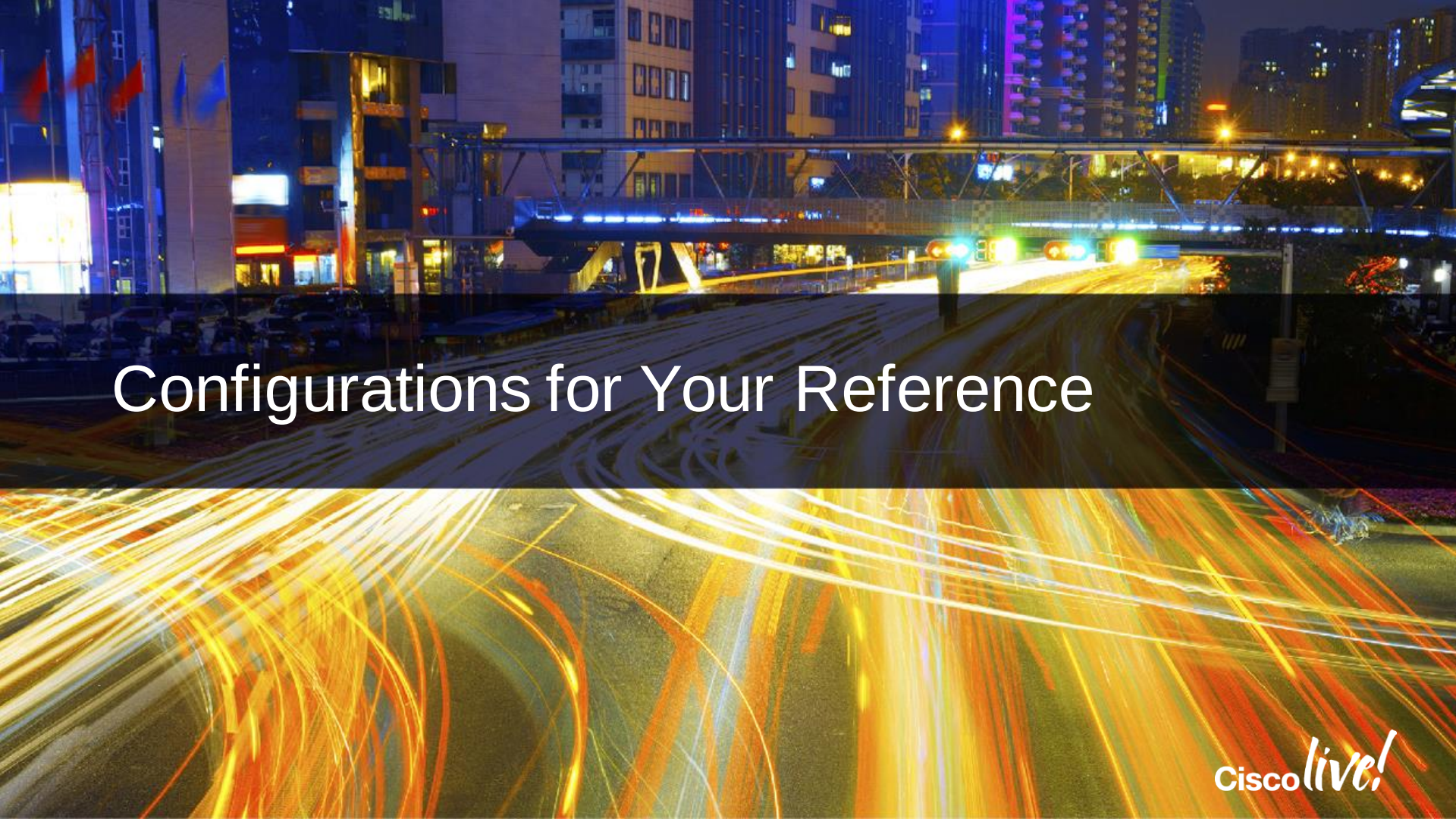
- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

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

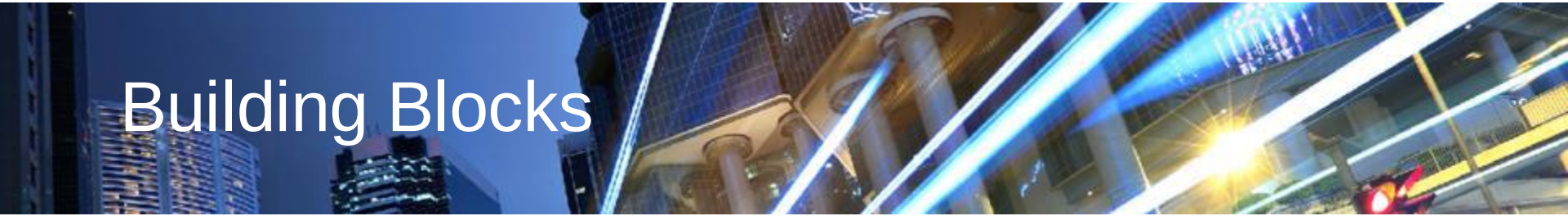

Thank you.
CISCO
Cisco live!


CISCO



Configurations for Your Reference

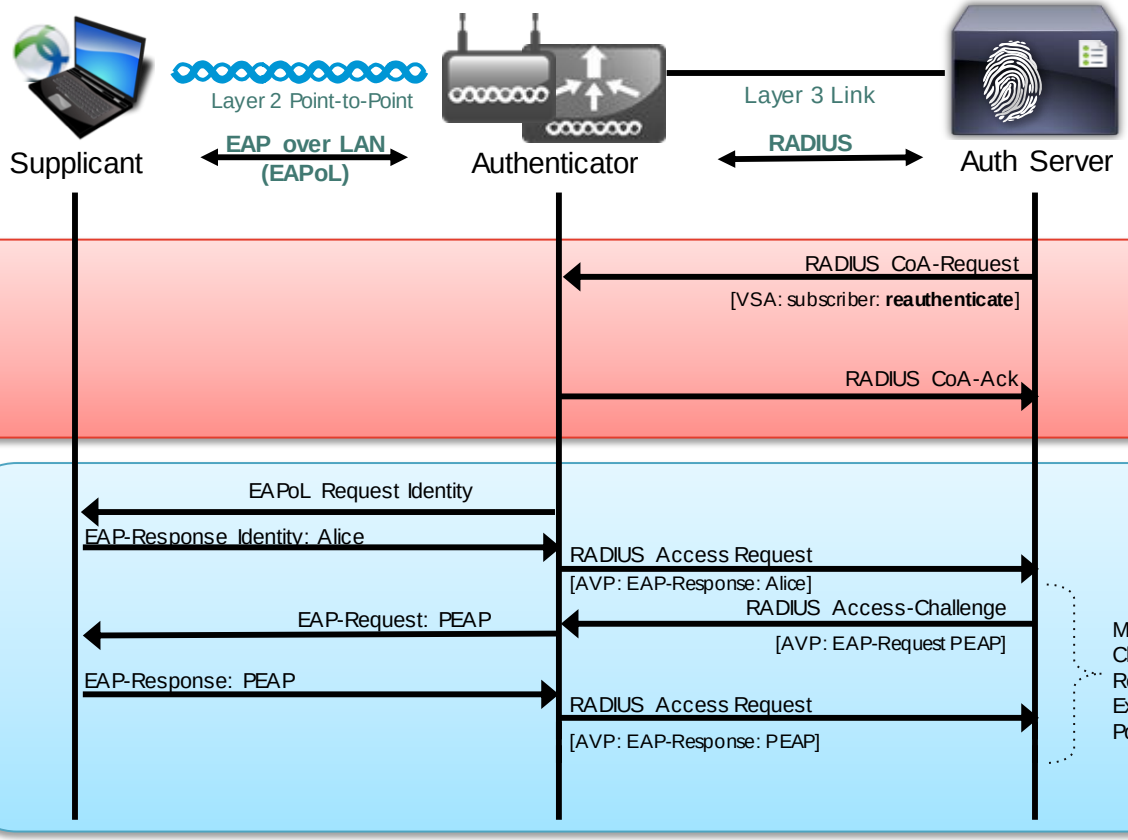
Cisco live!



Building Blocks

IEEE 802.1X with Change of Authorisation (CoA)

For your reference

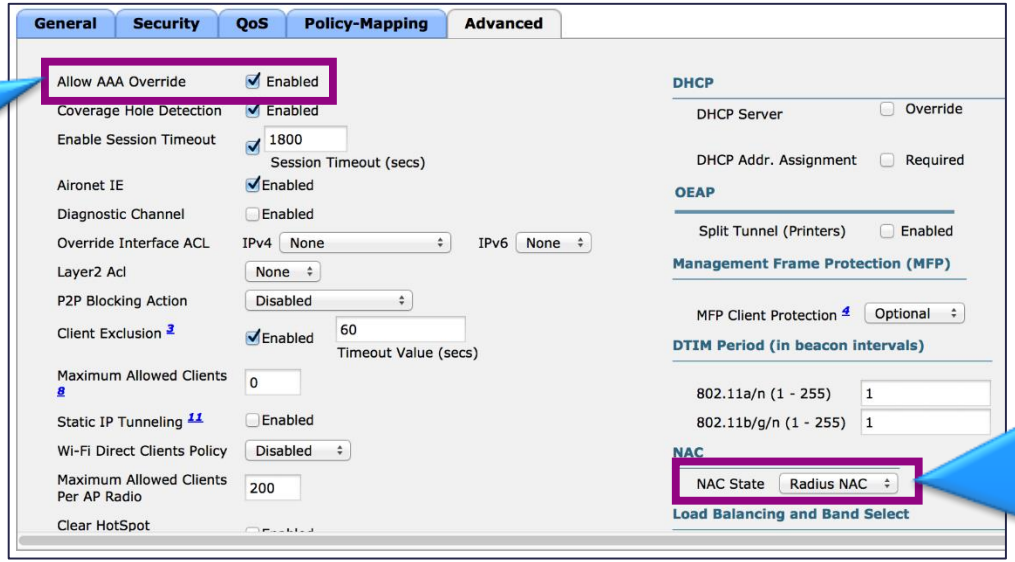


Enable CoA – AAA Override

For your reference

1

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



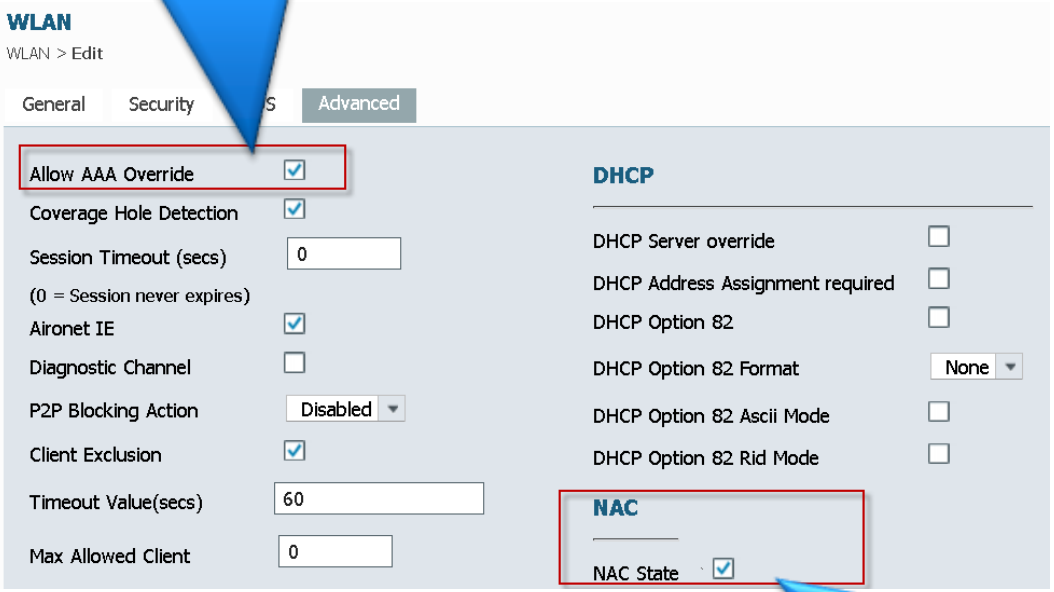
2

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

Converged Access BYOD Config

For your reference

Change Of Authorisation (CoA)



Network Access Control

Cisco live!

Cisco Wireless LAN Controller ACLs

For your reference

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

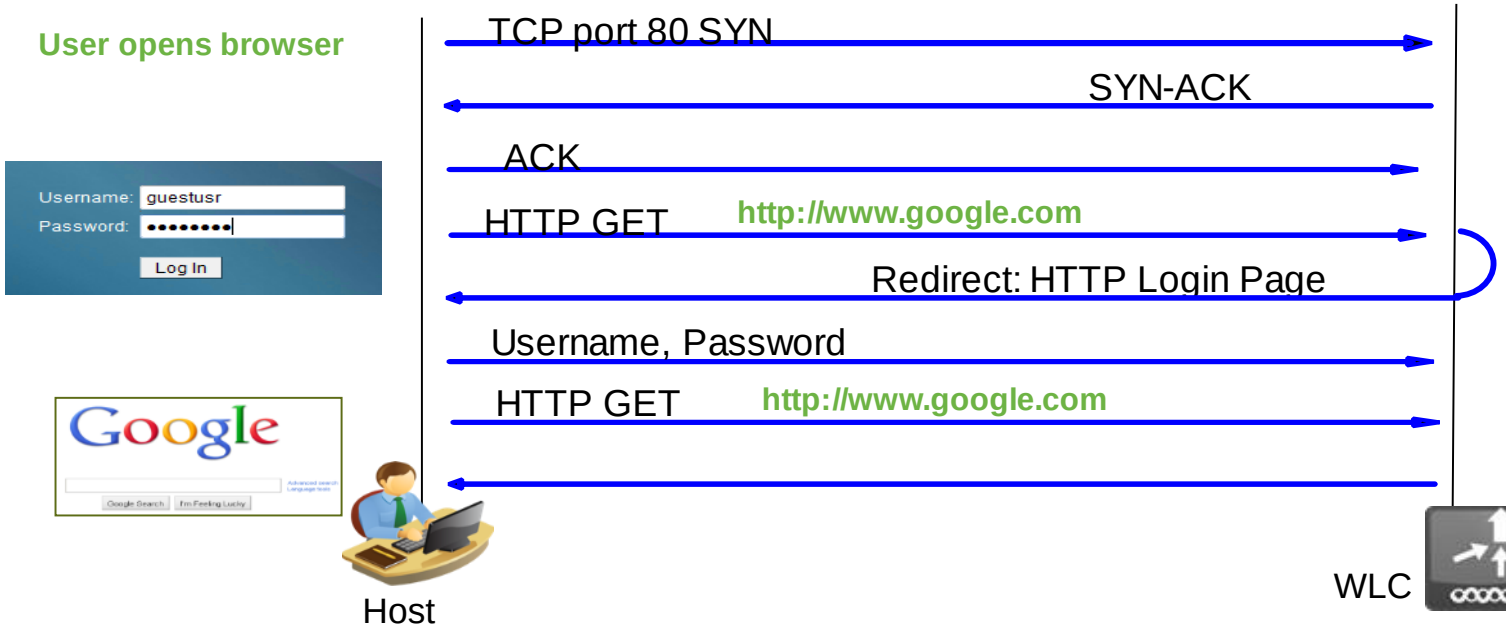
Implicit Deny All at the End

Cisco live!

URL Redirection

For your reference

- Example: TCP Traffic Flow for Login Page



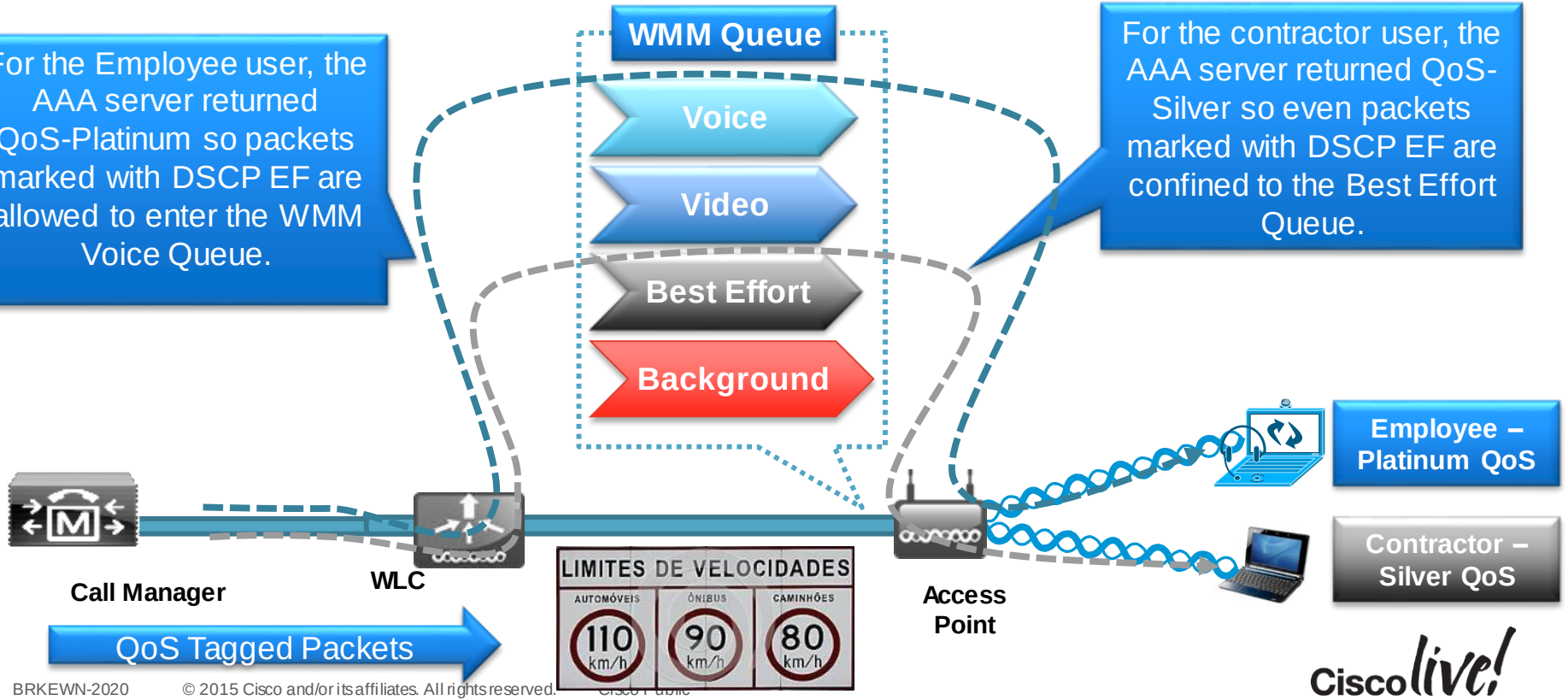
Cisco Wireless User-Based QoS Capabilities

For your reference

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

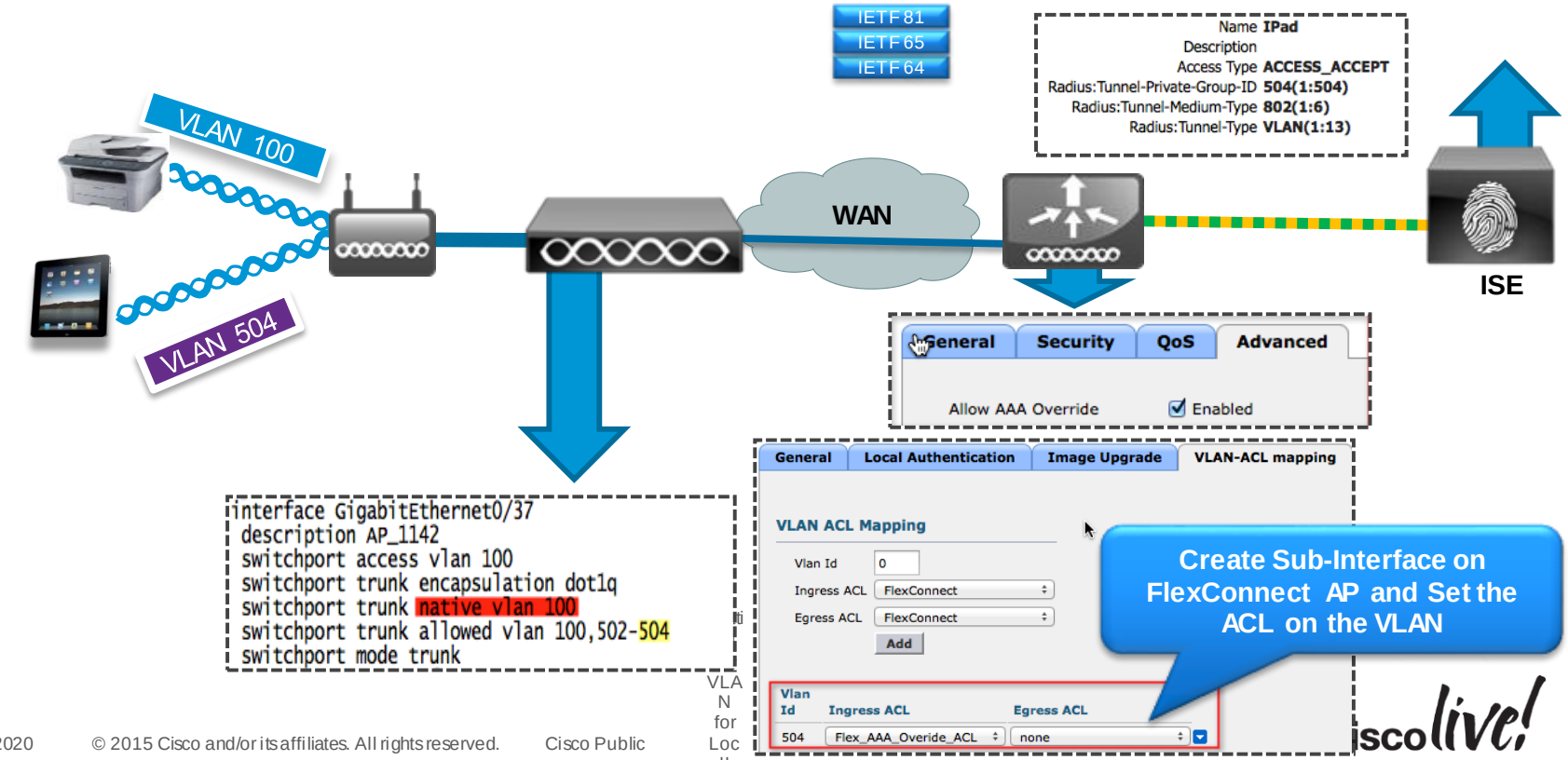
For the Employee user, the AAA server returned QoS-Platinum so packets marked with DSCP EF are allowed to enter the WMM Voice Queue.

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

For your reference



VLAN for Locally Switched

Integration of WLC and ISE

Cisco live!

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

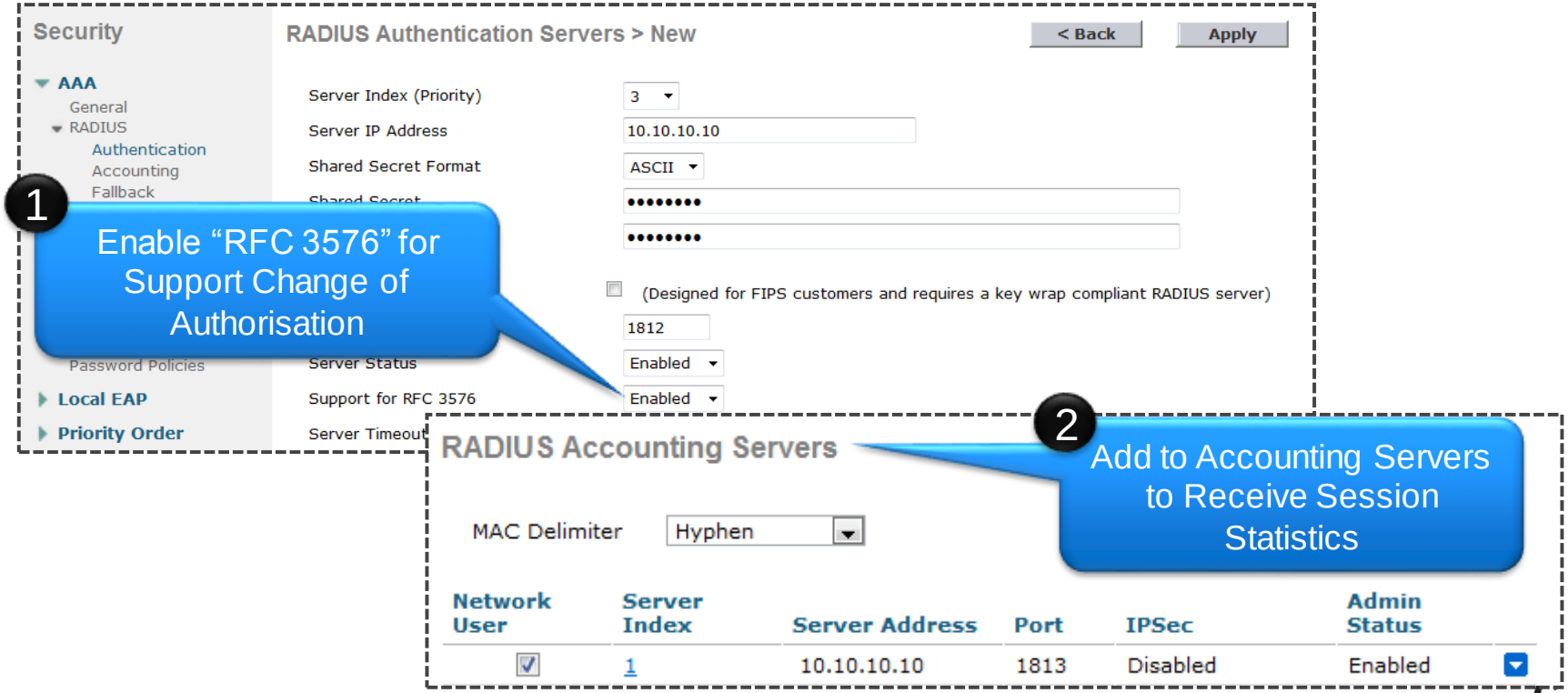
- Enable profiling sensors

3. Setup Access Restrictions

- Configure ACLs to filter and control network access.

Configuring ISE as the Authentication Server and Accounting Server

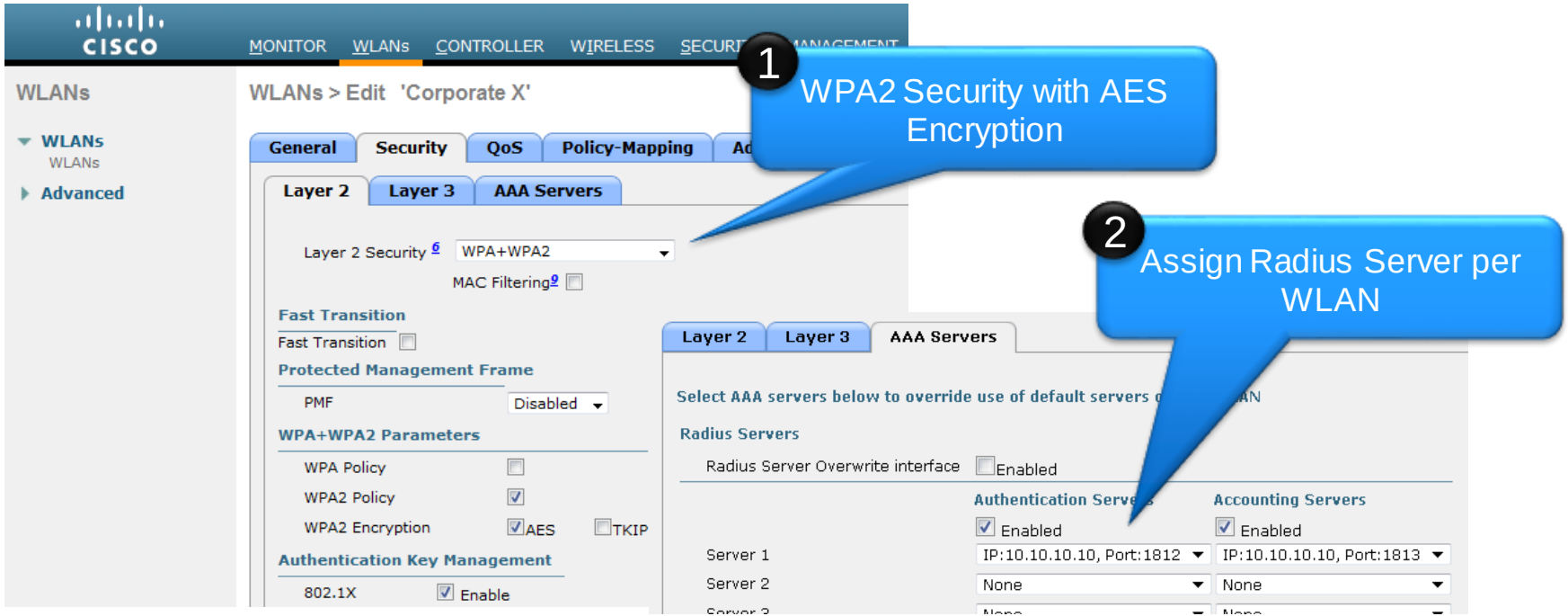
For your reference



Configuring the WLAN for Secure Connectivity

Enabling Secure Authentication and Encryption with WPA2-Enterprise

For your reference

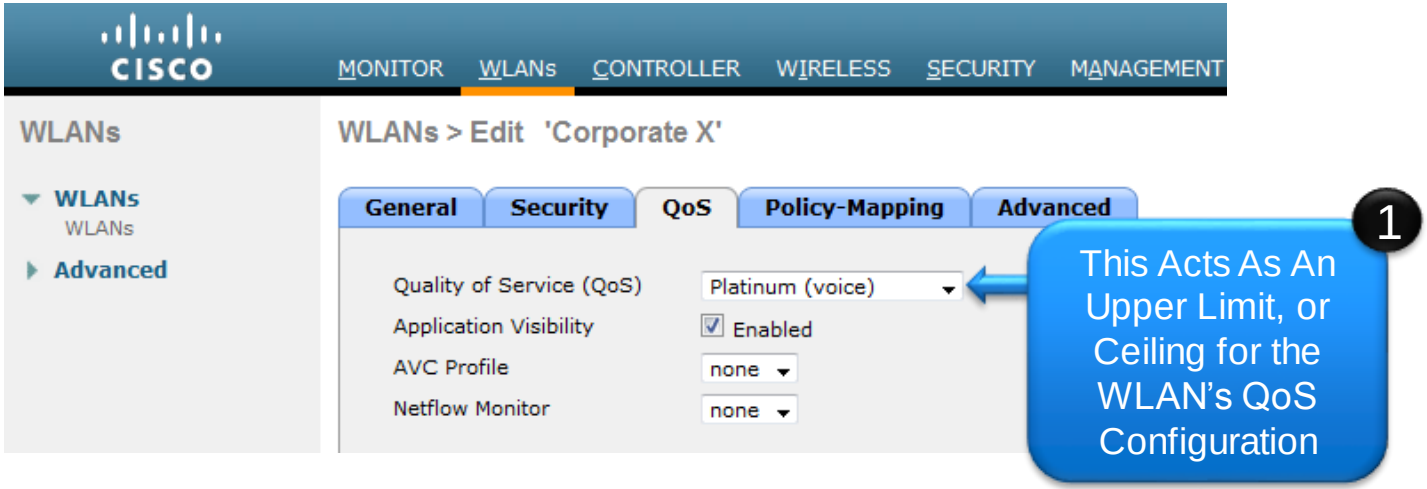


Cisco live!

Setting the WLAN QoS Level for Override

For your reference

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

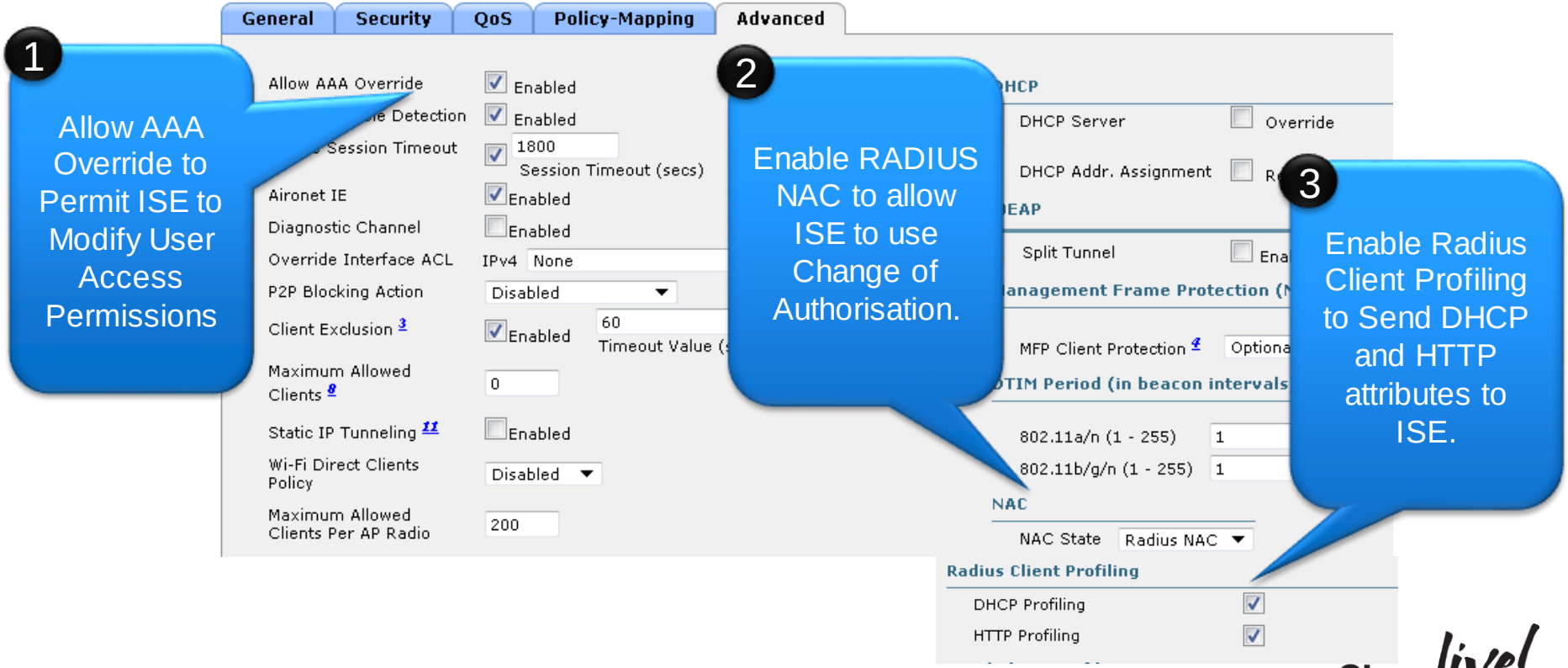


- If WMM is set to Allowed, the Quality of Service configuration serves as a limit for the entire SSID.
- Ensure all controller uplinks, media servers and Access Points have proper Quality of Service trust commands in IOS.

Cisco live!

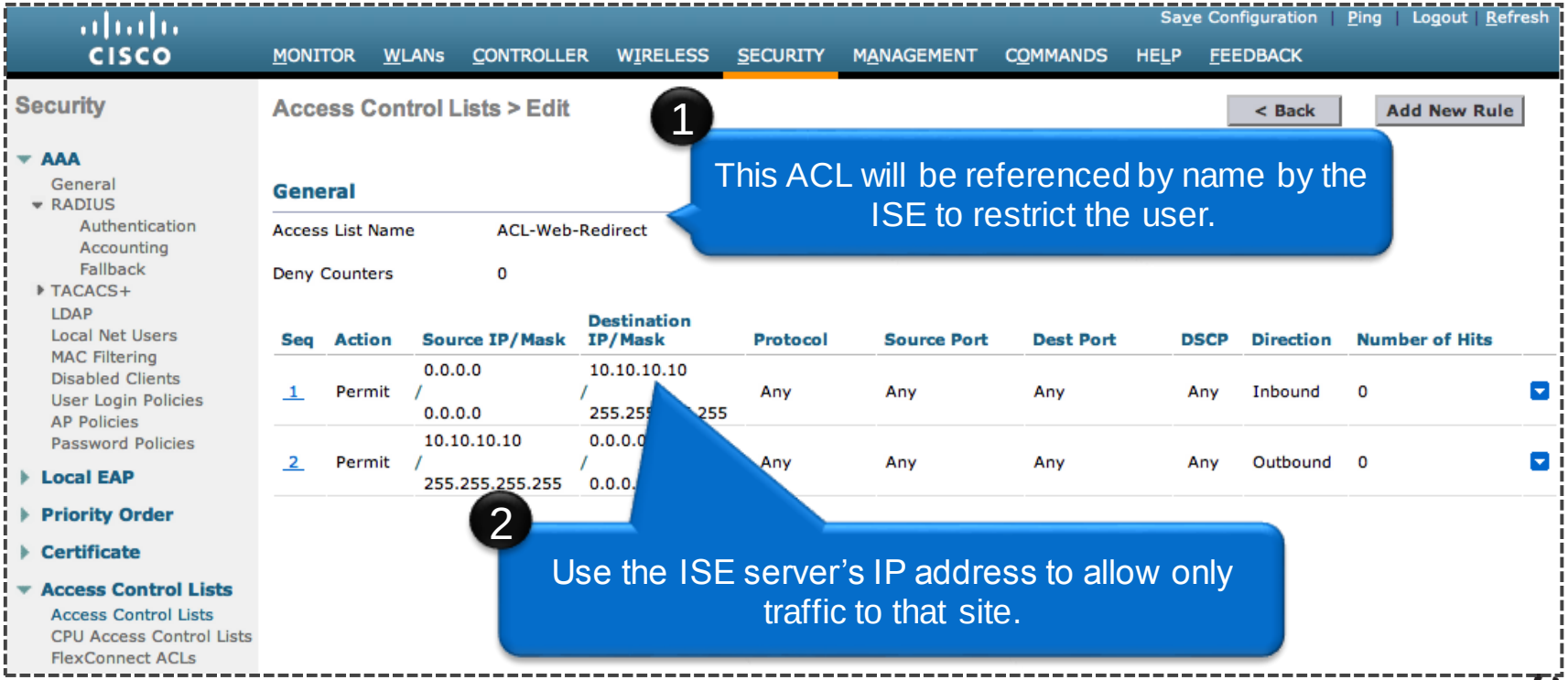
Configuring the WLAN for ISE Identity-based Networking Cont'd

For your reference



Configuring the Controller ACL

For your reference

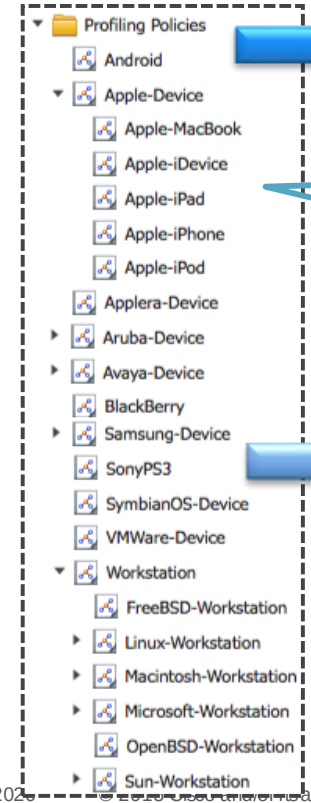


Cisco live!

ISE Device Profiling Capabilities

For your reference

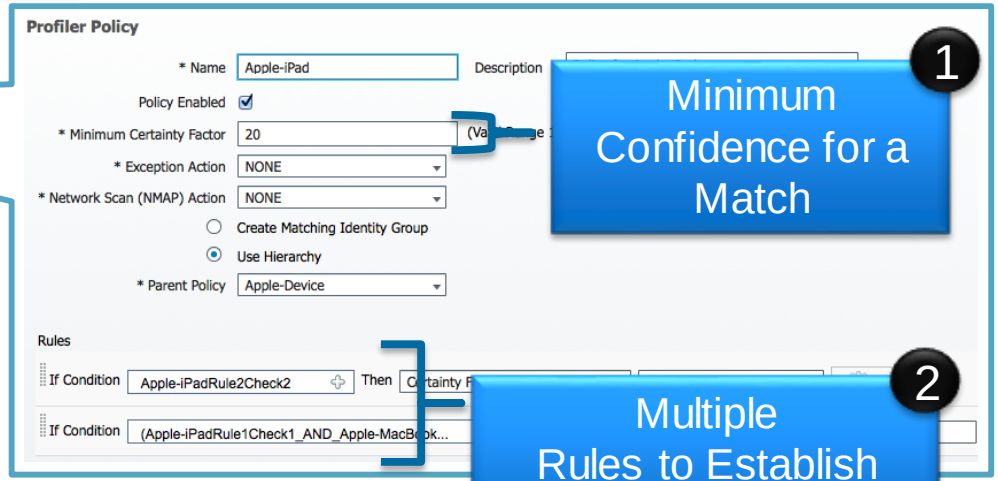
Over 200 Built-in Device Policies, Defined Hierarchically by Vendor



Smart Phones

Gaming Consoles

Workstations



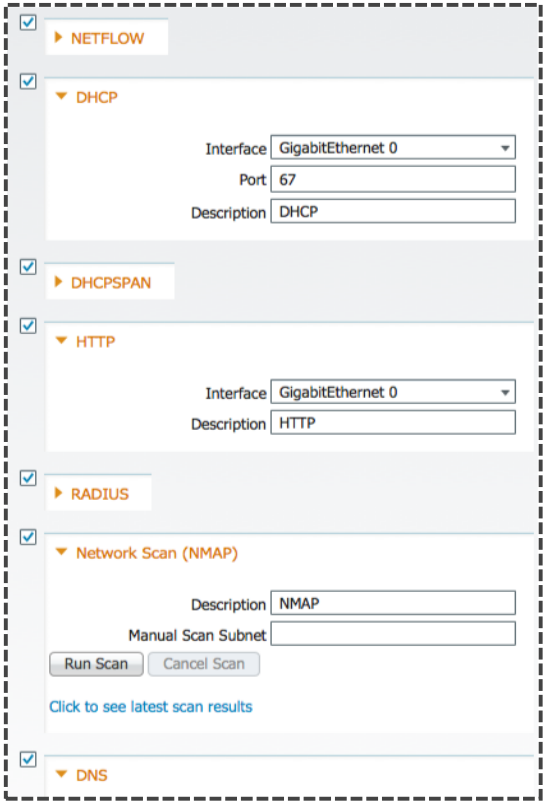
1 Minimum Confidence for a Match

2 Multiple Rules to Establish Confidence Level

Cisco live!

Configuring ISE Profiling Sensors

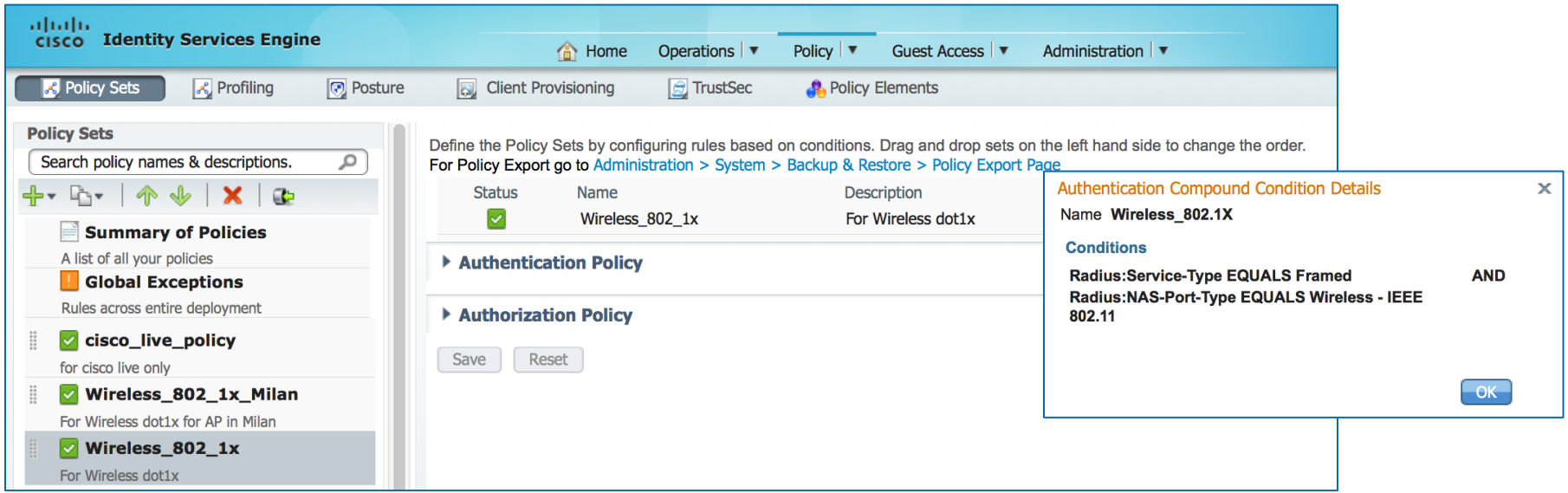
For your reference



- 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

For your reference



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.

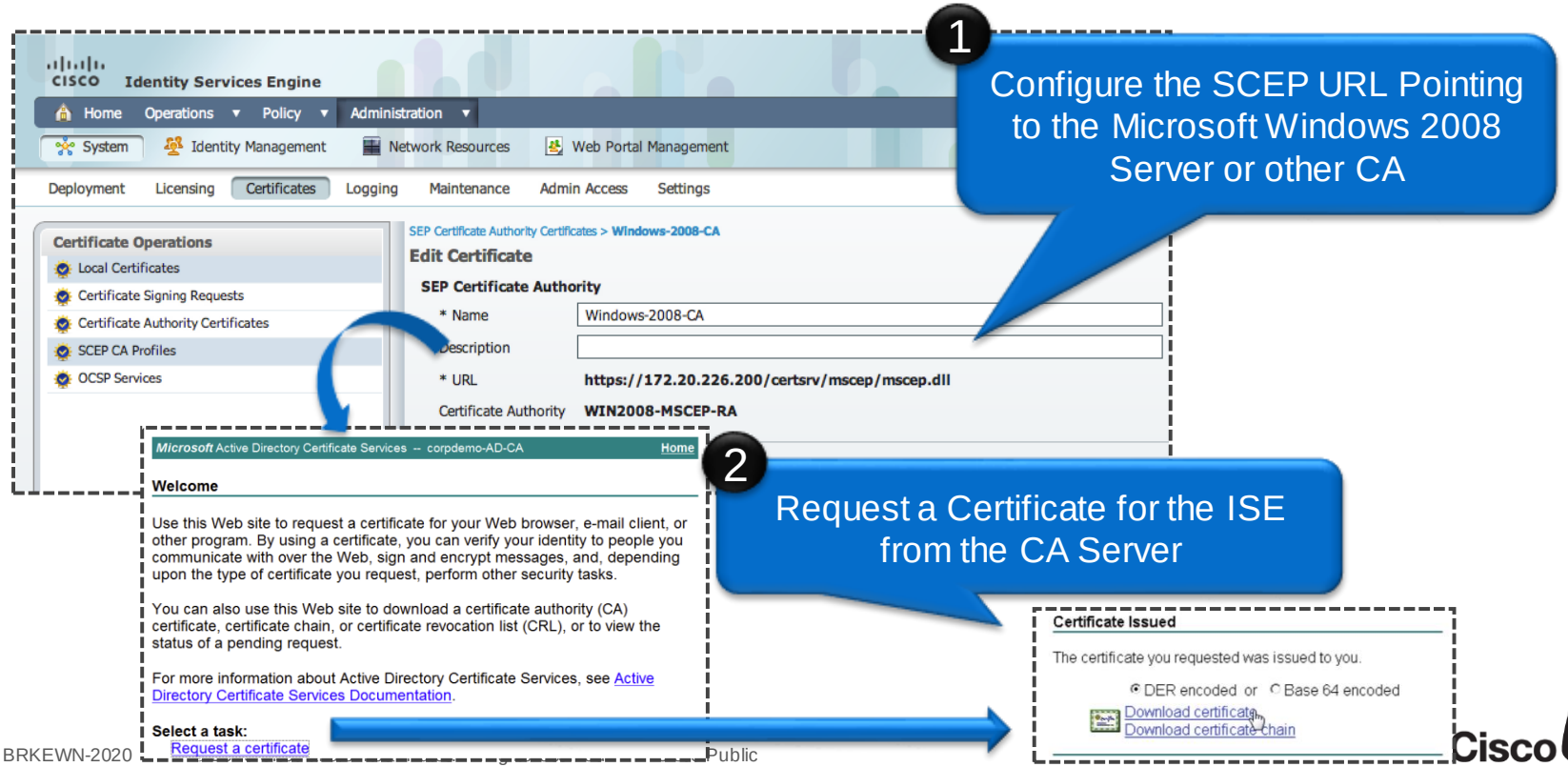
2. Define Supplicant Provisioning Profile

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

Configuring SCEP Integration on the ISE

For your reference

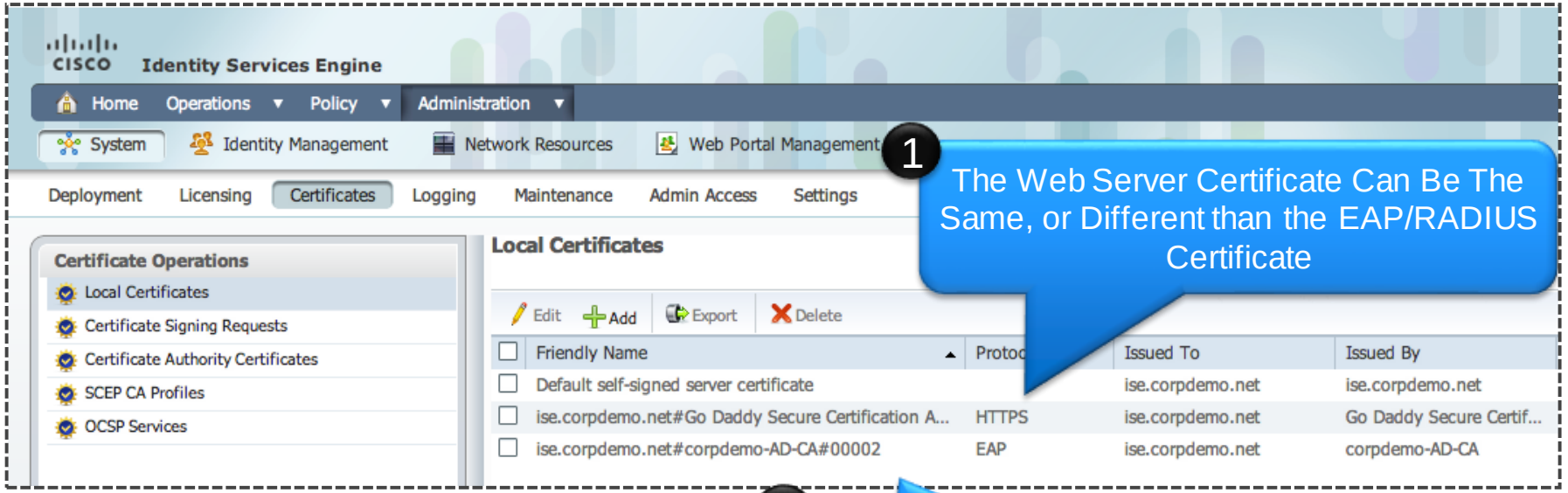
- The ISE Must Point to the SCEP Server and Have a Valid Certificate Signed by the CA



Configuring Certificates on the ISE

For your reference

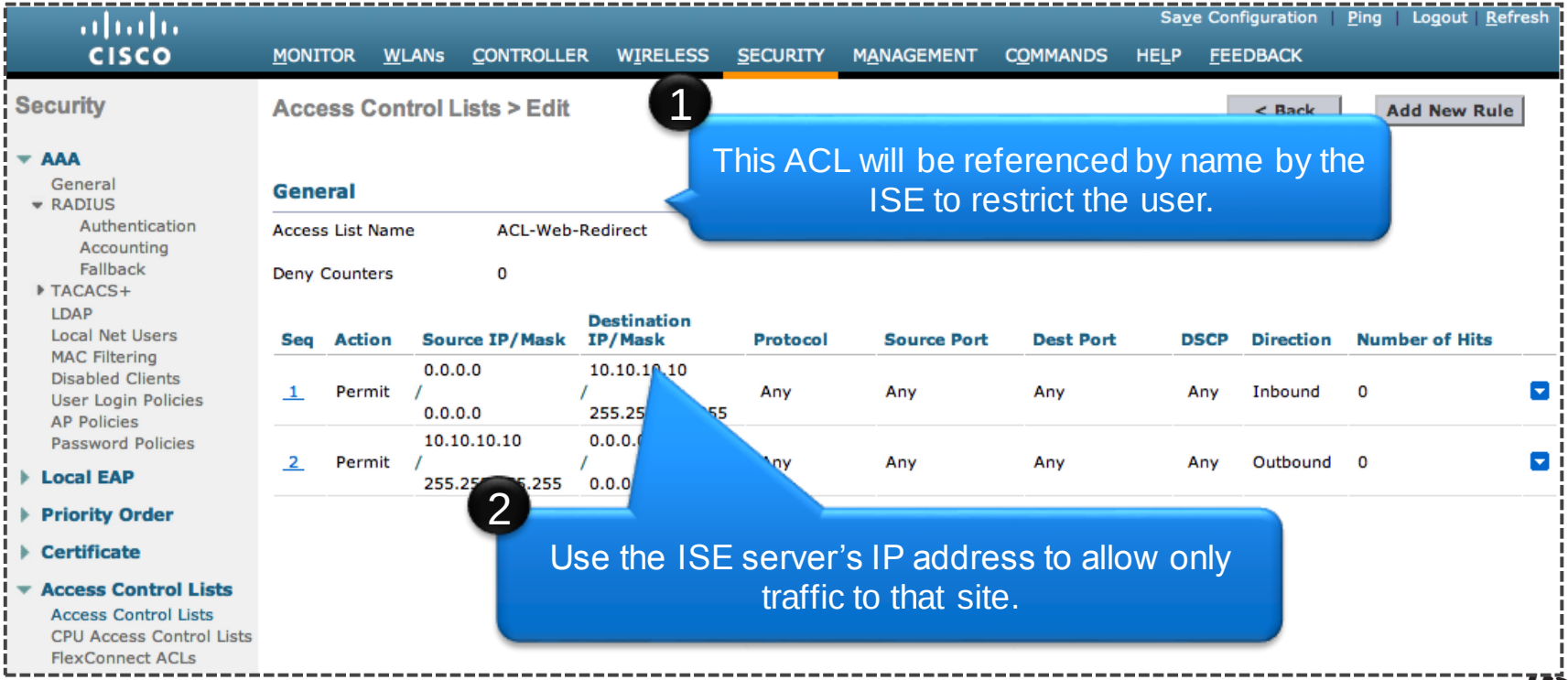
- Certificates are Used for HTTPS and EAP Connections



Configuring the Web-Authentication Redirect ACL

For your reference

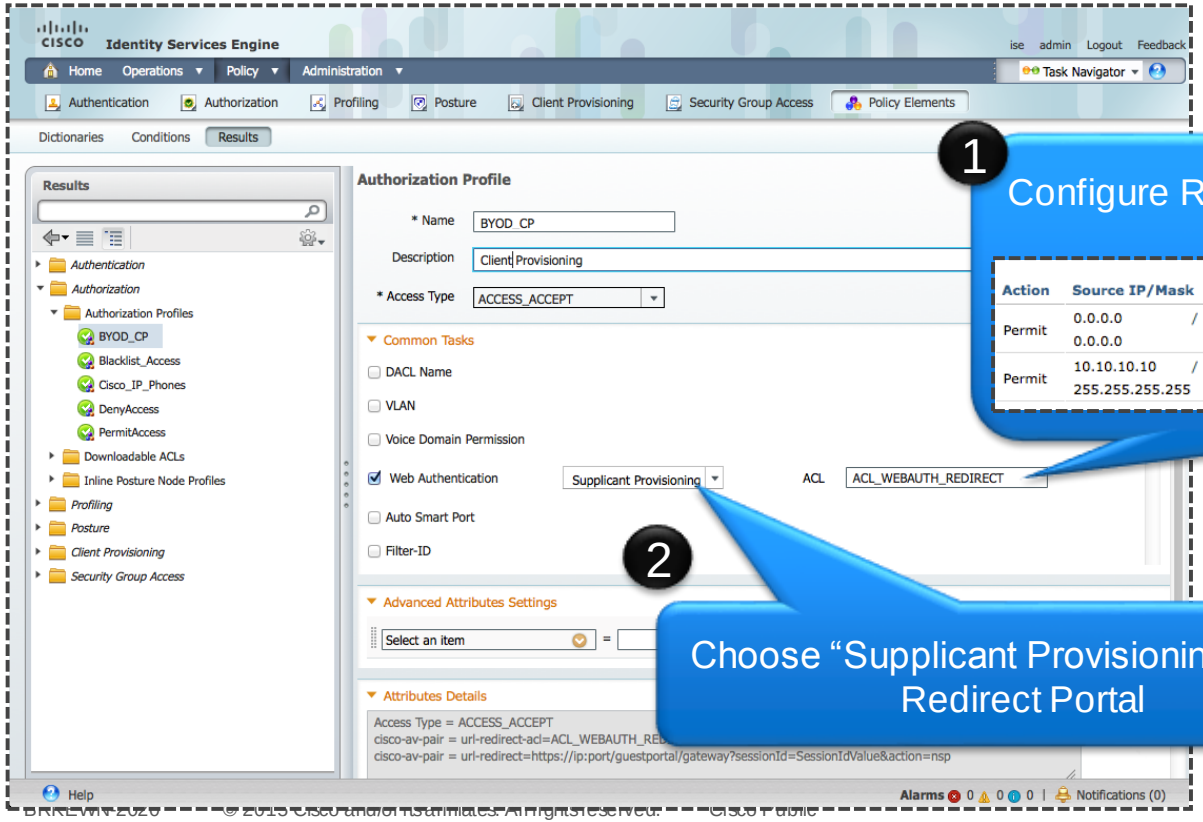
- The ACL is Used in HTTP Profiling as Well as Posture and Client Provisioning.



Cisco Live!

Defining the Supplicant Provisioning Authorisation Profile

For your reference



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

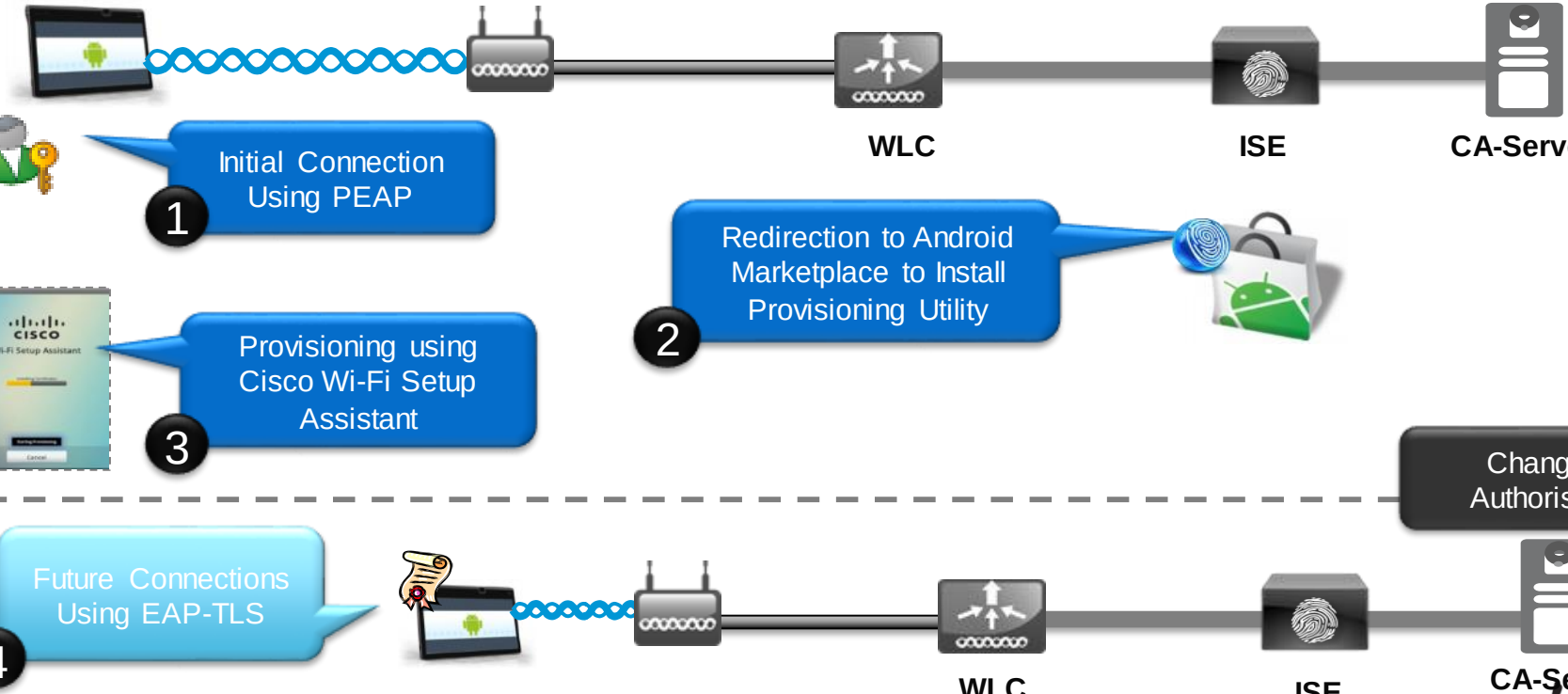
Cisco live!

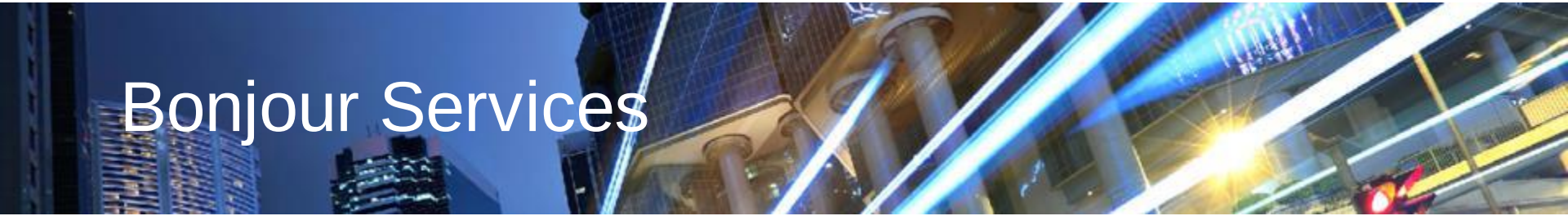
Apple Captive Network Assistant (CNA)

- 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

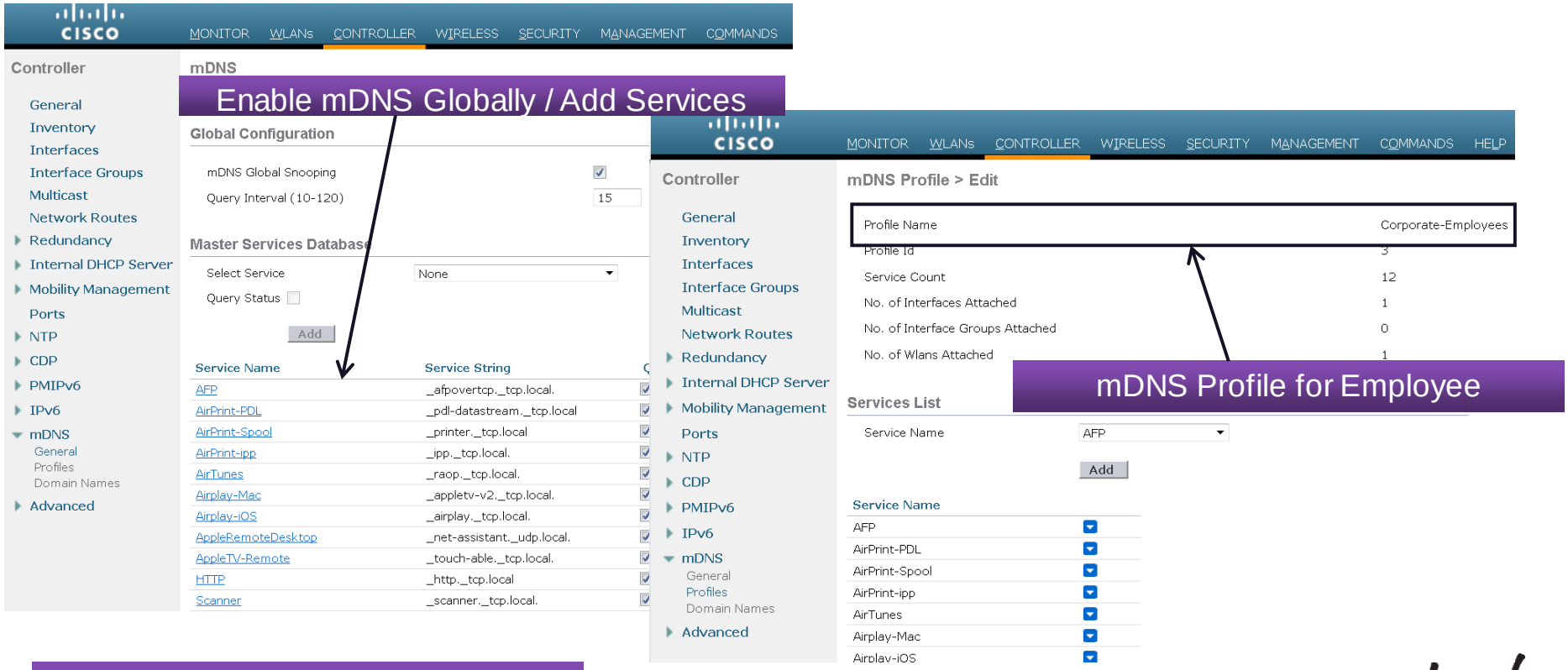
- Steps to enable location specific services on controller

Remote VLAN bonjour Service

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

Bonjour Gateway Services Filter

For your reference



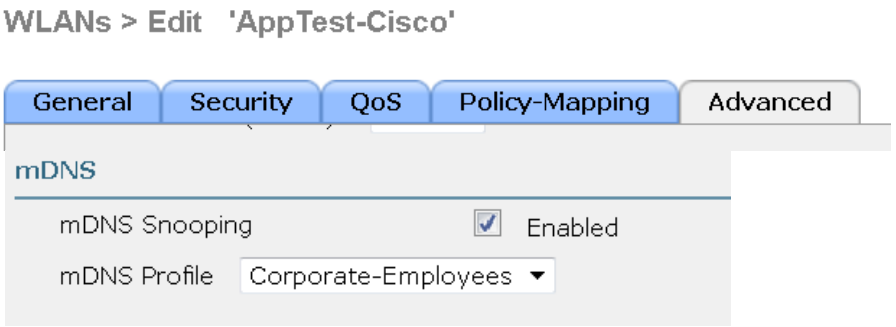
Max. of 64 services can be enabled

Cisco live!

Applying the Bonjour Gateway Profile

For your reference

WLAN



VLAN

Controlling Bonjour Gateway Profile per Interface

Cisco live!

Bonjour: Steps Configuring LSS service from CLI

For your reference

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.
```


Cisco live!

For your reference

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     VlanIder
------------------   --------------------  ------------------  ---------
AP6073.5caa.030b      60:73:5c:aa:03:0b           1                70
```

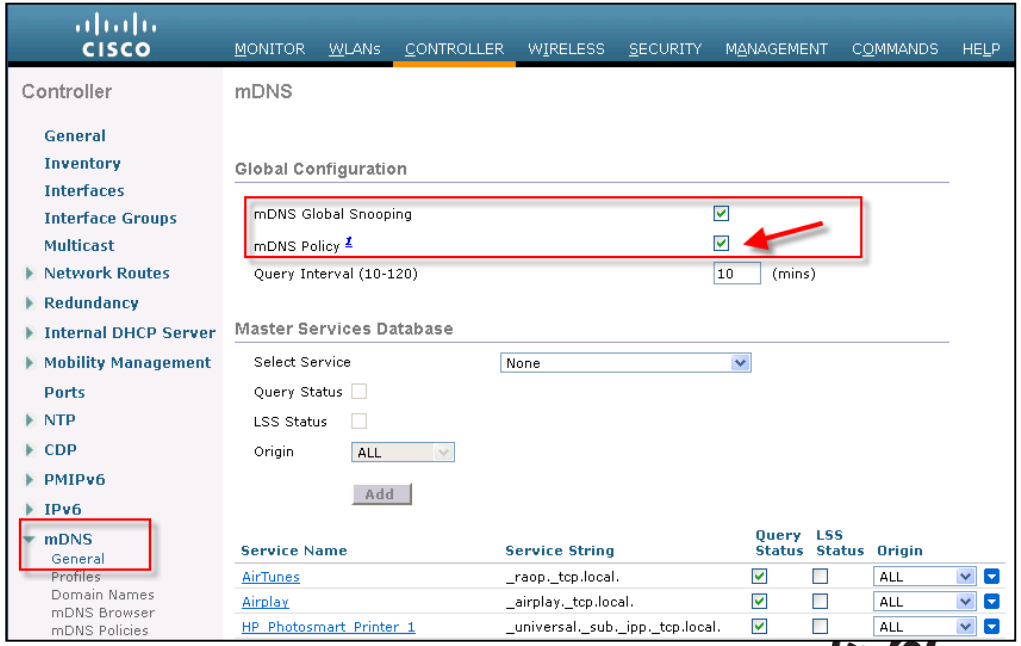
```
(Cisco Controller) >config mdns ap vlan add 71 AP6073.5caa.030b

(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

For your reference

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
```

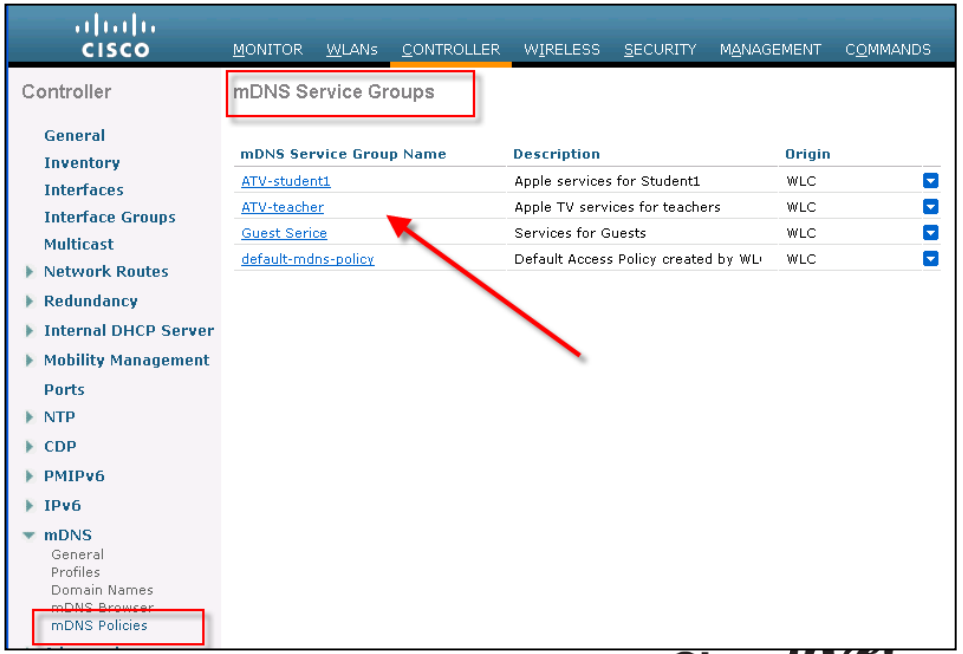


Bonjour Policy Configuration

For your reference

2. Create mDNS Service Group

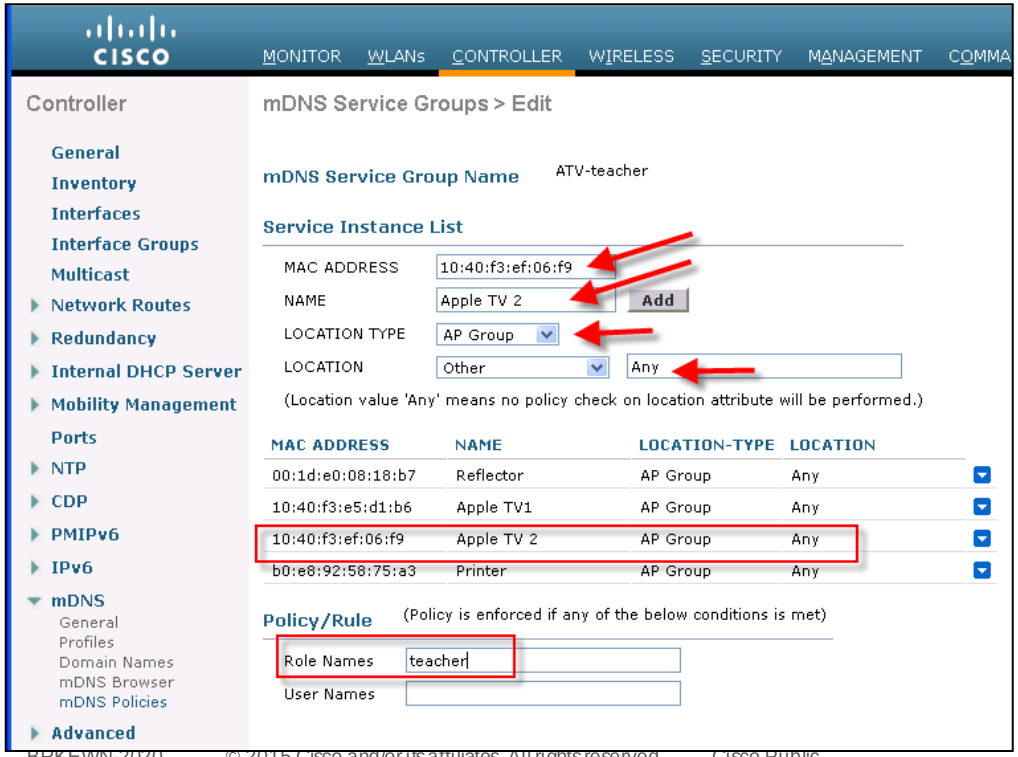
```
(Cisco Controller) >config mdns policy service-group create ?

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

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

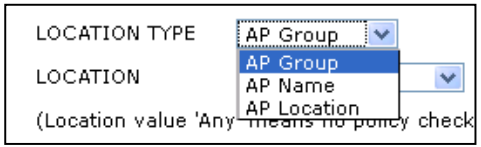


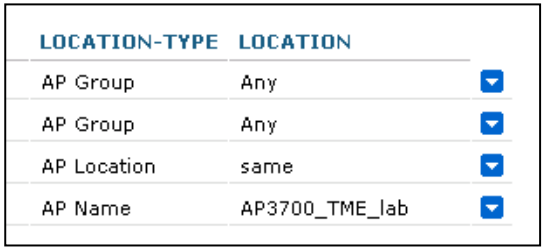
Bonjour Policy Configuration

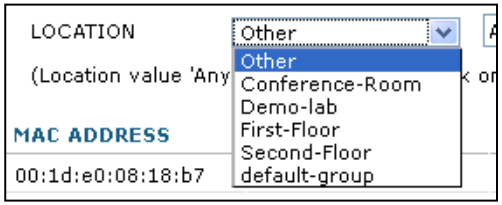
For your reference

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









Cisco live!


CISCO