TOMORROW starts here.

cisco

Cisco live!

Managing the BYOD Evolution

BRKEWN-2020

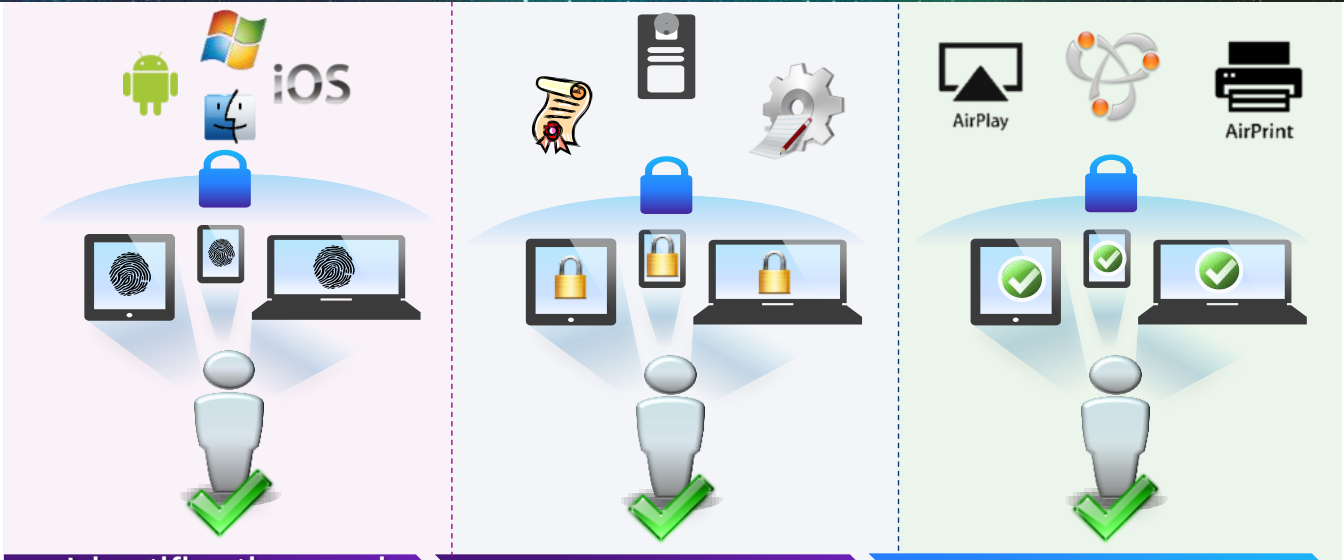
Scott Lee-Guard

Systems Engineer

Cisco live!

Agenda

Managing the BYOD Evolution



Personal Devices on Network

Identification and Security Policy Enforcement

Securely On-Board the Device

Simplified Bonjour Operations

Network Components

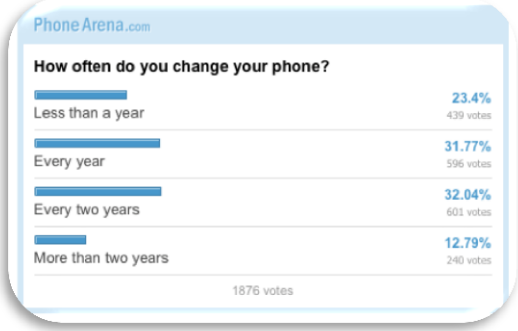
Wireless | Wired | Remote Access | ISE | Prime

Wireless BYOD

Drivers and Assumptions

Drivers

- Majority of new network devices have no wired port
- Users will change devices more frequently than in the past
- Mobile devices have become an extension of our personality
- Guest / Contractor access and accountability has become a mandatory business need



Assumptions

- Guest and Contractors must be isolated and accounted for.
- Users will have 1 wired and 2+ wireless devices moving forward
- The wireless network must be secure and as predictable as the wired network

Cisco Unique BYOD Value Proposition

Enable Any Device, Any Access, Any Policy Through One Network

More Than Just Personal Devices	Device ownership is irrelevant: corporate, personal, guest, etc…
More Than Just Wireless Access	BYO devices need wired, wireless, remote and mobile access
More Than Just iPads	BYO devices can be any device: Windows PCs, Mac OS devices, any tablet, any smartphone, gaming consoles, printers…

Spectrum of BYOD Strategies

Different Deployment Requirements for Different Environments

Cisco WLAN Controller

ISE

Cisco Catalyst Switch

ASA Firewall

Controller only BYOD

Controller + ISE-Wireless BYOD

Controller + ISE-Advanced BYOD

Wireless Only

Basic Profiling and Policy on WLC

Wireless Only

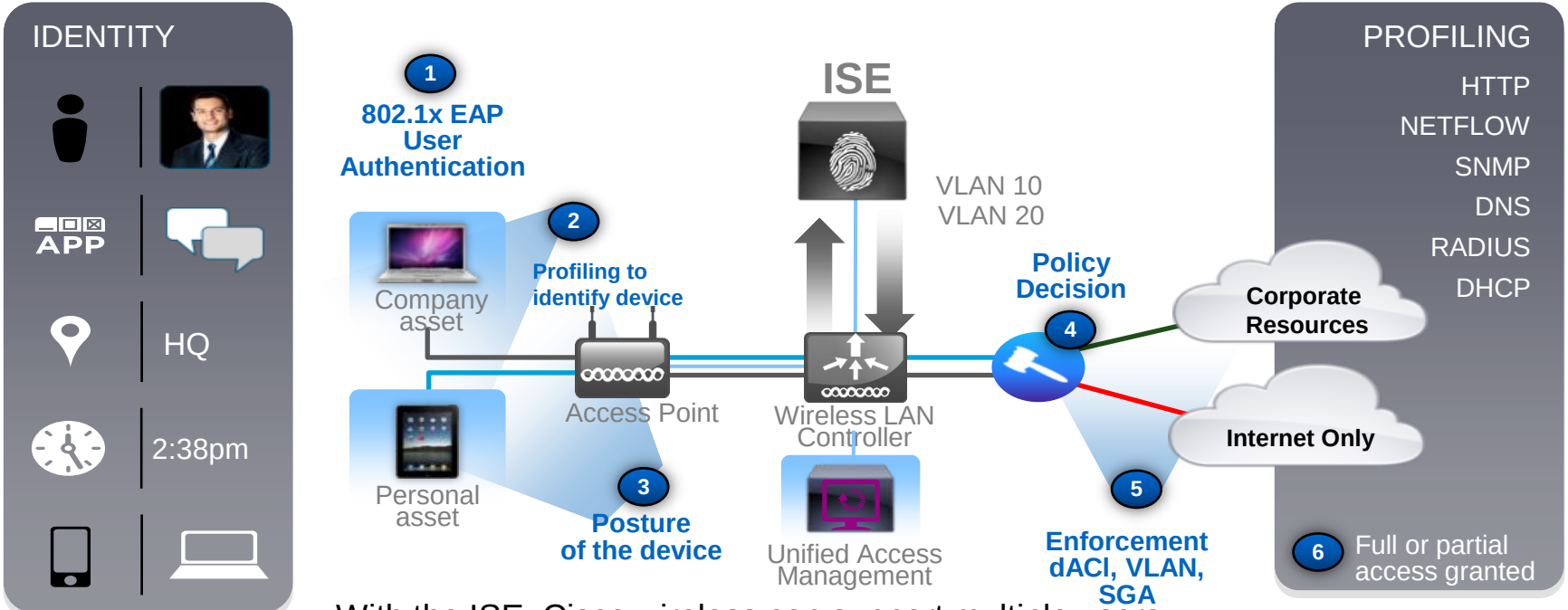
AAA+ Advanced Profiling + Device Posture + Client On-board + Guest + MDM

Wired + Wireless + Remote Access

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

Contextual Policy for BYOD Deployments

Control and Enforcement

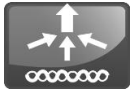


With the ISE, Cisco wireless can support multiple users and device types on a single SSID.

Required Network Components and Versions

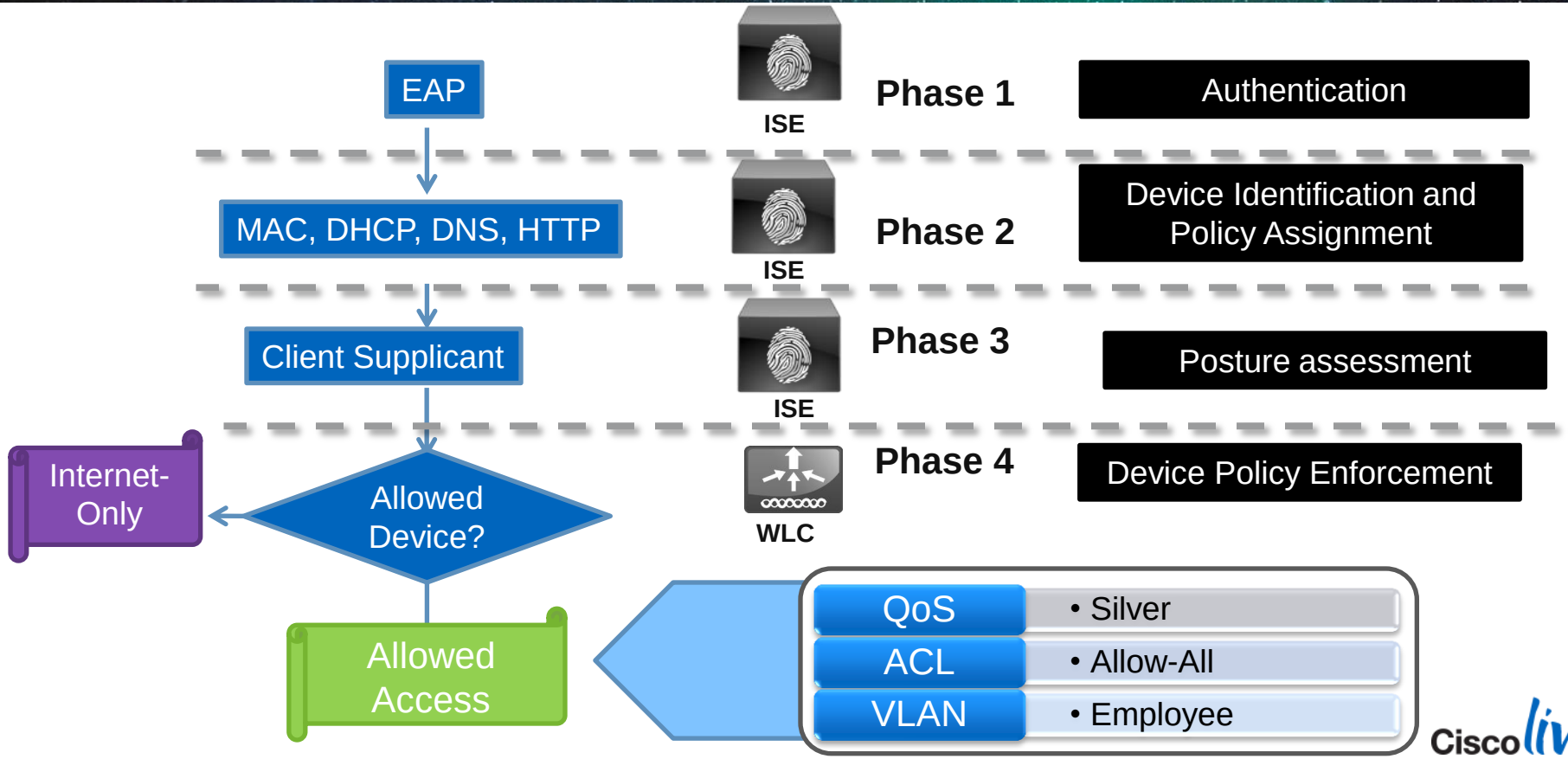
Cisco Wireless LAN and Identity Services Engine

- Cisco Wireless LAN Controller
  - Version 7.0.116 or greater (440X, WiSM1, Flex 7500, 210X or later)
    - Central Switching supported for device profiling and posture assessment.
    - 802.1x WLANs only supported for CoA.
  - Version 7.2.X or greater (5508, WiSM2, Flex 7500, 8500 *(7.3),* 250X or later)
    - Central and FlexConnect switching supported for device profiling and posture assessment.
    - 802.1x and Open (L3 Web authentication) supported for CoA.
  - Version 7.5.X or greater (5508, WiSM2, Flex 7500, 8500 *(7.3)*, 250X or later)
    - Central and Flexconnect Switching for Controller only Profiling and Policy enforcement



- Cisco Identity Services Engine
  - Version 1.1.1 or later
  - Advanced Package License for Profiling and Posture

Cisco BYOD Policy Steps






BYOD Policy Building Blocks: Tools of the Trade

Build BYOD Policy: Flexible Options

Policy Factors

- Access Method
- User Role
- Device Type
- Posture
- Guest Services
- Time
- Authentication
- Active Directory Member (Device or User)

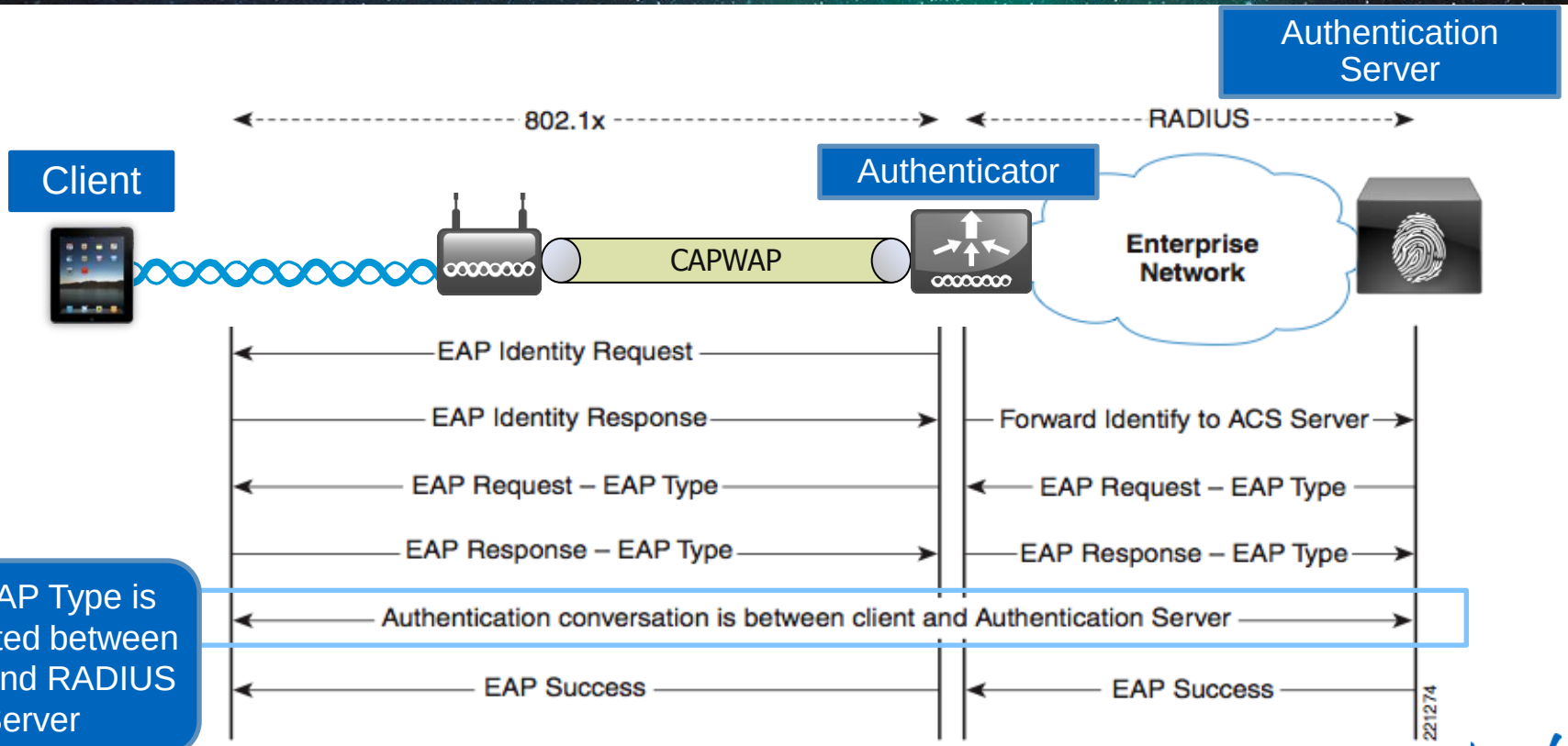
Policy Enforcement

- VLAN
- Access List
- Blackhole-URL
- QoS
- Session Timeout
- Client On-Board
- Login-URL
- dACL
- SGA
- Posture Remediation

Policy Management

- MyDevices Portal
- Reporting
- MDM Integration

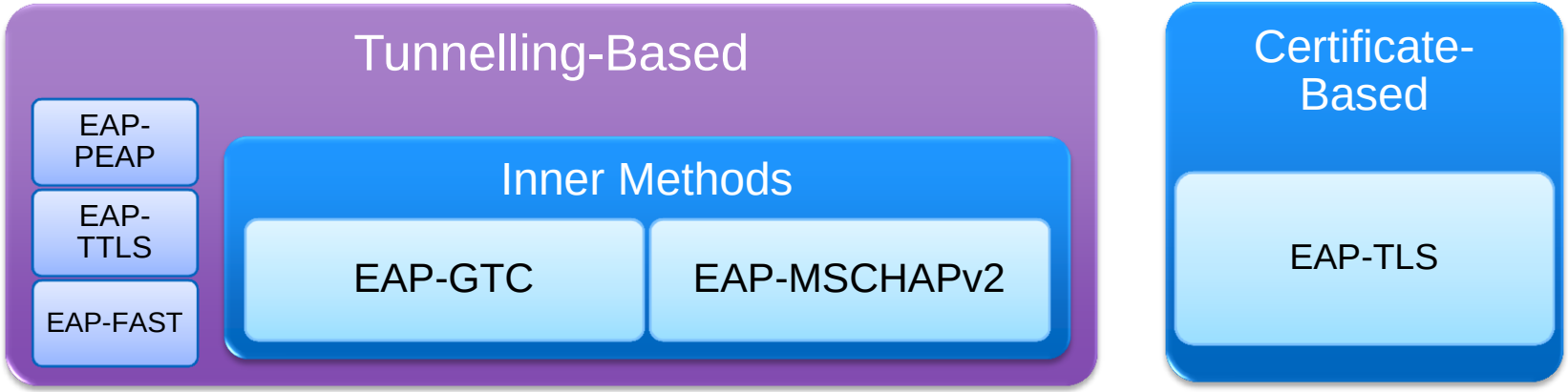
Extensible Authentication Protocol (EAP) — Protocol Flow



The EAP Type is negotiated between Client and RADIUS Server

EAP Authentication Types

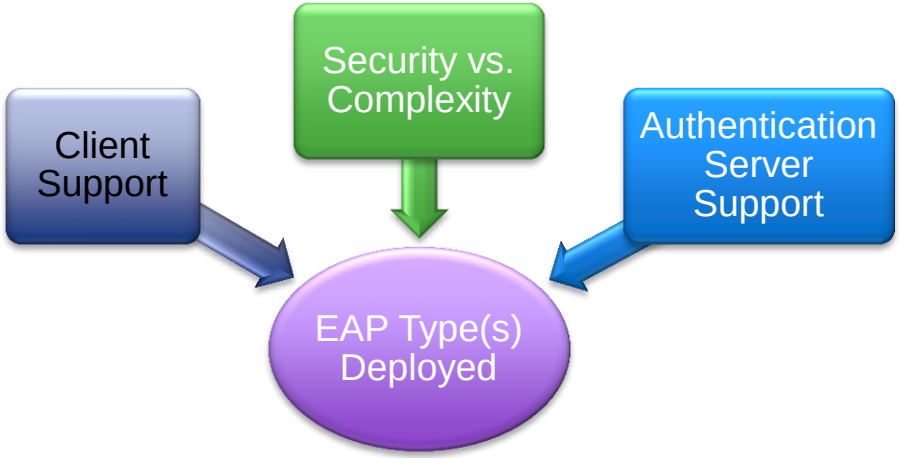
Different Authentication Options Leveraging Different Credentials



- 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.

Factors in Choosing an EAP Method

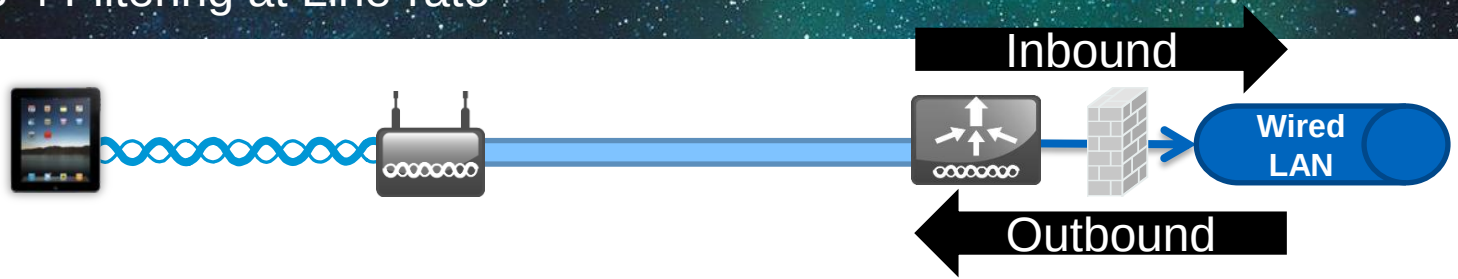
The Most Common EAP Types are PEAP and EAP-TLS



- Most clients support EAP-TLS, PEAP (MS-CHAPv2).
  - Additional supplicants can add more EAP types (Cisco AnyConnect).
- Certain EAP types can be more difficult to deploy.
- Cisco ISE Supplicant Provisioning can aid deployment.

Cisco Wireless LAN Controller ACLs

Layer 3-4 Filtering at Line-rate



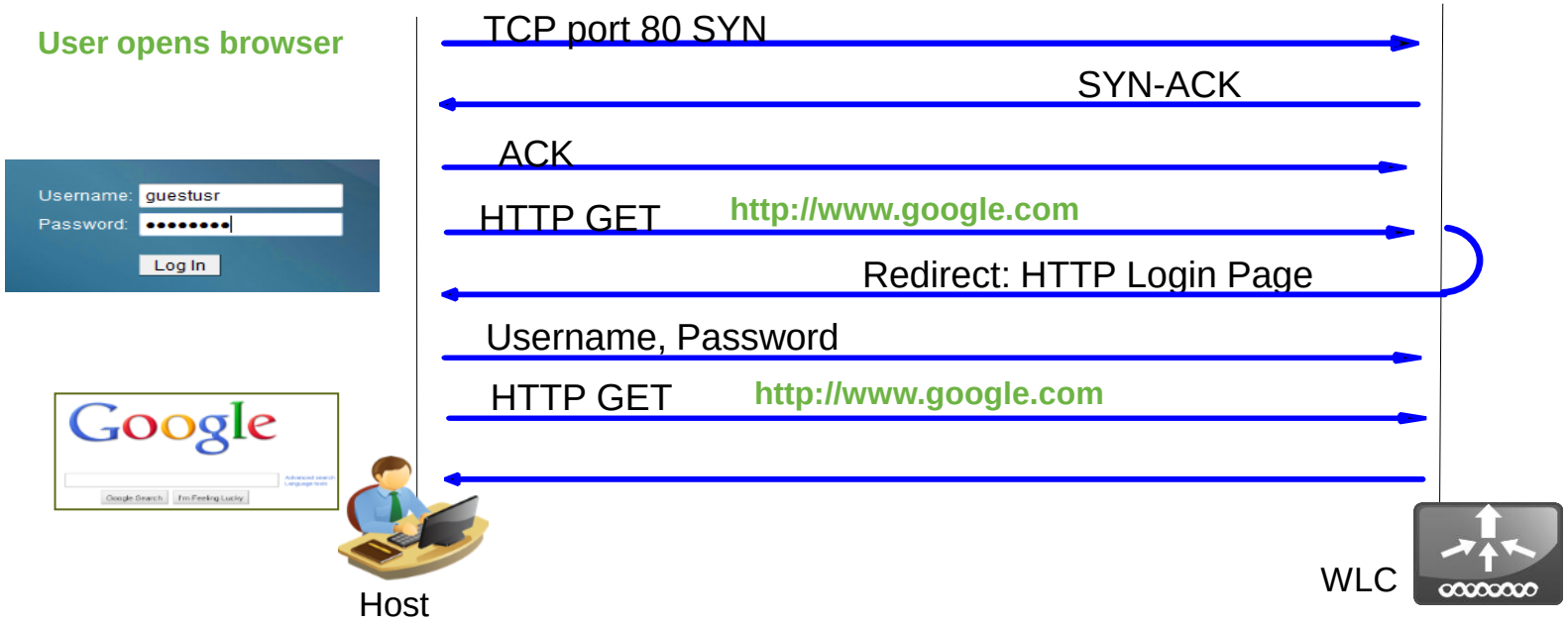
- ACLs provide L3-L4 policy and can be applied per interface or per user.
- Cisco 2500, 5508 and WiSM2 implement hardware, line-rate ACLs.
- Up to 64 rules can be configured per ACL.

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

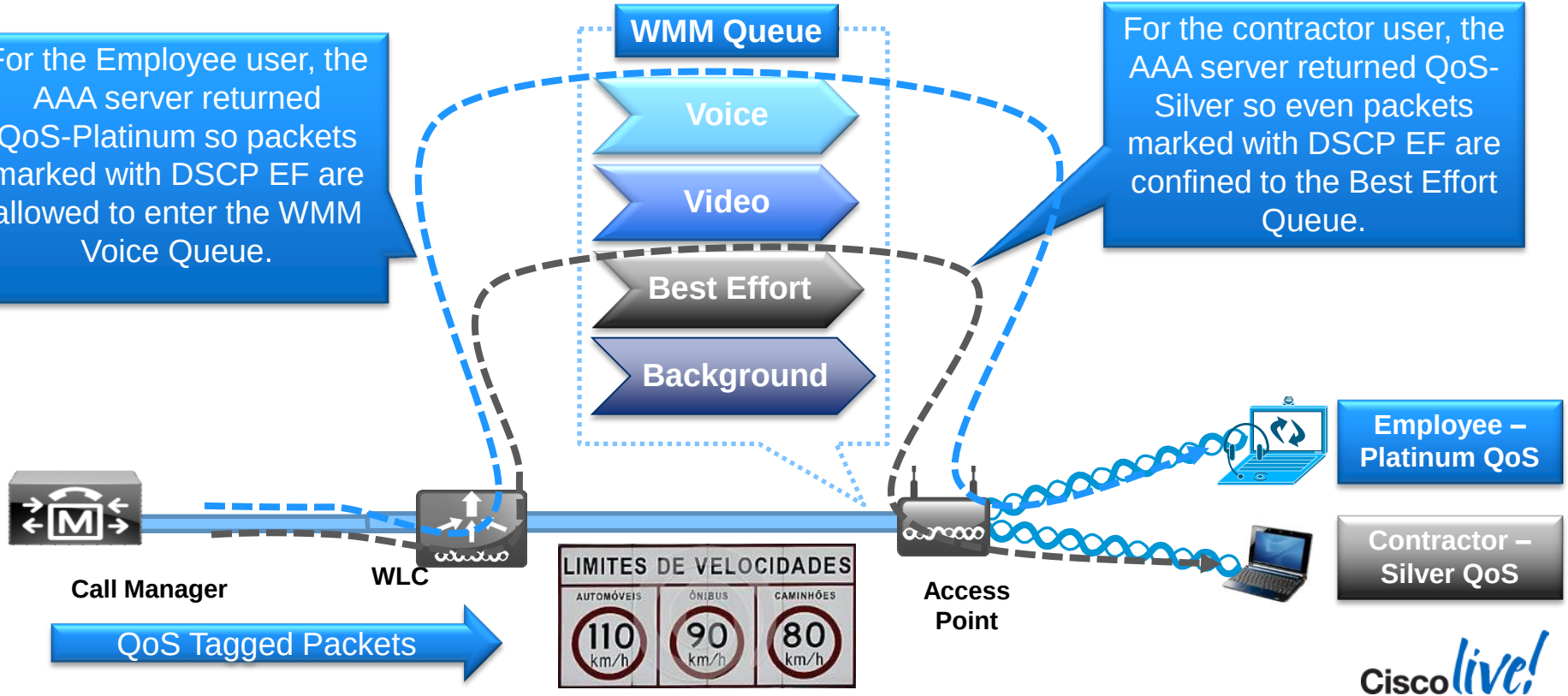


Cisco Wireless User-Based QoS Capabilities

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

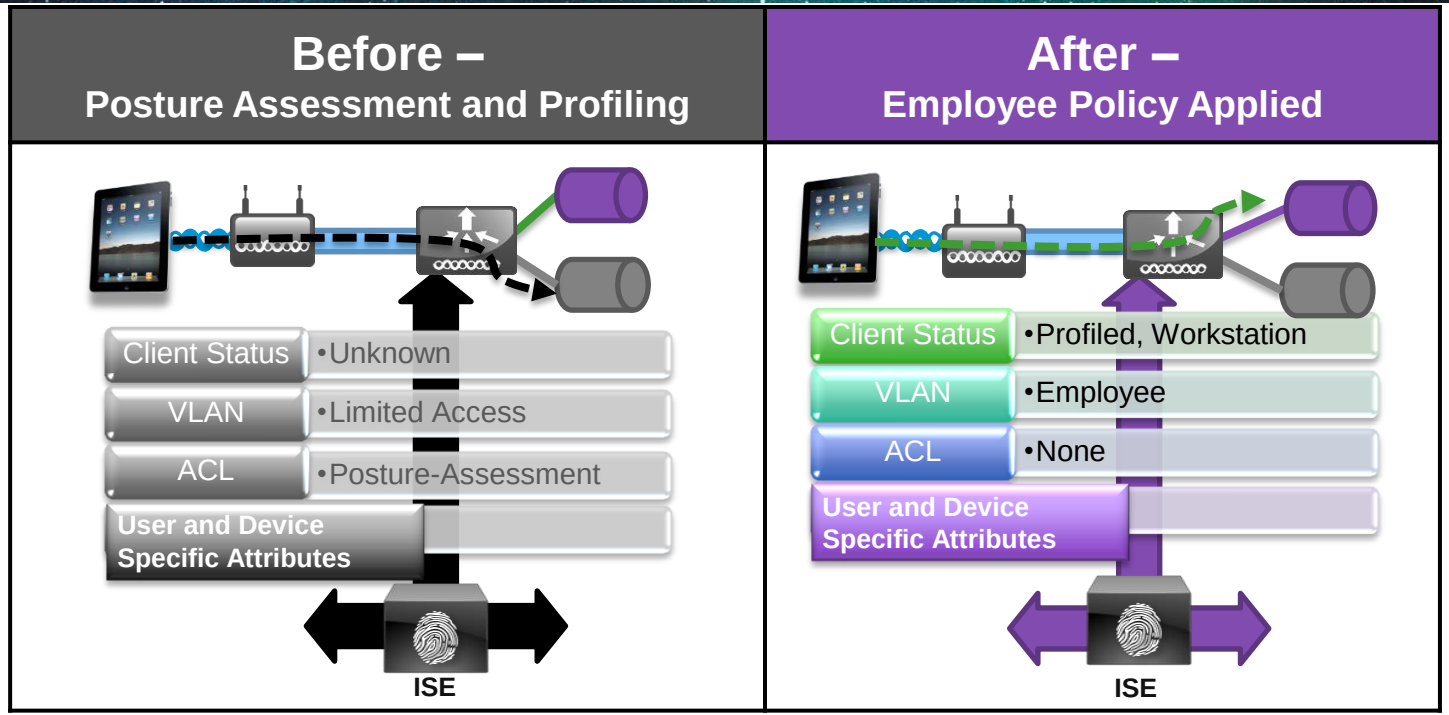
For the Employee user, the AAA server returned QoS-Platinum so packets marked with DSCP EF are allowed to enter the WMM Voice Queue.

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



Change of Authorisation (CoA)

Changing Connection Policy Attributes Dynamically

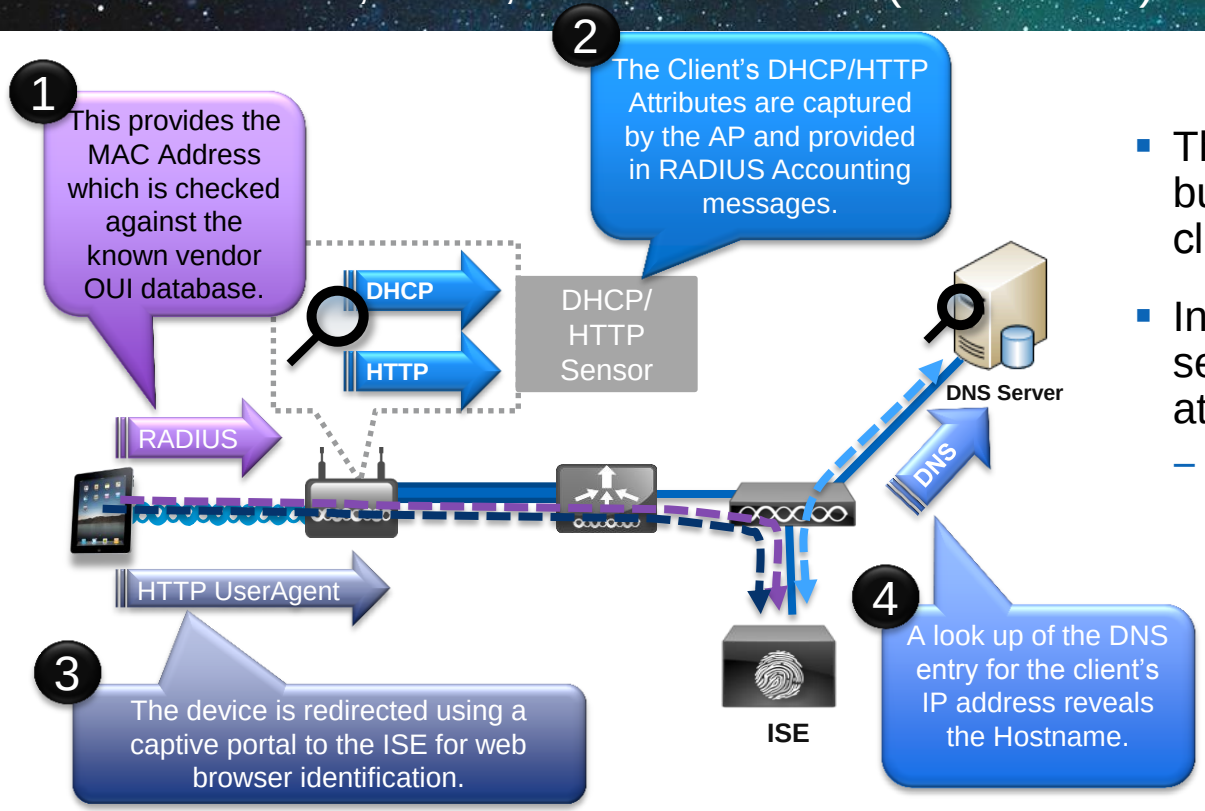





Profiling with ISE

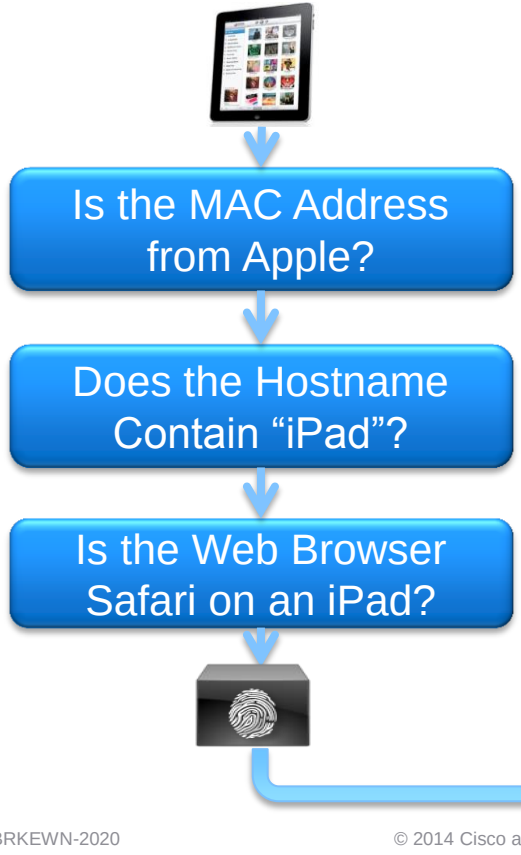
Client Attributes Used for ISE Profiling

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

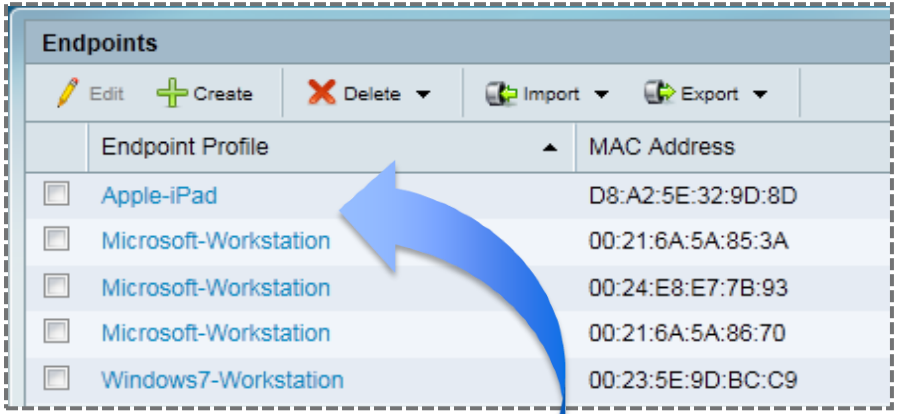


- The ISE uses multiple attributes to build a complete picture of the end client's device profile.
- Information is collected from sensors which capture different attributes
  - The ISE can even kick off an NMAP scan of the host IP to determine more details.

ISE Device Profiling Example - iPad



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



ISE Device Profiling Capabilities

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

- Profiling Policies
  - Android
  - Apple-Device
    - Apple-MacBook
    - Apple-iDevice
    - Apple-iPad
    - Apple-iPhone
    - Apple-iPod
  - Applera-Device
  - Aruba-Device
  - Avaya-Device
  - BlackBerry
  - Samsung-Device
  - SonyPS3
  - SymbianOS-Device
  - VMWare-Device
  - Workstation
    - FreeBSD-Workstation
    - Linux-Workstation
    - Macintosh-Workstation
    - Microsoft-Workstation
    - OpenBSD-Workstation
    - Sun-Workstation

Smart Phones

Gaming Consoles

Workstations

Profiler Policy

* Name	Apple-iPad
Description	
Policy Enabled	☑
* Minimum Certainty Factor	20
* Exception Action	NONE
* Network Scan (NMAP) Action	NONE
Create Matching Identity Group	○
Use Hierarchy	◉
* Parent Policy	Apple-Device

Rules

If Condition	Apple-iPadRule2Check2	Then
If Condition	(Apple-iPadRule1Check1_AND_Apple-MacBook...	

1 Minimum Confidence for a Match

2 Multiple Rules to Establish Confidence Level




Defining a Security Policy Within ISE

Steps for Configuring ISE Policies

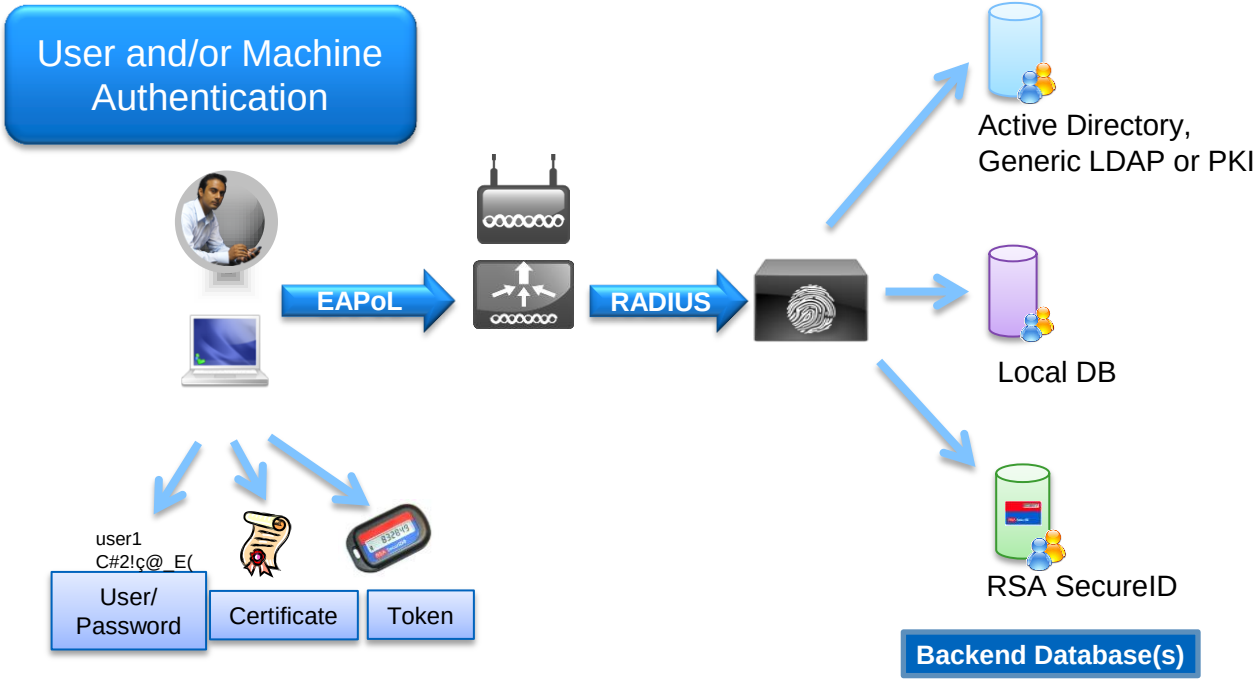
1. Authentication Rules

- Define what identity stores to reference.
  - Example – Active Directory, CA Server or Internal DB.

2. Authorisation Rules

- Define what users and devices get access to resources.
  - Example – All Employees, with Windows Laptops have full access.

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

Example for PEAP and EAP-TLS

Identity Services Engine

Home | Operations | Policy | Administr

Authentication | Authorization | Prof

Authentication Policy

Define the Authentication Policy by selecting the protocols

Policy Type: Simple / Rule-Based

Wireless	: If	Wireless_802.1X	allow protocols	Allowed Protoco : Default Networ	and...
PEAP	: if	Network Access:EapTunnel EQUAI	use	ActiveDirectory	
TLS	: if	Network Access:EapAuthenticati...	use	Cert_Auth	

Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

* Domain Name: corpdemo.net

* Identity Store Name: ActiveDirectory

One or more nodes may be selected for Jo leave operations. If a node is join operation is required befo join. Selec Connection

Join | Leave

ISE Node

ise

1 Reference Active Directory for PEAP Authentication

Certificate Authentication Profiles List > Cert_Auth

Certificate Authentication Profile

* Name: Cert_Auth

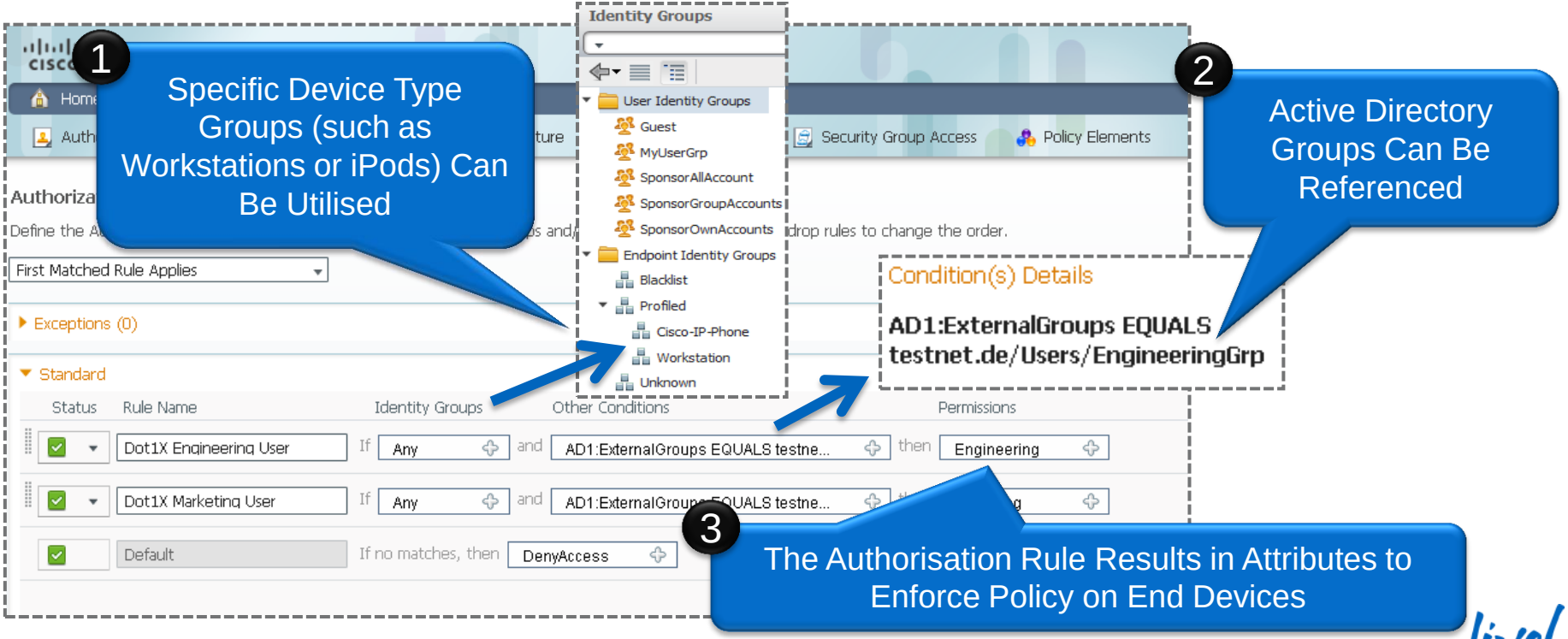
Description:

Principal Username X509 Attribute: Common Name

2 Create Another Profile to Reference the Certificate Store

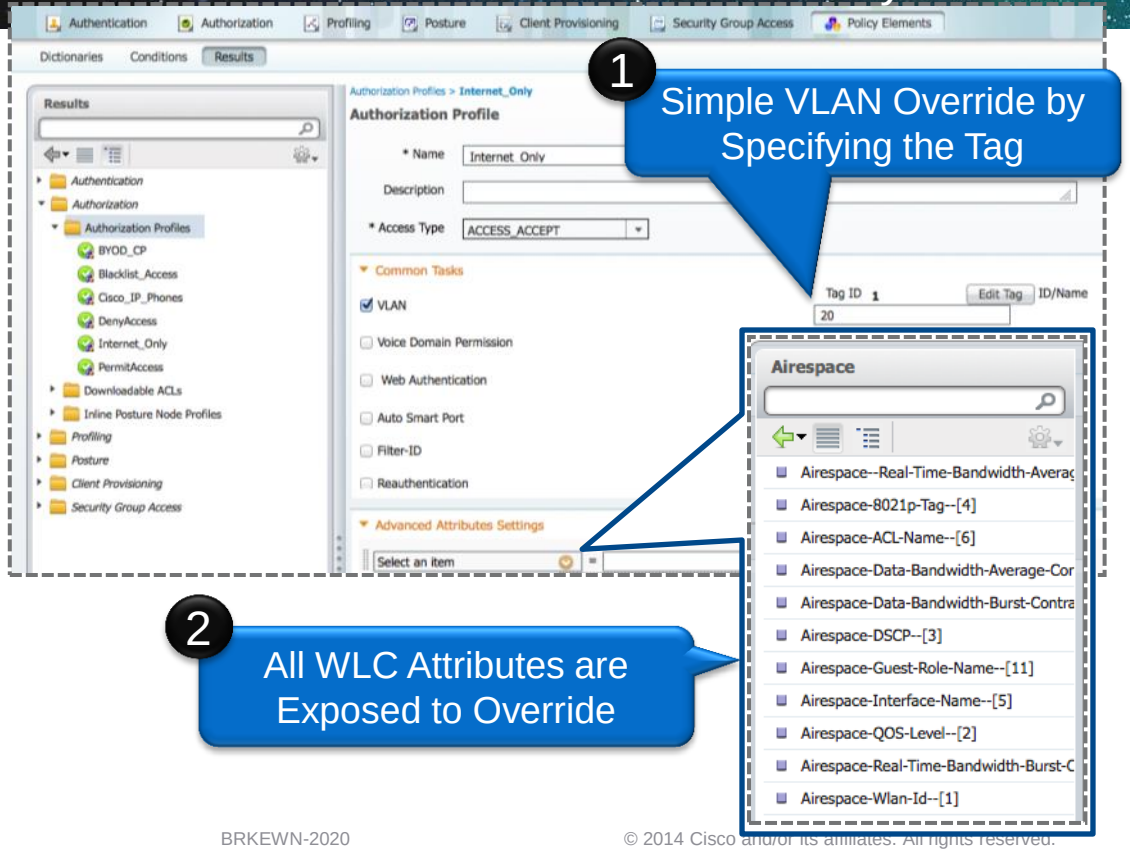
Authorisation Rules Configuration

Flexible Conditions Connecting Both User and Device



Authorisation Rule "Results"

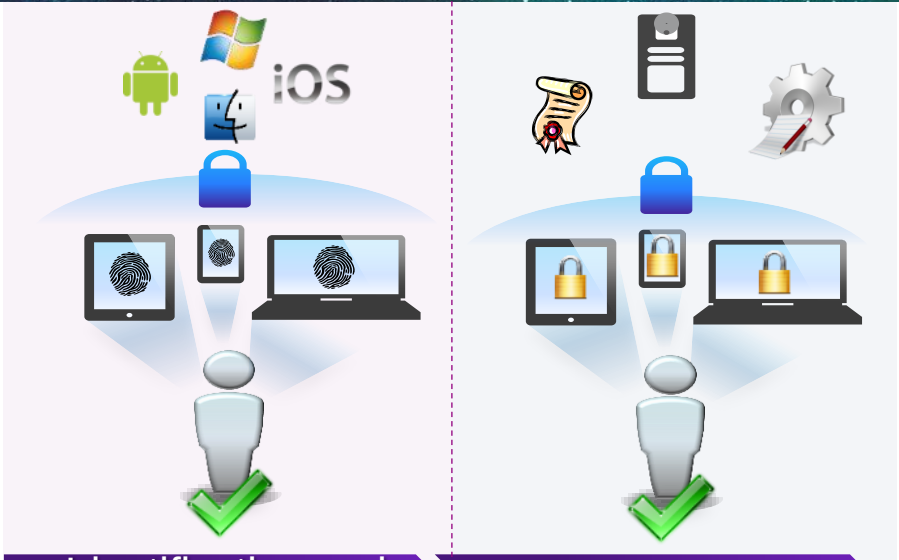
The Actual Permissions Referenced by the Authorisation Rules



- The authorisation rules provide a set of conditions to select an authorisation profile.
- The profile contains all of the connection attributes including VLAN, ACL and QoS.
- These attributes are sent to the controller for enforcement, and they can be changed at a later time using CoA (Change of Authorisation).

Agenda

Managing the BYOD Evolution



Personal Devices on Network

Identification and Security Policy Enforcement

Securely On-Board the Device

Network Components

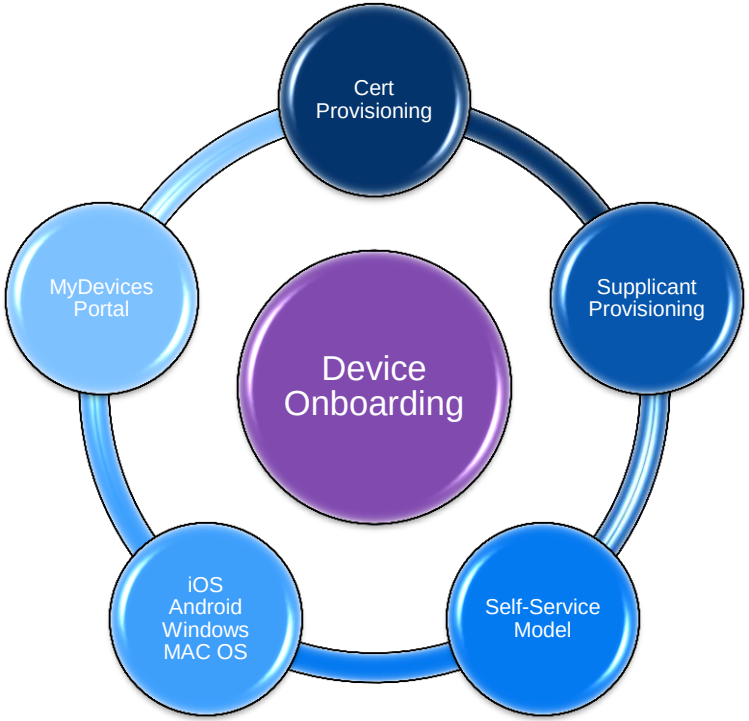
Wireless | Wired | Remote Access | ISE | Prime




BYOD Device Provisioning

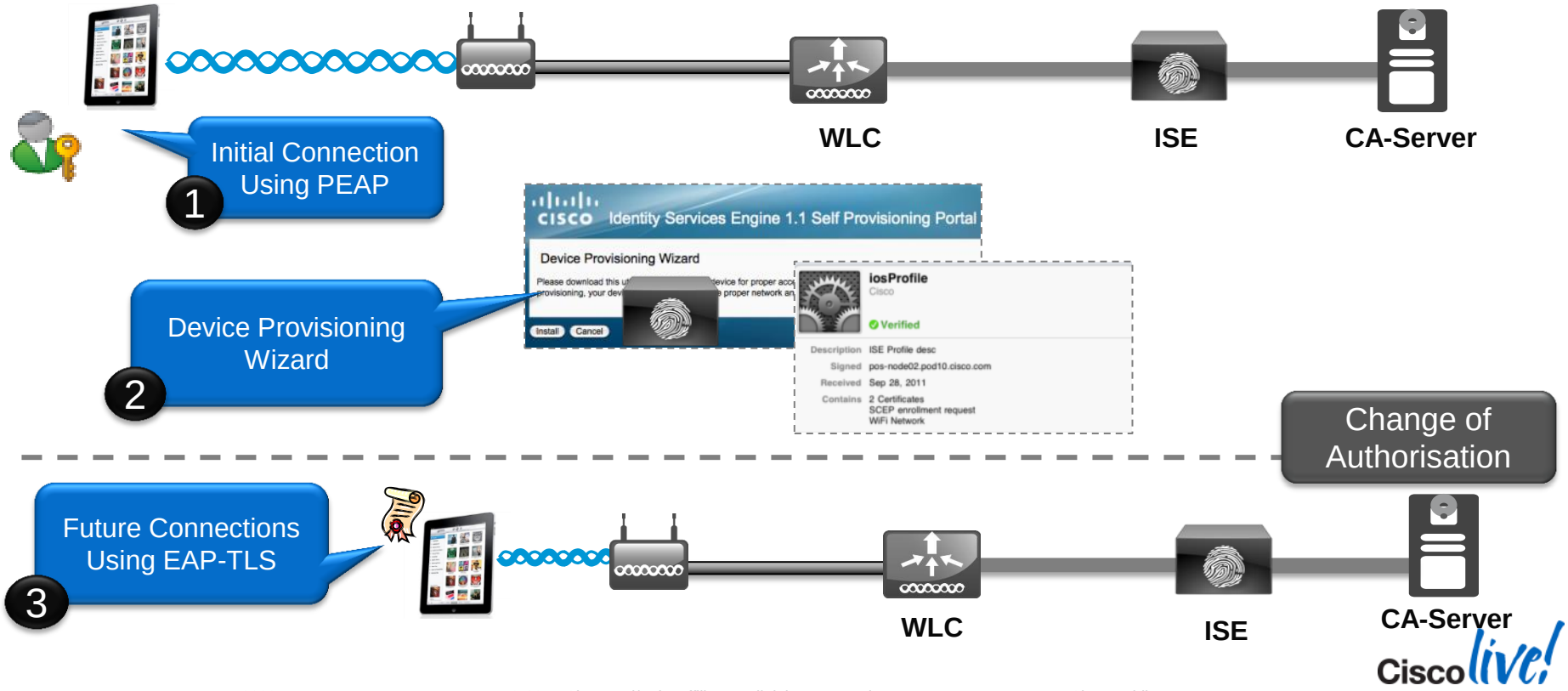
ISE BYOD Release

Identity Services Engine 1.1.1



- 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



Apple Captive Network Assistant (CNA)

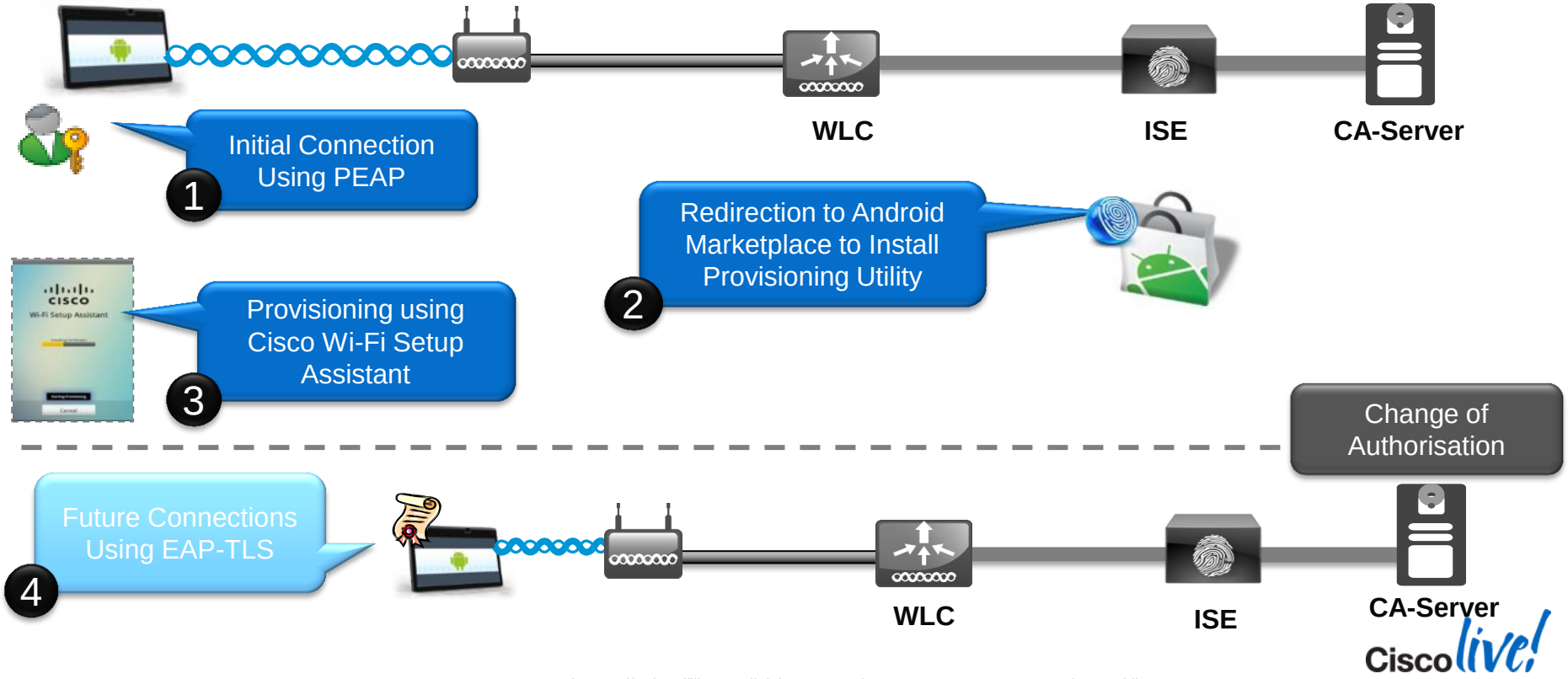
- Prior to iOS7, Apple iOS and current Mac OS X attempt to discover public Internet access using a crafted URL:
  - http://www.apple.com/library/test/success.html

- 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

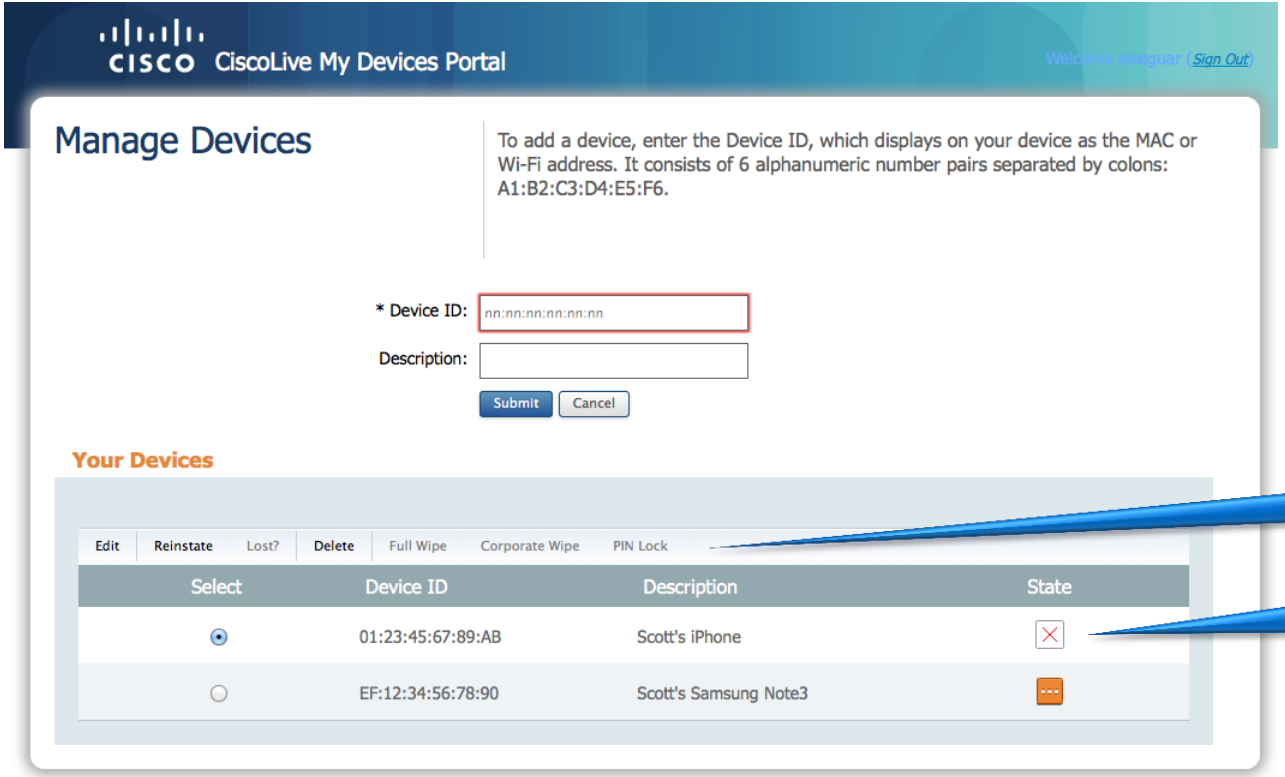


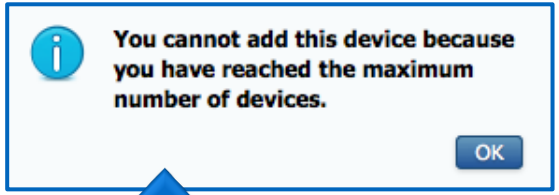
DNS-based ACLs

- 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
  - AP1130 / AP1240 do not support this feature

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




Native Profiling and Policy on WLC

Build BYOD Policy: Flexible Options

Policy Factors

- Access Method
- User Role
- Device Type
- Posture
- Guest Services
- Time
- Authentication
- Active Directory Member (Device or User)

Policy Enforcement

- VLAN
- Access List
- Blackhole-URL
- QoS
- Session Timeout
- Client On-Board
- Login-URL
- dACL
- SGA
- Posture Remediation

Policy Management

- MyDevices Portal
- Reporting
- MDM Integration

Build BYOD Policy: Flexible Options

Native Profiling & Policy on WLC

Policy Factors

- Access Method
- User Role
- Device Type
- Time
- Authentication

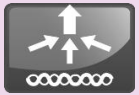
Policy Enforcement

- VLAN
- Access List
- QoS
- Session Timeout

Build BYOD Policy: Flexible Options

Native Profiling & Policy on WLC

Network Components



WLC

Radius Server
(eg. ISE Base, ACS)

Only Wireless

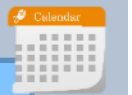
Factors

User Role

Device Type

Authentication

Time of Day

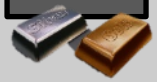


Policy Enforced

VLAN

Access List

QoS



Session Timeout

Configuring User-Role

User Role

Radius

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = role=User-Role

role=Employee

role=Contractor

Controller

MONITOR WLANs CONTROLLER WIRELESS SECURITY

Local Policies

Policy > Edit

Match Criteria

Match Role String User-Role

Employee

Contractor

Privilege

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

Step 3

88 Pre-Defined Device Signature

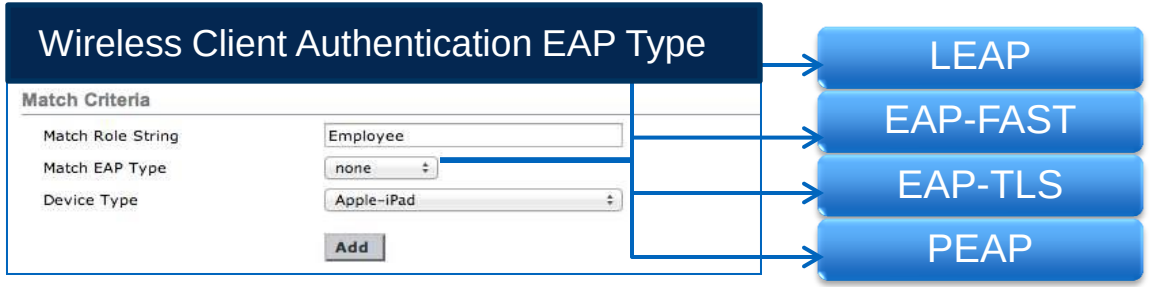
Clients — Entries 1 - 3 of 3

Current Filter: None [Change Filter] [Clear Filter]

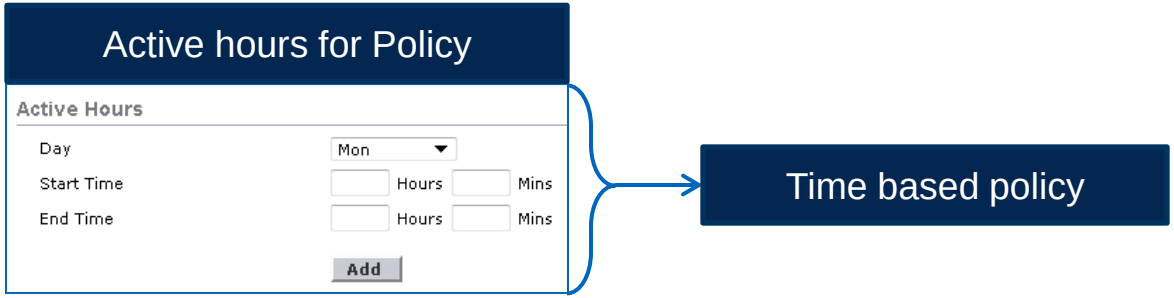
Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	WGB	Device Type
00:27:10:d3:a3:c0	AP2600	Demo-Employee	Demo-Employee	No	Windows7-Works
40:fc:89:75:64:43	AP2600	Demo-Employee	Demo-Employee	No	Android
70:de:e2:0e:ce:0	AP2600	Demo-Employee	Demo-Employee	No	Apple-iPad

Native Profiling Authentication and Time Policy

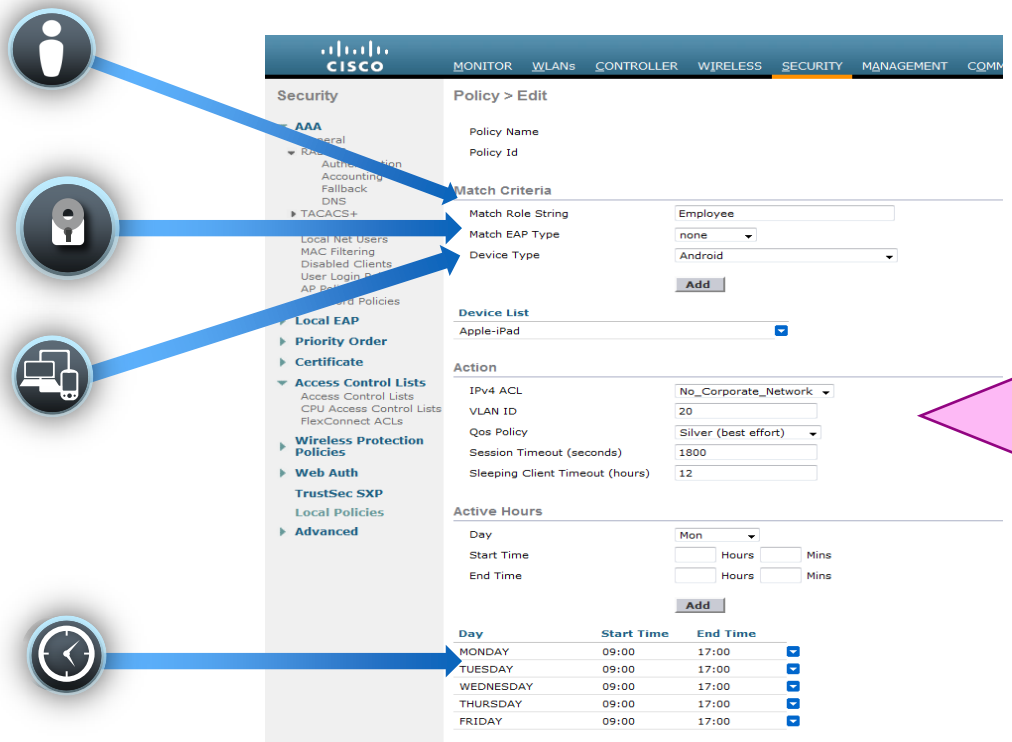
Authentication

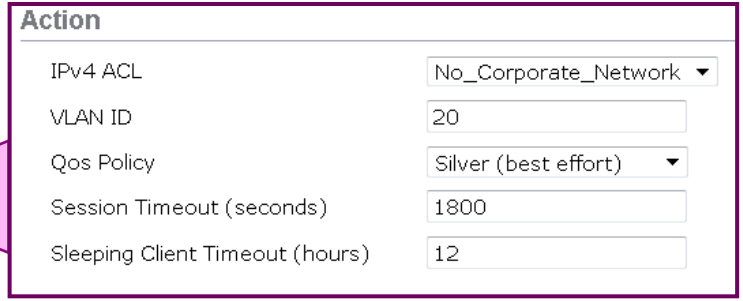


Time of Day



Enforce Policy on the WLC





Apply Policy per WLAN / AP Group

Native Profiling 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 Profiling per AP Group

Ap Groups > Edit 'Conference-Room-1'

General | WLANs | RF Profile | APs | 802.11u

Add New

WLAN ID	WLAN SSID[2]	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

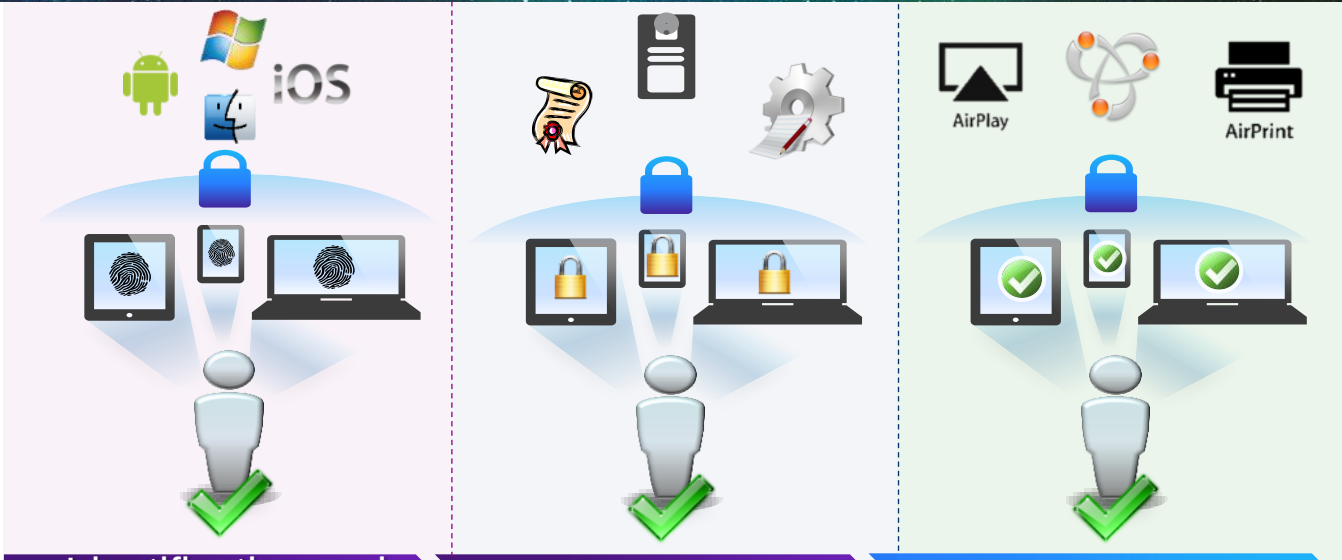
Priority Index	Local Policy Name
1	iPad-Policy
2	Android-Policy
3	iPhone-Policy
4	MacBook-Policy

Restriction: First Matched Rule Applies

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

Agenda

Managing the BYOD Evolution



Personal Devices on Network

Identification and Security Policy Enforcement

Securely On-Board the Device

Simplified Bonjour Operations

Network Components

Wireless | Wired | Remote Access | ISE | Prime

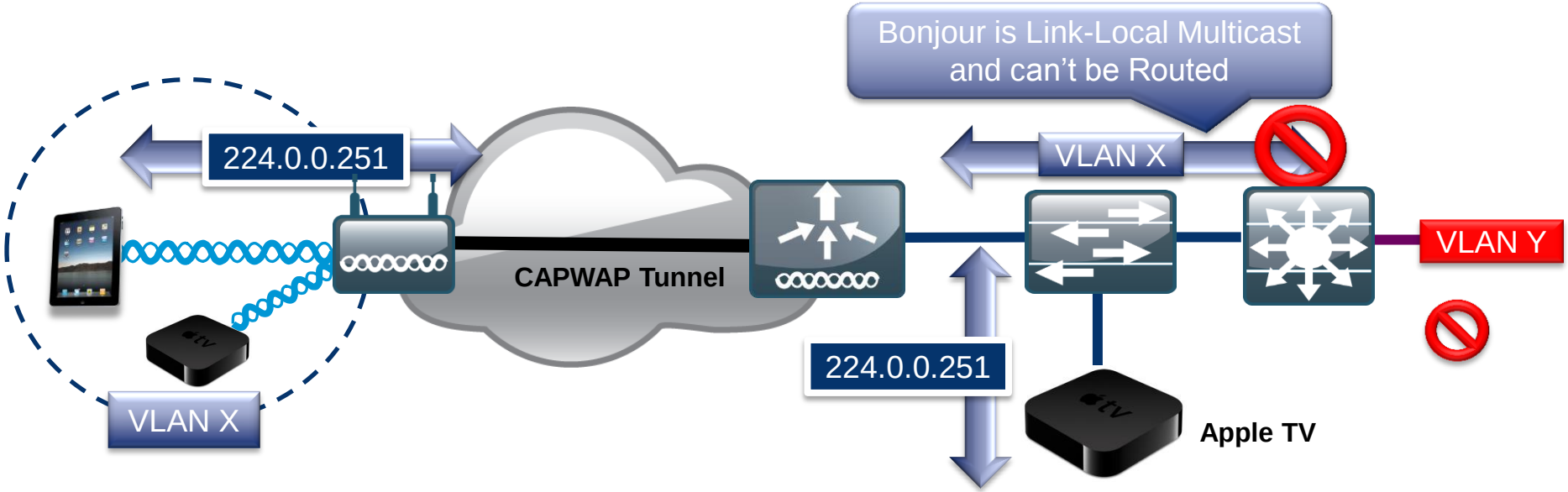



Bonjour Gateway on Cisco Wireless

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

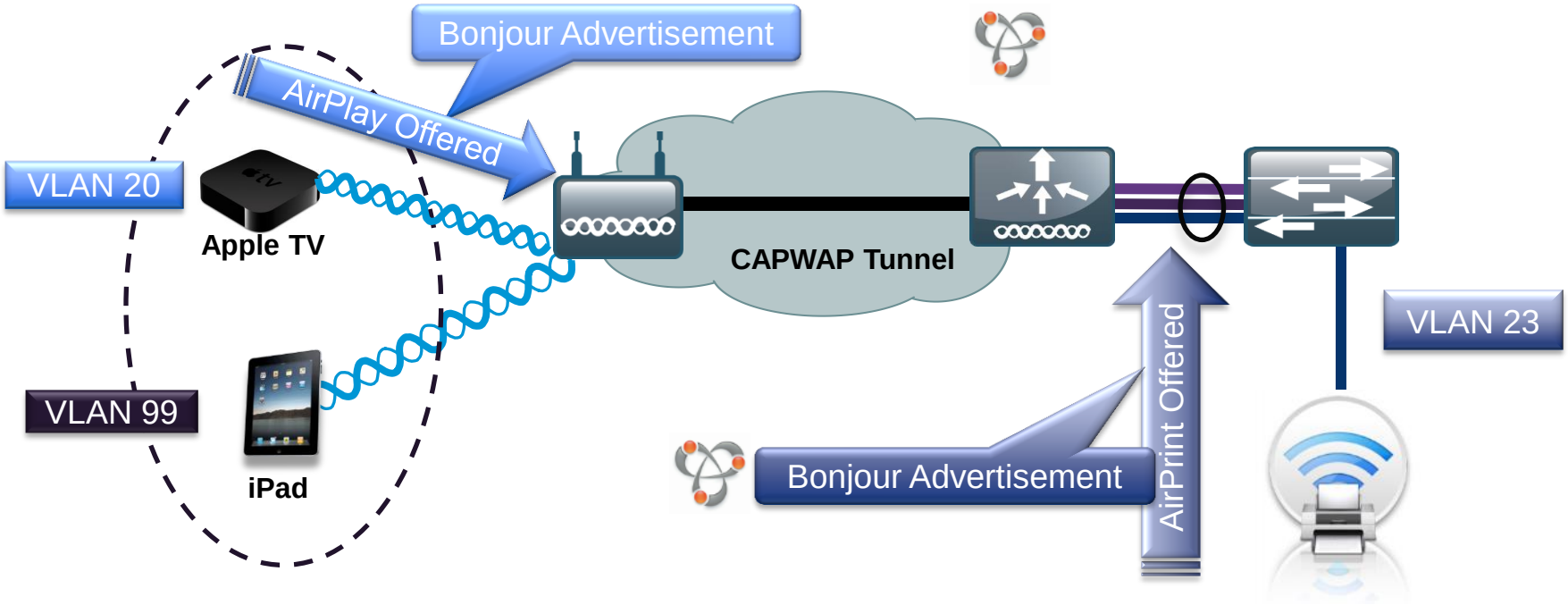


- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:

  IPv4 Group Address – 224.0.0.251

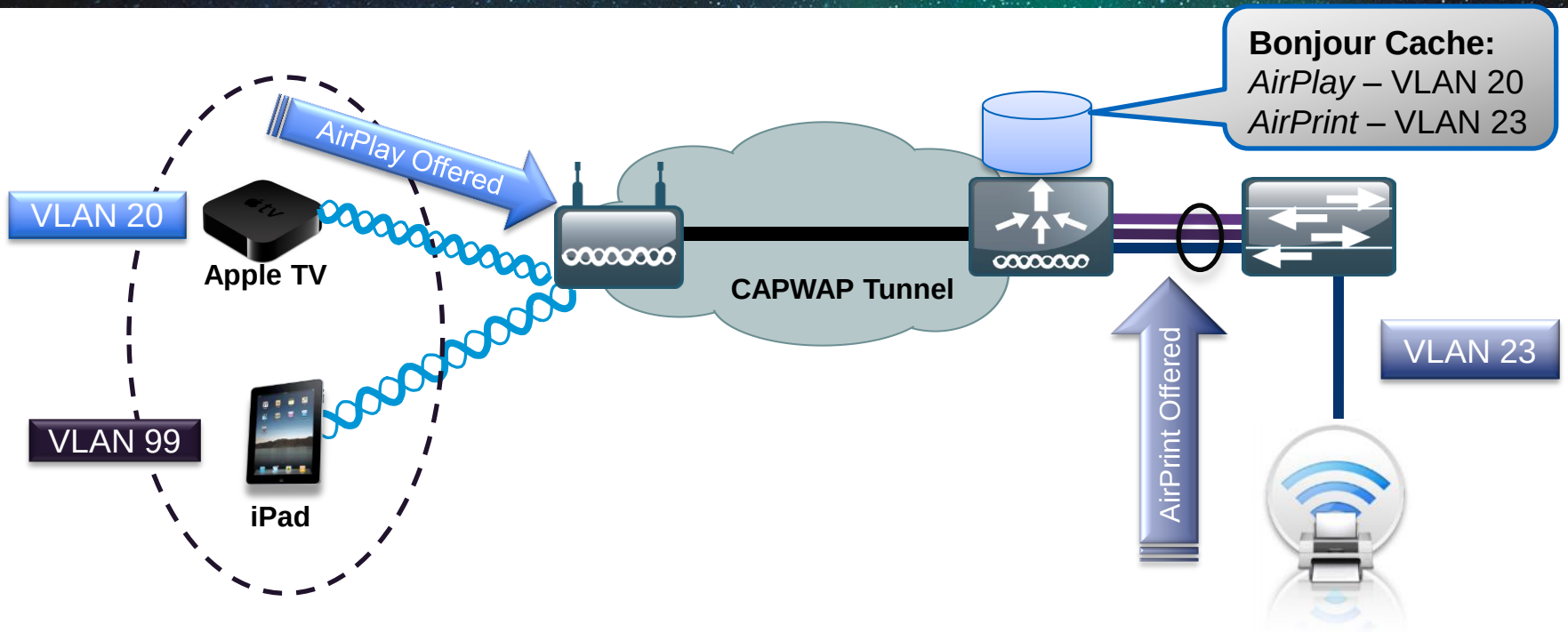
  IPv6 Group Address – FF02::FB

Bonjour mDNS Gateway on Cisco WLC



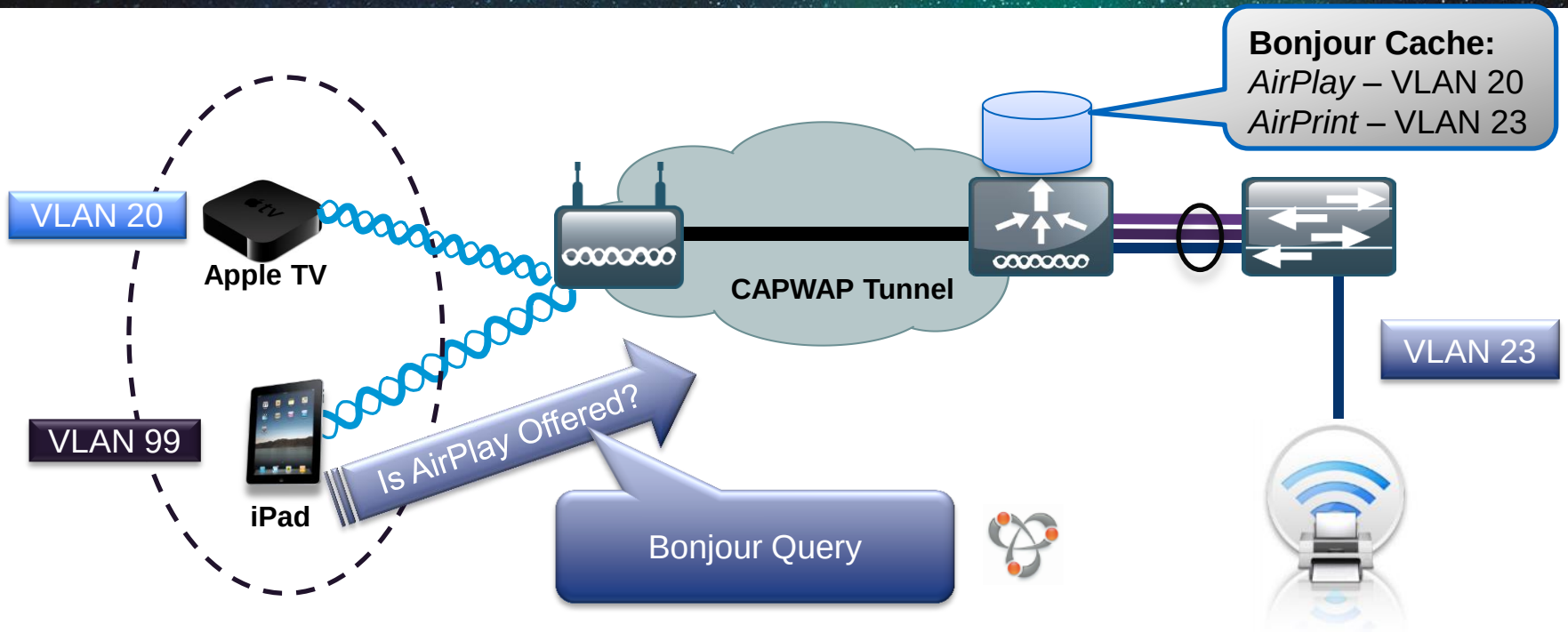
- Step 1 – Listen for Bonjour Services

Bonjour mDNS Gateway on Cisco WLC



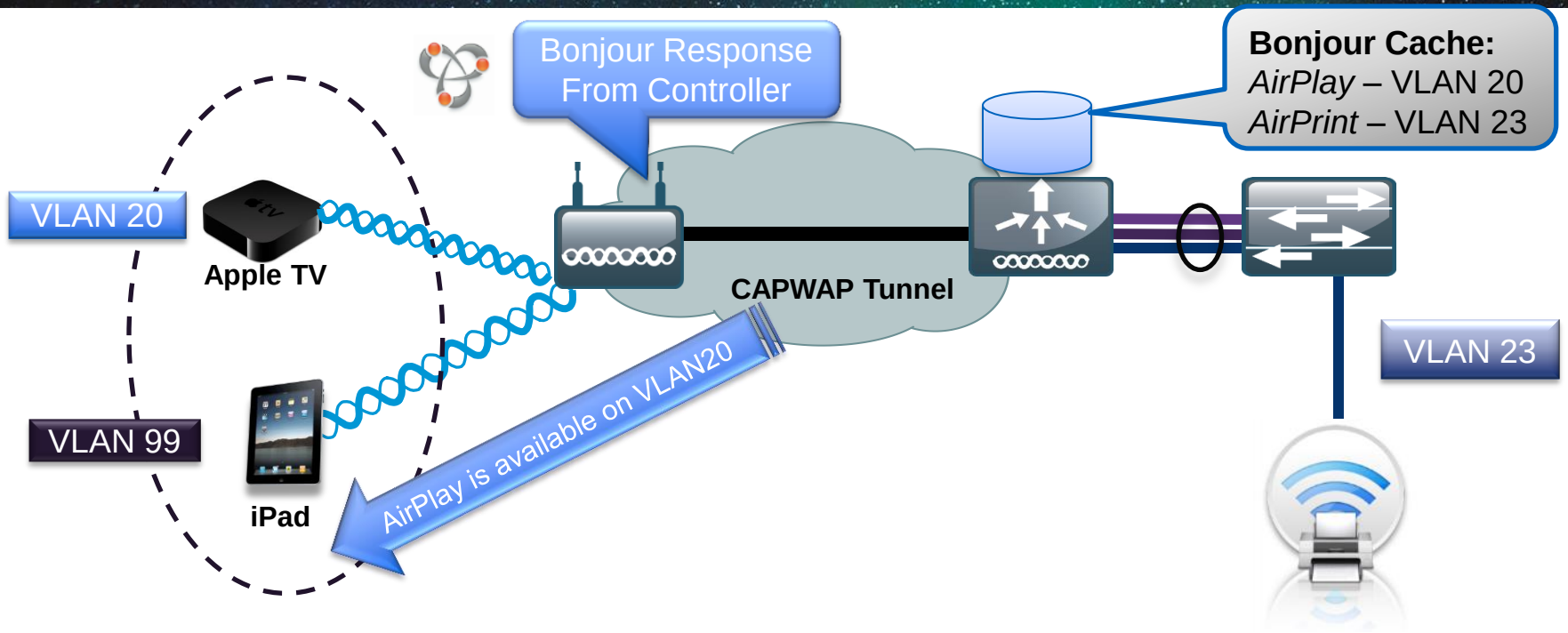
- Step 2 –Bonjour Services cached on the controller

Bonjour mDNS Gateway on Cisco WLC



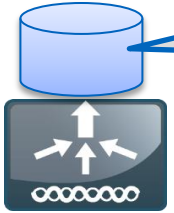
- Step 3 –Listen for Client Service Queries for Services

Bonjour mDNS Gateway on Cisco WLC



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

Bonjour Traffic Optimisation



Bonjour Cache:
AirPrint – VLAN 23
Airplay – VLAN 20

6400 Entries per Controller

Reason for Traffic optimisation

Bonjour Service query is cached on Controller

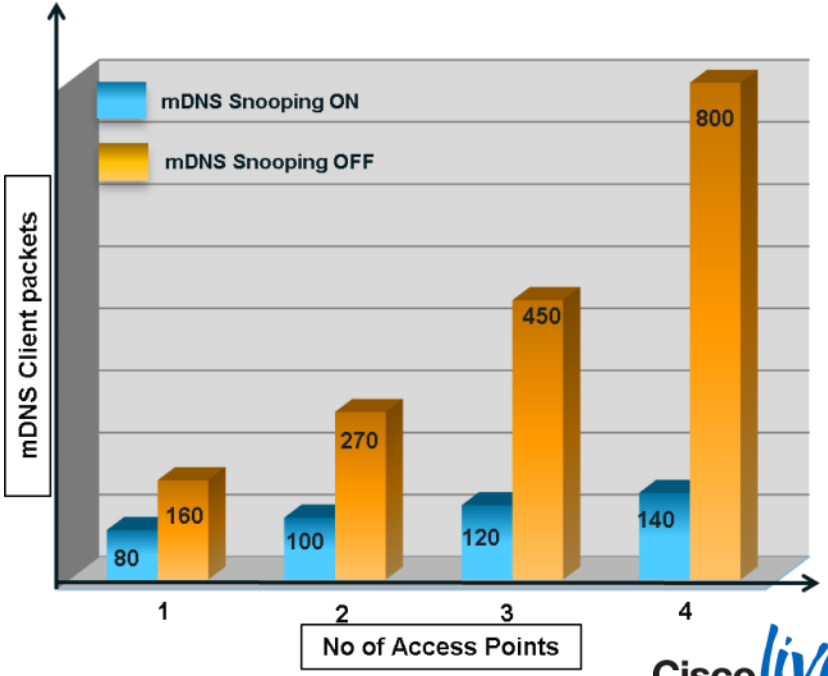
- ✓ Not forwarded

Bonjour Client Query

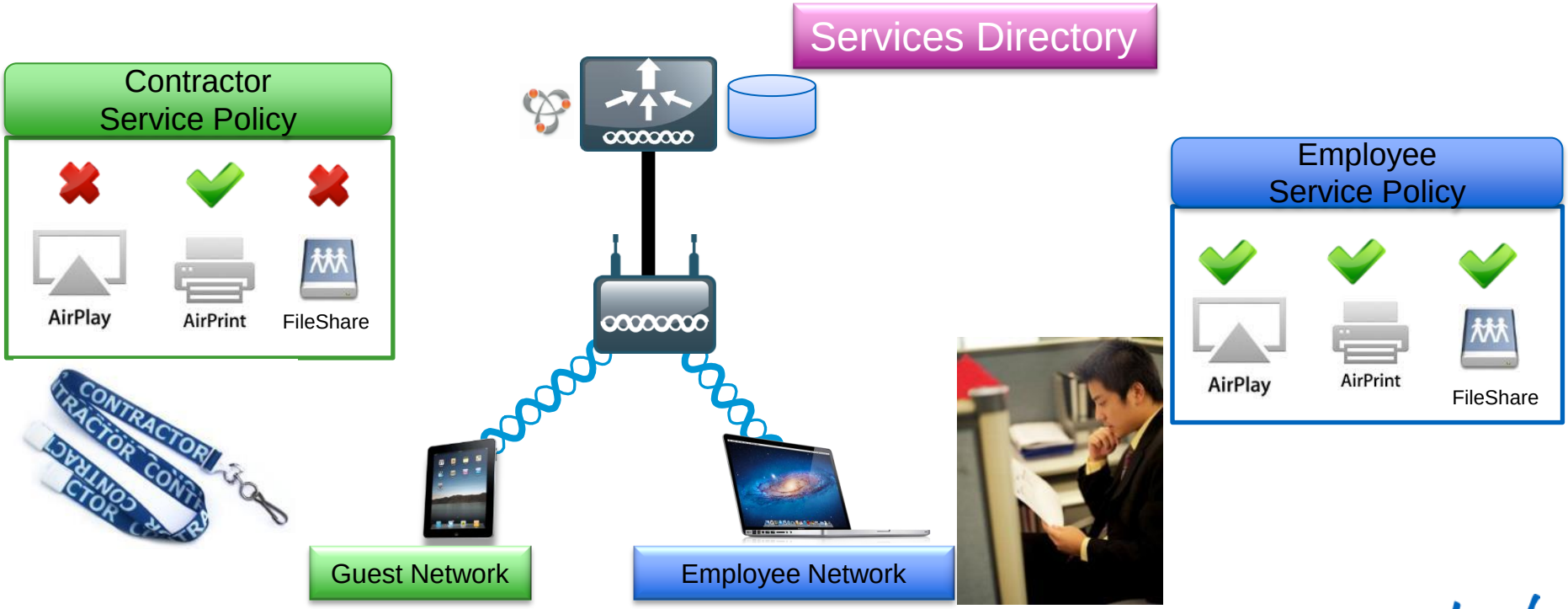
- ✓ Unicast Response
- ✓ Not forwarded

80% less Bonjour Traffic*

* For 4 Access Point Deployment



Filter Services by User Group



Common Bonjour Services

AirPlay

Airplay Services = 4

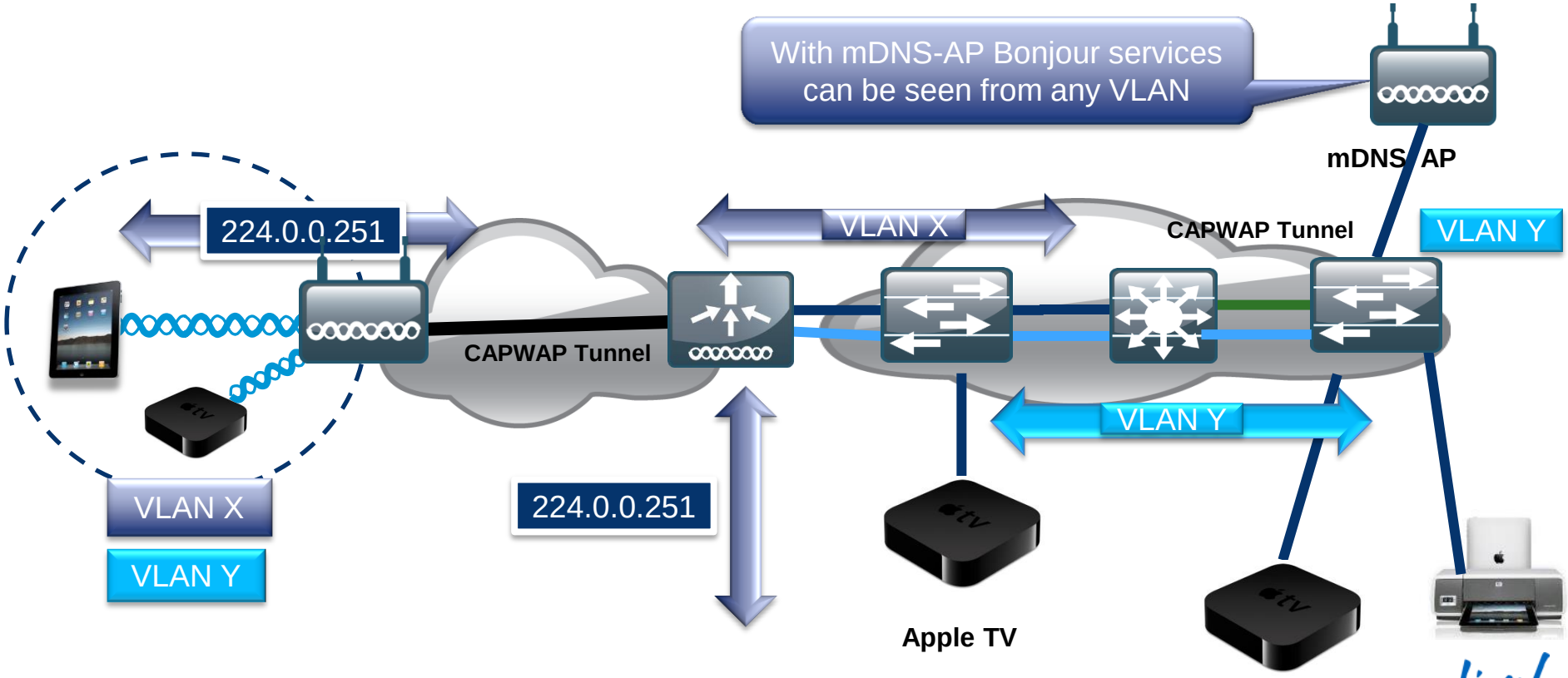
- Airplay for iOS *(_airplay._tcp)*
- Airplay for Mac OSX *(_appletv-v2._tcp)*
- Audio for Airplay *(_roap._tcp)*
- Remote *(_touch-able._tcp)*

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)*

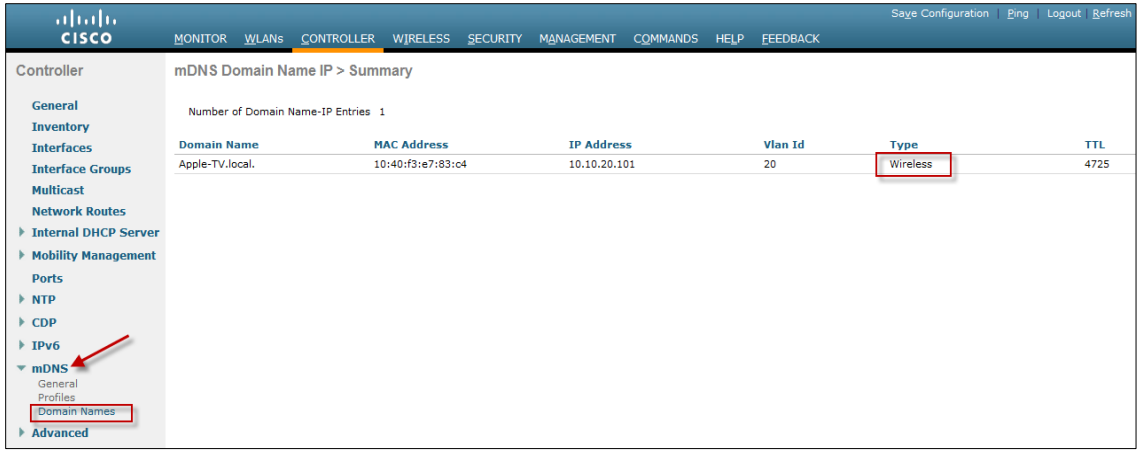
mDNS AP for a Non Layer 2 Adjacent Service

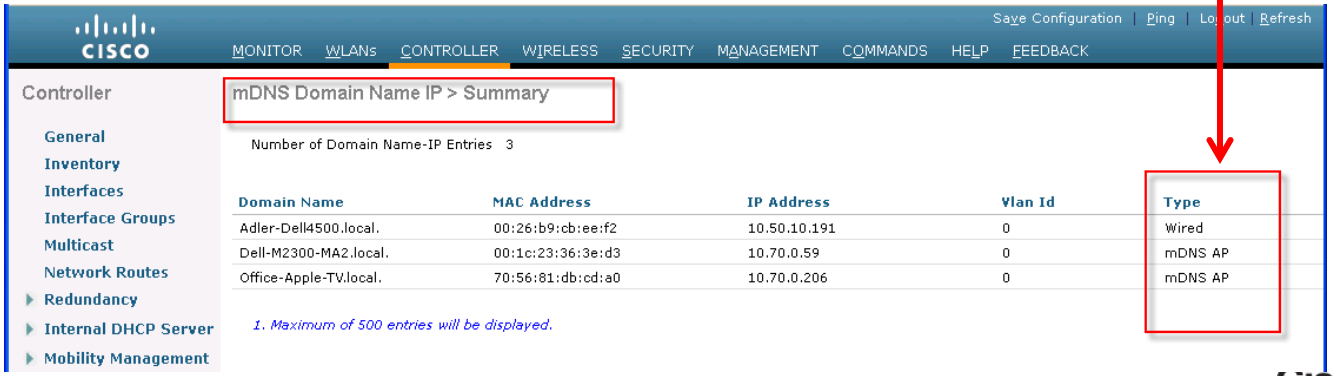


Apple Services

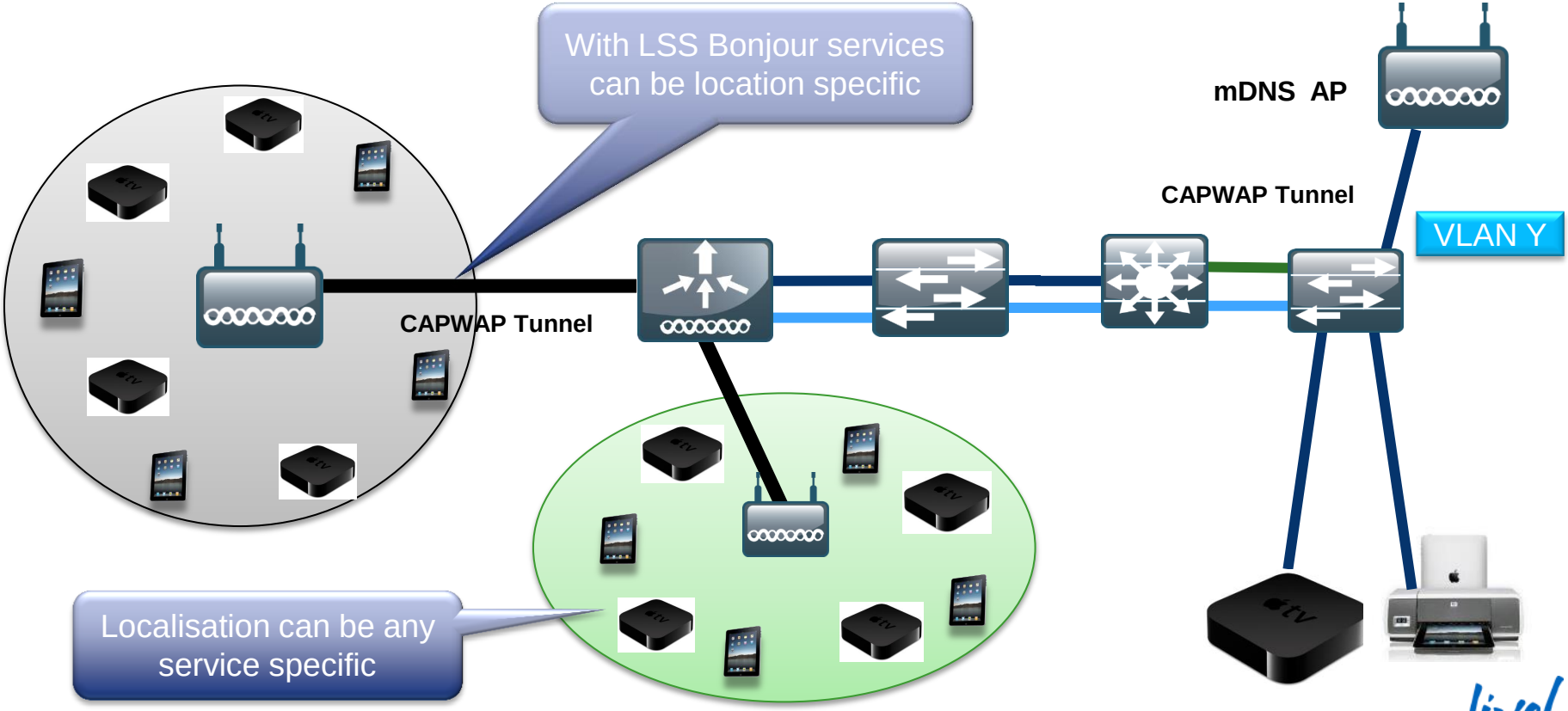
Summary of Bonjour Enabled Devices

For Your Reference



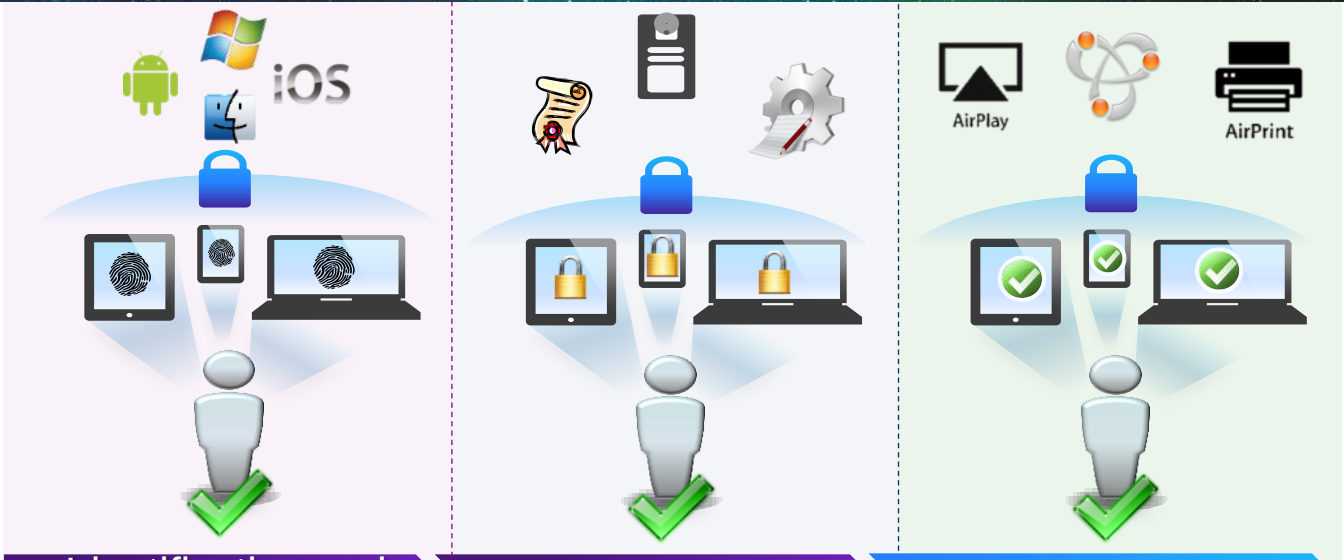


Location Specific Service for Bonjour



Summary

Managing the BYOD Evolution



Personal Devices on Network

Identification and Security Policy Enforcement

Securely On-Board the Device

Simplified Bonjour Operations

Network Components

Wireless | Wired | Remote Access | ISE | Prime




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo 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 www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 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

CISCO™

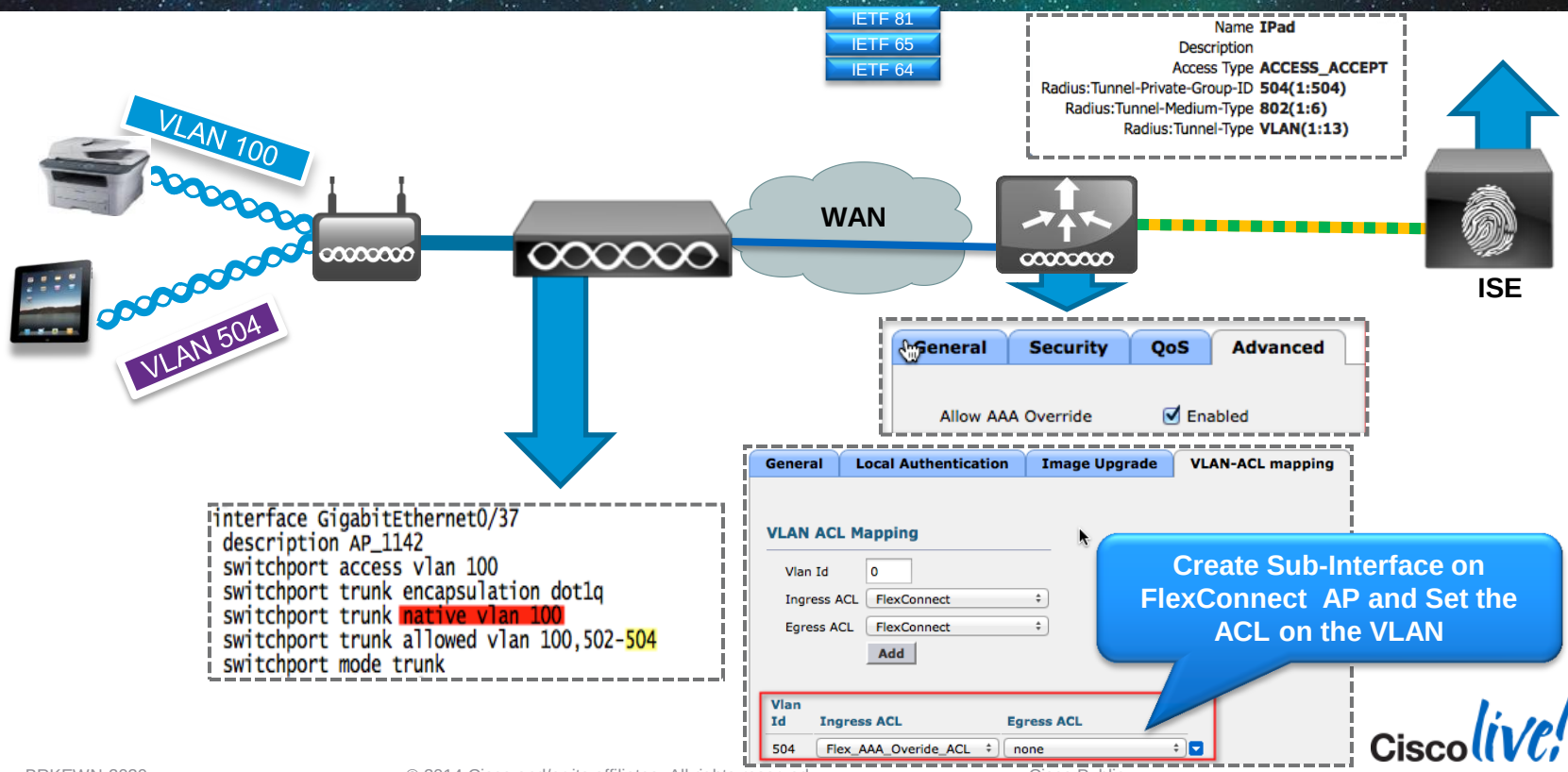



Configurations for Your Reference

FlexConnect and AAA Override

Setting the VLAN for Locally Switched Clients

For Your Reference




```
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
```

Steps for Integrating the Controller and ISE

For Your Reference

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.

Cisco Wireless Controller User-Based Policy AAA Override Attributes

For Your Reference

Network Access

- **"Airespace-Interface-Name"**
  - Sets the Interface to which the client is connected (VLAN).

Network Restrictions

- **"Airespace-ACL-Name"**
  - Sets the Access Control List used to filter traffic to/from the client.

Quality of Service

- **"Airespace-QOS-Level"**
  - Sets the maximum QoS queue level available for use by the client (Bronze, Silver, Gold or Platinum).
- **"Airespace-802.1p-Tag" and/or "Airespace-DSCP-Tag"**
  - Sets the maximum QoS tagging level available for use by the client.

URL Redirection

Central Web Auth, Client Provisioning, Posture

For Your Reference

- **Redirect URL:** For CWA, Client Provisioning, and Posture, URL value returned as a Cisco AV-pair RADIUS attribute.

  Ex: cisco:cisco-av-pair=url-redirect= https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa

- **Redirect ACL:** Access devices must be locally configured with ACL that specifies traffic to be permitted (= redirected) or denied (= bypass redirection)

  ACL value returned as a named ACL on NAD

  Ex: cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT

  ACL entries define traffic subject to redirection (permit) and traffic to bypass redirection (deny)

Configuring ISE as the Authentication Server and Accounting Server

For Your Reference

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	••••••••
	••••••••
	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	

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
☑	1	10.10.10.10	1813	Disabled	Enabled

2 Add to Accounting Servers to Receive Session Statistics

For Your Reference

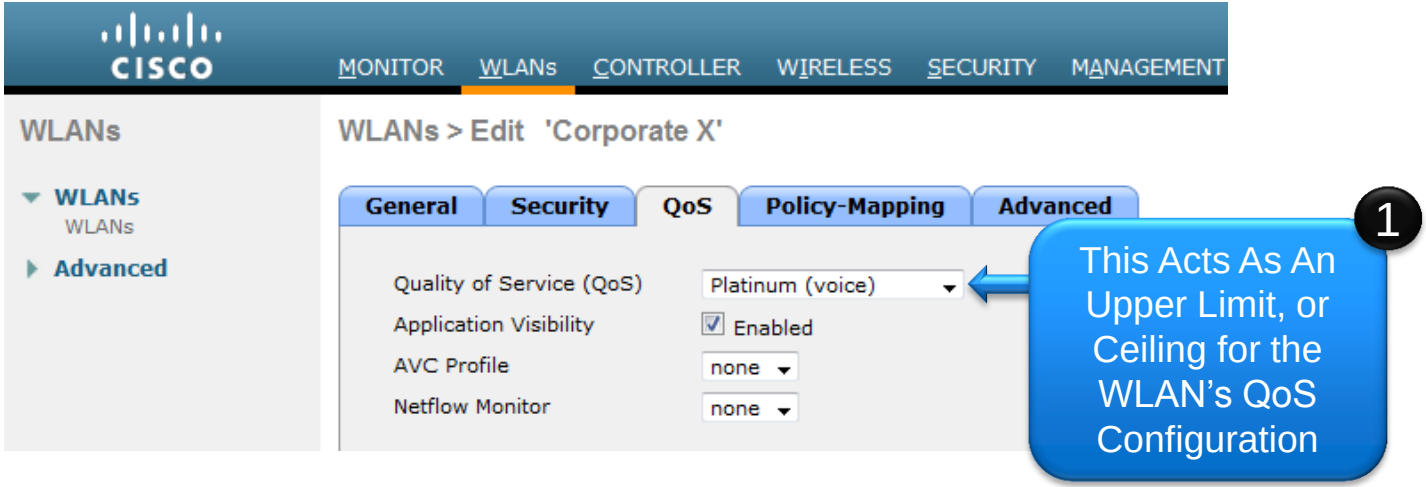
Configuring the WLAN for Secure Connectivity

Enabling Secure Authentication and Encryption with WPA2-Enterprise

For Your Reference

Setting the WLAN QoS Level for Override

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.

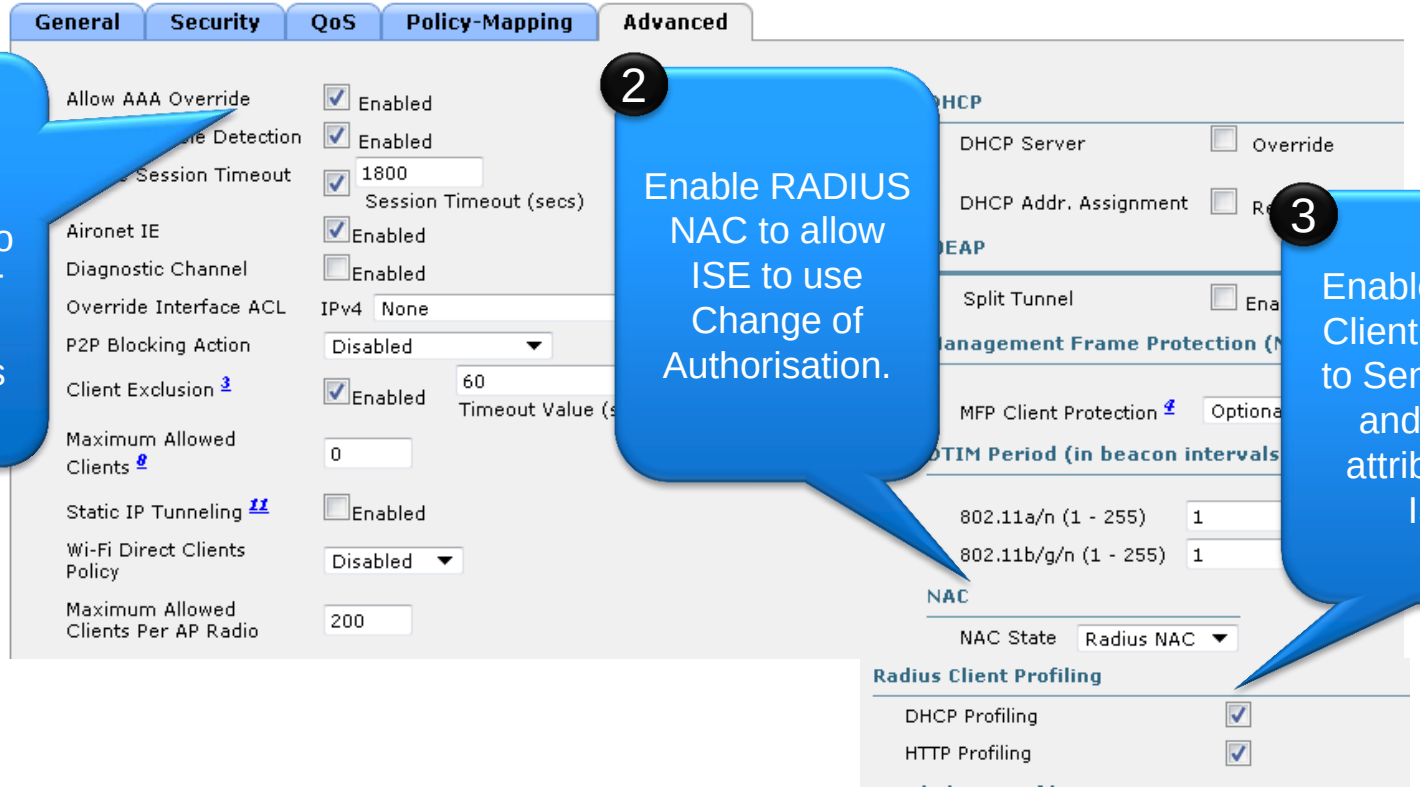
Configuring the WLAN for ISE Identity-based Networking Cont'd

For Your Reference

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

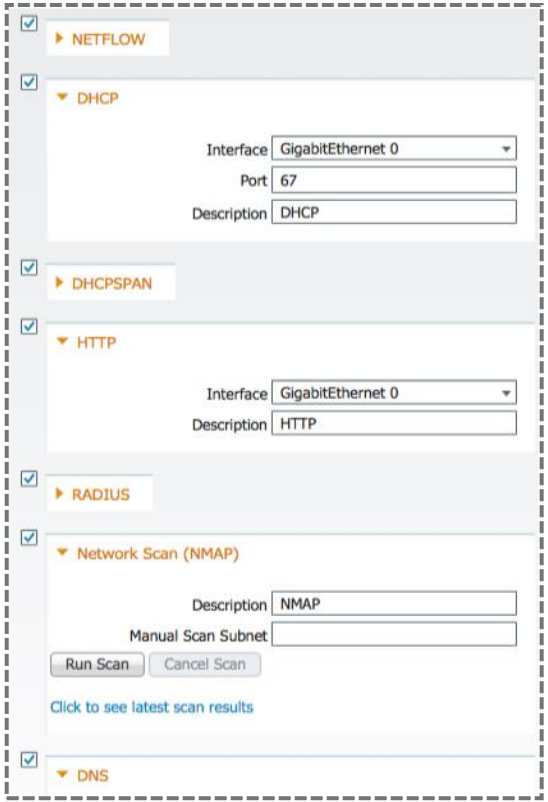
2 Enable RADIUS NAC to allow ISE to use Change of Authorisation.

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



Configuring 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.

Steps for Configuring Device Provisioning

For Your Reference

1. Configure Integration with External CA Server

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

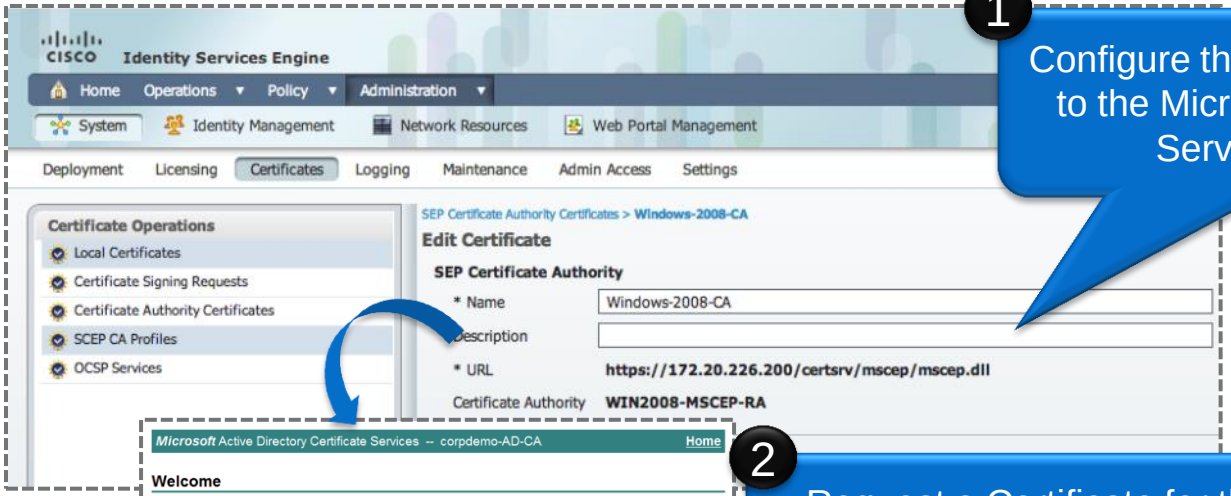
2. Define Supplicant Provisioning Profile

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

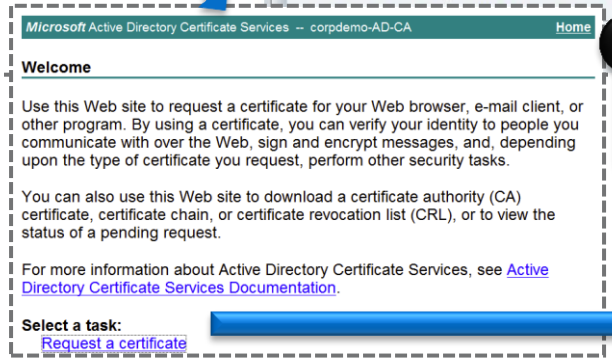
For Your Reference

Configuring SCEP Integration on the ISE

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



1 Configure the SCEP URL Pointing to the Microsoft Windows 2008 Server or other CA

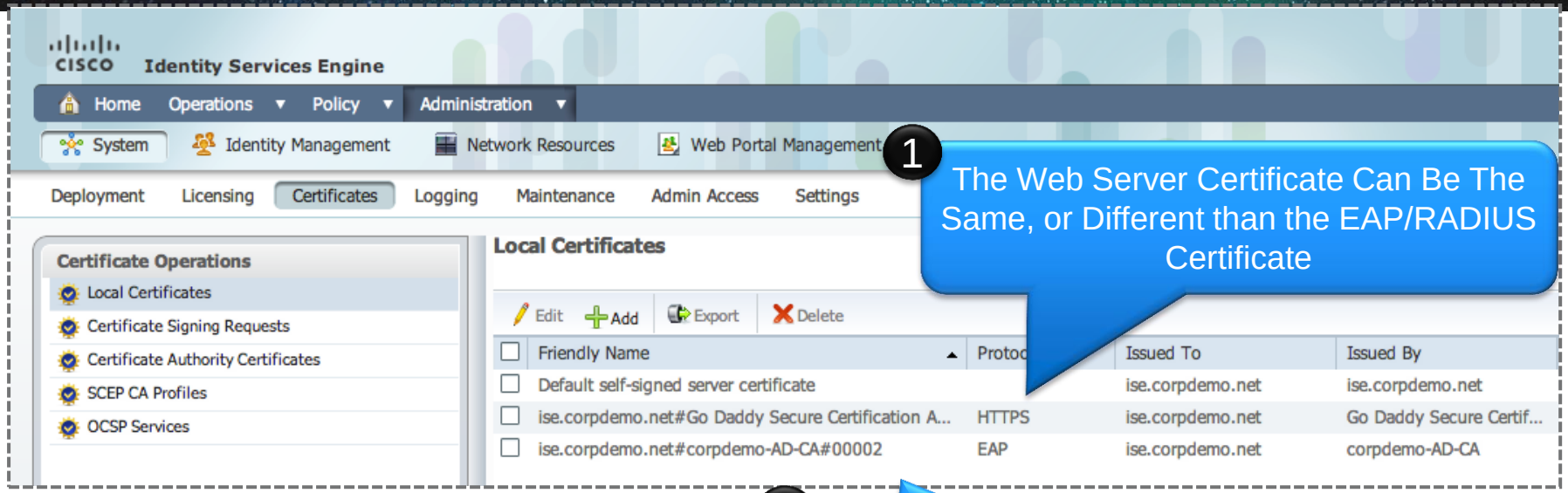


2 Request a Certificate for the ISE from the CA Server

For Your Reference

Configuring Certificates on the ISE

Certificates are Used for HTTPS and EAP Connections



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

For Your Reference

Configuring the Web-Authentication Redirect ACL

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

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

< Back | Add New Rule

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
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.10 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
2	Permit	10.10.10.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0

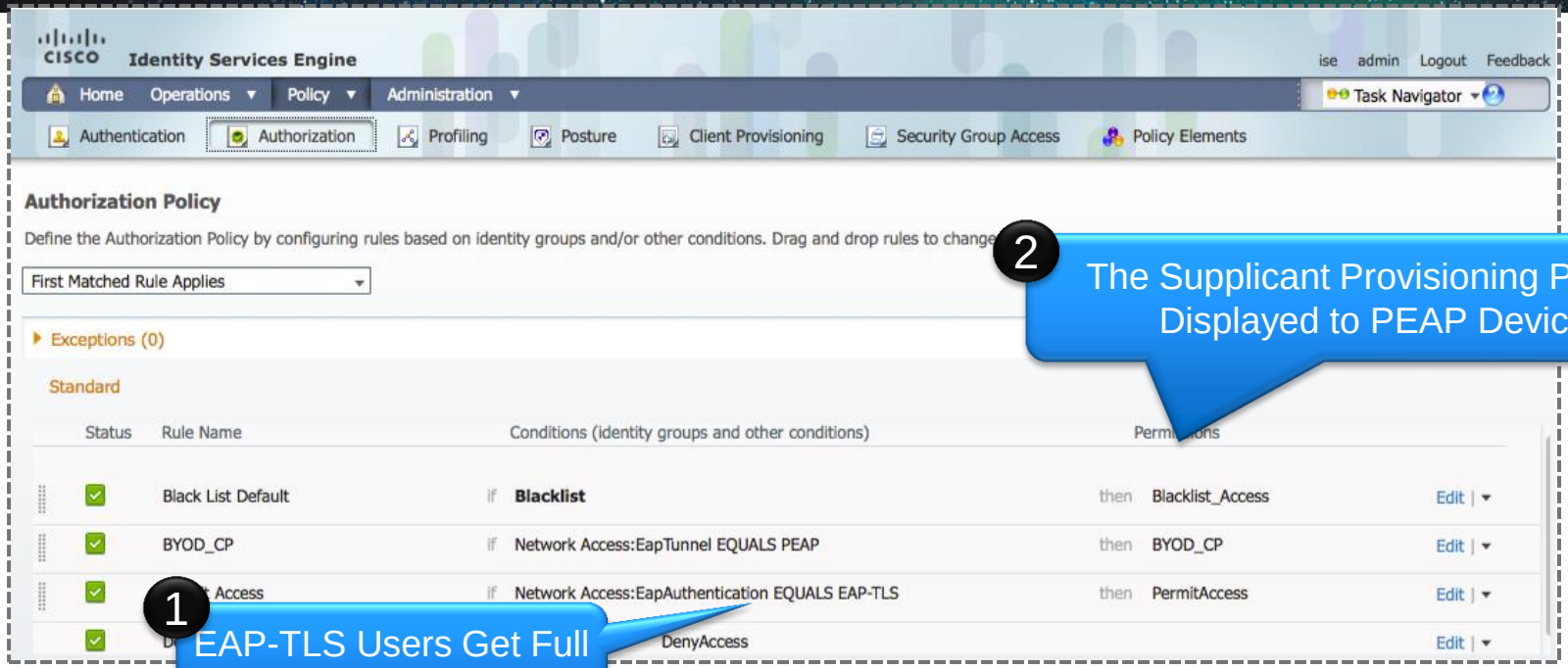
1 This ACL will be referenced by name by the ISE to restrict the user.

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

For Your Reference

Authorisation Rules for Supplicant Provisioning

Example Rule Set to Force PEAP Devices to Register.

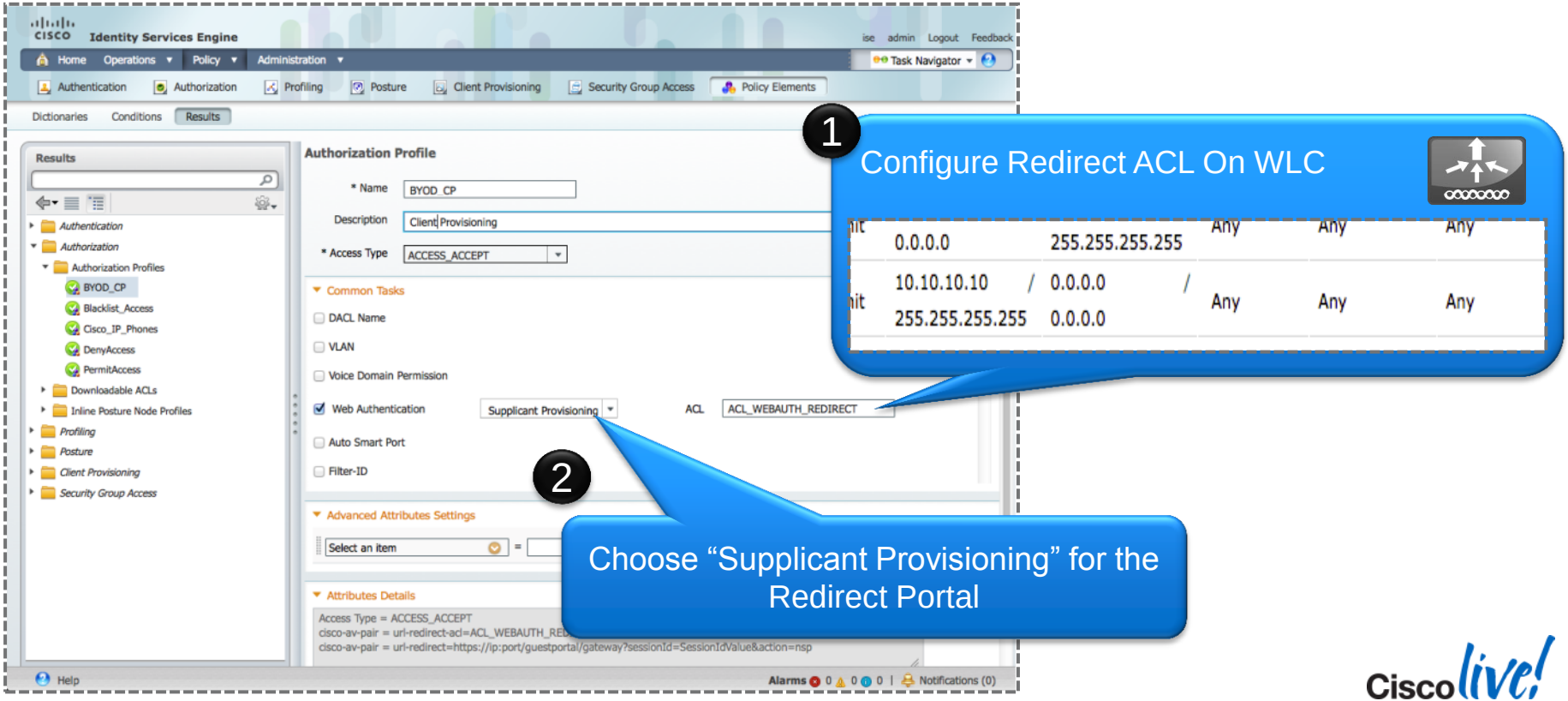


2 The Supplicant Provisioning Portal is Displayed to PEAP Devices

1 EAP-TLS Users Get Full Access

Defining the Supplicant Provisioning Authorisation Profile

For Your Reference



Supplicant Provisioning Configuration: EAP-TLS

For Your Reference

Using the ISE to Provision Certificates

Identity Services Engine

Home | Operations | Policy | Administration

Authentication | Authorization | Profiling | Posture | Client Provisioning | Security Group Access | Policy Element

For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
Windows	Any	Windows...	ActiveDirectory:ExternalGroups E...	NACAgent 4.9
Mac OSX	Any	Mac OSX	ActiveDirectory:ExternalGroups E...	NACAgent
BYOD IOS	Any	Mac iOS All	ActiveDirectory:ExternalGroups E...	EAP-TLS_Provis
BYOD Android	Any	Android	ActiveDirectory:ExternalGroups E...	EAP-TLS_Provision

Native Supplicant Profile

* Name: EAP-TLS_Provision
Description:
* Operating System: ALL
* Connection Type: Wired / Wireless
*SSID: CorporateX
Security: WPA2 Enterprise
* Allowed Protocol: TLS
* Key Size: 2048

1 Define Who Can Provision Devices

ActiveDirectory:ExternalGroups E... then EAP-TLS_Provision

Expression: ActiveDirectory:Exte | Equals | Employees

2 Use WPA2 Security and TLS for the EAP Type

Client Provisioning Policy

For Your Reference

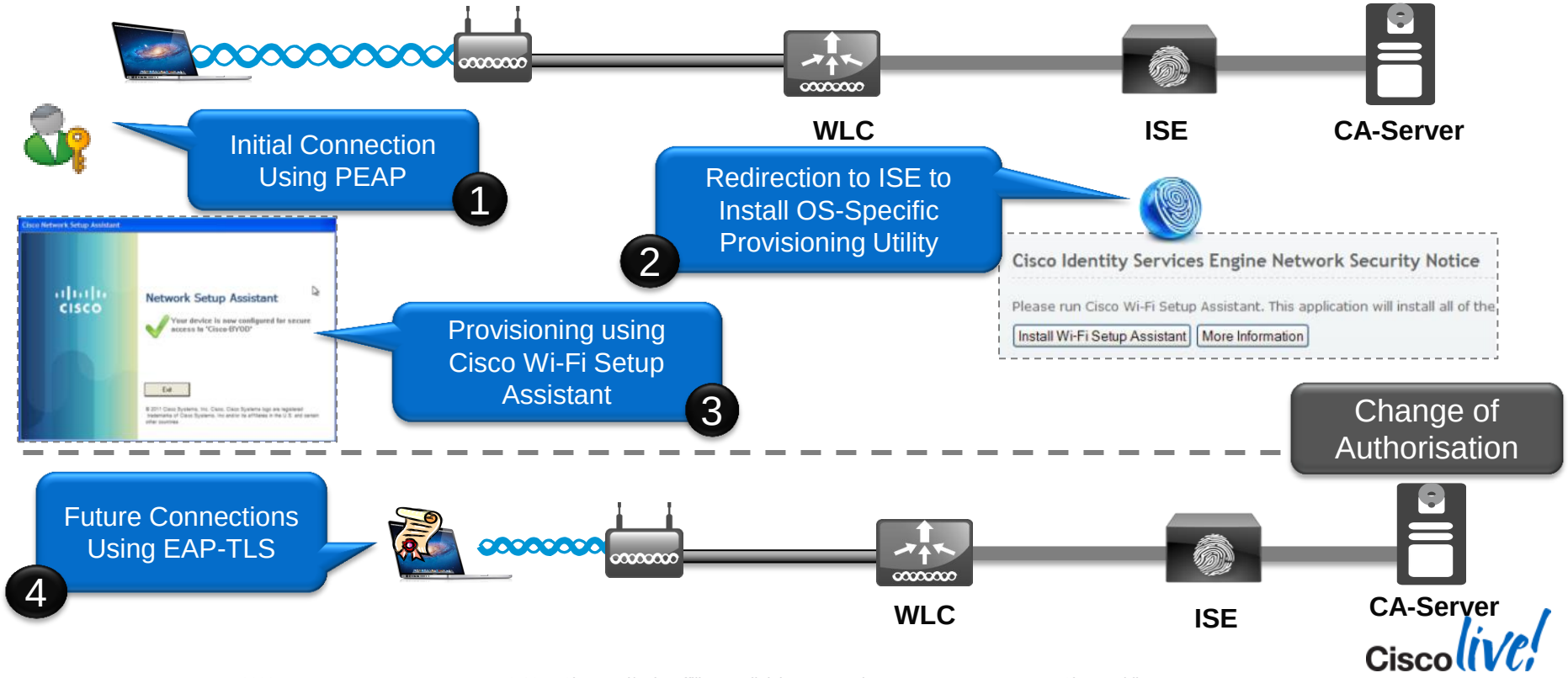
Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
✓	IOS	If	Any	and	Mac iOS All	and	AD1:ExternalGroups EQUALS cts.l...	then	WiFi_Profile
✓	Android	If	Any	and	Android	and	AD1:ExternalGroups EQUALS cts.l...	then	WiFi_Profile
✓	WinThings	If	Any	and	Windows...	and	AD1:ExternalGroups EQUALS cts.l...	then	WinSPWizard 1.0.0.14 And WiFi_Profile
✓	MAC-OSX	If	Any	and	Mac OSX	and	AD1:ExternalGroups EQUALS cts.l...	then	MacOsXSPWizard 1.0.0.6 And WiFi_Profile

Windows/Mac OS X Device Provisioning

For Your Reference



Staying Updated with Latest Applications

For Your Reference

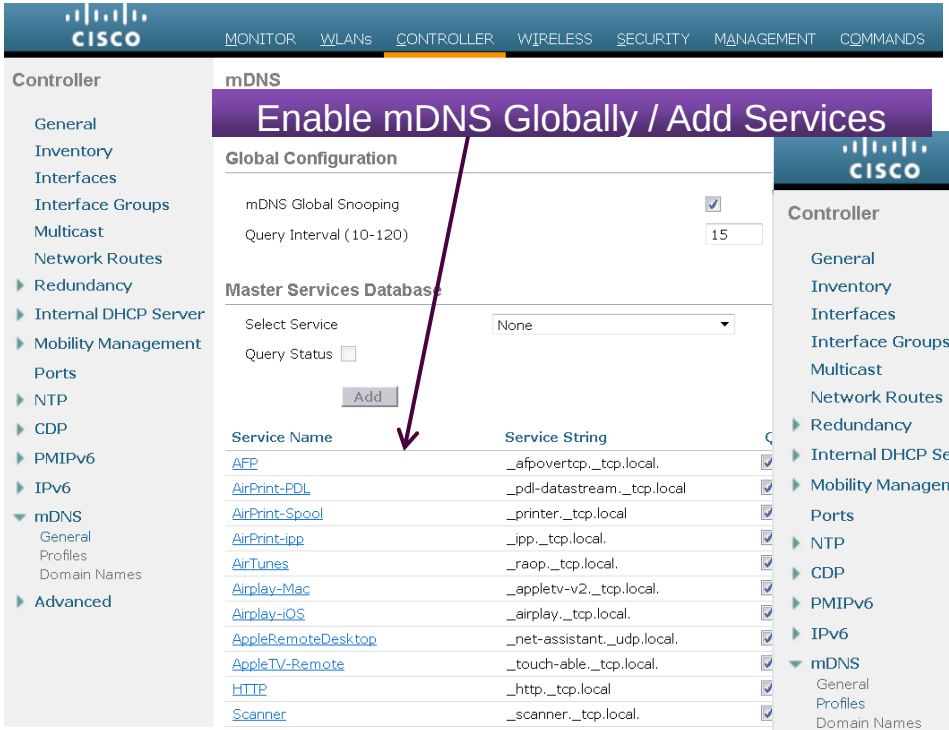
- Protocol Pack allows adding more applications without upgrading or reloading AireOS
- NBAR2 Protocol List: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6616/product_bulletin_c25-627831.html
- Protocol Pack are released for specific NBAR Engine
  - AireOS 7.5 WLC has NBAR Engine 13 (protocol pack will be pp-adv-asr1k-152-4.S-**13**-3.0.0.pac)

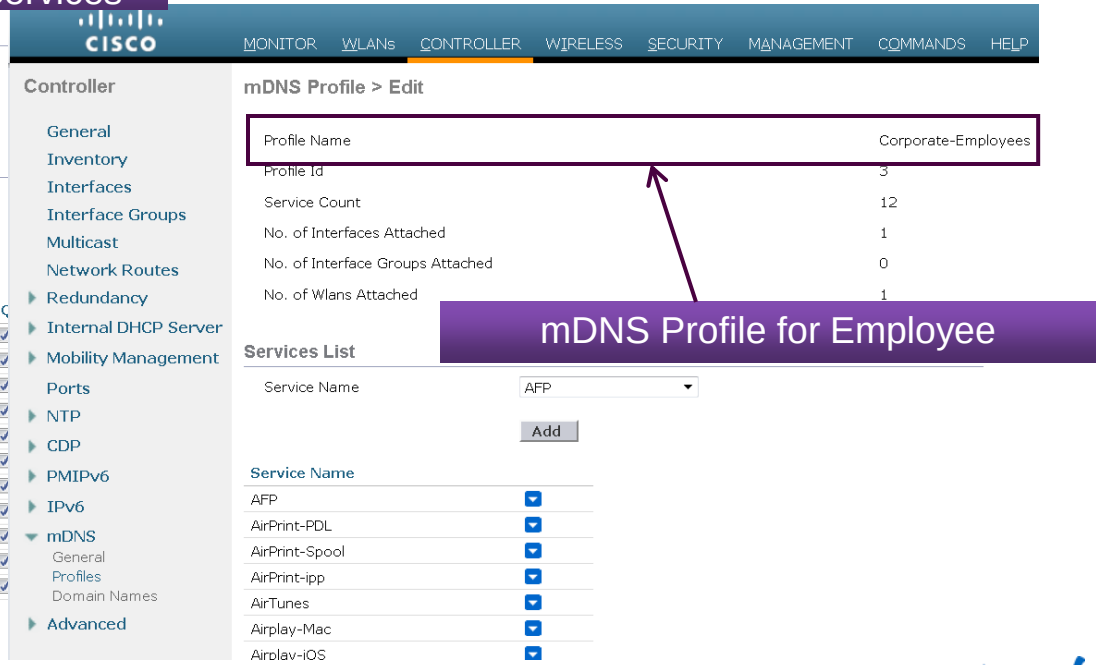
```
(Cisco Controller) >transfer download datatype avc-protocol-pack
(Cisco Controller) >transfer download start
Mode............................... FTP
Data Type......................... AVC Protocol Pack
FTP Server IP..................... A.B.C.D
FTP Server Port................... 21
FTP Path.......................... /
FTP Filename...................... pp-adv-asr1k-152-4.S-13-2.1.0.pack
FTP Username...................... cisco
FTP Password...................... *********
Starting tranfer of AVC Protocol Pack
This may take some time.
Are you sure you want to start? (y/N)
```

```
(5508-60-Active) >show avc engine version

 AVC Engine Version: 13

(5508-60-Active) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 1.0

(5508-60-Active) >
```

Bonjour Gateway Services Filter

For Your Reference





Applying the Bonjour Gateway Profile

For Your Reference

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

Configure mDNS- AP from CLI

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 or **Access Mode**:

(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
```

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:

```
(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™