

TOMORROW starts here.



Cisco *live!*

Managing the BYOD Evolution

BRKEWN-2020

Scott Lee-Guard

Systems Engineer

Agenda

Managing the BYOD Evolution



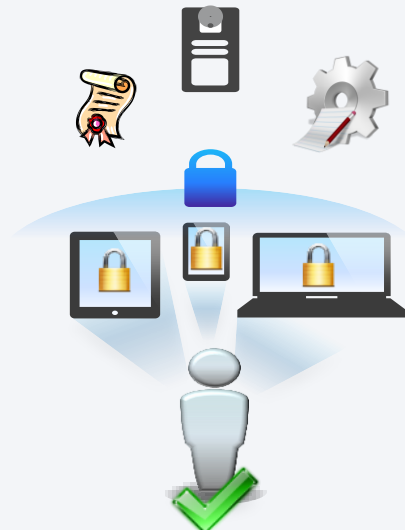
Personal Devices on Network

Network Components

BRKEWN-2020



Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations

Wireless Wired Remote Access ISE Prime

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public



Wireless BYOD

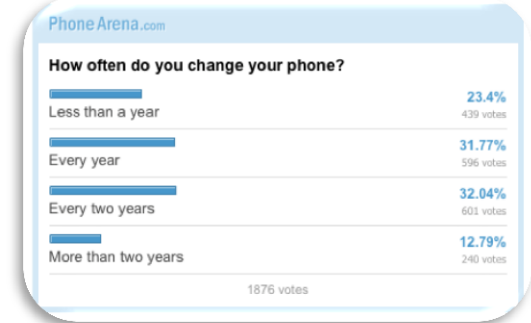
Drivers and Assumptions

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

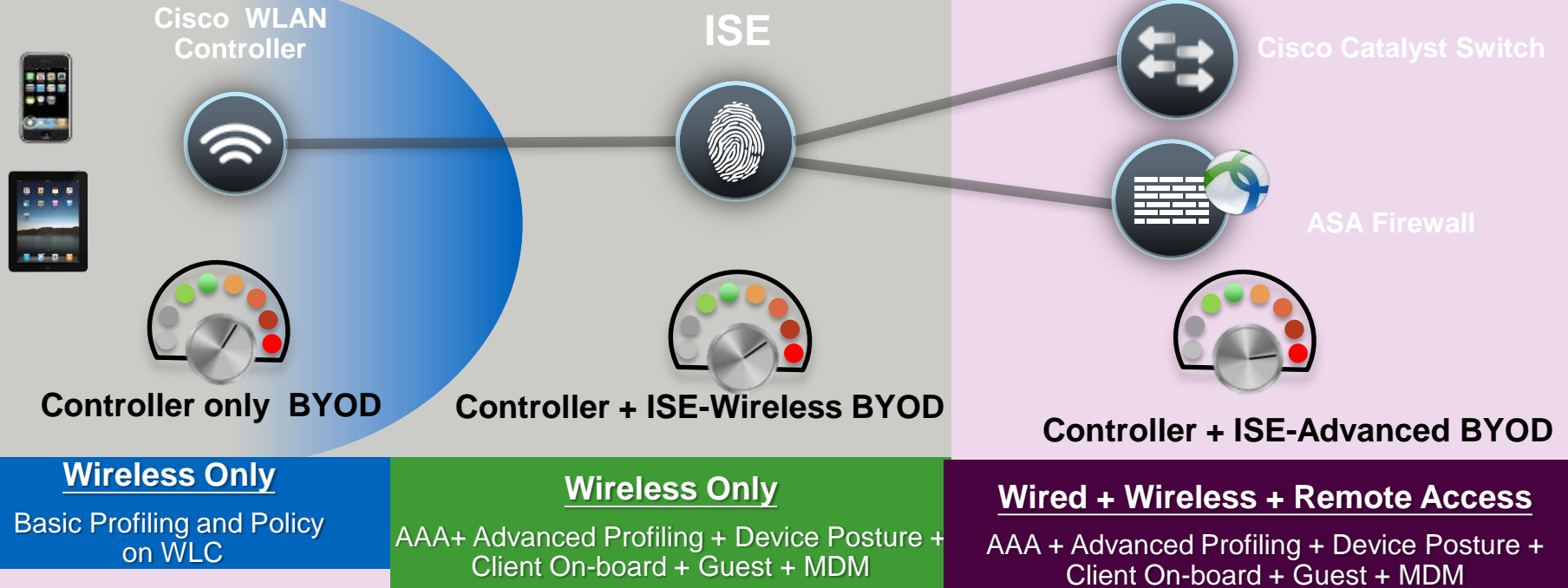
BYO devices need wired, wireless, remote and mobile access

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



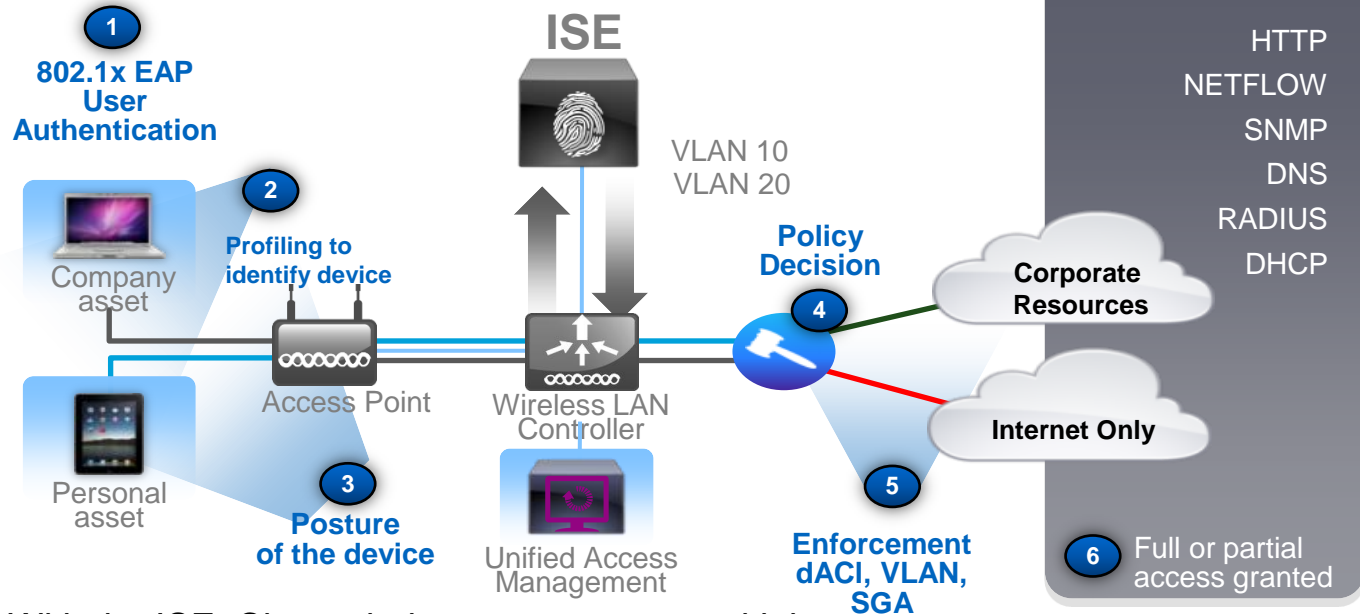


Contextual Policy for BYOD Deployments

Control and Enforcement

IDENTITY

-
-
- HQ
- 2:38pm
-



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

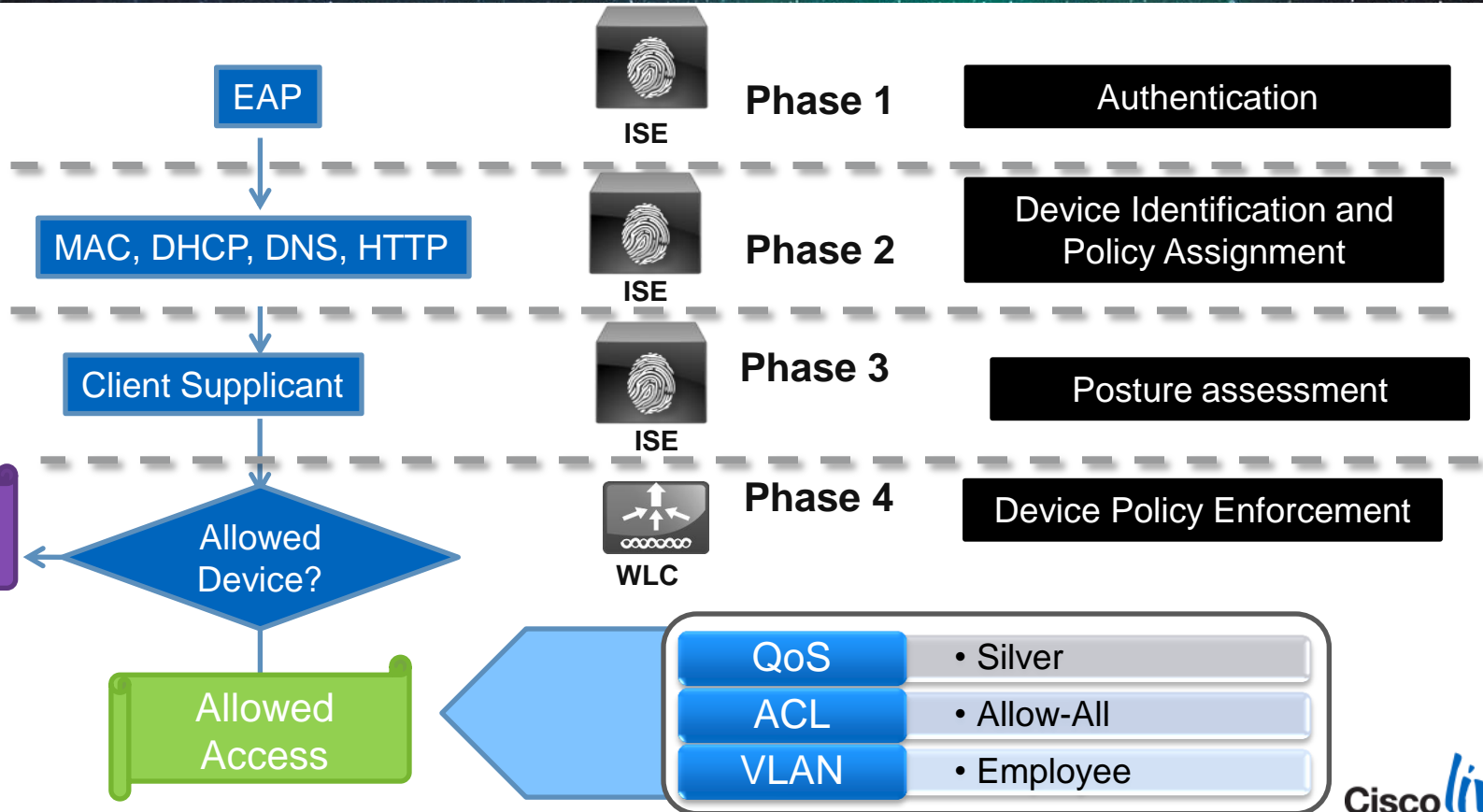


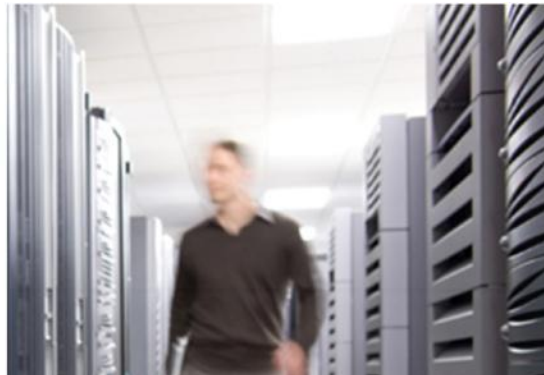
■ Cisco Identity Services Engine

- 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

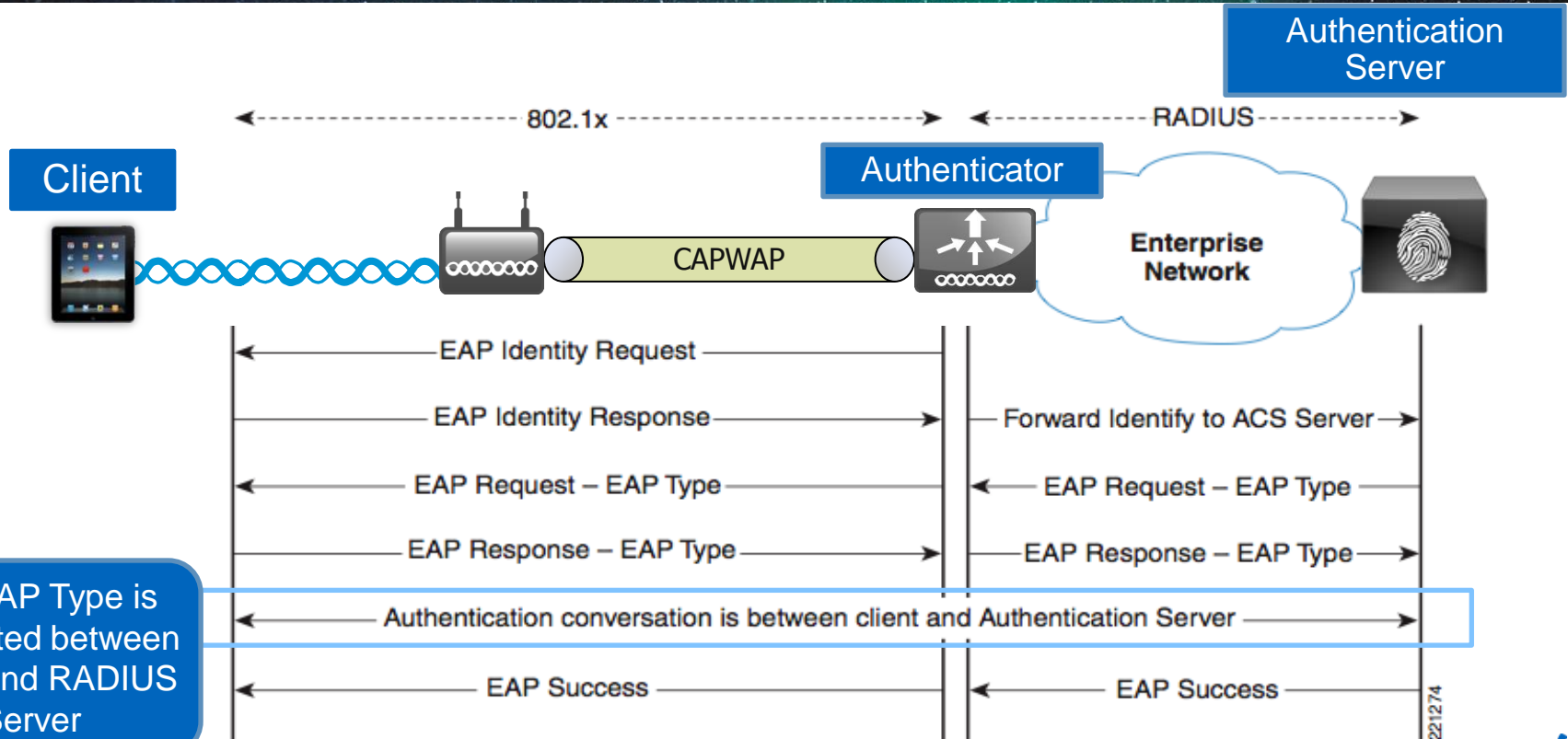


Reporting



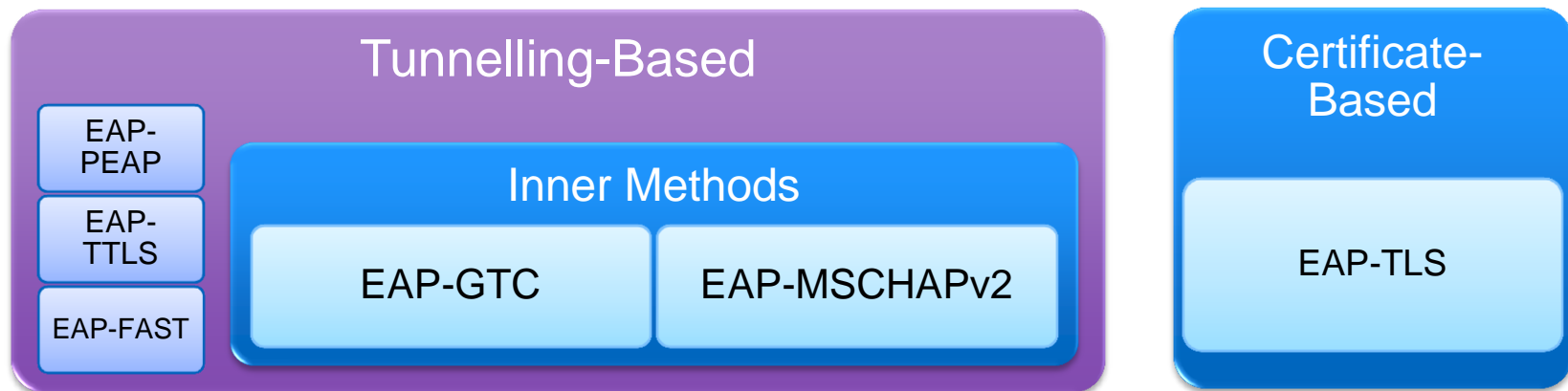
MDM Integration

Extensible Authentication Protocol (EAP) — Protocol Flow



EAP Authentication Types

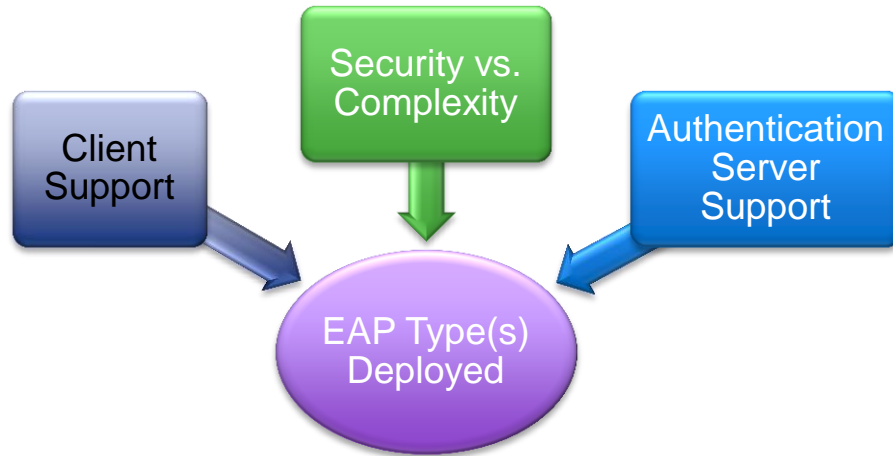
Different Authentication Options Leveraging Different Credentials



- 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

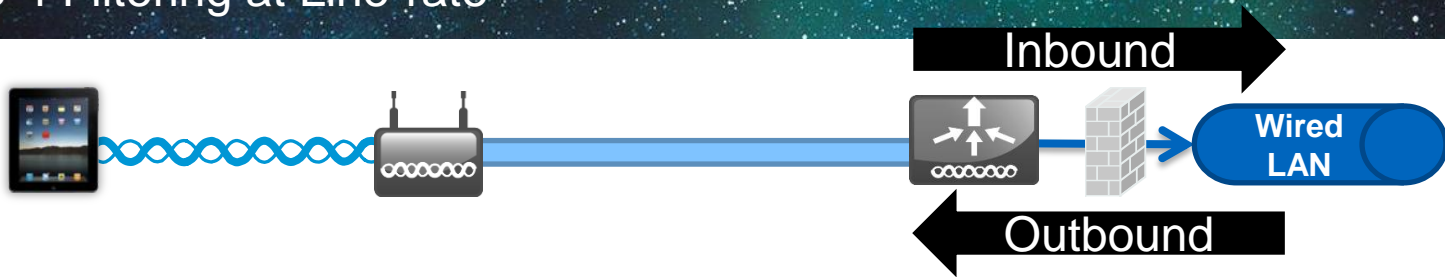
The Most Common EAP Types are PEAP and EAP-TLS



- 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



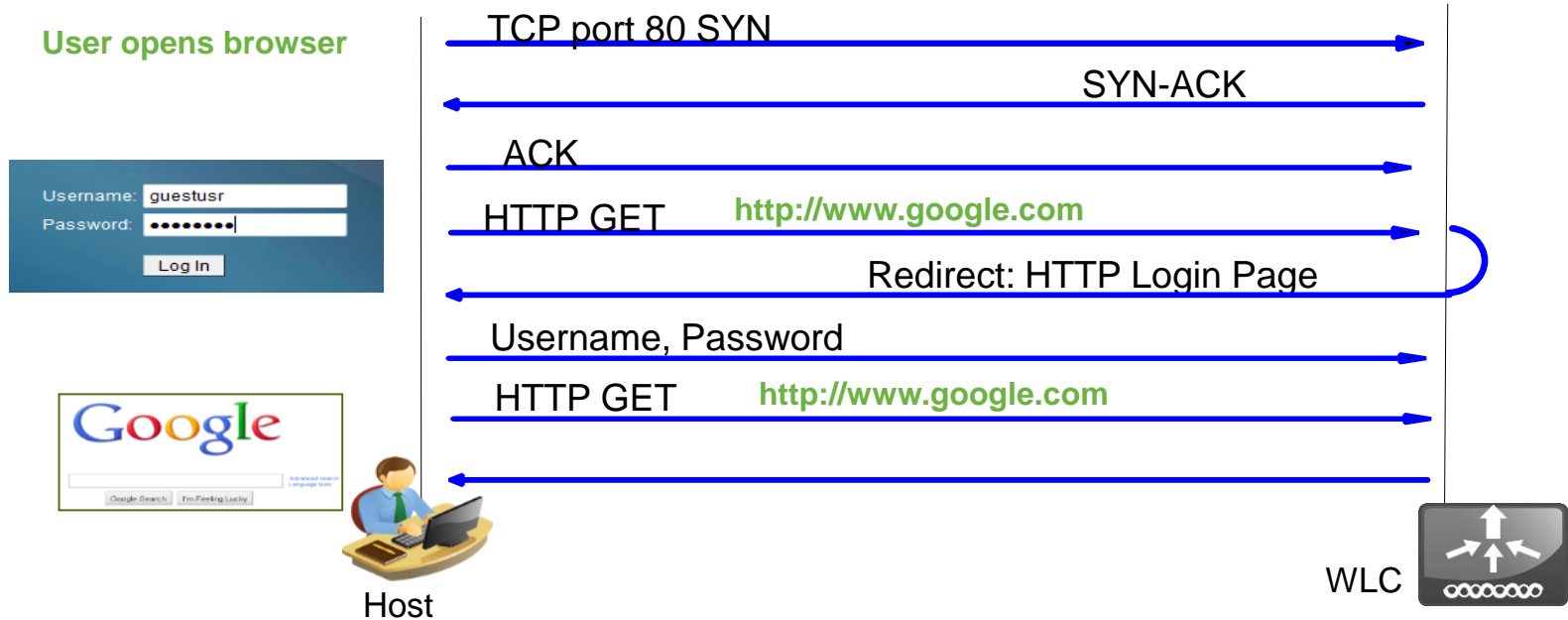
- ACLs provide L3-L4 policy and can be applied per interface or per user.
- Cisco 2500, 5508 and WiSM2 implement hardware, line-rate ACLs.
- Up to 64 rules can be configured per ACL.

| 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

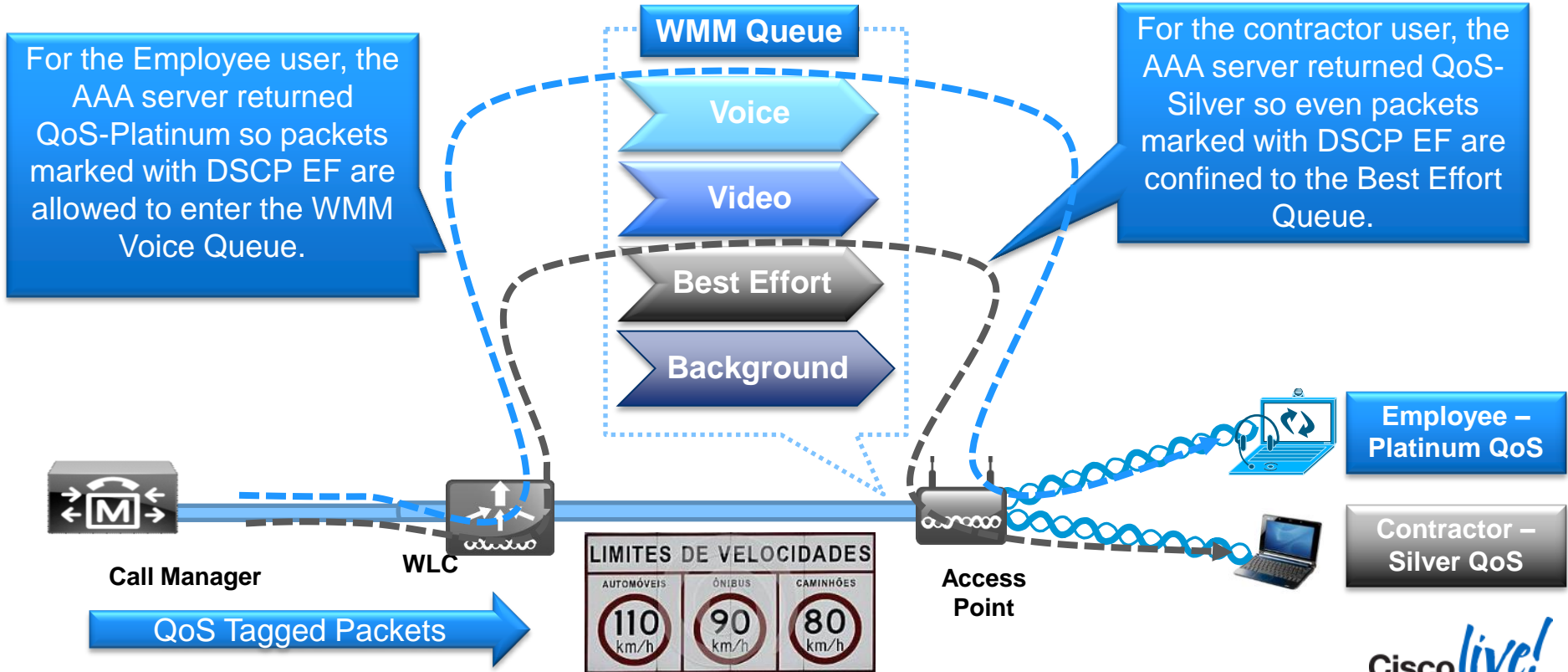
URL Redirection

- Example: TCP Traffic Flow for Login Page



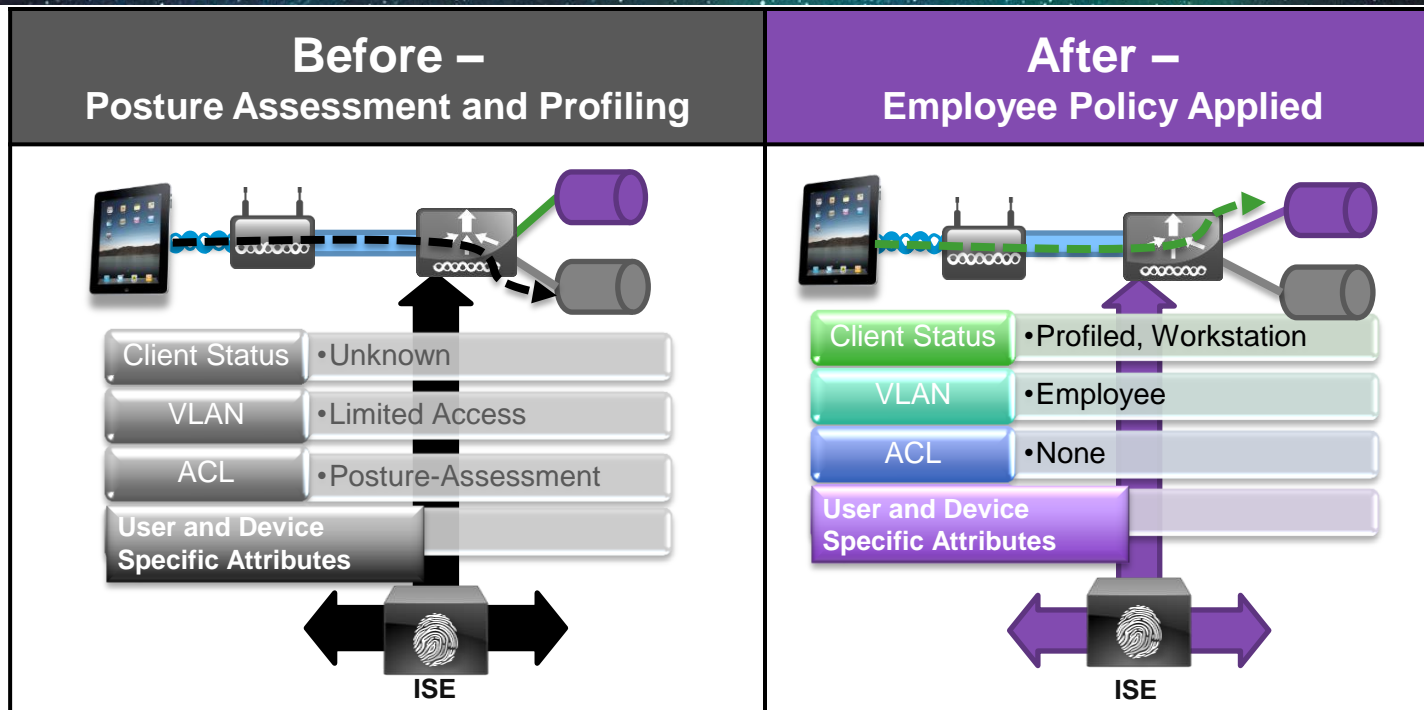
Cisco Wireless User-Based QoS Capabilities

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



Change of Authorisation (CoA)

Changing Connection Policy Attributes Dynamically

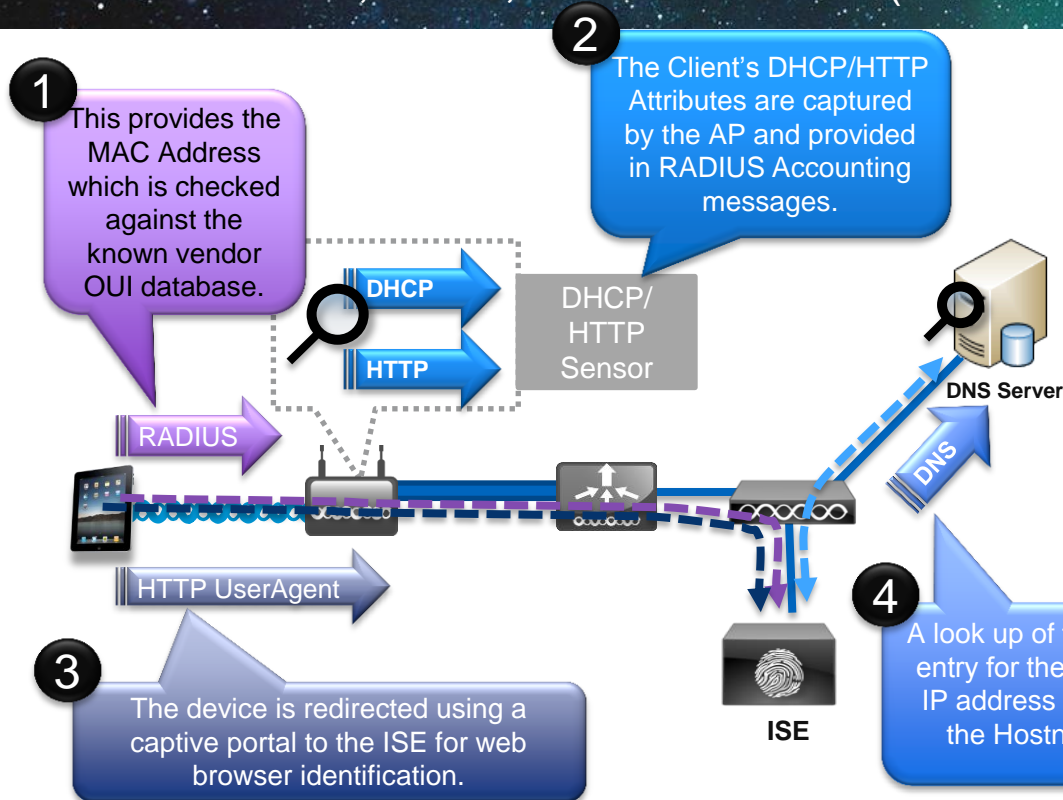




Profiling with ISE

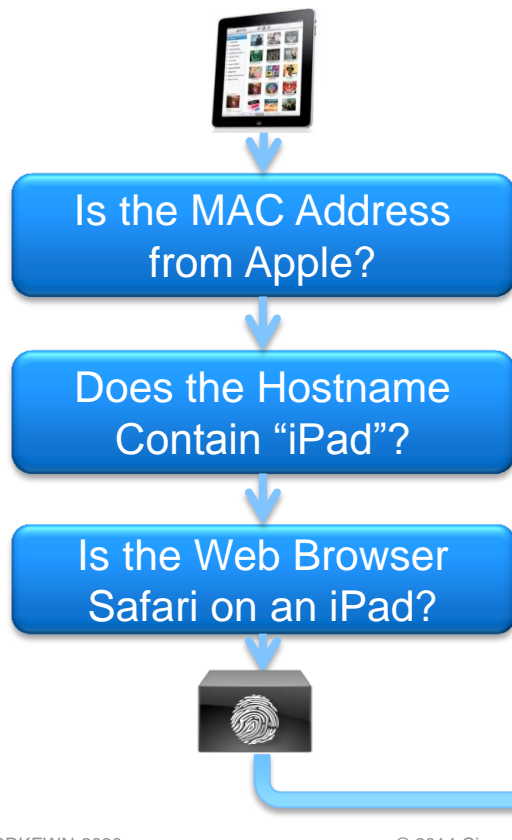
Client Attributes Used for ISE Profiling

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:

A screenshot of the ISE Endpoints table. The table has a header with "Endpoints" and a toolbar with "Edit", "Create", "Delete", "Import", and "Export" buttons. The table contains five rows of endpoint profiles. A blue arrow points from the "Apple-iPad" row to the "Apple iPad" box in the flowchart below.

| 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 |

ISE Device Profiling Capabilities

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

The image displays the ISE Profiling Policies hierarchy on the left and a detailed configuration for the 'Apple-iPad' policy on the right. The hierarchy is organized by vendor and device type, with callouts for 'Smart Phones', 'Gaming Consoles', and 'Workstations'. The configuration window shows settings for the 'Apple-iPad' policy, including a 'Minimum Certainty Factor' of 20 and a 'Parent Policy' of 'Apple-Device'. Two callouts highlight key features: 'Minimum Certainty for a Match' (1) and 'Multiple Rules to Establish Confidence Level' (2).

Smart Phones

Gaming Consoles

Workstations

Profiler Policy

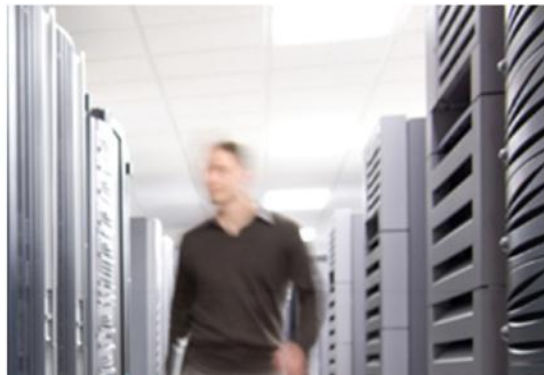
- * Name: Apple-iPad
- Description: [Empty]
- Policy Enabled:
- * Minimum Certainty Factor: 20 (Value range 1-100)
- * Exception Action: NONE
- * Network Scan (NMAP) Action: NONE
- Create Matching Identity Group
- Use Hierarchy
- * Parent Policy: Apple-Device

Rules

- If Condition: Apple-iPadRule2Check2 Then Certainty F...
- If Condition: (Apple-iPadRule1Check1_AND_Apple-MacBook...

1 Minimum Certainty for a Match

2 Multiple Rules to Establish Confidence Level



Defining a Security Policy Within ISE

Steps for Configuring ISE Policies

1. Authentication Rules

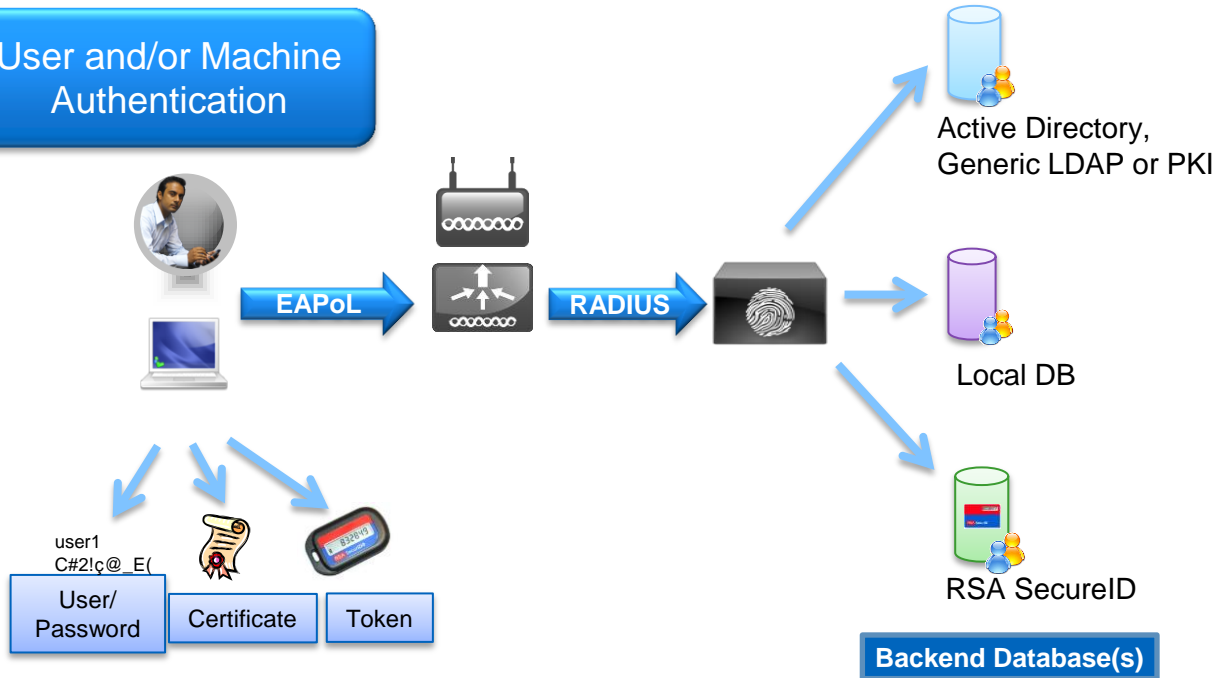
- Define what identity stores to reference.
 - Example – Active Directory, CA Server or Internal DB.

2. Authorisation Rules

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

ISE Authentication Sources

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

Example for PEAP and EAP-TLS

CISCO Identity Services Engine

Home Operations Policy Administration

Authentication Authorization Profile

Authentication Policy

Define the Authentication Policy by selecting the protocols

Policy Type Simple Rule-Based

Wireless : If Wireless_802.1X allow protocols Allowed Protocols: Default Network and...

PEAP : if Network Access:EapTunnel EQUAL 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 Join/Leave operations. If a node is joined/leaved, a Join/Leave operation is required before a Join/Leave operation. Select...

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

The screenshot shows the Cisco ISE Authorisation Rules configuration page. A table lists several rules, including 'Dot1X Engineering User' and 'Dot1X Marketing User'. A 'Condition(s) Details' window is open, showing the condition 'AD1:ExternalGroups EQUALS testnet.de/Users/EngineeringGrp'. A 'Identity Groups' list is also visible, showing 'Workstation' and 'Cisco-IP-Phone' under 'Endpoint Identity Groups'.

1 Specific Device Type Groups (such as Workstations or iPods) Can Be Utilised

2 Active Directory Groups Can Be Referenced

3 The Authorisation Rule Results in Attributes to Enforce Policy on End Devices

| Status | Rule Name | Identity Groups | Other Conditions | Permissions |
|--------|------------------------|---------------------|-------------------------------------|-------------|
| ✓ | Dot1X Engineering User | If Any and | AD1:ExternalGroups EQUALS testne... | Engineering |
| ✓ | Dot1X Marketing User | If Any and | AD1:ExternalGroups EQUALS testne... | Marketing |
| ✓ | Default | If no matches, then | DenyAccess | |

Condition(s) Details

AD1:ExternalGroups EQUALS testnet.de/Users/EngineeringGrp

Identity Groups

- User Identity Groups
 - Guest
 - MyUserGrp
 - SponsorAllAccount
 - SponsorGroupAccounts
 - SponsorOwnAccounts
- Endpoint Identity Groups
 - Blacklist
 - Profiled
 - Cisco-IP-Phone
 - Workstation
 - Unknown

Authorisation Rule “Results”

The Actual Permissions Referenced by the Authorisation Rules

1 Simple VLAN Override by Specifying the Tag

2 All WLC Attributes are Exposed to Override

Airespace

- Airespace--Real-Time-Bandwidth-Average
- Airespace-8021p-Tag--[4]
- Airespace-ACL-Name--[6]
- Airespace-Data-Bandwidth-Average-Cor
- Airespace-Data-Bandwidth-Burst-Contra
- Airespace-DSCP--[3]
- Airespace-Guest-Role-Name--[11]
- Airespace-Interface-Name--[5]
- Airespace-QOS-Level--[2]
- Airespace-Real-Time-Bandwidth-Burst-C
- Airespace-Wlan-Id--[1]

- 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



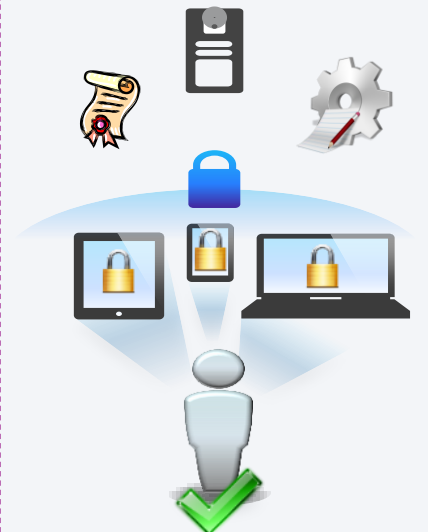
Personal Devices on Network

Network Components

BRKEWN-2020



Identification and Security Policy Enforcement



Securely On-Board the Device



Wireless



Wired



Remote Access



ISE



Prime

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

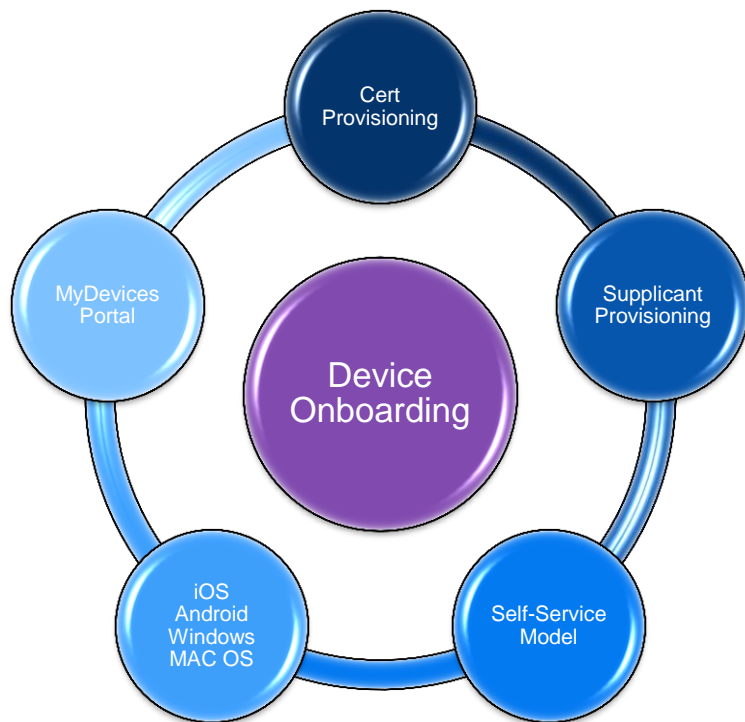
Cisco *live!*



BYOD Device Provisioning

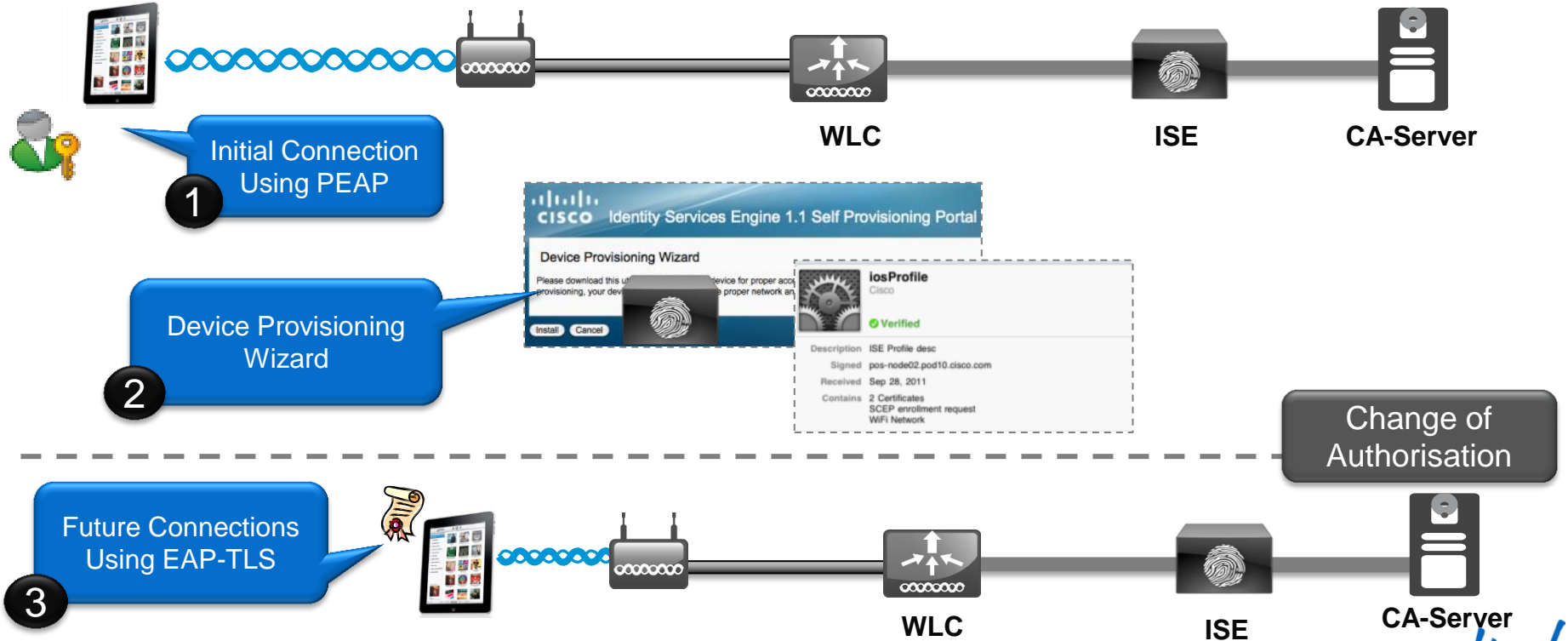
ISE BYOD Release

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.

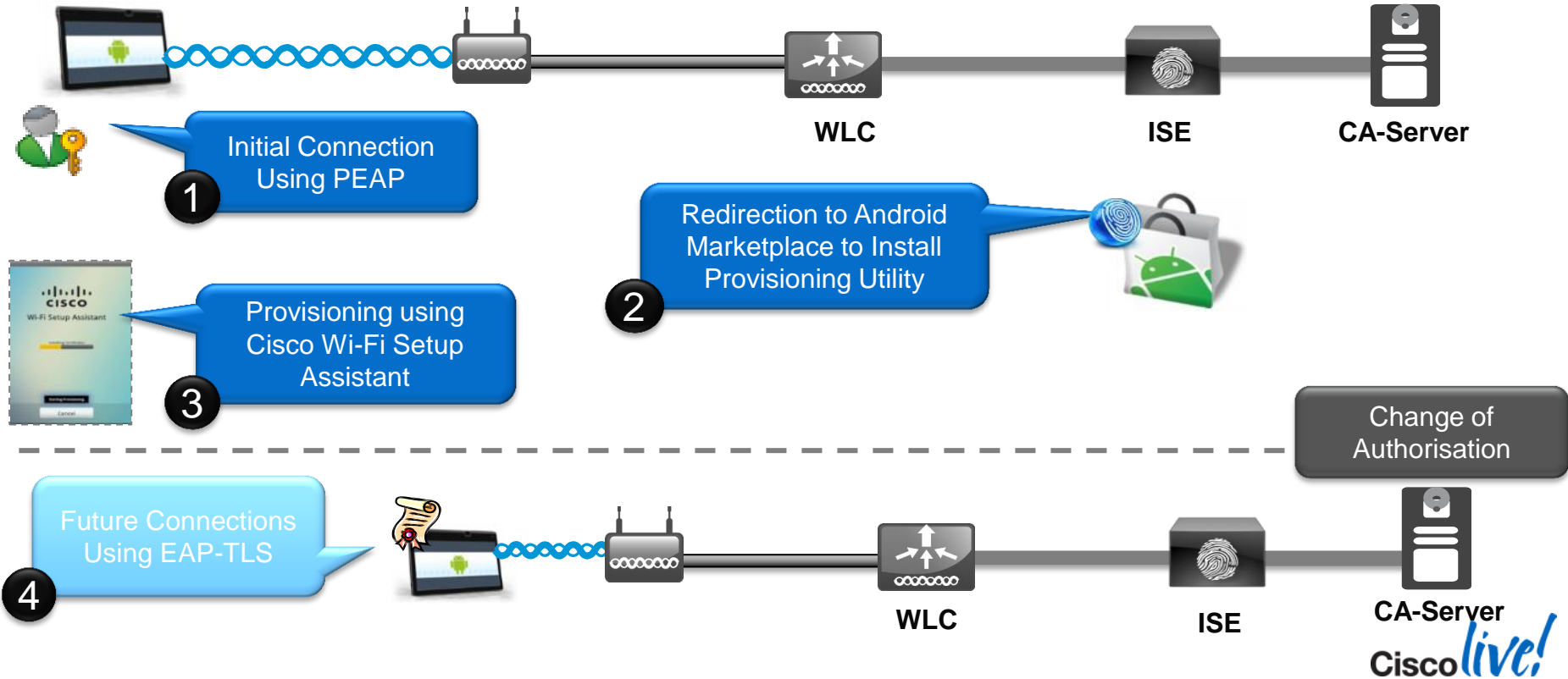
Apple iOS Device Provisioning



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



CiscoLive My Devices Portal

Welcome [denguan](#) ([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

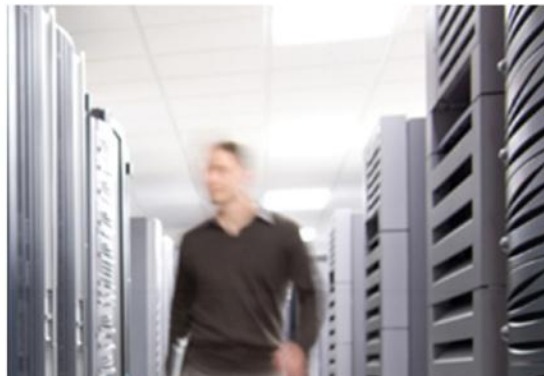
Devices Can be Self-Registered, Up to an Administrator Defined Limit

2

User can Self-Manage Lost/Found/Wipe etc

1

New Devices Can be Added with a Description



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

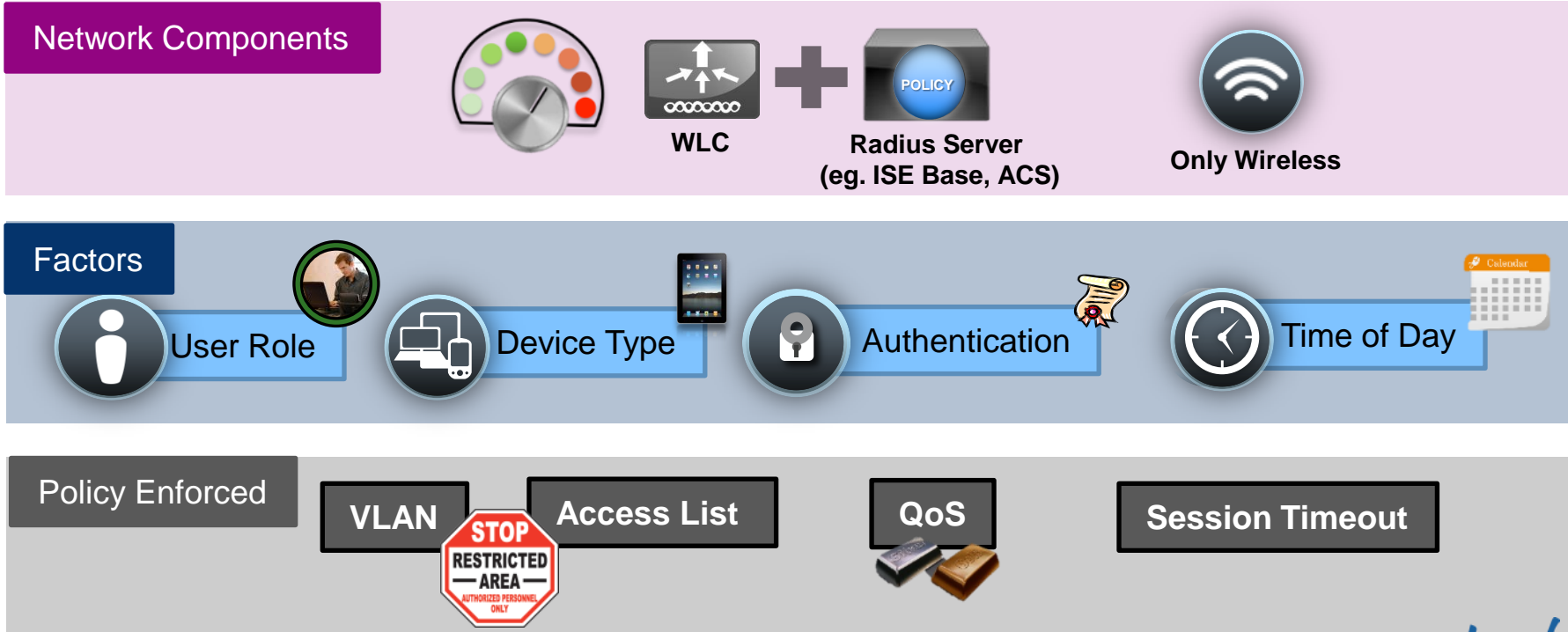
Access List

QoS

Session Timeout

Build BYOD Policy: Flexible Options

Native Profiling & Policy on WLC



Configuring User-Role



role=Employee

role=Contractor

Employee



Contractor



Radius

Attributes Details

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

Controller

MONITOR WLANS CONTROLLER WIRELESS SECURITY

Local Policies

Policy > Edit

Match Criteria

Match Role String

User-Role

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

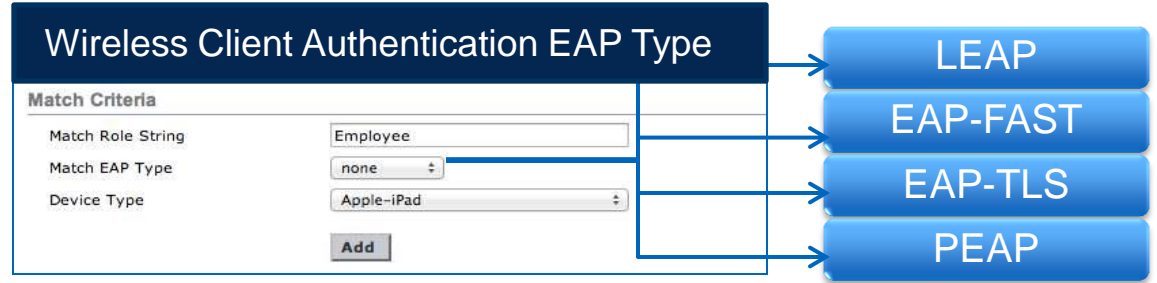
Current Filter None [Change Filter] [Clear Filter]

| Client MAC Addr | AP Name | WLAN Profile | WLAN SSID | WGB | Device Type |
|-----------------------------------|---------|---------------|---------------|-----|----------------|
| 00:27:10:d3:e3:1c | AP2600 | Demo-Employee | Demo-Employee | No | Windows7-Works |
| 40:1c:89:75:64:43 | AP2600 | Demo-Employee | Demo-Employee | No | Android |
| 70:de:e2:0e:ce:0f | AP2600 | Demo-Employee | Demo-Employee | No | Apple-iPad |

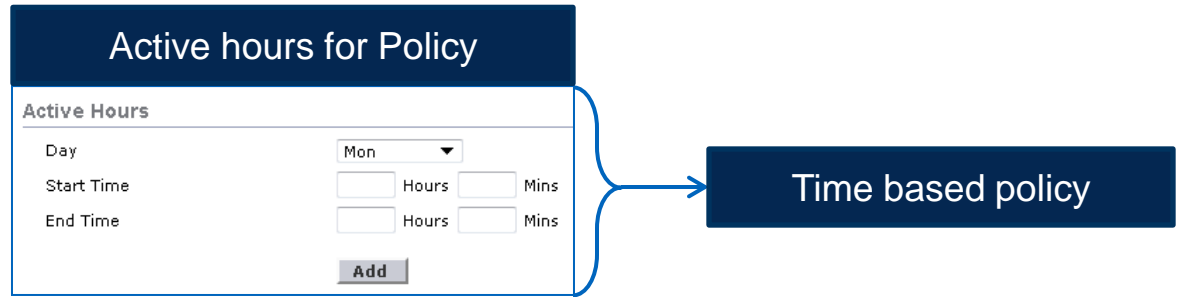
Native Profiling Authentication and Time Policy



Authentication



Time of Day



Enforce Policy on the WLC

The screenshot shows the Cisco WLC configuration interface for a Security Policy. The left sidebar contains a navigation tree with categories like AAA, Local EAP, and Access Control Lists. The main area is titled 'Policy > Edit' and contains several sections: Match Criteria, Device List, Action, and Active Hours. Blue callout boxes with icons point to specific fields: a person icon points to the Policy Name field, a key icon points to the Match EAP Type dropdown, a laptop and phone icon points to the Device Type dropdown, and a clock icon points to the Active Hours table. A pink callout box on the right highlights the Action section, which is detailed in the table below.

| Action | |
|---------------------------------|----------------------|
| IPv4 ACL | No_Corporate_Network |
| VLAN ID | 20 |
| Qos Policy | Silver (best effort) |
| Session Timeout (seconds) | 1800 |
| Sleeping Client Timeout (hours) | 12 |

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

| Priority Index | Local Policy Name |
|----------------|---|
| 1 | iPad-Policy <input type="button" value="v"/> |
| 2 | iPhone-Policy <input type="button" value="v"/> |
| 3 | Android-Policy <input type="button" value="v"/> |
| 4 | MacBook-Policy <input type="button" value="v"/> |
| 5 | Windows-Policy <input type="button" value="v"/> |

Native Profiling per AP Group

Ap Groups > Edit 'Conference-Room-1'

General WLANs RF Profile APs 802.11u

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

AP Group > Policy Mappings

AP Group Name Conference-Room-1

WLAN ID 1

Priority Index (1-16)

Local Policy Local_Policy

| Priority Index | Local Policy Name |
|----------------|---|
| 1 | iPad-Policy <input type="button" value="v"/> |
| 2 | Android-Policy <input type="button" value="v"/> |
| 3 | iPhone-Policy <input type="button" value="v"/> |
| 4 | MacBook-Policy <input type="button" value="v"/> |

NAC Enable
Remove

Restriction: First Matched Rule Applies

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

Agenda

Managing the BYOD Evolution



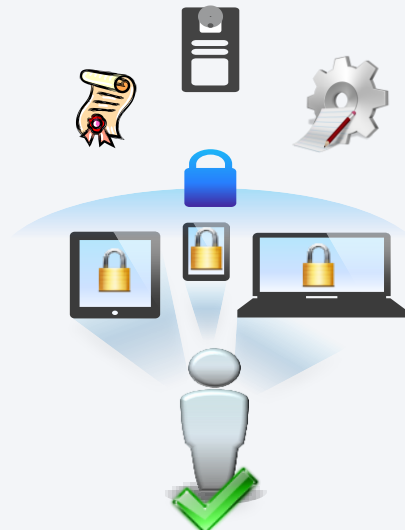
Personal Devices on Network

Network Components

BRKEWN-2020



Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations



Wireless



Wired



Remote Access



ISE



Prime

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Cisco *live!*



Bonjour Gateway on Cisco Wireless

Bonjour Protocol

VLAN 20



Services



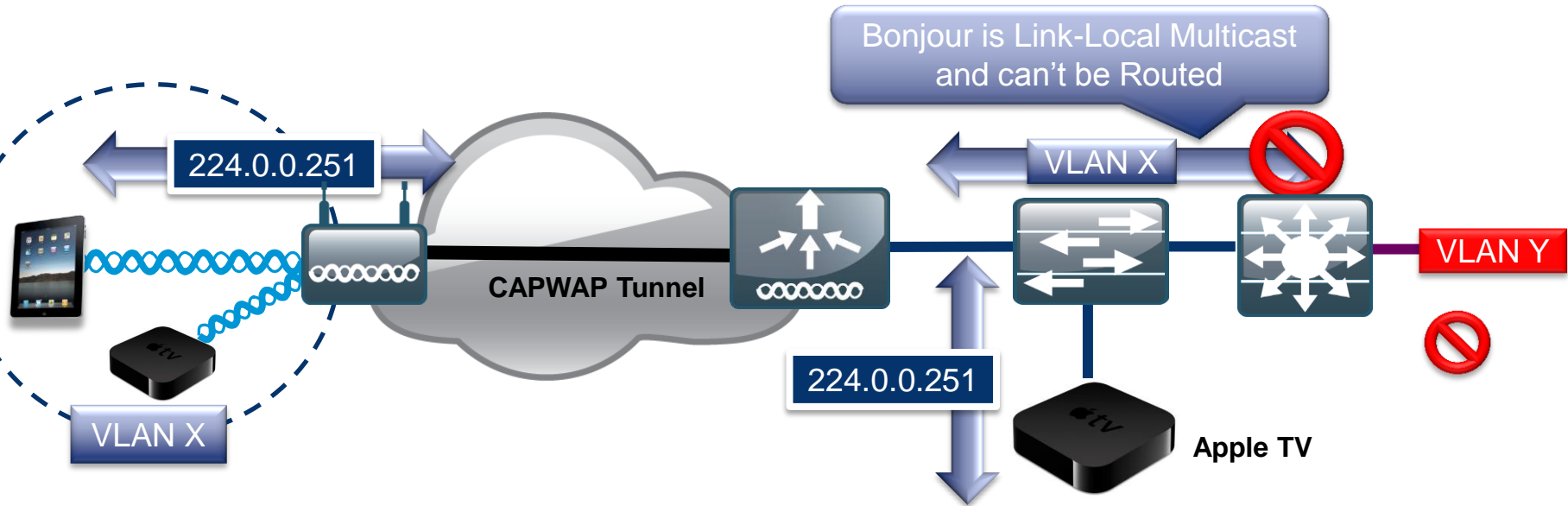
- Bonjour Protocol helps apple devices discover services
- Uses mDNS protocol to advertise and discover services
- Link Local: Does not cross subnets

VLAN 10



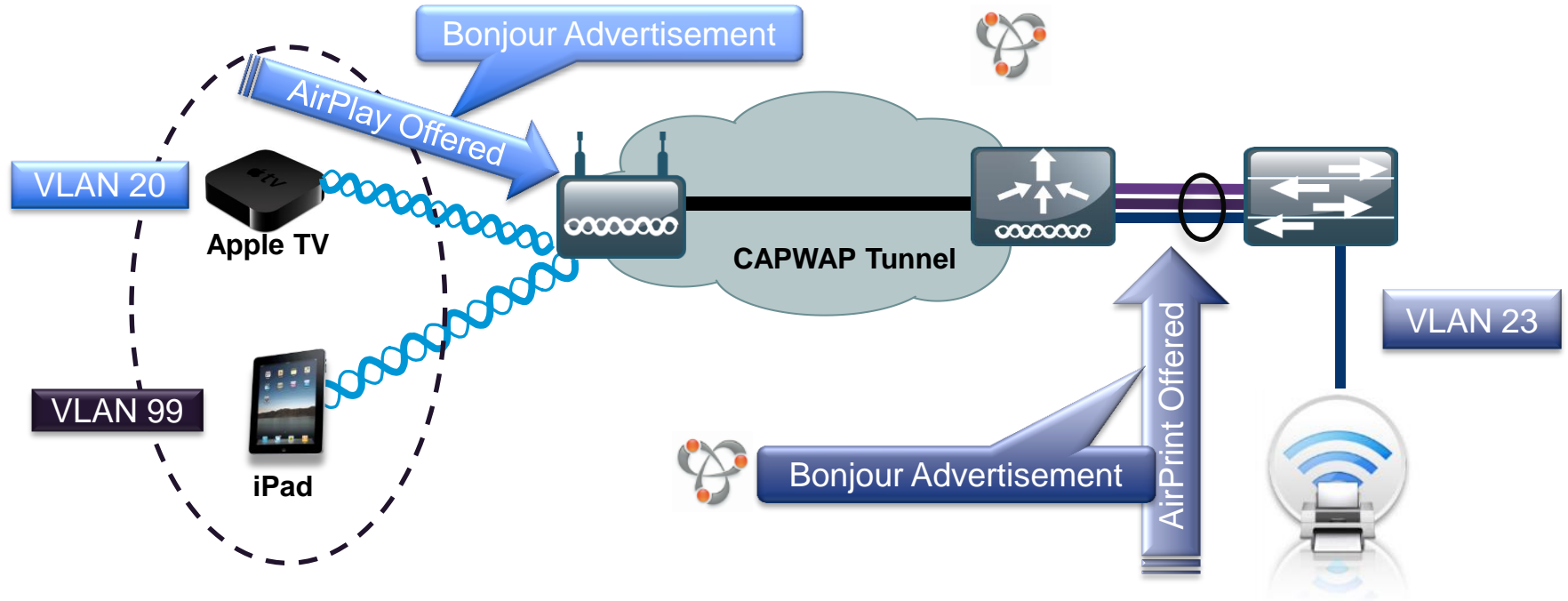
Clients

Bonjour Challenges across VLAN's



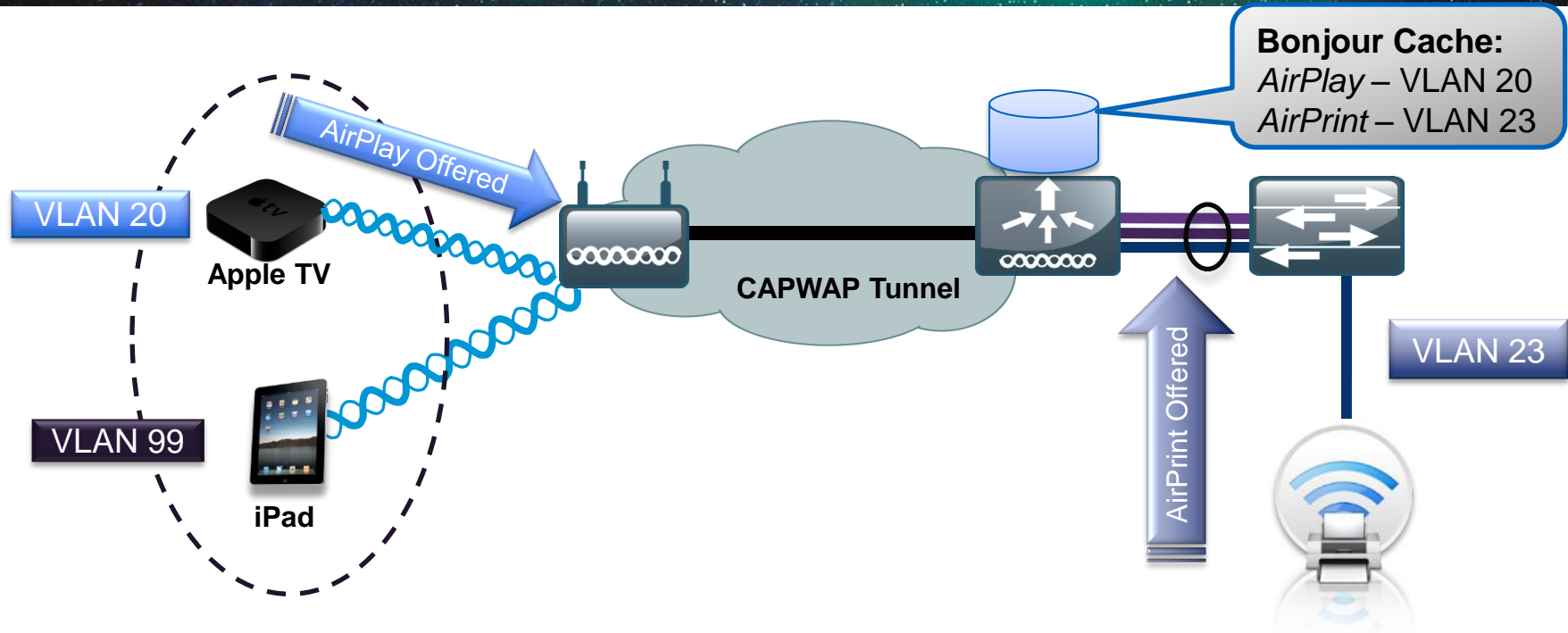
- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:
 - IPv4 Group Address – 224.0.0.251
 - IPv6 Group Address – FF02::FB

Bonjour mDNS Gateway on Cisco WLC



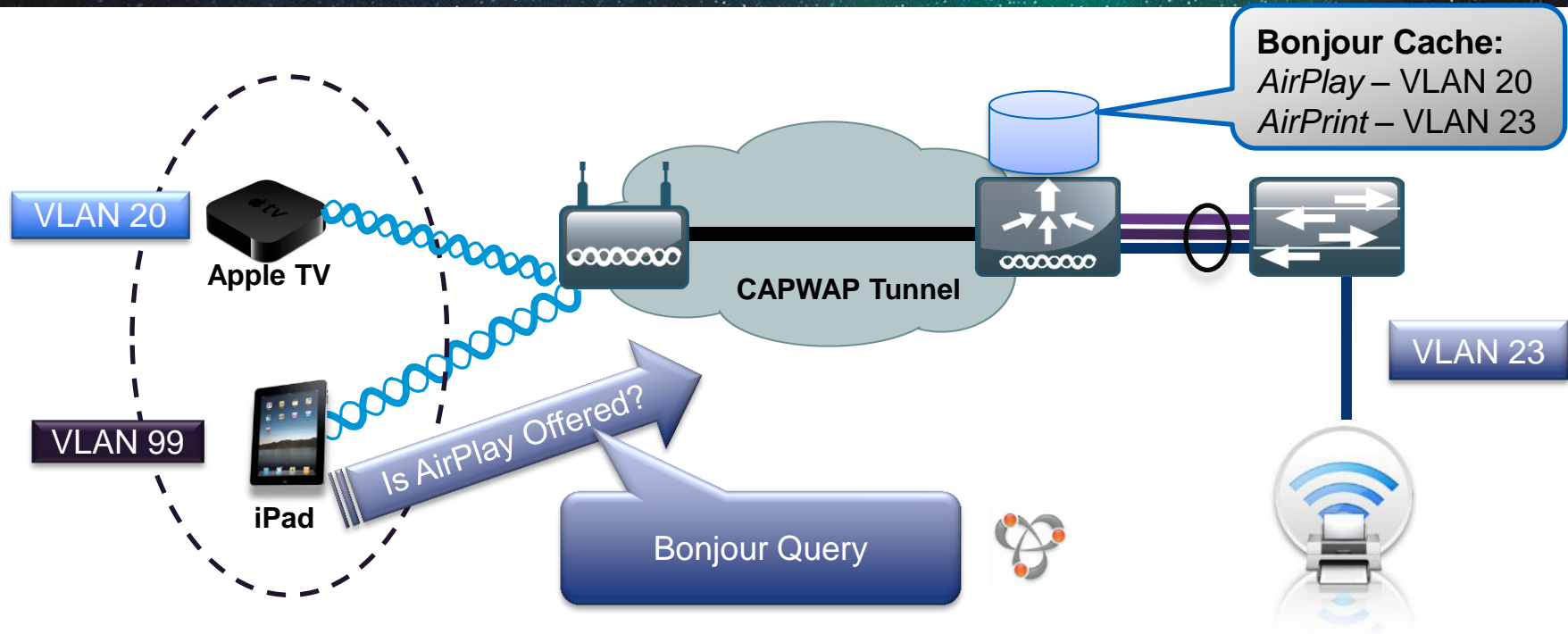
- Step 1 – Listen for Bonjour Services

Bonjour mDNS Gateway on Cisco WLC



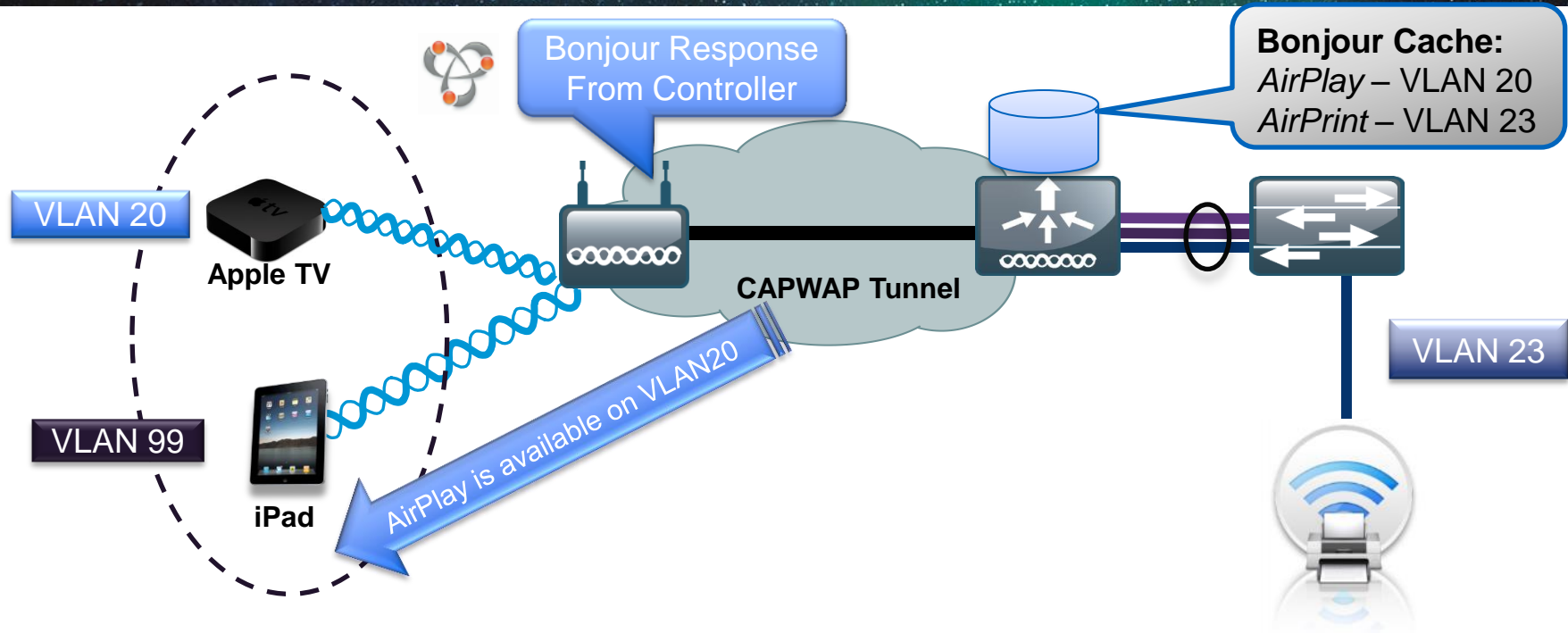
- Step 2 –Bonjour Services cached on the controller

Bonjour mDNS Gateway on Cisco WLC



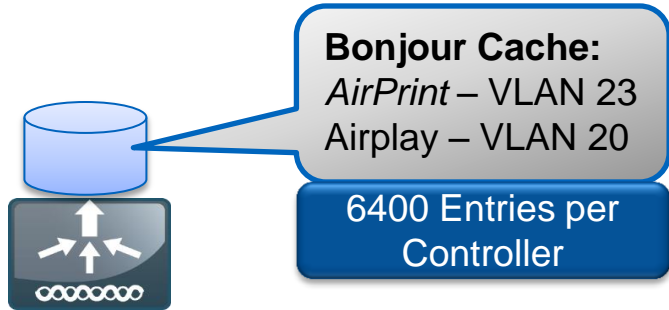
- Step 3 –Listen for Client Service Queries for Services

Bonjour mDNS Gateway on Cisco WLC



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

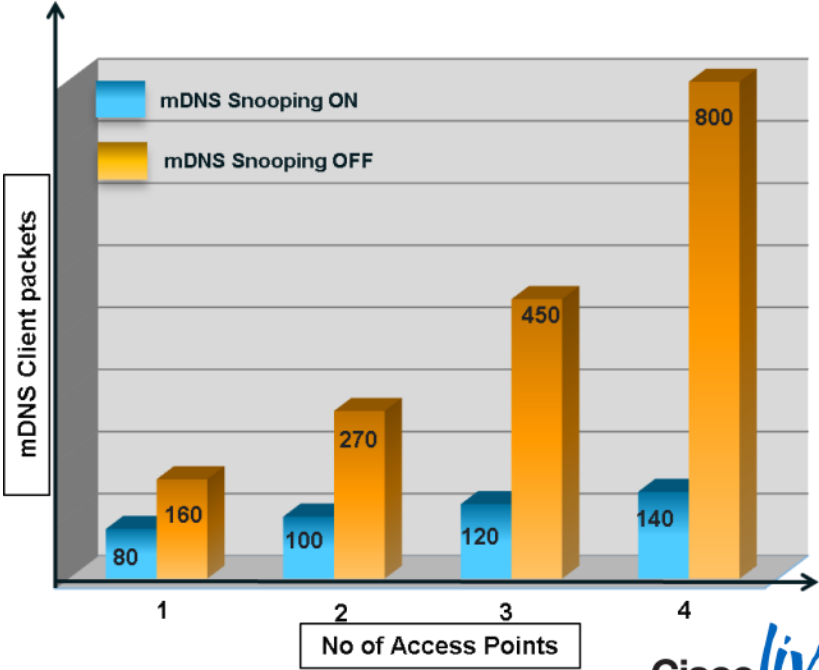
Bonjour Traffic Optimisation



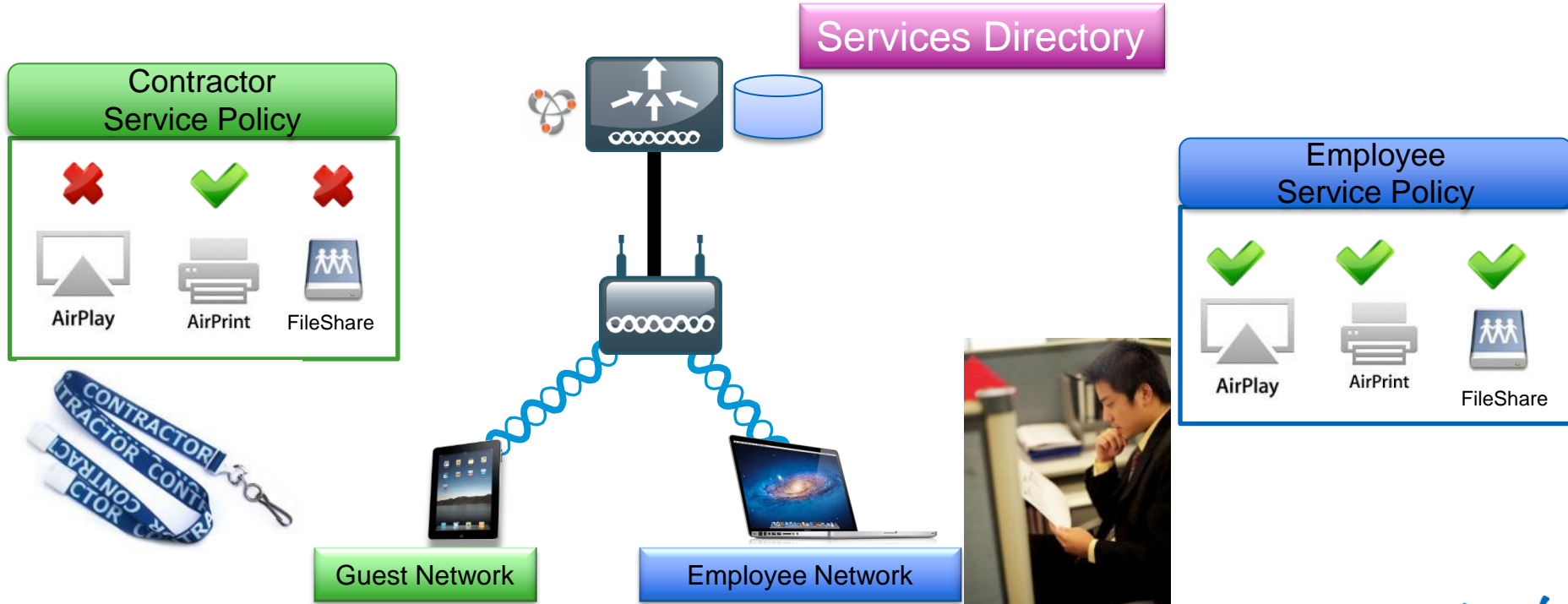
- Reason for Traffic optimisation**
- Bonjour Service query is cached on Controller
 - ✓ Not forwarded
 - Bonjour Client Query
 - ✓ Unicast Response
 - ✓ Not forwarded

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*)

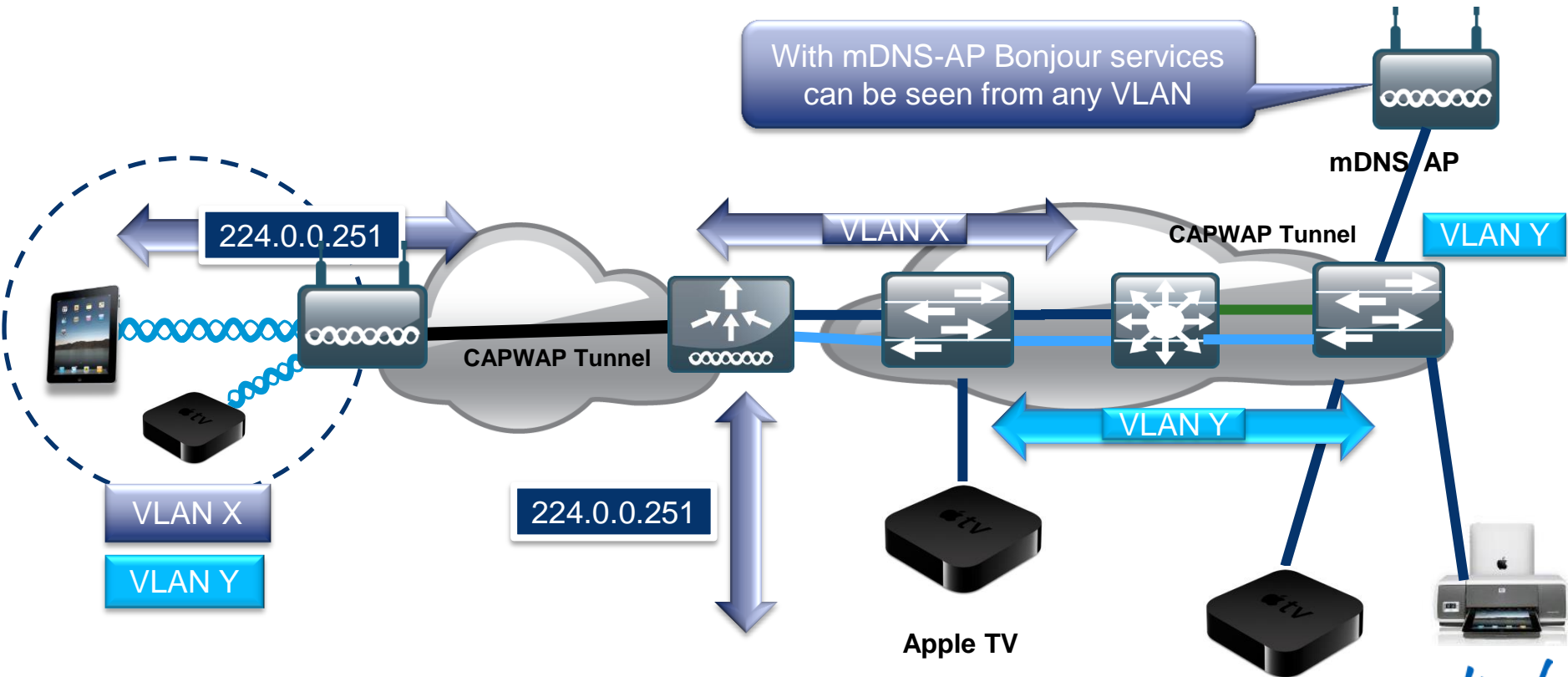
Printer Spool (*_printer._tcp*)

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

HTTP (*_http._tcp*)

Scanner (*_scanner._tcp*)

mDNS AP for a Non Layer 2 Adjacent Service



Summary of Bonjour Enabled Devices



For Your Reference

Controller mDNS Domain Name IP > Summary

Number of Domain Name-IP Entries 1

| Domain Name | MAC Address | IP Address | Vlan Id | Type | TTL |
|-----------------|-------------------|--------------|---------|----------|------|
| Apple-TV.local. | 10:40:f3:e7:83:c4 | 10.10.20.101 | 20 | Wireless | 4725 |

Navigation menu: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK

Left sidebar: Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, IPv6, mDNS (selected), Domain Names (highlighted), Advanced

Controller mDNS Domain Name IP > Summary

Number of Domain Name-IP Entries 3

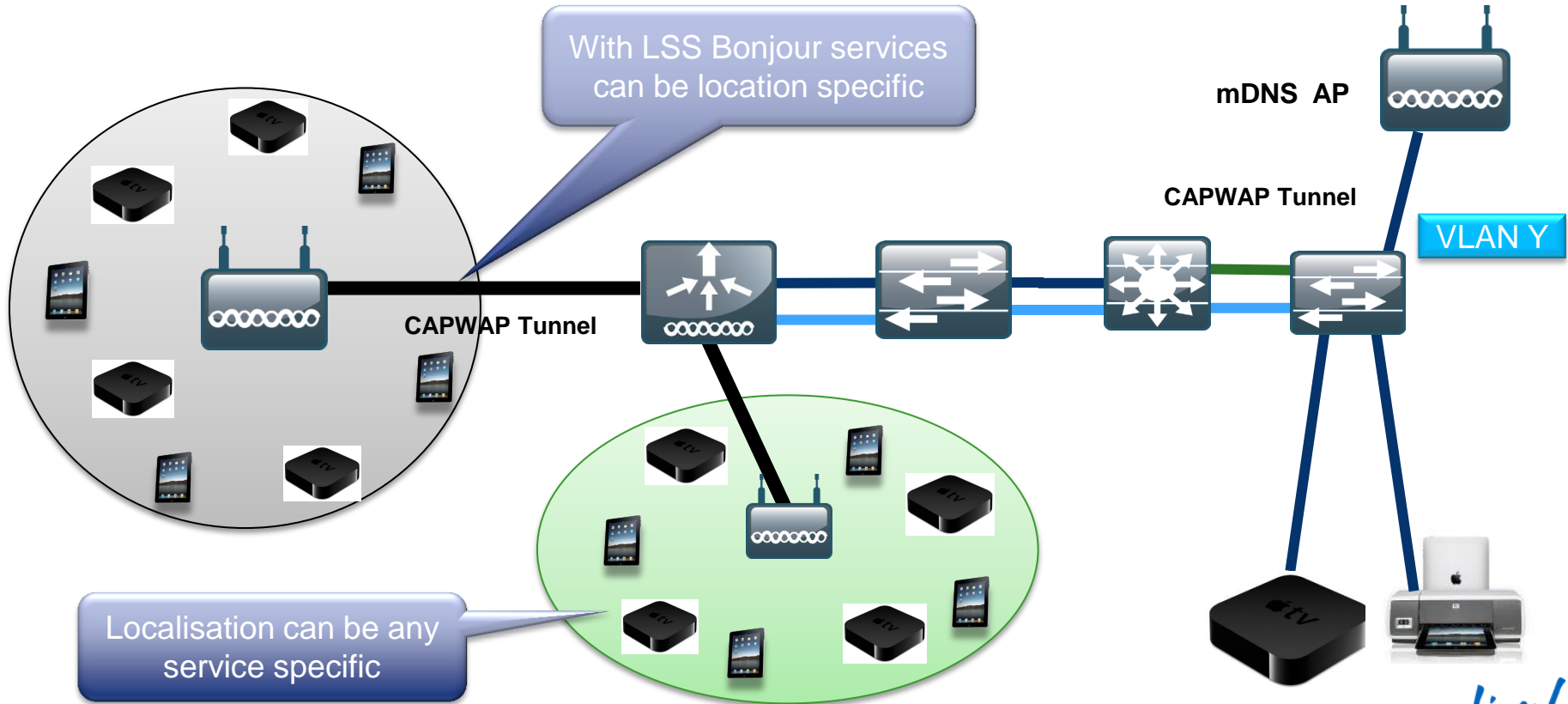
| Domain Name | MAC Address | IP Address | Vlan Id | Type |
|------------------------|-------------------|--------------|---------|---------|
| Adler-Dell4500.local. | 00:26:b9:cb:ee:f2 | 10.50.10.191 | 0 | Wired |
| Dell-M2300-MA2.local. | 00:1c:23:36:3e:d3 | 10.70.0.59 | 0 | mDNS AP |
| Office-Apple-TV.local. | 70:56:81:db:cd:a0 | 10.70.0.206 | 0 | mDNS AP |

1. Maximum of 500 entries will be displayed.

Navigation menu: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK

Left sidebar: Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, Internal DHCP Server, Mobility Management

Location Specific Service for Bonjour



Summary

Managing the BYOD Evolution



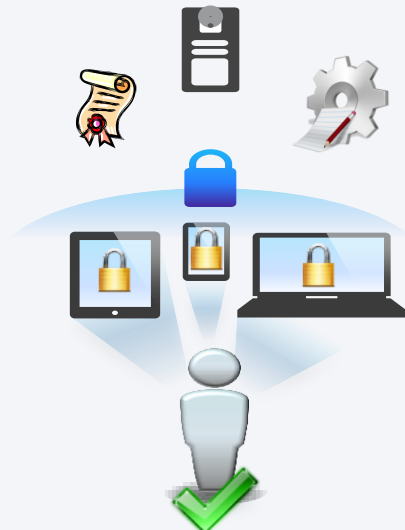
Personal Devices on Network

Network Components

BRKEWN-2020



Identification and Security Policy Enforcement



Securely On-Board the Device



Simplified Bonjour Operations



Wireless



Wired



Remote Access



ISE



Prime

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Cisco *live!*



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



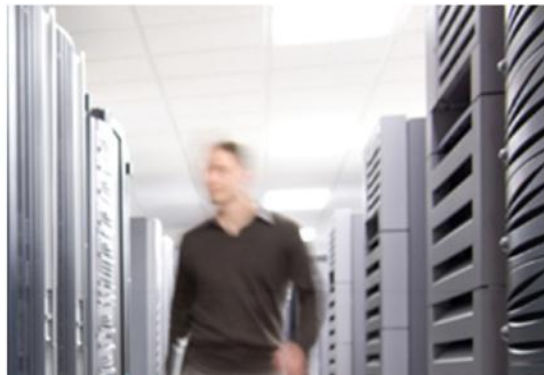
Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



CISCO TM

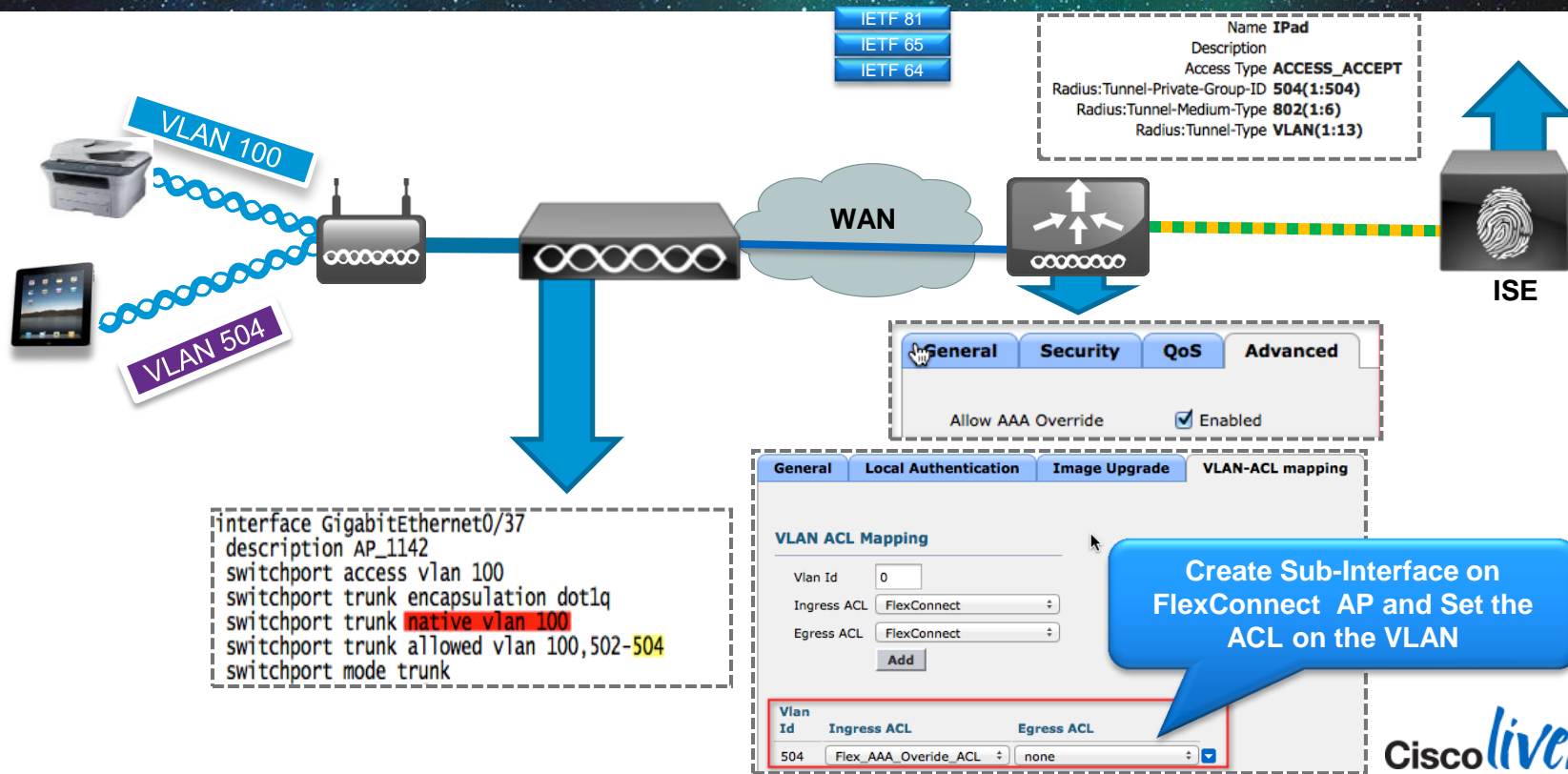


Configurations for Your Reference



FlexConnect and AAA Override

Setting the VLAN for Locally Switched Clients





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.

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

- **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)

Server IP Address

Shared Secret Format

Shared Secret

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

Server Status

Support for RFC 3576

Server Timeout

1

Enable "RFC 3576" for Support Change of Authorisation

2

Add to Accounting Servers to Receive Session Statistics

RADIUS Accounting Servers

MAC Delimiter

| Network User | Server Index | Server Address | Port | IPSec | Admin Status |
|-------------------------------------|--------------|----------------|------|----------|---|
| <input checked="" type="checkbox"/> | <u>1</u> | 10.10.10.10 | 1813 | Disabled | Enabled <input checked="" type="checkbox"/> |



Configuring the WLAN for Secure Connectivity

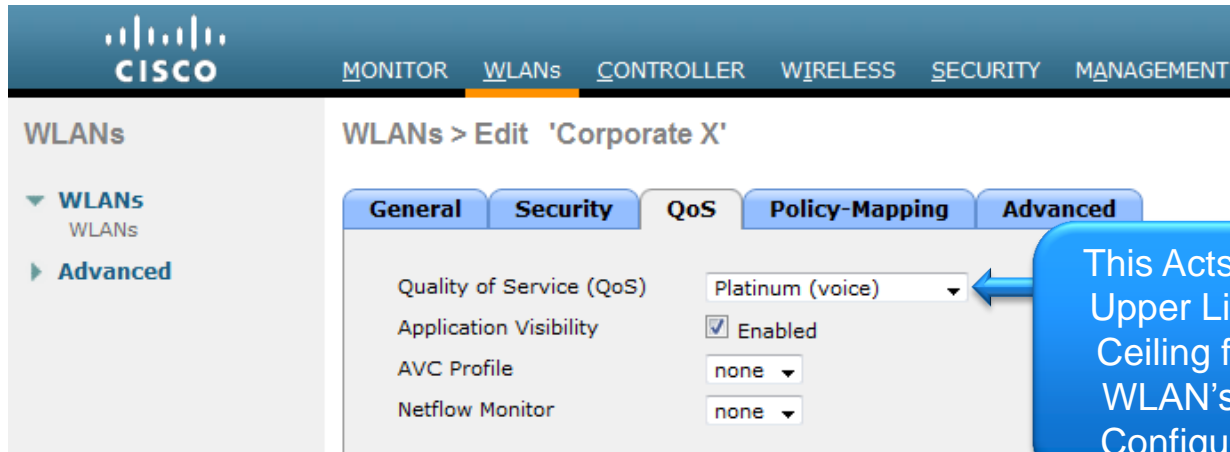
Enabling Secure Authentication and Encryption with WPA2-Enterprise

The screenshot shows the Cisco WLAN configuration interface for a WLAN named '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'. Below this, 'MAC Filtering' is disabled. The 'Fast Transition' section has 'Fast Transition' disabled. The 'Protected Management Frame' section has 'PMF' set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA Policy' disabled, 'WPA2 Policy' checked, and 'WPA2 Encryption' with 'AES' checked and 'TKIP' disabled. The 'Authentication Key Management' section has '802.1X' checked and 'Enable' selected.

1
WPA2 Security with AES Encryption

Setting the WLAN QoS Level for Override

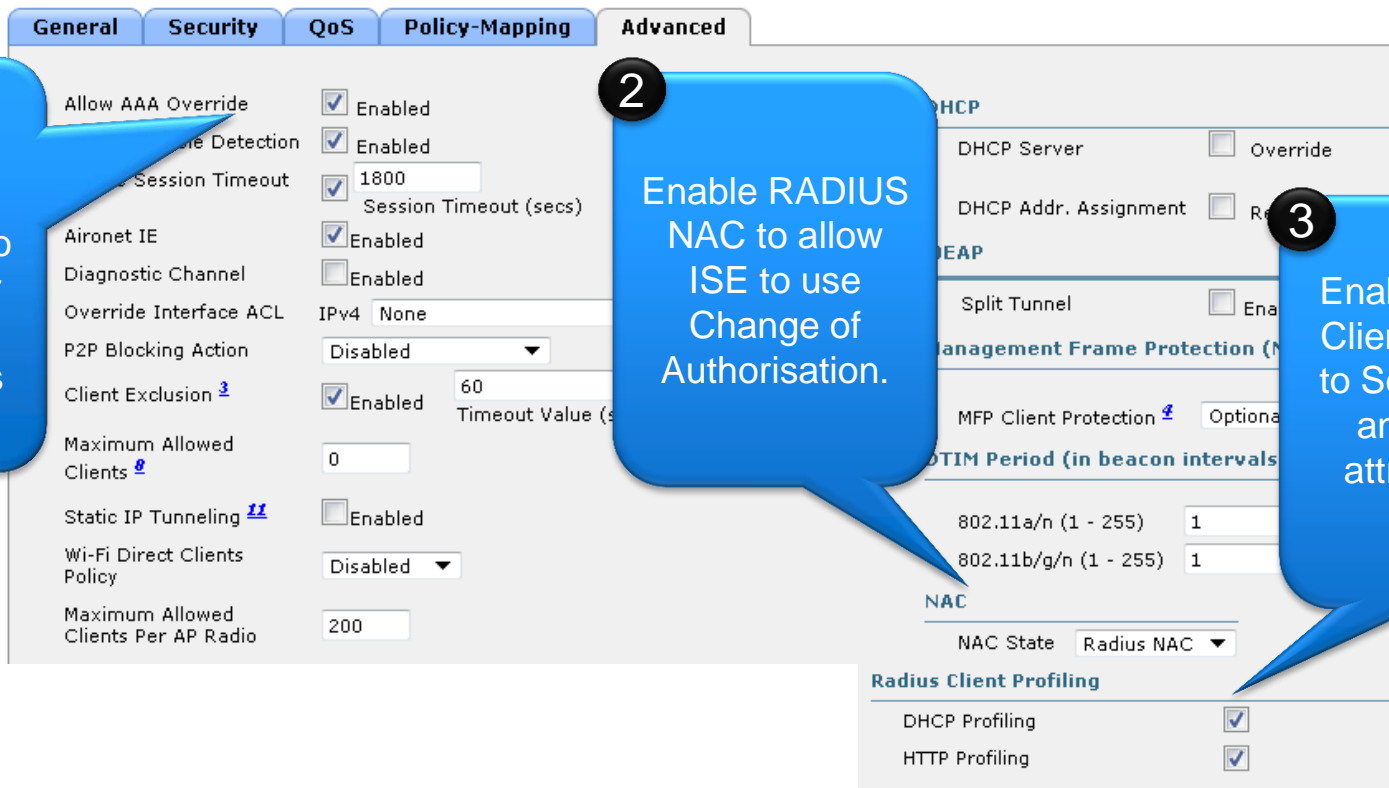
Using WMM, the QoS Level is Based on the Marking of the Packet.



The screenshot shows the Cisco configuration interface for a WLAN named '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'. Other settings include 'Application Visibility' (Enabled), 'AVC Profile' (none), and '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



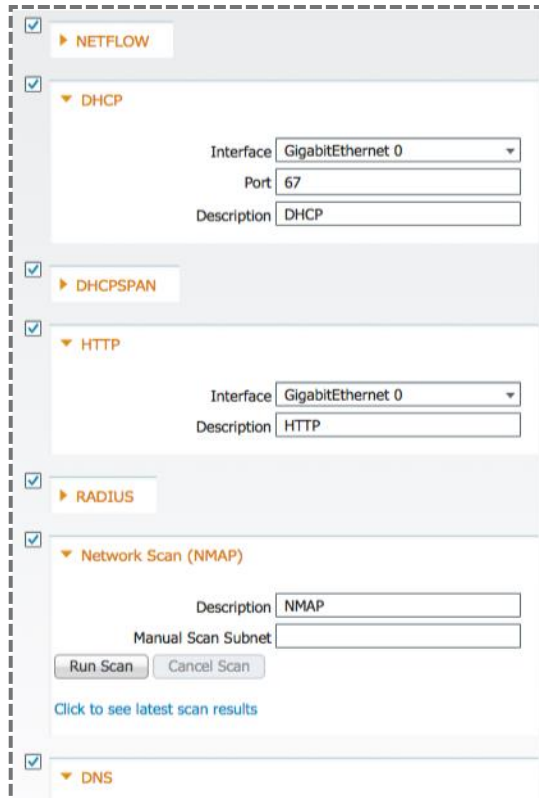
The screenshot shows the 'Advanced' tab of a WLAN configuration page. Three callouts highlight specific settings:

- 1** Callout: "Allow AAA Override to Permit ISE to Modify User Access Permissions". Points to the "Allow AAA Override" checkbox, which is checked and labeled "Enabled".
- 2** Callout: "Enable RADIUS NAC to allow ISE to use Change of Authorisation.". Points to the "NAC State" dropdown menu, which is set to "Radius NAC".
- 3** Callout: "Enable Radius Client Profiling to Send DHCP and HTTP attributes to ISE.". Points to the "Radius Client Profiling" section, where both "DHCP Profiling" and "HTTP Profiling" checkboxes are checked.

Other visible settings include:

- Session Timeout: 1800 (secs)
- Client Exclusion: Enabled
- Static IP Tunneling: Disabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200
- DHCP Profiling: Enabled
- HTTP Profiling: Enabled

Configuring ISE Profiling Sensors



The screenshot shows the configuration interface for ISE Profiling Sensors. It is organized into several sections, each with a checkbox on the left and a title on the right:

- NETFLOW**: A section with a checked checkbox and a right-pointing arrow.
- DHCP**: A section with a checked checkbox and a downward-pointing arrow. It contains three input fields:
 - Interface: GigabitEthernet 0
 - Port: 67
 - Description: DHCP
- DHCPSPAN**: A section with a checked checkbox and a right-pointing arrow.
- HTTP**: A section with a checked checkbox and a downward-pointing arrow. It contains two input fields:
 - Interface: GigabitEthernet 0
 - Description: HTTP
- RADIUS**: A section with a checked checkbox and a right-pointing arrow.
- Network Scan (NMAP)**: A section with a checked checkbox and a downward-pointing arrow. It contains:
 - Description: NMAP
 - Manual Scan Subnet: (empty input field)
 - Buttons: Run Scan and Cancel Scan
 - Link: [Click to see latest scan results](#)
- DNS**: A section with a checked checkbox and a downward-pointing arrow.

- 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

1. Configure Integration with External CA Server

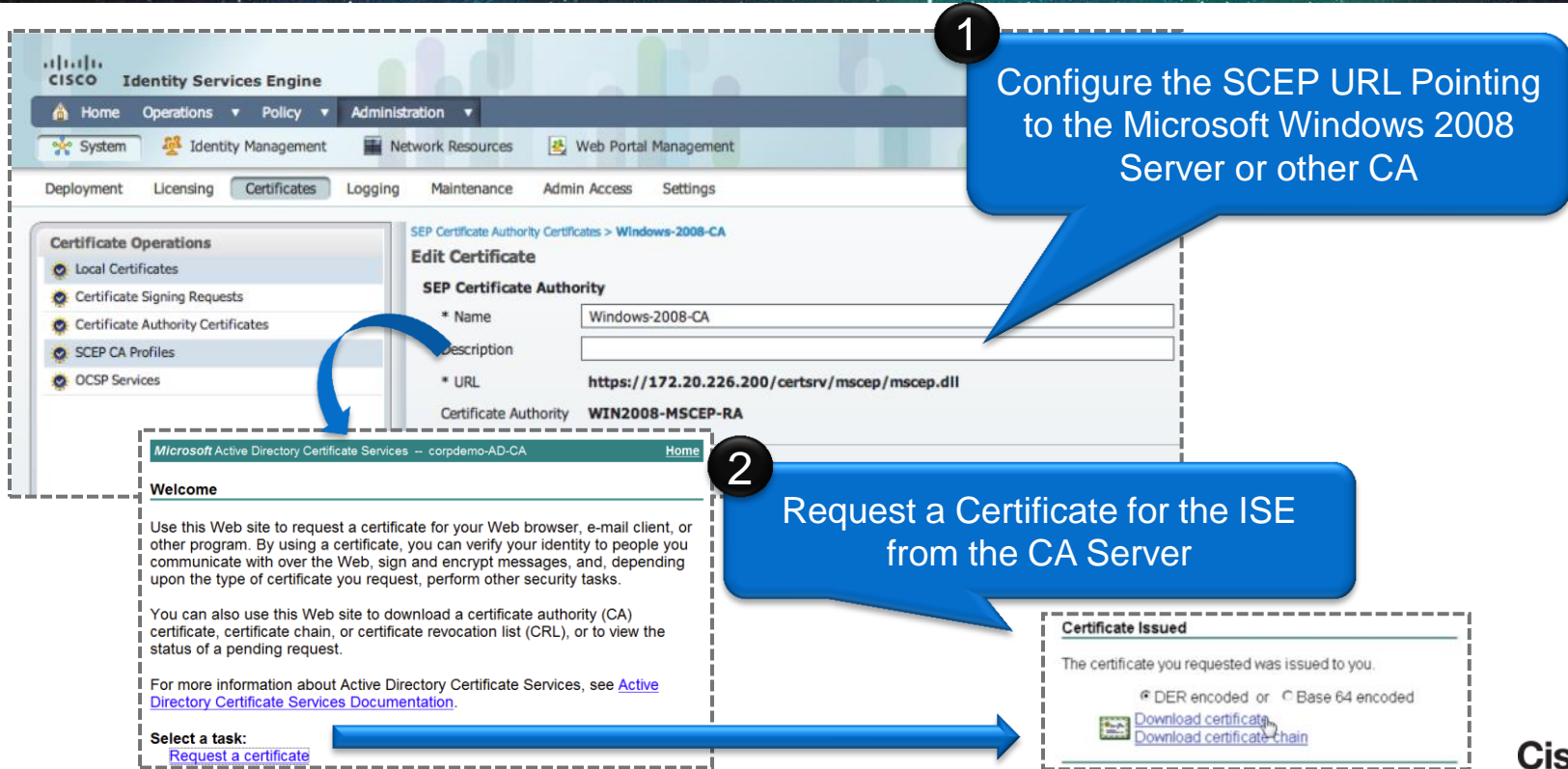
- Define SCEP URL and certificates.
- Example – Active Directory, CA Server or Internal DB.

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



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

Microsoft Active Directory Certificate Services -- corpdemo-AD-CA

Welcome

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](#)

Certificate Issued

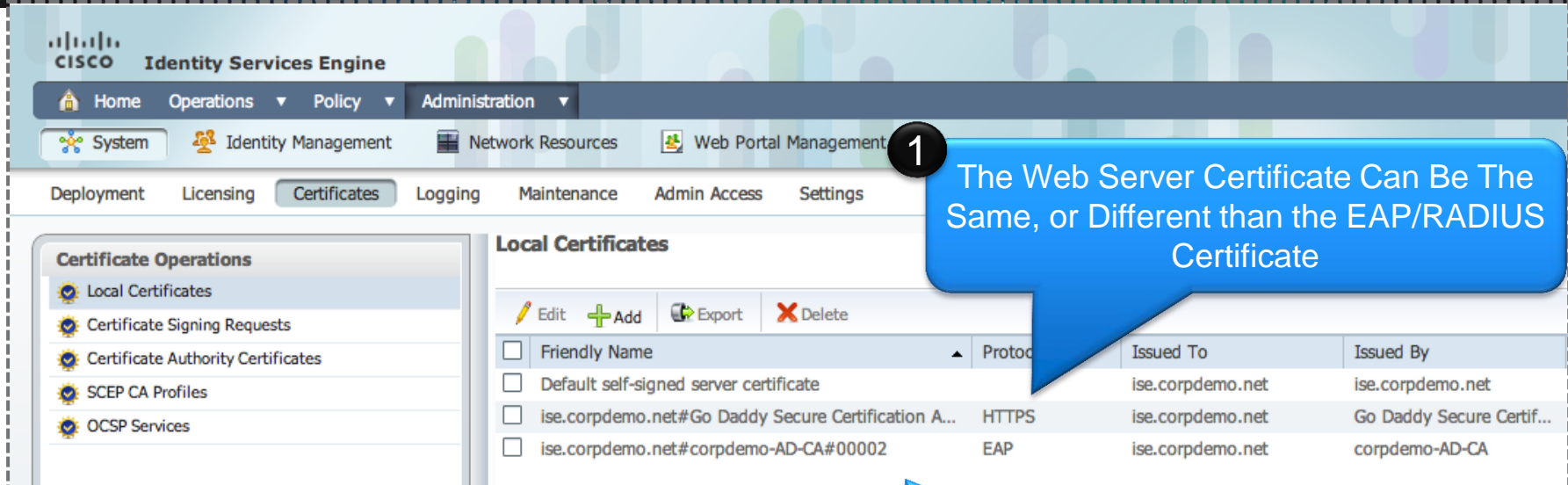
The certificate you requested was issued to you.

DER encoded or Base 64 encoded

[Download certificate](#)
[Download certificate chain](#)

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 section is active, showing options for Deployment, Licensing, Certificates, Logging, Maintenance, Admin Access, and Settings.

The main content area displays "Local Certificates" with a table of existing certificates. A blue callout bubble with the number "1" points to the table, stating: "The Web Server Certificate Can Be The Same, or Different than the EAP/RADIUS Certificate".

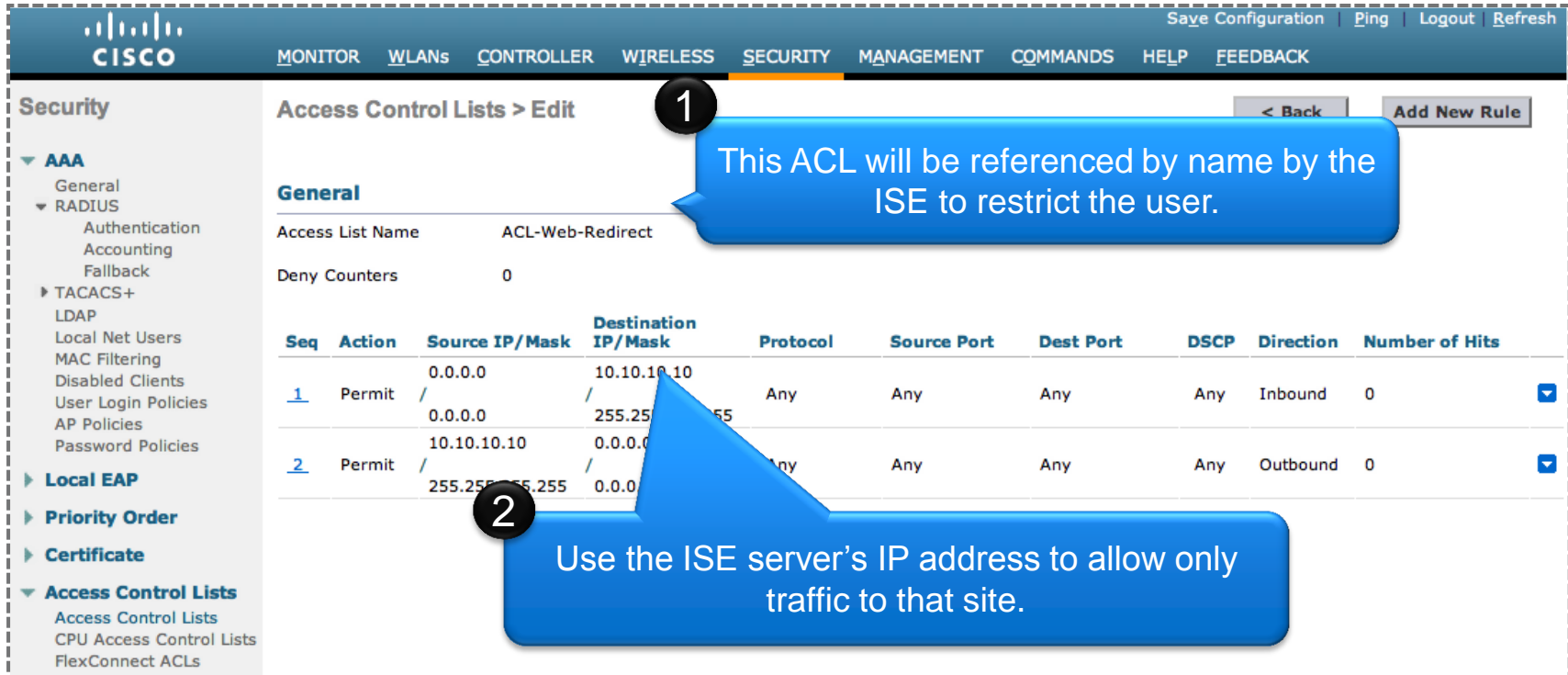
| <input type="checkbox"/> | Friendly Name | Protocol | Issued To | Issued By |
|--------------------------|---|----------|------------------|---------------------------|
| <input type="checkbox"/> | Default self-signed server certificate | | ise.corpdemo.net | ise.corpdemo.net |
| <input type="checkbox"/> | 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 |

2

Use the Certificate from Your CA Server for EAP Authentication

Configuring the Web-Authentication Redirect ACL

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



Security

Access Control Lists > Edit

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 / | 10.10.10.10 / | Any | Any | Any | Any | Inbound | 0 |
| 2 | Permit | 10.10.10.10 / | 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.



Authorisation Rules for Supplicant Provisioning

Example Rule Set to Force PEAP Devices to Register.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change

First Matched Rule Applies

Exceptions (0)

Standard

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|--------|-------------------------------|--|--|
| ✓ | Black List Default | if Blacklist | then Blacklist_Access Edit ▾ |
| ✓ | BYOD_CP | if Network Access:EapTunnel EQUALS PEAP | then BYOD_CP Edit ▾ |
| ✓ | EAP-TLS Users Get Full Access | if Network Access:EapAuthentication EQUALS EAP-TLS | then PermitAccess Edit ▾ |
| ✓ | DenyAccess | | DenyAccess Edit ▾ |

1 EAP-TLS Users Get Full Access

2 The Supplicant Provisioning Portal is Displayed to PEAP Devices

Defining the Supplicant Provisioning Authorisation Profile

1 Configure Redirect ACL On WLC

| | | | | | |
|--------|-----------------|-----------------|-----|-----|-----|
| Permit | 0.0.0.0 | 255.255.255.255 | Any | Any | Any |
| Permit | 10.10.10.10 | / 0.0.0.0 | / | Any | Any |
| | 255.255.255.255 | 0.0.0.0 | Any | Any | Any |

2 Choose "Supplicant Provisioning" for the Redirect Portal



Supplicant Provisioning Configuration: EAP-TLS

Using the ISE to Provision Certificates

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The main view displays a table of rules for Native Supplicant Configuration. The table has columns for Rule Name, Identity Groups, Operating Systems, Other Conditions, and Results. The rules are:

| 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 |

A callout box labeled '1' points to the 'BYOD Android' rule, specifically to the 'Other Conditions' field. A second callout box labeled '2' points to the 'Native Supplicant Profile' configuration window, which shows the following settings:

- Name: EAP-TLS Provision
- Description: (empty)
- Operating System: ALL
- Connection Type: Wired, Wireless
- *SSID: CorporateX
- Security: WPA2 Enterprise
- * Allowed Protocol: TLS
- * Key Size: 2048

1

Define Who Can Provision Devices

Expression
 ActiveDirectory:ExternalGroups E... Equals Employees

2

Use WPA2 Security and TLS for the EAP Type

Client Provisioning Policy

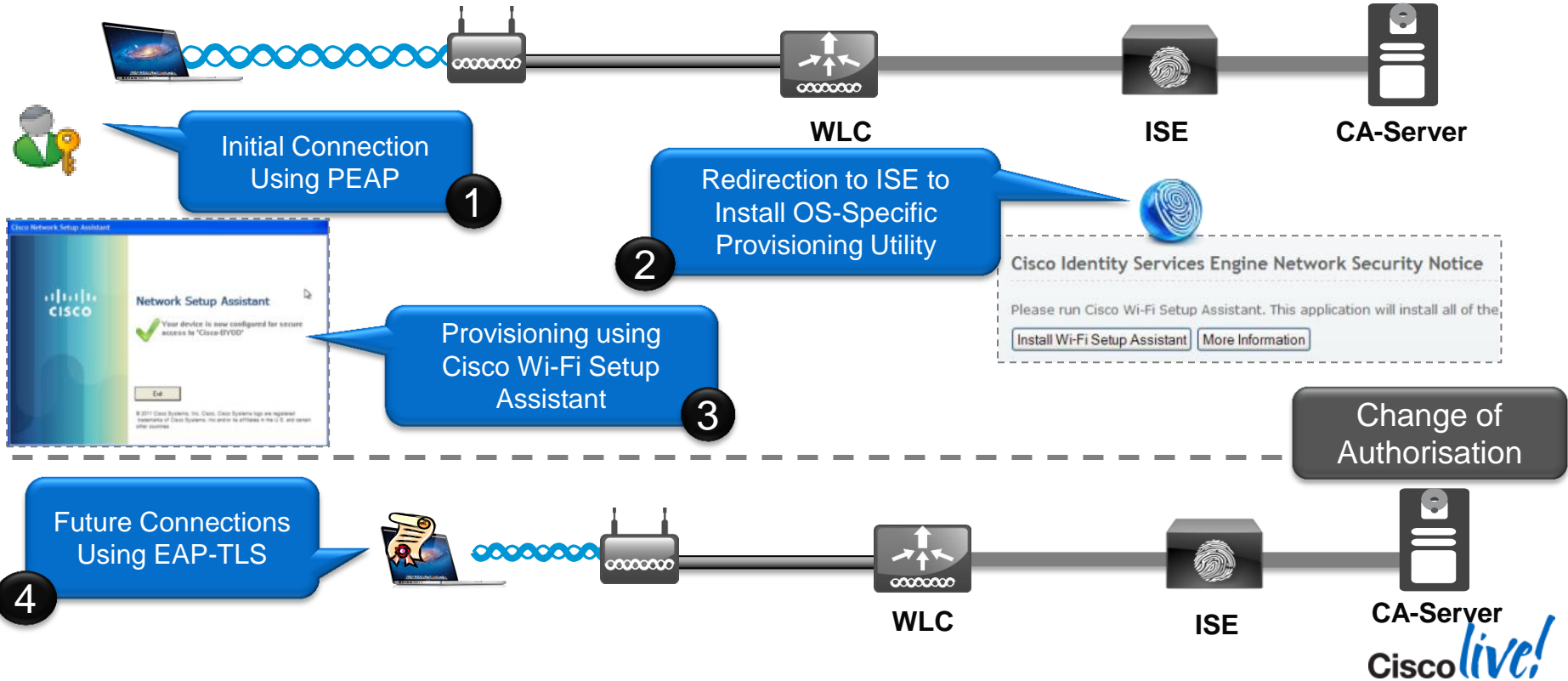


Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive when 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 |
|---|-----------------|-------------------|------------------------------------|---|
| <input checked="" type="checkbox"/> IOS | If Any | Mac iOS All | AD1:ExternalGroups EQUALS cts.I... | WiFi_Profile |
| <input checked="" type="checkbox"/> Android | If Any | Android | AD1:ExternalGroups EQUALS cts.I... | WiFi_Profile |
| <input checked="" type="checkbox"/> WinThings | If Any | Windows... | AD1:ExternalGroups EQUALS cts.I... | WinSPWizard 1.0.0.14 And WiFi_Profile |
| <input checked="" type="checkbox"/> MAC-OSX | If Any | Mac OSX | AD1:ExternalGroups EQUALS cts.I... | MacOsXSPWizard 1.0.0.6 And WiFi_Profile |

Windows/Mac OS X Device Provisioning





Staying Updated with Latest Applications

- 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.pac
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



- 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

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 | |
|------------------------------------|-----------------------------|-------------------------------------|
| AFP | _afpovertcp._tcp.local. | <input checked="" type="checkbox"/> |
| AirPrint-PDL | _pdl-datastream._tcp.local. | <input checked="" type="checkbox"/> |
| AirPrint-Spool | _printer._tcp.local. | <input checked="" type="checkbox"/> |
| AirPrint-ipp | _ipp._tcp.local. | <input checked="" type="checkbox"/> |
| AirTunes | _raop._tcp.local. | <input checked="" type="checkbox"/> |
| Airplay-Mac | _appletv-v2._tcp.local. | <input checked="" type="checkbox"/> |
| Airplay-iOS | _airplay._tcp.local. | <input checked="" type="checkbox"/> |
| AppleRemoteDesktop | _net-assistant._udp.local. | <input checked="" type="checkbox"/> |
| AppleTV-Remote | _touch-able._tcp.local. | <input checked="" type="checkbox"/> |
| HTTP | _http._tcp.local. | <input checked="" type="checkbox"/> |
| Scanner | _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 |

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"/> |

mDNS Profile for Employee





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

Configure mDNS- AP from CLI

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 | 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 |

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:

```
(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™