TOMORROW starts here.
Design and Deployment of Enterprise WLANs
BRKEWN-2010

Sujit Ghosh
Senior Manager Technical Marketing
Enterprise Networking Group
Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture
Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture
Cisco Unified Wireless Principles

- **Components**
  - Wireless LAN controllers
  - Aironet access points
  - Management (Prime Infrastructure)
  - Mobility Service Engine (MSE)

- **Principles**
  - AP must have CAPWAP connectivity with WLC
  - Configuration downloaded to AP by WLC
  - All Wi-Fi traffic is forwarded to the WLC
Centralised Wireless LAN Architecture

What Is CAPWAP?

- CAPWAP: Control and Provisioning of Wireless Access Points is used between APs and WLAN controller and based on LWAPP
- CAPWAP carries control and data traffic between the two
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (optional)
- LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless
- CAPWAP is not supported on Layer 2 mode deployment
CAPWAP State Machine

- AP Boots UP
- Discovery
- DTLS Setup
- Join
- Reset
- Image Data
- Config
- Run
AP Controller Discovery

Controller Discovery Order:

- Layer 2 join procedure attempted on LWAPP APs
  - (CAPWAP does not support Layer 2 APs)
  - Broadcast message sent to discover controller on a local subnet

- Layer 3 join process on CAPWAP APs and on LWAPP APs after Layer 2 fails
  - Previously learned or primed controllers
  - Subnet broadcast
  - DHCP option 43
  - DNS lookup
Efficient CAPWAP Operation

Best Practices

- Define the Wireless Access Point Device DHCP Scopes
- Default router IP Address for Access Point scope
- Helper address (forwarding UDP 5246 to the WLCs management interface)
- Domain name
- Appropriate DHCP Lease timer for Aps
- Pool sizes for WLAN devices in accordance to different types of sites
- If NAT is used, static 1-to-1 NAT to an outside address is recommended
7.4, 7.5, 7.6 ? Which Version Should I Use?

- WLC 5508 supports 6.0 and above
- WLC7500, WiSM-2 and WLC2504 only supported in 7.0 onwards
- 7.4.110 is the latest MD AssureWave (Blue Ribbon)
- Please note the current revision of 7.4.121 is the recommended one for you today with latest fixes
- AP3700 (7.6), AP3600+11ac (7.5), AP1600(7.4), AP2600 (7.3), AP3600(7.2)
## Release Recommendations

<table>
<thead>
<tr>
<th>Software Release</th>
<th>Deployed Release</th>
<th>Recommended Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Deployment (MD) release</td>
<td>7.0 MD release train</td>
<td>7.4 MD release train</td>
</tr>
<tr>
<td>Early Deployment (ED) releases for pre-802.11ac deployments</td>
<td>7.2 ED releases</td>
<td>7.4 MD release train (7.4.121.0 is the minimum recommended release)</td>
</tr>
<tr>
<td></td>
<td>7.3 ED releases</td>
<td></td>
</tr>
<tr>
<td>Early Deployment (ED) releases for 802.11ac deployments</td>
<td>7.5 ED release</td>
<td>7.6 ED release</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software Release</th>
<th>ISE</th>
<th>Prime Infra</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0 (MD train)</td>
<td>1.2</td>
<td>2.0</td>
<td>7.6</td>
</tr>
<tr>
<td>7.4 (MD train)</td>
<td>1.2</td>
<td>2.0</td>
<td>7.6</td>
</tr>
<tr>
<td>7.6 (ED)</td>
<td>1.2</td>
<td>1.4.1</td>
<td>7.6</td>
</tr>
</tbody>
</table>

Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture
Mobility Defined

- Mobility is a key reason for wireless networks
- Mobility means the end-user device is capable of moving location in the networked environment
- **Roaming** occurs when a wireless client moves association from one AP and re-associates to another, typically because it’s **mobile**!
- Mobility presents new challenges:
  - Need to scale the architecture to support client roaming—roaming can occur intra-controller and inter-controller
  - Need to support client roaming that is seamless (fast) and preserves security
Scaling the Architecture with Mobility Groups

- Mobility Group allows controllers to peer with each other to support seamless roaming across controller boundaries.
- APs learn the IPs of the other members of the mobility group after the CAPWAP Join process.
- Support for up to 24 controllers, 24000 APs per mobility group.
- Mobility messages exchanged between controllers.
- Data tunnelled between controllers in EtherIP (RFC 3378).
- 7.5 has the option of using EOIP or CAPWAP tunnels between controllers.
Scaling the Architecture with Mobility Groups

With Inter Release Controller Mobility (IRCM) roaming is supported between 7.4 7.5 and 7.6

One WLC Network → Mobility Group → 24 WLCs in a Mobility Group → Mobility Domain

- Mobility Group (7.4)
- Mobility Group (7.5)
- Mobility Group (7.6)

72 WLCs in a Mobility Domain
How Long Does an STA Roam Take?

- Time it takes for:
  - Client to disassociate +
  - Probe for and select a new AP +
  - 802.11 Association +
  - 802.1X/EAP Authentication +
  - Rekeying +
  - IP address (re) acquisition

- All this can be on the order of seconds… Can we make this faster?
Roaming Requirements

- Roaming must be fast … Latency can be introduced by:
  - Client channel scanning and AP selection algorithms
  - Re-authentication of client device and re-keying
  - Refreshing of IP address

- Roaming must maintain security
  - Open auth, static WEP—session continues on new AP
  - WPA/WPAv2 Personal—New session key for encryption derived via standard handshakes
  - 802.1x, 802.11i, WPA/WPAv2 Enterprise—Client must be re-authenticated and new session key derived for encryption
How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact

- Eliminating the (re)IP address acquisition challenge
- Eliminating full 802.1X/EAP reauthentication
Intra-Controller Roaming: Layer 2 Roaming

- Client Roams to a Different AP
  - Client database entry with new AP and appropriate security context
  - No IP address refresh needed

WLC-1 Client Database ➔ Client Data (MAC, IP, QoS, Security) ➔ VLAN X ➔ WLC-2 Client Database

WLC-1 ➔ Mobility Message Exchange ➔ WLC-2

WLC-1 CAPWAP Tunnel ➔ CAPWAP Tunnel ➔ WLC-2

WLC-1 Client

WLC-2 Client Database

- Mobility Message Exchange
- Roaming Data Path
- VLAN X
- CAPWAP Tunnel
Client Roaming Between Subnets:
**Layer 3**

- **VLAN X**: WLC-1 Client Database
  - Prerooting Data Path
  - Anchor Controller
- **VLAN Z**: WLC-2 Client Database
  - Mobility Message Exchange
  - Data Tunnel
  - Foreign Controller

**WLC-1 Client Database**

**WLC-2 Client Database**

**VLAN X** to **VLAN Z**

**CAPWAP Tunnel**

**Client Roams to a Different AP**
Roaming: Inter-Controller
Layer 3

- L3 inter-controller roam: STA moves association between APs joined to the different controllers but client traffic bridged onto different subnets
- Client must be re-authenticated and new security session established
- Client database entry copied to new controller – entry exists in both WLC client DBs
- Original controller tagged as the “anchor”, new controller tagged as the “foreign”
- WLCs must be in same mobility group or domain
- No IP address refresh needed
- Symmetric traffic path established -- asymmetric option has been eliminated as of 6.0 release
- Account for mobility message exchange in network design
How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact

✓ Eliminating the (re)IP address acquisition challenge
  ▪ Eliminating full 802.1X/EAP reauthentication
Fast Secure Roaming
Standard Wi-Fi Secure Roaming
Note: Mechanism Is Needed to Centralise Key Distribution

- 802.1X authentication in wireless today requires three “end-to-end” transactions with an overall transaction time of > 500 ms
- 802.1X authentication in wireless today requires a roaming client to reauthenticate, incurring an additional 500+ ms to the roam

1. 802.1X Initial Authentication Transaction
2. 802.1X Reauthentication After Roaming
Cisco Centralised Key Management (CCKM)

- Cisco introduced CCKM in CCXv2 (pre-802.11i), so widely available, especially with application specific devices (ASDs)

- CCKM ported to CUWN architecture in 3.2 release

- In *highly controlled test environments*, CCKM roam times consistently measure in the 5-8 msec range!

- CCKM is most widely implemented in ASDs, especially VoWLAN devices

- To work across WLCs, WLCs must be in the same mobility group

- CCX-based laptops may not fully support CCKM – depends on supplicant capabilities

- CCKM is standardised in 802.11r, Apple iOS 6.0, iOS 7.0
802.11r Introduction

- IEEE Standard for Fast Roaming – CCKM / OKC.
- Introduces a new concept of roaming where the handshake with the new AP is done even before the client roams to the target AP.
- The initial handshake allows the client and APs to do PTK calculation in advance, thus reducing roaming time.
- The pre-created PTK keys are applied to the client and AP once the client does the re-association request / response exchange with new target AP.
- 802.11r provides 2 ways of roaming:
  1) Over-the-Air
  2) Over-the-DS (Distribution System)
- The FT (Fast Transition) key hierarchy is designed to allow the client to make fast BSS transitions between APs without the need to re-authenticate at every AP.
- WLAN configuration will have new AKM type called FT (Fast Transition)
Legacy clients may not associate with a WLAN that has 802.11r enabled along with 802.11i. If the driver or the supplicant that is responsible for parsing the Robust Security Network Information Element (RSN IE) is old and confused by the additional AKM (Authentication Key Management) suites advertised in the IE (IE48), the driver will not attempt to start the association process. Due to this limitation, legacy clients cannot send association requests to WLANs with a FT PSK or FT 802.1x configuration.

These legacy clients, however, can still associate with non-802.11r WLANs. Therefore the recommendation is to have a new unique WLAN. With unique SSIDs for the addition 802.11r FT WPA clients. And an additional WLAN for the 802.11r FT 802.1x clients.

An iPhone with 6.0 or 7.0 iOS could Authenticate to WLAN with both of these AKM’s. But because of legacy clients this is NOT recommended. A non-6.0/7.0 iOS client can’t associate.
# Multiple WLANs for Multiple Auth Types Each with a Unique SSID

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Type</th>
<th>Profile Name</th>
<th>WLAN SSID</th>
<th>Status</th>
<th>Security Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WLAN</td>
<td>1x Voice</td>
<td>1Voice</td>
<td>Enabled</td>
<td>[WPA2][Auth(802.1x)]</td>
</tr>
<tr>
<td>2</td>
<td>WLAN</td>
<td>1x Voice FT</td>
<td>1VoiceFT</td>
<td>Enabled</td>
<td>[WPA2][Auth(FT 802.1x)]</td>
</tr>
<tr>
<td>3</td>
<td>WLAN</td>
<td>PSK Voice</td>
<td>pskVoice</td>
<td>Enabled</td>
<td>[WPA2][Auth(PSK)]</td>
</tr>
<tr>
<td>4</td>
<td>WLAN</td>
<td>PSK Voice FT</td>
<td>pskVoiceFT</td>
<td>Enabled</td>
<td>[WPA2][Auth(FT-PSK)]</td>
</tr>
</tbody>
</table>

## 802.1x & 802.1x FT WLANs Unique SSIDs

## PSK & PSK FT WLANs With Unique SSIDs
802.11r (Fast Transition) and Client Devices
It can get a little Complex...

- An iPhone with iOS 6.0 can authenticate to a WLAN with and without “FT”.
- A non-6.0 iOS client can’t associate.
- Both iPhone 4 models will take the 6.0iOS upgrade.
- But iPhone 4 does not do 11r.
- The iPhone 4s does 11r (The iPhone 5 also).
- So, which one is it?

Do an internet search to find the Model if unsure.
Designing a Mobility Group/Domain

Design Considerations

- Less roaming is better – clients and apps are happier

- While clients are authenticating/roaming, WLC CPU is doing the processing – not as much of a big deal with latest controllers which has dedicated management/control processor

- L3 roaming & fast roaming clients consume client DB slots on multiple controllers – consider “worst case” scenarios in designing roaming domain size

- Leverage natural roaming domain boundaries

- Mobility Message transport selection: multicast vs. unicast

- Make sure the right ports and protocols are allowed
New Mobility and MC Support

- New mobility enables client to roam across AireOS and IOS based solutions in Central as well as Converged Access mode.
- Client cannot roam across AireOS WLC1 configured with old mobility and another AireOS WLC2 configured with new mobility.
- UA FCS - 5508 & WiSM2 can operate on 7.5/7.6 & 7.3.112.
New Mobility Configuration

- You have to change your mobility mode from Flat to Hierarchical

Message from webpage:

Changing new architecture will change current WLC mobility architecture. Configuration Changes will be saved and the System will Reboot. Are you sure you want to continue?

OK
Cancel
Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture
# CUWN Release - Key Controller Features

<table>
<thead>
<tr>
<th>s/w release</th>
<th>May 2012</th>
<th>Sep 2012</th>
<th>Dec 2012</th>
<th>May 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2MR1</td>
<td>AP 2600 802.11n G2</td>
<td>Outdoor AP Uni Band Antenna</td>
<td>WLC 8500 Target customer - SP</td>
<td>AP 1600 802.11n G2</td>
</tr>
<tr>
<td></td>
<td>Outdoor AP Honeywell integration</td>
<td>Virtual Controller</td>
<td>Scale Flex7500 6K APs</td>
<td>AP3600 Security Module</td>
</tr>
<tr>
<td></td>
<td>802.11r L2 Fast Roaming</td>
<td>Controller Resiliency - AP SSO HA Licensing</td>
<td>FlexConnect Split Tunnelling</td>
<td>Application visibility and control (AVC)</td>
</tr>
<tr>
<td></td>
<td>ISE - Flex integration Flex / Local Mode parity with ISE</td>
<td>FlexConnect - 802.11r - Flex Modes</td>
<td>Bi-directional rate-limiting</td>
<td>Bonjour Services Directory Phase 1</td>
</tr>
<tr>
<td></td>
<td>Local and FlexConnect support on RAP</td>
<td>Voice/Video: 11n CAC</td>
<td>PMIPv6 on WLC</td>
<td>AP neighbor list (Subset of 802.11k)</td>
</tr>
<tr>
<td></td>
<td>Outdoors AP Internal Antenna</td>
<td>LAG on Flex7500, WLC 8500, WLC 2500</td>
<td>Guest Anchor on WLC2500</td>
<td>Scale WLC 2500</td>
</tr>
<tr>
<td></td>
<td>Outdoor AP Honeywell integration</td>
<td>802.11w (local mode) Protected Mgmt Frame</td>
<td>HA Licensing, N:1</td>
<td>HA Licensing, N:1</td>
</tr>
<tr>
<td></td>
<td>802.11r L2 Fast Roaming</td>
<td>FlexConnect Additions: PEAP / EAP-TLS AAA ACL and QoS 802.11w</td>
<td>Guest Anchor on WLC2500</td>
<td>OWAP 600 Split Tunnelling</td>
</tr>
<tr>
<td></td>
<td>ISE - Flex integration Flex / Local Mode parity with ISE</td>
<td>Profiling and Policy on WLC</td>
<td>Guest Anchor on WLC8500</td>
<td>Controller Resiliency Client SSO Over any L2</td>
</tr>
<tr>
<td></td>
<td>Local and FlexConnect support on RAP</td>
<td>Guest Anchor on WLC2500</td>
<td>Bonjour Services Directory Phase 2</td>
<td>Guest Anchor on WLC8500</td>
</tr>
<tr>
<td></td>
<td>Outdoors AP Internal Antenna</td>
<td>N+1 Redundancy with WLC2504</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Controller Product Portfolio

Features / Performance

Scale (# of clients, APs)

SRE – WLCM2
- 50 APs
- 500 Clients
- 2500
- 75 Aps
- 1000 Clients

Virtual Controller
- 200 APs
- 3000 Clients

WiSM2
- 1000 APs
- 15000 Clients
- 5500
- 500 APs
- 7000 Clients

Flex7500
- 8000 Aps
- 84000 Clients
- 8500
- 6000 APs
- 64000 Clients

FlexConnect
- Multi-architecture capable
- Support Flex and Local-mode

Scale (# of clients, APs)

Roadmap is highly confidential and reflects current plan. Subject to change without notice.
Cisco Aironet 3700 Access Point Series
Best-in-Class 802.11ac

- Industry’s first 4x4 MIMO:3 SS 802.11ac AP
- 3X performance of 802.11n 5Ghz WiFi
  - higher performance at a greater distance
- RF Excellence enabled in hardware
- High Density Experience Technology
  - Client density scale and performance
- Future proof,
  - Modular Architecture = investment protection
  - Security, 3G Small Cell or Wave 2 802.11ac module options

with Integrated 802.11ac (4x4:3SS)
Cisco Aironet Indoor Access Point
Industry’s Best 802.11n and 802.11ac Series

Mission Specific
600 & 700
- Up to 600 Mbps
- 702w: Wall Plate AP
  - Dorms, hospitality
- 702i: Compact Mid-market AP
- 600: Teleworker

Enterprise Class
1600
- Up to 600 Mbps
- CleanAir Express*
- ClientLink 2.0
- VideoStream

Mission Critical
2600
- Up to 900 Mbps
- High Client Scalability
- CleanAir
- ClientLink 2.0
- VideoStream

Best in Class
3700
- Over 1 Gbps, 802.11ac support
- High Density Experience
- CleanAir 80 MHz, ClientLink 3.0, VideoStream
- Future proof modularity: Security, 3G Small Cell or Wave 2 802.11ac
Understanding PoE with AP-3700 using 15.4W (802.3af)

- AP3700 supports full 3x3:3 using the lower 15.4 Watt (802.3af) PoE

Medium means we are conserving power and not running in 4x4:3 but it is in 3x3:3 reduced power
3700 supports full 4x4:3 using higher power (802.3at), Local Power supply or the AIR-PWRINJ-4 injector
Channel Planning, 802.11ac, and DCA Best Practices

- Do you have spectrum available for 80 Mhz?
  - Evaluate by Regulatory

- Do you use 40 MHz for 802.11n AP’s today?
  - If not – why not?
  - Does it make sense to use 80 MHz?

- Plan the Implementation – and understand that this is a major change to your existing spectrum plan

- Let DCA help you
Best Practices for Implementing 802.11ac

- Decide what Channel Width you will use
- Implement new hardware
- Initialise DCA in Startup Mode – FROM the RF group Leader(s)
- Remember – all of this is 5 GHz only!

7.3 and above – from the CLI - **Config 802.11a channel global restart**
# AP-3700 Setting 80 MHz (Manually)

![Image of AP-3700 configuration interface with 80 MHz highlighted]

## 802.11a/n Cisco APs > Configure

### General
- **AP Name**: AP7cad.74ff.33b6
- **Admin Status**: Enable
- **Operational Status**: DOWN
- **Slot #**: 1

### 11n Parameters
- **11n Supported**: Yes

### CleanAir
- **CleanAir Capable**: Yes
- **CleanAir Admin Status**: Enable

### RF Channel Assignment
- **Current Channel**: (36,40,44,48)
- **Channel Width**: 80 MHz
- **Assignment Method**: Custom

### Tx Power Level Assignment
- **Current Tx Power Level**: 1
- **Assignment Method**: Global

### Antenna Parameters
- **Antenna Type**: Internal
- **Antenna**: A, B, C, D

---

*Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.*
RF Group leader should be configured with 80MHz channel width
Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
Client Profiling

- ISE offers a rich set of BYOD features: e.g. device identification, onboarding, posture and policy
- Customers who do not deploy ISE but still require some of ISE features directly in WLC:
  - Native profiling of identifying network end devices based on protocols like HTTP, DHCP
  - Device-based policies enforcement per user or per device policy on the network.
  - Statistics based on per user or per device end points and policies applicable per device.
WLC-based local policy consists of 2 separate elements.

- **Profiling** can be based on:
  - *Role* - defining user type or the user group the user belongs to.
  - *Device type* – e.g. Windows, OS_X, iPad, iPhone, Android, etc.
  - *EAP Type* - check what EAP method the client is getting connected to.

- **Action** is policy that can be enforced after profiling:
  - *VLAN* - override WLAN interface with VLAN id on WLC
  - *QoS level* – override WLAN QoS
  - *ACL* – override with named ACL
  - *Session timeout* – override WLAN session timeout value
  - *Time of day* – policy override based on time of the day, else default to WLAN.
  - 7.5 release contains 88 pre-existing profiles:
Configuring Client Profiles

- Client profiling uses pre-existing profiles in the controller
  - Custom profiles are not supported in this release
- Wireless clients are profiled based on the MAC OUI, DHCP, HTTP user agent
  - DHCP is required for DHCP profiling, Webauth for HTTP user agent
- 7.5 release contains 88 pre-existing profiles:

```
(Cisco Controller) >show profiling policy summary

Number of Built-in Classification Profiles: 88

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Parent</th>
<th>Min CM</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Android</td>
<td>None</td>
<td>30</td>
<td>Yes</td>
</tr>
<tr>
<td>1</td>
<td>Apple-Device</td>
<td>None</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Apple-MacBook</td>
<td>1</td>
<td>20</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Apple-iPad</td>
<td>1</td>
<td>20</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Apple-iPhone</td>
<td>1</td>
<td>20</td>
<td>Yes</td>
</tr>
</tbody>
</table>

.../...
```
Local Client Profiling Configuration

- At the WLAN level, enable Local Client Profiling (DHCP and HTTP)
  - DHCP required is checked automatically when selecting DHCP profiling

```
config wlan profiling {local | radius} {dhcp | http | all} <wlan ID>
(Cisco Controller) > config wlan profiling local all enable 1
```
Client Profiles in 7.6

Local Profiling > Device Stats

Device Stats

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Count</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple-Device</td>
<td>5</td>
<td>23.81</td>
</tr>
<tr>
<td>Apple-iPad</td>
<td>5</td>
<td>23.81</td>
</tr>
<tr>
<td>OS_X-Workstation</td>
<td>5</td>
<td>23.81</td>
</tr>
<tr>
<td>Apple-iPhone</td>
<td>3</td>
<td>14.29</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>2</td>
<td>9.52</td>
</tr>
<tr>
<td>Android</td>
<td>1</td>
<td>4.76</td>
</tr>
</tbody>
</table>

Manufacturer Stats

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Count</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple-Device</td>
<td>13</td>
<td>61.90</td>
</tr>
<tr>
<td>Macintosh-Workstation</td>
<td>5</td>
<td>23.81</td>
</tr>
<tr>
<td>Workstation</td>
<td>2</td>
<td>9.52</td>
</tr>
<tr>
<td>Android</td>
<td>1</td>
<td>4.76</td>
</tr>
</tbody>
</table>
## Security Local Policies

### Match - How to Identify a Device
- Role
- EAP Type
- Device Type

### Action - Policy to Enforce
- VLAN
- QoS
- Session Timeout
- Sleeping Client Timeout
- Time of Day

---

**Table:**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Policy Id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Match Criteria:**

<table>
<thead>
<tr>
<th>Match Role String</th>
<th>Match EAP Type</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Device List:**

- Apple-iPhone

**Action:**

<table>
<thead>
<tr>
<th>Action</th>
<th>IPv4 ACL</th>
<th>VLAN ID</th>
<th>QoS Policy</th>
<th>Session Timeout (seconds)</th>
<th>Sleeping Client Timeout (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Active Hours:**

<table>
<thead>
<tr>
<th>Day</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours</td>
<td>Mins</td>
</tr>
<tr>
<td></td>
<td>Hours</td>
<td>Mins</td>
</tr>
</tbody>
</table>

---

**Note:**

- The image contains a screenshot of a configuration interface for security local policies, showing how to match criteria and configure actions such as VLAN, QoS, session timeout, and sleeping client timeout. The interface includes fields for policy name, policy ID, match criteria (role, EAP type, device type), device list, and active hours.
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
Controller Redundancy
Most Common (N+1)

- Redundant WLC in a geographically separate location
- Layer-3 connectivity between the AP connected to primary WLC and the redundant WLC
- Redundant WLC need not be part of the same mobility group
- Configure high availability (HA) to detect failure and faster failover
- Use AP priority in case of over subscription of redundant WLC

JAVA CLASS

Most Common (N+1)

APs Configured With:
Primary: WLAN-Controller-1
Secondary: WLAN-Controller-BKP

APs Configured With:
Primary: WLAN-Controller-2
Secondary: WLAN-Controller-BKP

APs Configured With:
Primary: WLAN-Controller-n
Secondary: WLAN-Controller-BKP

NOC or Data Centre
WLAN-Controller-BKP

WLAN-Controller-1
WLAN-Controller-2
WLAN-Controller-n
Controller Redundancy – High Availability

- **High Availability Principles:**
  - AP is registered with a WLC and maintain a backup list of WLC.
  - AP use heartbeats to validate WLC connectivity
  - AP use Primary Discovery message to validate backup WLC list
  - When AP loose 3 heartbeats it start join process to first backup WLC candidate
  - Candidate Backup WLC is the first alive WLC in this order: primary, secondary, tertiary, global primary, global secondary.
  - AP does not re-initiate discovery process.

**TCP MSS**
- Global TCP Adjust MSS

**AP Retransmit Config Parameters**
- AP Retransmit Count
- AP Retransmit Interval

**New Timers 7.2**
- Heartbeat Timeout: 1-30 secs
- Fast Heartbeat Timer: 1-10 secs
- AP Retransmit Interval: 2-5 secs
- AP Retransmit with FH Enabled: 3-8 Times
- AP Fallback to next WLC: 12 secs
**HA-SKU as Secondary WLC - Configuration**

```
(Cisco Controller) # show redundancy summary

Redundancy Mode = SSO DISABLED
Local State = ACTIVE
Peer State = N/A
Unit = Secondary - HA SKU
Unit ID = 70:81:05:CF:CE:40
Redundancy State = N/A
Mobility MAC = 70:81:05:CF:CE:40

Redundancy Management IP Address............... 0.0.0.0
Peer Redundancy Management IP Address............... 0.0.0.0
Redundancy Port IP Address........................ 0.0.0.0
Peer Redundancy Port IP Address................... 169.254.0.0
```

**Controller**

- **Redundant Unit**: Secondary
- **Redundancy Mgmt Ip**: 0.0.0.0
- **Peer Redundancy Mgmt Ip**: 0.0.0.0
- **Redundancy port Ip**: 0.0.0.0
- **Peer Redundancy port Ip**: 169.254.0.0
- **Keep Alive Timer (100 - 400)**: 100
- **Keep Alive Timer (60 - 120)**: 120
- **AP SSO**: Disabled

**Global Configuration**

- **Redundancy Global Configuration**
- **Redundancy Network Routes**
- **Redundancy Internal DHCP Server**
High Availability (AP and Client SSO)

- 5500/7500/8500 WLC have dedicated Redundancy Port which is used to sync configuration from Active to Standby WLC.
- Keepalives are sent on RP port from Standby to Active WLC every 100 msec (default timer) to check the health of Active WLC.
- ICMP packets are also sent every one second from each WLC to check reachability to gateway using Redundant Management interface (RMI).

---

**WLC 5500**

- Active Controller
- Hot Stand-by Controller
- Redundancy Port Connectivity
- RP 1
- RP 2

---

**Flex 7500 or WLC 8500**
High Availability (AP and Client SSO)

- WiSM-2 WLC have dedicated **Redundancy Vlan** which is used to sync configuration from Active to Standby WLC
- Keepalives are sent on Redundancy Vlan from Standby to Active WLC every 100 msec (default timer) to check the health of Active WLC
- To achieve HA between WiSM-2 WLCs it can be deployed in single chassis OR can also be deployed between multiple chassis using VSS as well as by extending Redundancy VLAN between two chassis
High Availability AP SSO Support 7.3/7.4

- Model is 1:1 (Active : Hot-Standby)
- Supported on 5500 / 7500 / 8500 and WiSM-2
- Same hardware and software version
- Two new interfaces
  - Redundancy Port
  - Redundancy Management Interface
- Same management IP on Active and Standby
- Static & dynamic system configurations synced to standby.

- AP information synced to the standby.
  - Synced when AP Joins or it's configuration changes.
  - AP CAPWAP re-join is avoided on switchover.

- Detection time : 5-996 msec for box failover, 3-4 seconds for management gateway failover

- Back-to-back Connectivity on the Redundancy Port between the two WLCs

- Clients are de-authenticated on failover ; forced to re-associate

Effective service downtime – Detection time + Switch Over Time (Network recovery/convergence) + Client re-association time
Stateful HA with Client SSO 7.5

- Client’s information is synced to the Standby
  - Client information is synced when client moves to RUN state.
  - Client re-association is avoided on switch over
- Fully authenticated clients (RUN state) are synced to the peer.
- The intermediate client state events are not synced
- Transient clients are dis-associated after switch over.

Effective service downtime – Detection time + Switch Over Time (Network recovery/convergence)
# Web-GUI Configuration

## Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy Mgmt Ip</td>
<td>9.5.56.10</td>
</tr>
<tr>
<td>Peer Redundancy Mgmt Ip</td>
<td>9.5.56.11</td>
</tr>
<tr>
<td>Redundancy port ip</td>
<td>169.254.56.10</td>
</tr>
<tr>
<td>Peer Redundancy port ip</td>
<td>169.254.56.11</td>
</tr>
<tr>
<td>Redundant Unit</td>
<td>Primary</td>
</tr>
<tr>
<td>Mobility Mac Address</td>
<td>6C:20:56:64:89:A0</td>
</tr>
<tr>
<td>Keep Alive Timer</td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>Peer Search Timer</td>
<td>120 seconds</td>
</tr>
<tr>
<td>SSO</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

---

1. Redundancy management and Peer redundancy management are mandatory parameters for AP SSO enable.
2. Configure the keep-alive timer in milliseconds between 100 and 400 in multiples of 50.
3. Disabling AP SSO will result in standby reboot and administratively disabling all the ports on current Standby to avoid IP conflict.
Supported HA Topologies – 7.5

1. Two 5508, 7500 or 8500 connected via back-to-back RP port in the same Data Centre
2. Two 5508, 7500 or 8500 connected via RP port over L2 VLAN/fibre in the same or different Data Centre
3. Two 5508, 7500 or 8500 connected to a VSS pair.

1. Two WiSM-2 on the same chassis
2. Two WiSM-2 on different chassis with redundancy VLAN extended over L2 network
3. Two WiSM-2 on different chassis in VSS mode
WLC 5508/7500/8500 Back-to-back RP Connectivity

Configuration on Primary WLC:

- configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11
- configure redundancy unit primary
- configure redundancy mode sso

Configuration on Hot Standby WLC:

- configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10
- configure redundancy unit secondary
- configure redundancy mode sso

Management GW is monitored with 12 pings (~15 sec)
WLC 5508/7500/8500 RP Connectivity via Switches

Configuration on Primary WLC:
- configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11
- configure redundancy unit primary
- configure redundancy mode sso

Configuration on Hot Standby WLC:
- configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10
- configure redundancy unit secondary
- configure redundancy mode sso

RTT Latency: 80 ms or less default; Bandwidth: 60 Mbps or more; MTU: 1500
WiSM-2 Connectivity Over L2 Redundancy VLAN

Configuration on Cat6k

wism service-vlan 192 (service port VLAN)
wism redundancy-vlan 169 (redundancy port VLAN)
wism module 6 controller 1 allowed-vlan 24-38 (data VLAN)
SSO Behaviour and Recommendations

- RTT latency on Redundancy Link: 80 milliseconds or less. 80% of keepalive timer.
- Preferred MTU on Redundancy Link: 1500 or above.
- Bandwidth on Redundancy Link: 60Mbps or more.

5500 / 7500 / 8500: RP Connectivity between Active and Standby
- Via Switches (7.5)
- Back-to-back (7.3, 7.4, 7.5)
- WiSM-2: single 6500 chassis OR different chassis using VSS setup/extending redundancy VLAN.

Recommended to have Redundancy Link and RMI Connectivity between WLCs on different switches or on different L2 networks
- Keepalive/Peer Discovery timers should be left with default timer values for better performance
- Default box failover detection time is 3 *100 = 300 + 60 = 360 + jitter (12 msec) = ~400 msec
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
**AP-Groups - Default AP-Group**

- The first 16 WLANs created (WLAN IDs 1–16) on the WLC are included in the default AP-Group.
- Default AP-Group cannot be modified.
- APs with no assignment to a specific AP-Group will use the Default AP-Group.
- The 17th and higher WLAN (WLAN IDs 17 and up) can be assigned to any AP-Groups.
- Any given WLAN can be mapped to different dynamic interfaces in different AP-Groups.
- WLC 2106 (AP groups: 50), WLC 2504 (AP groups:50), WLC 4400 and WiSM (AP groups: 300), WLC 5508 & WiSM-2 (AP groups: 500), WLC 7500 (AP Groups : 500)
AP-Grouping in Campus

Access
Distribution
Core
Distribution
Access

VLAN 100
VLAN 100
VLAN 100

WLC-1
WLC-2

Data Centre
Internet

Single SSID = Employee

© 2014 Cisco and/or its affiliates. All rights reserved.
Cisco Public
AP-Grouping in Campus

- AP-Group-1: VLAN 60 /23
- AP-Group-2: VLAN 70 /23
- AP-Group-3: VLAN 80 /23

Single SSID = Employee
Default AP-Group

Network Name

Default AP Group

Only WLANs 1–16 Will Be Added in Default AP Group
### Multiple AP-Groups

#### AP Group 1

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>WLAN SSID</th>
<th>Interface/Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Employee</td>
<td>vlan60</td>
</tr>
</tbody>
</table>

#### AP Group 2

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>WLAN SSID</th>
<th>Interface/Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Employee</td>
<td>vlan70</td>
</tr>
</tbody>
</table>

#### AP Group 3

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>WLAN SSID</th>
<th>Interface/Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Employee</td>
<td>vlan80</td>
</tr>
</tbody>
</table>
RF-Profiles

7.2 and 7.3

- RF Profiles allow the administrator to tune groups of AP’s sharing a common coverage zone together.
  - Selectively changing how RRM will operate the AP’s within that coverage zone

- RF Profiles are created for either the 2.4 GHz radio or 5GHz radio
  - Profiles are applied to groups of AP’s belonging to an AP Group, in which all AP’s in the group will have the same Profile Settings

- There are two components to this feature:
  - RF Profile – New in 7.2 providing administrative control over:
    - Min/Max TPC values
    - TPCv1 Threshold
    - TPCv2 Threshold
    - Data Rates
    - High Density
    - Client Load Balancing
“Normal” Profile

- A normal profile can be built to match your exact criteria
- You may wish to increase the mandatory data Rate to match your coverage (higher if dense, lower if sparse)
- Change the RRM coverage thresholds to match your exact architecture
- Make a custom load balancing plan that suits the environment
High Density Profile

- For High Density, RF profiles will differ significantly

Higher "Mandatory data Rate"
More Disabled Rates

Enforce "Minimum Power"
TPCv1-2 thresholds hotter
RF-Profile in Campus

Access

Distribution

Core

Distribution

Access

WLAN 60/23
WLAN 61/23
WLAN 70/23
WLAN 71/23
WLAN 80/23
WLAN 81/23

Single SSID = Employee
Multiple RF-Profiles

RF Profile -1

RF Profile -2

RF Profile -3
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
Application Visibility & Control

What applications are in the air? Why is my key application running slow? How do I support a new application for a set of users?
AVC Supported Features

• Classification: Identification of Application/Protocol, supports Stateful L4 - L7 classification. WLC can classify 1039 applications.

• AVC (Application Visibility Control): Provides visibility of classified traffic and also gives an option to control the same, using – Drop OR Mark (DSCP) action.
  • Action DROP (Traffic for that application will be dropped)
  • Action MARK (Particular applications can be marked with different QOS profiles available on WLC OR administrator can custom define DSCP value for that application)
  • AVC Marking overrides all other QoS markings

• NetFlow: Updating NBAR stats to Netflow collector like Cisco Prime Assurance Manager (PAM).

  • AVC is supported on 2500, 5500, 7500, 8500 and WiSM2 controllers on Local and Flex Mode APs
  • WLC can support 16 AVC profiles
  • WLAN can support only 1 AVC profile and each profile can contain 32 rules, thus each WLAN can support 32 application actions of mark or drop.
Enabling AVC

- AVC enabled on per WLAN basis

  - WLANs
    - WLANs
      - Advanced

  - WLANs > Edit 'secure-1'

  - General
  - Security
  - QoS
  - Policy-Mapping
  - Advanced

  - Quality of Service (QoS) Platinum (voice):
  - Application Visibility Enabled
  - AVC Profile jabber:
  - Netflow Monitor none:

- Global summary of top applications on Controller Monitor screen
AVC Profile

- Custom AVC Profiles created to do traffic shaping

- Apply the custom profile per WLAN
Netflow Monitor

- Configuring Netflow Exporter on the Controller and apply to WLAN
AVC Summary

- Application Statistics per WLAN with more details UP/Down Streams

This shows the current level of Lync Client 2013 identification.

The stats are updated on a 90 second interval.

Protocol Pack - Compatibility

- Protocol packs are released for specific NBAR engine versions
  - For example, rel 7.5 WLC has NBAR engine 13, so protocol packs for it are written for engine 13 (pp-adv-asr1k-152-4.S-13-3.0.0.pack)

- Loading a protocol pack can be done if the engine version on the platform is same or higher than the version required by the protocol pack (13 in the example above).

- Therefore:
  - PP 3.0 for version 13 can be loaded on top of version 13 or version 14
  - BUT PP 3.0 for version 14 could not be loaded in engine version 13
  - Loading the wrong version will generate an error

- It is strongly recommended to use the protocol pack that is the exact match for the engine
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
The Protocol Problem

- Why Bonjour services need modifications?

Bonjour

- Apple service discovery protocol
- mDNS packets advertise and discover services clients
- Does not cross subnets or VLANs.

Result: Clients can’t see services on other subnets
Deployment Challenges

- Bonjour is link local multicast and thus forwarded on Local L2 domain
- AirPlay (Apple TV) and AirPrint supported only on a single VLAN
- 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 GW on WLC

- Step 1 – Listen for Bonjour Services

- In 7.4 Bonjour Services with mDNS gateway on the controller don’t require multicast services to be enabled.
Bonjour mDNS GW on WLC

- Step 2 – Bonjour Services cached on Controller

Bonjour Cache:
- AirPlay – VLAN 20
- AirPrint – VLAN 23

With deployment of mDNS gateway Bonjour Services don’t flood subnet with mDNS advertisements
Bonjour GW on WLC

- Step 3 – Listen for Client Service Queries for Services

WLC will snoop all Bonjour discovery packets and will not forward the same on AIR or Infra network
Bon jour GW on WLC

- Step 4 – Respond to Client Queries for Bon jour Services

Only Clients that require Bon jour services will receive those services

Bonjour Cache:

- AirPlay – VLAN 20
- AirPrint – VLAN 23
Configuring mDNS Snooping

- Enable mDNS snooping globally and add services

Maximum of 100 services can be configured
Configure mDNS Profile per WLAN

- Create custom profile per WLAN

Enable mDNS snooping profile on the desired VLAN or WLAN
Bonjour Phase 2 – mDNS AP

- Given that mDNS Bonjour is a L2 multicast protocol and cannot be routed makes it enterprise unfriendly.
- In rel 7.5 any of the AP’s associated with the WLC as “mDNS-AP” forwards the mDNS packets received at the AP from the switch.
- This enhancement allows the controller to have the visibility of wired service providers, which are on VLANs that are not visible to the controller.
- VLAN visibility at the WLC is achieved by APs forwarding the mDNS advertisements to the controller.
- The mDNS packet between AP and controller will be forwarded in CAPWAP data tunnel similar to mDNS packets from wireless client. Both capwap v4 and v6 tunnels will be supported.
- APs can be either in access mode or trunk mode to learn the mDNS packets from wired side and forward to the controller.
- The maximum number of VLANs that AP can snoop is 10.
- This feature is supported on local and monitor mode AP, and not on FlexConnect Mode APs.
Deployment Changes with Bonjour Services Phase 2

- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS AP snoop Bonjour services behind the Router or not L2 adjacent VLANs and forwards them to WLC in CAPWAP tunnel.

With mDNS-AP Bonjour services can be seen from any VLAN
Bonjour  Phase 2 – Location Specific Service

- Prior to rel 7.5 WLC responds with the complete SP-DB for the service being queried subject to the client profile – which could be overwhelming
- With LSS all valid wireless only mDNS service advertisements received at the WLC will be tagged with the MAC address of the AP associated with the service
- In 7.5 rel wireless entries are filtered in the SP list based on the querying client location using the RRM database and respond sent with a subset of the SP-DB
- Querying-client’s AP base radio MAC address is used to query the RRM-DB to get the AP-NEIGHBOR-LIST.
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service.
- If LSS is disabled for any service then the wireless SP-DB entries will not be filtered while responding to any query from a wireless client for the said service.
- Wired SP-DB entries are never filtered.
- LSS status cannot be enabled for services with ORIGIN set to WIRED and vice-versa.
Deployment Changes with LSS

With LSS Bonjour services can be location specific

- WLC responds with the sub-set of SP-DB for the service being queried subject to the client profile
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service
Configure LSS Services 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.

   Configure LSS services from CLI:

   (WLC) >config mdns service lss <enable / disable> <service_name/all>

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

<table>
<thead>
<tr>
<th>Service-Name</th>
<th>LSS</th>
<th>Origin</th>
<th>No SP</th>
<th>Service-string</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPrint</td>
<td>No</td>
<td>All</td>
<td>1</td>
<td><em>ipp</em>.tcp.local.</td>
</tr>
<tr>
<td>AirTunes</td>
<td>No</td>
<td>All</td>
<td>2</td>
<td><em>raop</em>.tcp.local.</td>
</tr>
<tr>
<td>AppleTV</td>
<td>No</td>
<td>All</td>
<td>2</td>
<td><em>airplay</em>.tcp.local.</td>
</tr>
<tr>
<td>HP_Photosmart_Printer_1</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td><em>universal</em>.sub_.ipp_.tcp.local.</td>
</tr>
<tr>
<td>HP_Photosmart_Printer_2</td>
<td>No</td>
<td>All</td>
<td>1</td>
<td><em>cups</em>.sub_.ipp_.tcp.local.</td>
</tr>
<tr>
<td>Printer</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td><em>printer</em>.tcp.local.</td>
</tr>
<tr>
<td>Scanner</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td><em>scanner</em>.tcp.local.</td>
</tr>
</tbody>
</table>

2. Configure LSS services from CLI:

   (WLC) >config mdns service lss enable all

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

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

<table>
<thead>
<tr>
<th>Service-Name</th>
<th>LSS</th>
<th>Origin</th>
<th>No SP</th>
<th>Service-string</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPrint</td>
<td>Yes</td>
<td>All</td>
<td>1</td>
<td><em>ipp</em>.tcp.local.</td>
</tr>
<tr>
<td>AirTunes</td>
<td>Yes</td>
<td>All</td>
<td>2</td>
<td><em>raop</em>.tcp.local.</td>
</tr>
<tr>
<td>AppleTV</td>
<td>Yes</td>
<td>All</td>
<td>2</td>
<td><em>airplay</em>.tcp.local.</td>
</tr>
<tr>
<td>HP_Photosmart_Printer_1</td>
<td>Yes</td>
<td>All</td>
<td>0</td>
<td><em>universal</em>.sub_.ipp_.tcp.local.</td>
</tr>
<tr>
<td>HP_Photosmart_Printer_2</td>
<td>Yes</td>
<td>All</td>
<td>1</td>
<td><em>cups</em>.sub_.ipp_.tcp.local.</td>
</tr>
<tr>
<td>Printer</td>
<td>Yes</td>
<td>All</td>
<td>0</td>
<td><em>printer</em>.tcp.local.</td>
</tr>
<tr>
<td>Scanner</td>
<td>Yes</td>
<td>All</td>
<td>0</td>
<td><em>scanner</em>.tcp.local.</td>
</tr>
</tbody>
</table>
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
In releases prior to 7.2, enabling IPv6 bridging provided a limited solution with no Layer 3 mobility and non-optimised delivery of essential ICMPv6 messages to clients.

- IPv6 ICMPv6 multicast messages sent to all clients (including L3 roamed clients) at low data rates.
- All IPv6 packets are bridged on the VLAN transmitting unnecessary ICMPv6 messages in both directions.
In releases 7.2, the controller now processes ICMPv6 messages allowing for optimised delivery, Layer 3 mobility and first hop security.

- IPv6 ICMPv6 multicast messages are unicast to each client at high data rates.
- IPv6 ICMPv6 messages are interpreted by the controller and forwarded only as needed.
Wireless IPv6 Client Support

- Supports IPv4, Dual Stack and Native IPv6 clients on single WLAN simultaneously

- Supports the following IPv6 address assignment for wireless clients:
  - IPv6 Stateless Autoconfiguration [SLAAC]
  - Stateless, Stateful DHCPv6
  - Static IPv6 configuration

- Supports up to 8 IPv6 addresses per client

- Clients will be able to pass traffic once IPv4 or IPv6 address assignment is completed after successful authentication
IPv6 Client Connectivity on Multiple WLANs

- Access Points keep track of individual clients and unicast the Router Advertisement to the clients depending on the WLAN they belong to.
- Access Point support up to 16 WLANs/SSIDs for dual stack clients.
- To maintain proper routing capability, mobile clients need to have proper global unique unicast prefix from router within their own network.
Cisco Supports Many IPv6 Addresses Per Client

- Support for many IPv6 addresses per client is necessary because:
  - Clients can have multiple address types per interface
  - Clients can be assigned addresses via multiple methods such as SLAAC and DHCPv6
  - Most clients automatically generate a temporary address in addition to assigned addresses.

Up to 8 IPv6 Addresses are Tracked per Client.
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
  - Understanding FlexConnect AP Deployment
  - Understanding Branch Controller Deployment
- Guest Access Deployment
- Home Office Design
Branch Office Deployment
FlexConnect

- Hybrid architecture
- Single management and control point
  - Centralised traffic (split MAC)
  - Or
  - Local traffic (local MAC)
- HA will preserve local traffic only
## FlexConnect Design Considerations

WAN Limitations Apply

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>WAN Bandwidth (Min)</th>
<th>WAN RTT Latency (Max)</th>
<th>Max APs per Branch</th>
<th>Max Clients per Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>128 kbps</td>
<td>300 ms</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>Data+Voice</td>
<td>128 kbps</td>
<td>100 ms</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>Data</td>
<td>128 kbps</td>
<td>1 sec</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Monitor</td>
<td>128 kbps</td>
<td>2 sec</td>
<td>5</td>
<td>N/A</td>
</tr>
<tr>
<td>Data</td>
<td>1.44 Mbps</td>
<td>1 sec</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Data+Voice</td>
<td>1.44 Mbps</td>
<td>100 ms</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Monitor</td>
<td>1.44 Mbps</td>
<td>2 sec</td>
<td>50</td>
<td>1000</td>
</tr>
</tbody>
</table>
Economies of Scale for Lean Branches

Flex 7500 Wireless Controller

Key Differentiation

- **WAN Tolerance**
  - High Latency Networks
  - WAN Survivability

- **Security**
  - 802.1x based port authentication

- **Voice support**
  - Voice CAC
  - OKC/CCKM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Points</td>
<td>300 - 6,000</td>
</tr>
<tr>
<td>Clients</td>
<td>64,000</td>
</tr>
<tr>
<td>Branches</td>
<td>2000</td>
</tr>
<tr>
<td>Access Points / Branch</td>
<td>100</td>
</tr>
<tr>
<td>Deployment Model</td>
<td>FlexConnect</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1 RU</td>
</tr>
<tr>
<td>IO Interface</td>
<td>2x 10GE</td>
</tr>
<tr>
<td>Upgrade Licenses</td>
<td>100, 200, 500, 1K</td>
</tr>
</tbody>
</table>
Understanding FlexConnect Groups

- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys
  - Local/backup RADIUS servers IP/keys
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade

- Scaling information

<table>
<thead>
<tr>
<th>Scaling</th>
<th>Flex 7500</th>
<th>CT-5508</th>
<th>WiSM2</th>
<th>CT-2504</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexConnect Groups</td>
<td>2000</td>
<td>100</td>
<td>100</td>
<td>30</td>
</tr>
<tr>
<td>AP per Group</td>
<td>100</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>7.2</td>
<td>7.3 &amp; 7.4</td>
<td>7.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Smart AP Image Upgrade</td>
<td>- Flex 7500 Scale Update</td>
<td>- PEAP and EAP-TLS Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ACL’s on FlexConnect AP</td>
<td>- VLAN Based Central Switching</td>
<td>- FlexConnect Group specific WLAN-VLAN mapping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- AAA Over-ride of VLAN - dynamic VLAN assignment for locally switched clients</td>
<td>- Split Tunnelling</td>
<td>- AAA Client ACL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- FlexConnect Re-branding</td>
<td>- Central DHCP Processing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Fast Roaming for Voice Clients</td>
<td>- WGB/uWGB Support with local switching</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Peer to Peer Blocking</td>
<td>- Bidirectional Rate Limiting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Support for ISE BYOD Registration &amp; Provisioning</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EAP-TLS/PEAP Overview

- Local Authentication on FlexConnect AP
  - FlexConnect AP contacting RADIUS Server
  - FlexConnect AP acting as RADIUS Server
- EAP Methods when AP acting as RADIUS Server: LEAP, EAP-FAST, **PEAP**, **EAP-TLS**
- PEAP and EAP-TLS Support in
  - Standalone Mode
  - Local Authentication
- Continued support for RADIUS Servers on FlexConnect Group.
- RADIUS Server Configuration takes precedence over FlexConnect AP acting as RADIUS Server.
- Access points 1040, 1140, 1520, 1550, 1600, 3700, 3500, 3600, 2600, 1250, 1260, are supported
PEAP/EAP-TLS Web-GUI

- Enable AP Local Authentication
- Radius Server configured on the FlexConnect group takes precedence over ‘AP Local Authentication’
Local Switching Access Lists (7.2)

Description

- Support for ACL in FlexConnect local switching mode
- ACL mapped to local VLAN per AP or FlexConnect Group
- 512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 ACL
Local Switching Access Lists (7.2)

**Configuration**

- ACL rule creation and application for FlexConnect is identical to WLC rule creation for Local Mode

---

### Step 1

Click to add ACL rules

---

### Step 2

Provision to assign separate Inbound & Outbound ACLs

---

### Step 3

Click to add ACL rules
Local Switching Peer-to-Peer Blocking (7.2)

Description

- Support for Peer-to-Peer blocking in FlexConnect AP
- Apply for clients on same FlexConnect AP
- P2P blocking modes: disable or drop
- For P2P blocking inter-AP use ACL or Private VLAN fonction
FlexConnect AAA VLAN Override (7.2)

Description

- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- If VLAN ID does not exist, default VLAN is used
- QoS and ACL Override is not supported.
FlexConnect AAA VLAN Override (7.2)

Configuration

Create Sub-Interface on FlexConnect AP
Deploying BYOD with FlexConnect and Local Switching

- No difference for centrally switched traffic.

- For locally switched traffic differences are:
  - No Dynamic ACL with AAA override -> Specific « Web Policies ACL » for BYOD
  - No HTTP Profiling probes (Traffic is not sent to WLC)
  - DHCP Profiling probes mandate central DHCP redirection
  - Registration & Provisioning flow will go outside the CAPWAP tunnel
FlexConnect ACL – Split Tunnelling

- Split tunnelling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunnelling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunnelling is using the AP IP@ for the NAT/PAT feature
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- IPv6 Deployment with Controllers
- mDNS Gateway
- Branch Office Designs
  - Understanding FlexConnect AP Deployment
  - Understanding Branch Controller Deployment
- Guest Access Deployment
- Home Office Design
Branch Office WLAN Controller Options

- Appliance controllers
  - Cisco 2504
  - Cisco 5508
- Integrated controller
  - WLAN controller module (WLCM-2) for ISR G2
- Virtual WLC (vWLC)

Number of Users: 100–500
Number of APs: 5–25

Number of Users: 20–100
Number of APs: 1–5
**Branch Office WLAN Controller Options**

- Cisco Unified Wireless Network with controller-based
- Multiple Integrated WAN options on ISR
- Consistent branch-HQ services, features, and performance
- Standardised branch configuration extends the unified wired and wireless network
- Branch configuration management from central WCS

**AP Count Vary Depending on Channel Utilisation and Data Rates**
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design
Guest Access Deployment

WLAN Controller Deployments with EoIP Tunnel

- Use of up to 71 EoIP tunnels to logically segment and transport the guest traffic between remote and anchor controllers
- Other traffic (employee for example) still locally bridged at the remote controller on the corresponding VLAN
- No need to define the guest VLANs on the switches connected to the remote controllers
- Original guest’s Ethernet frame maintained across CAPWAP and EoIP tunnels
- Redundant EoIP tunnels to the Anchor WLC
- With 7.4 release 2504 series EoIP connections can terminate 10 EoIP tunnels
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Designs
- Cisco controller installed in the DMZ of the corporate network
- OfficeExtend AP (OEAP) installed at teleworker’s home
- Corporate access to employee over centrally configured SSID
- Family Internet access over a locally configured SSID
Centralise traffic flow to enhance operational IP address/VLAN management

Place all controllers in the same Mobility Domain to allow seamless mobility across L2 and L3 transitions

Provide coverage in all possible locations leveraging mesh and outdoor Access Points.

Use BYOD for device security and policy

Use AP Group, Interface group and RF Profile
Best Practices – Branch Deployment

- Select correct architecture for branch office – local controller or FlexConnect
- Prioritise the right traffic over the WAN
- Have correct WAN survivability model
- Proper WAN bandwidth and Latency to support voice and multimedia applications
- Enable Enhanced Local Mode (ELM) or WiPS using WSSI module for security.
- Take advantage of latest BYOD enhancements with FlexConnect architecture
Summary – Key Takeways

- Take advantage of the standards (CAPWAP, DTLS, 802.11 i, e, k, r…..)
- Wide range of architecture / design choices
- Brand new controllers (WiSM-2, WLC 7500, WLC 8500, WLC 2504, Virtual WLC) portfolio with investment protection
- Take advantage of innovations from Cisco (11ac, CleanAir, BandSelect, ClientLink, Security, CCX, FlexConnect, etc)
- Cisco’s investment into technology – Cisco Prime, ISE, New hardware, Cloud controller


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