TECH-MOB: WLAN jako primární přístupová vrstva
Konvergovaný LAN + WLAN přístup – návrh, konfigurace a troubleshooting

TECH-WLAN P3 / L2

Jaroslav Čížek – Cisco
Jiří Beneš – CCIE #27063
Viktor Bohdal
Agenda
TECH-WLAN P3 / L2

- Úvod
- Converged Access – architektura a principy
- Demo - ukázka základní konfigurace
- Case Study - zkušenosti z nasazení
- Best practises
- Prime Infrastructure CA šablony a workflow
- CA Troubleshooting
# Unified Access—Wireless Deployment Modes

## Autonomous
- **Standalone APs**
- Traffic Distributed at AP

## FlexConnect
- Traffic Distributed at AP

## Centralized
- Traffic Centralized at Controller

## Converged Access
- Traffic Distributed at Switch

### Target Positioning

<table>
<thead>
<tr>
<th>Target Positioning</th>
<th>Small Wireless Network</th>
<th>Branch</th>
<th>Campus</th>
<th>Branch and Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purchase Decision</strong></td>
<td>Wireless only</td>
<td>Wireless only</td>
<td>Wireless only</td>
<td>Wired and Wireless</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>• Simple and cost-effective for small networks</td>
<td>• Highly scalable for large number of remote branches</td>
<td>• Simplified operations with centralized control for Wireless</td>
<td>• Wired and Wireless common operations</td>
</tr>
<tr>
<td></td>
<td>• Simple wireless operations with DC hosted controller</td>
<td>• Wireless Traffic visibility at the controller</td>
<td>• One Enforcement Point</td>
<td>• One OS (IOS)</td>
</tr>
<tr>
<td></td>
<td>• Limited RRM, no Rogue detection</td>
<td>• L2 roaming only</td>
<td>• Traffic visibility at every network layer</td>
<td>• Traffic visibility at every network layer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAN BW and latency requirements</td>
<td>• Performance optimized for 11ac</td>
<td>• Performance optimized for 11ac</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• System throughput</td>
<td>• Catalyst 3850/3650/4K in the access layer</td>
</tr>
</tbody>
</table>
One Network, with Converged Access
A New Deployment Option for Wired / Wireless

**IOS Based WLAN Controller**
- Consistent IOS and ASIC w/ Catalyst 3850
- Required to scale beyond 250 AP or 16K client domains

**Converged Access Mode**
- Integrated wireless controller
- Distributed wired/wireless data plane (CAPWAP termination on switch)

New 5760
Catalyst 3850
Catalyst 3650
Catalyst 4500-Sup8

One Network
Corporate Network
Internet
Cisco Firewall
One Policy
ISE
One Management
Prime
LAN Mgmt Solution
Identity Mgmt
NAC Profiler
Cisco Public
Access Control Server
Cisco Wireless LAN Controller
Internal Resources
Catalyst Switch
Cisco Firewall
Cisco Access Point
Catalyst Switch
Catalyst 3850
Catalyst 3650
Catalyst 4500-Sup8

Consistent IOS and ASIC w/ Catalyst 3850
Required to scale beyond 250 AP or 16K client domains
Integrated wireless controller
Distributed wired/wireless data plane (CAPWAP termination on switch)
UA One Network: Converged Wired/Wireless Access Portfolio Overview

**One Policy**
with Identity Services Engine (ISE)
- BYOD policy management
- Device profiling and posture
- Guest access portal

**One Management**
with Cisco Prime 2.2
- Full wired and wireless management
- User/device centric view
- Intuitive troubleshooting workflows

---

**Catalyst 3650/3850**
- Industry’s first fully integrated wired and wireless switch
- Wireless: 480G stack (3850), 25/50 APs, 2K clients, 20/40G
- Flexible Netflow, Granular QoS

**Sup 8E on Catalyst 4500E**
- 888 Gbps. Sup 7-E equiv TCAM
- Wireless: 20G Capacity, 50 APs, 2K clients
- 8 x 10G SFP+
- FNF, VSS*

**5760 Wireless Controller**
- Consistent IOS with Catalyst 3850
- 60G, 1K APs, 12K Clients, N+1 Redundancy
- FNF, Granular QoS

---

**Best-in-Class Performance, Security, and Resiliency**
Converged Wired/Wireless Access

Benefits

**Single platform** for wired and wireless
Common IOS, same administration point, one release

**Network wide visibility** for faster troubleshooting
Wired and wireless traffic visible at every hop

**Consistent security and quality of service control**
Hierarchical bandwidth management and distributed policy enforcement

**Maximum resiliency** with fast stateful recovery
Layered network high availability design with stateful switchover

**Scale** with distributed wired and wireless data plane
160G stack bandwidth; 40G wireless/switch; efficient multicast

Unified Access - One Policy | One Management | One Network
Converged Access
– architektura a principy
Campus Design: Converged Access
Distributed Architecture

Notes –
- MC – Mobility Controller
- MA – Mobility Agent
Converged Access Mobility Architecture

Mobility Subdomain A
- Peer Group 1
- Mobility Controller
- Mobility Agent

Mobility Subdomain B
- Peer Group 2
- Mobility Group N

Mobility Group M

Mobility Domain

Fast Roam
Full Authentication

14ms 50ms 80ms 120ms > 250ms
Converged Access – Components
Physical and Logical Entities

Physical Entities –

- **Mobility Agent (MA)** – Terminates CAPWAP tunnel from AP
- **Mobility Controller (MC)** – Manages mobility within and across Sub-Domains
- **Mobility Oracle (MO)** – Superset of MC, allows for Scalable Mobility Management within a Domain

Logical Entities –

- **Mobility Groups** – Grouping of Mobility Controllers (MCs) to enable Fast Roaming, Radio Frequency Management, etc.
- **Mobility Domain** – Grouping of MCs to support seamless roaming
- **Switch Peer Group (SPG)** – Localizes traffic for roams within a Distribution Block

MA, MC, Mobility Group functionality all exist in today’s controllers (4400, 5500, WiSM2)
Converged Access – Physical Entities
Mobility Agents (MAs)

• MA is the first level in the hierarchy of MA / MC / MO
• One MA per Catalyst 3x50 Stack / 4K
• Maintains Client DB of locally served clients
• Interfaces to the Mobility Controller (MC)
Converged Access – Physical Entities
Mobility Controllers (MCs)

- Mandatory element in design
- Can be hosted on a MA (smaller deployments)
- Manages mobility-related state of the downstream MAs
- Maintains Client DB within a Sub-Domain (1 x MC = One Sub-Domain)
- Handles RF functions (including RRM)
- Multiple MCs can be grouped together in a Mobility Group for scalability
- Supported platforms are Catalyst 3x50, 4K / Sup-8E, WiSM2, 5508 & 5760 (preferred platform as external MC)
Converged Access – Logical Entities
Switch Peer Groups and Mobility Group

- Made up of multiple Converged Access switches as Mobility Agents (MAs), plus an MC (on controller as shown)
- Handles roaming across SPG (L2 / L3)
- MAs within an SPG are fully-meshed (auto-created at SPG formation)
- Fast Roaming within an SPG
- Multiple SPGs under the control of a single MC form a Sub-Domain

- Made up of Multiple Mobility Controllers (MCs)
- Handles roaming across MG (L2 / L3)
- RF Management (RRM, handled by RF Group), Key Distribution for Fast Roaming
- One Mobility Controller (MC) manages RRM for the entire RF Group
- Fast Roams are limited to Mobility Group member MCs
Converged Access – Physical Entities

Mobility Oracle (MO)

- Top level in the MA / MC / MO Hierarchy – Optional
- Further enhances scalability and performance by coordinating Inter-MC roams (removes need for $N^2$ communications between MCs, improves client join performance)
- Maintains database of clients across multiple Mobility Controllers (MCs)
- Can be a Software-Upgraded WiSM2, 5508 or 5760 Controller
Converged Access – Small Site
No Discrete Controllers, 3x50s / 4K Sup 8-Es as MCs / MAs

Up to 25 / 50 APs

Characteristics –

- Independent of WAN link (compared to FlexConnect) as bandwidth and latency are a concern only for Guest traffic
- **Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless and wired traffic**
- Supports Layer 3 roaming
- Supports VideoStream and optimized multicast
- Good availability due to MA/MC redundancy within the 3x50 stack – provides wireless continuity with either WAN outage or switch failure within the stack

Applicable to a Small Site Deployment
Converged Access – Small / Medium Site
No Discrete Controllers, 3x50s / 4K Sup 8-Es as MCs / MAs, Single SPG

Up to 25 / 50 APs

Deployment could consist of multiple stacks – one stack as MC/MA, rest of stacks as MAs only

Central Location

Characteristics –

- No discrete controllers deployed, even with multiple wiring closets
- Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless ad wired traffic
- Supports Layer 3 roaming
- Supports VideoStream and optimized multicast
- Good availability due to MA/MC redundancy within the switch stacks – provides wireless continuity with either WAN outage or switch failure within the stack

Applicable to a Small to Medium Site Deployment

Switch Peer Group

Guest Anchor(s)
Converged Access – Medium Site
No Discrete Controllers, 3x50s / 4K Sup 8-Es as MCs / MAs, Multiple SPGs

Scalability … up to 8 x 3x50 / 4K Sup 8-E MCs
(2 x such MCs recommended)

Up to 200 / 250 APs
(50 / 100 APs max. recommended)

Note – MCs handling one or more SPGs each, all MCs meshed into a single Mobility Group for the site. 1 Guest tunnel per MC to Anchor.

Characteristics –
- No discrete controllers deployed, even at a medium-sized site
- Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless ad wired traffic
- Supports Layer 3 roaming
- Supports VideoStream and optimized multicast
- Good availability due to MA/MC redundancy within the switch stacks – provides wireless continuity with either WAN outage or switch failure within the stack
Converged Access – Larger Site
Controllers as MCs, 3x50s / 4K Sup 8-Es as MAs Only, Multiple SPGs

> 250 APs
(600 APs max. recommended with 1 x 5760-based MC,
1200 APs max. recommended with 2 x 5760-based MCs)

Characteristics –

• **Greater scalability** via the use of discrete controllers as MCs, in conjunction with Catalyst switches as MAs
• Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless and wired traffic
• Supports Layer 3 roaming, VideoStream, and optimized multicast
• Good availability due to MA redundancy (switch stacks) and MC redundancy (controllers) – provides wireless continuity with either WAN outage or switch / controller failure
• **Simplified Mobility deployment** vs. the use of CA switches as MCs / MAs
Converged Access – Larger Site with Nomadic Roaming

3x50s / 4K Sup 8-Es as MCs / MAs, Multiple SPGs and Multiple MGs

Scalability… Multiple x 3x50 / 4K Sup 8-E MCs = > 100 APs total (w/o inter-dist. roaming)

Characteristics –

- No discrete controllers deployed, even at a larger site
- Allows for Advanced QoS, NetFlow, and other services for wireless and wired traffic
- Supports Layer 3 roaming
- No support for roaming across distribution layers (no inter-dist. RF coverage)

- Good availability due to MC/MA redundancy within the CA switch stacks – more scalable using Catalyst 3x50s (up to 8 total per Mobility Group – 2 recommended) as MCs, combined with multiple Mobility Groups in the deployment

Note – MC handling one or more SPGs each, with MCs meshed into multiple Mobility Groups for the site. Guest tunnel per MC to Anchor.

May be Applicable to a Site without any inter-building wireless coverage

No inter-dist. roaming – no RRM and other MC-based functions across separate Mob. Groups

Characteristics –

- No discrete controllers deployed, even at a larger site
- Allows for Advanced QoS, NetFlow, and other services for wireless and wired traffic
- Supports Layer 3 roaming
- No support for roaming across distribution layers (no inter-dist. RF coverage)
Converged Access – Basic Roam Types
Layer 2 and Layer 3

- When a wireless client roams to a switch where the client VLAN is present, it is considered as an L2 Roam –
  - In CUWN this would imply that the PoP moves to the new switch
  - In Converged Access this is configurable and by default the data path is anchored at the home switch (feature called “Sticky / L2 anchoring”)

- When a wireless client roams across L3 subnets (i.e. to switches where its own VLAN is not present), it is considered as an L3 Roam –
  - same as CUWN, tunneling is used to keep the client’s IP address

- In both cases, client will continue to maintain its original IP address – this is called seamless mobility.
Converged Access – Traffic Flow and Roaming
Small Site, Single Catalyst 3x50 Stack

Notice how the CA switch shown is an MC (as well as an MA) – in a branch such as this with 50 APs or less, no discrete controller is necessarily required …

Roaming, Single Converged Access switch / switch stack –

- In this example, the user roams within their CA switch – for a small Branch site, this may be the only type of roam

Roaming within a stack does not change the user’s PoP or PoA – since the stack implements a single MA (redundant within a stack), and thus a user that roams to another AP serviced by the same switch / switch stack does not cause a PoA move (PoA stays local to the switch / switch stack)

Very common roaming case

Roaming across Stack (small branch)
Roaming, Within a Switch Peer Group (Branch) –

- Now, let’s examine a roam at a larger branch, with multiple CA switches / switch stacks joined together via a distribution layer.
- In this example, the larger Branch site consists of a single Switch Peer Group – and the user roams within that SPG – again, at a larger Branch such as this, this may be the only type of roam.

The user may or may not have roamed across an L3 boundary (depends on wired setup) – however, users are always* taken back to their PoP for policy application.

Again, notice how the CA switch on the left is an MC (as well as an MA) in this picture – in a larger branch such as this with 50 APs or less, no discrete controller is necessarily required …

* Adjustable via setting, may be useful for L2 roams (detailed on slides in following section of this slide deck).
Converged Access – Traffic Flow and Roaming
Larger Site, L2 / L3 Roam (within SPG)

Roaming, Within an SPG (Larger Site) –

- Now, let’s examine a few more types of user roams
- In this example, the user roams within their Switch Peer Group – since SPGs are typically formed around floors or other geographically-close areas, this is the most likely and most common type of roam

The user may or may not have roamed across an L3 boundary (depends on wired setup) – however, users are always* taken back to their PoP for policy application.

Note – the traffic in this most common type of roam did not have to be transported back to, or via, the MC (controller) servicing the Switch Peer Group – traffic stayed local to the SPG only (i.e. under the distribution layer in this example – not back through the core).

This is an important consideration for Switch Peer Group, traffic flow, and Controller scalability.
Converged Access – Traffic Flow and Roaming
Guest / Mobility Anchor

Quick note –
Catalyst 3x50 / 4K Sup8-E switches can be used as MCs (with appropriate licensing) – however, they cannot be used as the destination for Guest Anchor tunnels (Guest Anchors must be discrete controllers).

- When using Guest / Mobility Anchors, all Guest traffic has its PoP set to the uplink of the Mobility Anchor controller – while the user's PoA moves within the network as they roam.

- This is always the case for user traffic that is anchored to another controller within the network – and always has been … this is inherent to how Mobility Anchors work …

- When anchored users roam, their PoP stays fixed at the Mobility Anchor point (Guest Anchor controller in this diagram), while their PoA moves in the network as the user moves.
Demo - ukázka základní konfigurace
Demo – ukázka základní konfigurace
Case Study
- zkušenosti z nasazení
Zdravotní ústav a Converged Access

- 1 budova, 5 podlaží, požadavek na vysokou dostupnost
- páteřní vrstva
  - dva oddělené centrální datové rozváděče/datová centra pro centrální aktivní prvky, firewall a servery
  - firewall + remote VPN,
  - stávající + nové servery, replikace dat mezi datovými centry
- přístupová vrstva
  - požadováno cca 400 non-PoE GigE portů + možnost PoE pro AP a kamery
  - v každém patře dva datové rozváděče
  - 50 AP
  - Guest Access – Central WebAuth pomocí Cisco ISE
  - BYOD – Dual SSID, omezení počtu zařízení
Zdravotní ústav a Converged Access

- Plánuje se
  - TrustSec + MACsec
  - Unified Posture – AnyConnect 4
  - Nasazení pouze jednoho MC

- Zvažuje se
  - MC managing MA
WebAuth vs DMZ/ASA

HTTP Redirect
CWA Portal

Src = guest IP; Dst = cisco.com

HTTP request?

Spoof Source IP

Send redirect

Src = cisco.com
Dst = guest IP

RPF check

Fail

TCP SYN?

Src = cisco.com; Dst = guestIP

#sh ip route cisco.com
0.0.0.0/0
nexthop 172.20.2.2 vlan2

FAIL

interface vlan 200
description Management
ip address 172.20.200.1 255.255.255.0
ip verify unicast source reachable-via rx

VLAN guest

VLAN mgmt 200

VLAN P2P
IP Device Tracking

- Funkce – sledování vazby IP a MAC adresy
- Proč – vyžadováno pro funkci WebAuth a další
- Problém – klientské stanice hlásí duplicitu IP
- Řešení – nastavení IP adresy pro ARP probe

```
ip device tracking probe auto-source fallback 0.0.0.X 255.255.255.0 override
```

Best practises
Wireless Best Practices – IOS-XE - Infrastructure

- Upgrade to recommended software version
- Configure GUI Settings
- Apply right-to-use licenses
- Configure default gateway
- Enable NTP/Time
- Enable ap capwap multicast
- Configure DHCP Snooping
- Enable Local Profiling
- Enable AVC(Application Visibility and Control)

<table>
<thead>
<tr>
<th>Model</th>
<th>5760</th>
<th>3850</th>
<th>3650</th>
<th>5508</th>
<th>MSE</th>
<th>ISE</th>
<th>ACS</th>
<th>Prime</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.0SE</td>
<td>3.2.0SE</td>
<td>-</td>
<td>7.3.112</td>
<td>-</td>
<td>1.1.1MR</td>
<td>5.2</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3.2.1SE</td>
<td>3.2.1SE</td>
<td>-</td>
<td>7.3.112</td>
<td>-</td>
<td>1.1.3,1.1.2</td>
<td>5.2, 5.3</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3.2.2SE</td>
<td>3.2.2SE</td>
<td>-</td>
<td>7.3.112/7.5+</td>
<td>-</td>
<td>1.1.3,1.1.2</td>
<td>5.2, 5.3</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3.2.3SE</td>
<td>3.2.3SE</td>
<td>-</td>
<td>7.3.112/7.5+</td>
<td>7.4</td>
<td>1.1.3,1.1.2</td>
<td>5.2, 5.3</td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td>3.3.0SE</td>
<td>3.3.0SE</td>
<td>3.3.0SE</td>
<td>7.3.112/7.5+</td>
<td>7.5</td>
<td>1.2</td>
<td>2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.xSE</td>
<td>3.3.xSE</td>
<td>3.3.xSE</td>
<td>7.3.112/7.5+</td>
<td>7.5</td>
<td>1.2</td>
<td>2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.0SE</td>
<td>3.6.0SE</td>
<td>3.6.0SE</td>
<td>7.6/8.0</td>
<td>8.0</td>
<td>1.2/1.3</td>
<td>2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7.0SE</td>
<td>3.7.0SE</td>
<td>3.7.0SE</td>
<td>8.0</td>
<td>8.0</td>
<td>1.2/1.3</td>
<td>2.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended software versions

## Infrastructure Best Practices - Initial Setup

<table>
<thead>
<tr>
<th>Areas</th>
<th>What to Check for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Software Image</td>
<td>3.3.5 – Use 3.6/3.7 if features are needed</td>
</tr>
<tr>
<td>Web UI Access</td>
<td>Enable local authentication:</td>
</tr>
<tr>
<td></td>
<td><code>WLC5760(config)#ip http authentication local</code></td>
</tr>
<tr>
<td></td>
<td>(enabled by default in 3.3.3 and above)</td>
</tr>
<tr>
<td>AP Join</td>
<td>Apply right-to-use licenses</td>
</tr>
<tr>
<td></td>
<td>Set NTP and check controller time</td>
</tr>
<tr>
<td></td>
<td>Check Reg domain and Country Code</td>
</tr>
<tr>
<td>Configure Wireless Management Interface</td>
<td>AP will not join without it.</td>
</tr>
<tr>
<td></td>
<td><code>WLC5760(config)#wireless management interface vlan 100</code></td>
</tr>
<tr>
<td>Configure Default Gateway</td>
<td>The 5760 controller does not support routing.</td>
</tr>
<tr>
<td></td>
<td><code>WLC5760(config)#ip default-gateway &lt;gateway_ip_addr&gt;</code></td>
</tr>
<tr>
<td>Enable Application Visibility and Control (AVC)</td>
<td>Better Network Visibility</td>
</tr>
<tr>
<td>Enable Local Profiling</td>
<td>Better Network Visibility</td>
</tr>
</tbody>
</table>
Infrastructure: Multicast Optimization

- Enable the wireless multicast/broadcast only if needed.
- Configure the wireless multicast forwarding mode as multicast to avoid the replications on the controller.

```
(config)#wireless multicast
(config)#ap capwap multicast <unique-multicast-ip-per-box>
```
Infrastructure: DHCP Snooping and IP Learning

- Enable the dhcp snooping to avoid the wireless broadcast of the DHCP response packets like OFFER.

  5760(config)#ip dhcp snooping
  (config)#ip dhcp snooping vlan <client-vlan-list>

- Configure the trust option on the upstream ports/port channel or client VLANs:

  **Upstream switch:**

  (config)#interface vlan <dhcp-server-vlan>
  (config-if)#ip dhcp relay information trusted

  - Relay agent

  5760(config)#interface vlan <client-vlan>
  (config-if)#ip dhcp relay information trusted

  - Same VLAN

  5760(config)#interface <upstream port/port channel>
  (config-if)#ip dhcp snooping trust

  - Anchored scenario

  Anchor 5760(config)#interface <upstream port/port channel>
  (config-if)#ip dhcp snooping trust
Infrastructure: DHCP Snooping and IP Learning

- Enable the support of broadcast flag in the DHCP DISCOVER packets.
  
  ```
  5760 (config)#ip dhcp snooping wireless bootp-broadcast enable
  ```

- Disable the device tracking on the upstream ports to avoid the false IP theft notifications. **NOTE:** Configure this only on the port channel if present. Fixed in 3.3.4

  ```
  5760 (config)#interface <upstream port/port channel>
  (config-if)#ip device tracking max 0
  ```
Wireless Best Practices – IOS-XE- RF/WLAN

- Enable Band Select
- Enable Fast ssid change
- Disable Low data rate
- Enable Platinum QoS for Voice WLAN
- Enable RRM(DCA and TPC) to be auto
- Configure WebAuth best practices
- Enable CleanAir
- Enable DFS Channels
- Limit the number of SSIDs to 3

RF/WLAN Best Practices: RF Optimization

- Site survey is recommended for both 2.4GHz and 5GHz bands for optimal RF environment.
- Disable lower data rates selectively for better throughput and airtime utilization. NOTE: This requires to bring down the radio and recommended in the off hours.
  - Enable the lower data rates only if coverage is more important than speed, for instance in a hotspot scenario.
- Enable Clean-Air functionality
- Enable DFS channels

```
(config)#ap dot11 24ghz rate RATE_1M disable
(config)#ap dot11 24ghz rate RATE_2M disable
(config)#ap dot11 24ghz rate RATE_5_5M disable
(config)#ap dot11 24ghz rate RATE_6M disable
(config)#ap dot11 24ghz rate RATE_24M supported
(config)#ap dot11 24ghz rate RATE_54M supported
(config)#ap dot11 5ghz rate RATE_6M mandatory
(config)#ap dot11 24ghz cleanair
(config)#ap dot11 5ghz cleanair

WLC5760(config)#ap dot11 24ghz cleanair
WLC5760(config)#ap dot11 5ghz cleanair

WLC5760(config)#ap dot11 5ghz rrm channel dca add <channel>
```
# RF/WLAN Best Practices: RF Optimization

## 802.11b/g/n Global Parameters

### General

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b Network Status</td>
<td>✓</td>
</tr>
<tr>
<td>802.11g Support</td>
<td>✓</td>
</tr>
<tr>
<td>Beacon Period (milliseconds)</td>
<td>100</td>
</tr>
<tr>
<td>Short Preamble</td>
<td>✓</td>
</tr>
<tr>
<td>Fragmentation Threshold (bytes)</td>
<td>2346</td>
</tr>
<tr>
<td>DTPC Support</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 11n Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Link</td>
<td>✓</td>
</tr>
</tbody>
</table>

### CCX Location Measurement

<table>
<thead>
<tr>
<th>Mode</th>
</tr>
</thead>
</table>

## Data Rates

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>disable</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>disable</td>
</tr>
<tr>
<td>5.5 Mbps</td>
<td>disable</td>
</tr>
<tr>
<td>6 Mbps</td>
<td>disable</td>
</tr>
<tr>
<td>9 Mbps</td>
<td>supported</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>mandatory</td>
</tr>
<tr>
<td>12 Mbps</td>
<td>supported</td>
</tr>
<tr>
<td>18 Mbps</td>
<td>supported</td>
</tr>
<tr>
<td>24 Mbps</td>
<td>mandatory</td>
</tr>
<tr>
<td>36 Mbps</td>
<td>supported</td>
</tr>
<tr>
<td>48 Mbps</td>
<td>supported</td>
</tr>
<tr>
<td>54 Mbps</td>
<td>supported</td>
</tr>
</tbody>
</table>
RF/WLAN Best Practices: WLAN and Roaming Config

- Disable the WLANs that are not used and limit the number of WLANs to a few.

- Enable the band-select to promote least congested 5GHz band

- Enable load-balance if there is a large client count on single AP like class-room scenario.

- Enable the fast-ssid switching to work with some of the Apple devices switching between the WLANs.

```
(config)#wlan <profile-name> <id> <ssid>
(config-wlan)#band-select
(config-wlan)#load-balance
```

```
(config)# wireless client fast-ssid-change
```
RF/WLAN Best Practices: WLAN and Roaming Config

WLAN

- WLAN > Edit
- General
- Security
- QOS
- AVC
- Policy Mapping

DHCP

- DHCP Server IP Address: 0.0.0.0
- DHCP Address Assignment required
- DHCP Option 82
- DHCP Option 82 Format: None
- DHCP Option 82 Ascii Mode
- DHCP Option 82 RId Mode

NAC

- NAC State

Load Balancing and Band Select

- Load Balance
- Band Select
RF/WLAN Best Practices: Web Authentication

- 3.3.5 SE is the recommended release
- **Local Web Authentication (LWA):**
  - Configure the virtual-ip under the global parameter-map to drop the unauthenticated HTTPS traffic.
  - Configure per user max HTTP connections (15) to limit per user activity
  - Configure web-auth state time out 5 mins to limit the Idle client activity.

```
(config)#parameter-map type webauth global
(config-params-parameter-map)#virtual-ip ipv4 <virtual-ip>
(config-params-parameter-map)#timeout init-state min 5
(config-params-parameter-map)#max-http-conns 15
```
RF/WLAN Best Practices: Web Authentication

- **Central Web Authentication (CWA):**
  - Configure **only** HTTP redirect in the redirect ACL.
  - **NOTE:** Redirect ACL is a PUNT ACL and the semantics are different from regular ACL. The keyword deny means pass-through and permit means Punt it to CPU.

- **Enable the RADIUS server load-balancing if there are multiple backend servers.**

```bash
(config)#ip access-list extended cwa_redirect_acl
(config-ext-nacl)#deny udp any eq bootps any
(config-ext-nacl)#deny udp any any eq bootpc
(config-ext-nacl)#deny udp any eq bootpc any
(config-ext-nacl)#deny udp any any eq domain
(config-ext-nacl)#deny udp any eq domain any
(config-ext-nacl)#deny ip any host <ISE ip address>
(config-ext-nacl)#permit tcp any any eq www
```

```bash
(config)#radius-server load-balance method least-outstanding
```
RF/WLAN Best Practices: Voice WLAN

- Enable Voice acm and sip CAC on both the 2.4 GHz and 5 GHz bands under global Config

```plaintext
For 2.4 GHz band:
WLC5760(config)#ap dot11 24ghz shutdown
WLC5760(config)#ap dot11 24ghz cac voice acm
WLC5760(config)#ap dot11 24ghz cac voice sip
WLC5760(config)#no ap dot11 24ghz shutdown
```

- Applying Qos Policy to WLAN
  Note: Platinum is default policy

```plaintext
WLC5760(config-wlan)##service-policy output platinum
WLC5760(config-wlan)##service-policy input platinum-up
```

- Enable SIP Snooping under the WLAN if SIP calling is required

```plaintext
WLC5760(config-wlan)#call-snoop
```
Wireless Best Practices – IOS-XE- Security

- Enable 802.1x and WPA/WPA2 on WLAN/SSID
- Change advanced EAP and Radius timers
- Enable Client Exclusion Policies
- Enable Rogue Classification
- Enable “Max Concurrent Logins for a user name”
- Enable strong password policies
- Enable ACL on your WLAN
- Enable SNMPv3 and SSHv2

Security Best Practices: Client Exclusion

- Enable Client Exclusion Policies

WLC5760(config)#wireless wps client-exclusion?
all Configure response to all of these events
dot11-assoc Configure response to excess 802.11 association failures
dot11-auth Configure response to excess 802.11 authentication failures
dot1x-auth Configure response to excess 802.1x authentication failures
ip-theft Configure response to IP theft or re-use
web-auth Configure response to excess web authentication failures
Security Best Practices: Username Settings and Rogue Classification

- Enable “Max Concurrent Logins for a user name”
  ```
  WLC5760(config)#wireless client max-user-login 5
  ```

- Enable Strong Password Policies
  ```
  WLC5760(config)#wireless security strong-password
  ```

- Enable Rogue Classification Policies
  ```
  WLC5760(config)#wireless wps rogue detection min-rssi -70
  WLC5760(config)#wireless wps rogue detection min-transient-time 1200
  WLC5760(config)#wireless wps rogue rule rule1 priority 1
  WLC5760(config-rule)#classify malicious
  ```
Security Best Practices: SSH / SNMP / ACL

- Enable SSHv2 and disable Telnet
  
  ```
  WLC5760(config)#ip ssh version 2
  ```

- Enable SNMPv3
  
  ```
  WLC5760(config)#snmp-server user admin IT v3 auth md5 password
  ```

- Enable ACL on your WLAN
  
  ```
  WLC5760(config)#ip access-list extended testACL
  WLC5760(config-ext-nacl)#deny ip any 172.20.229.5 255.255.255.255
  ```
Wireless Best Practices – IOS-XE- High Availability

- Full ring setup for stack cable redundancy
- Connect powered down 5760 when pairing WLCs
- Same HW and SW version on both WLCs
- Upgrade the HA Pair instead of individual WLCs
- Add APs when Permanent count WLC is Active
- HA-SKU Standby handles APSSO for 1000 APs
- Set switch priority for deterministic Active election
- Configure LAG for port redundancy

5760 HA AP SSO Deployment Guide:
High Availability Connectivity on 5760

- HA is enabled using Cisco StackWise-480 technology in Full Ring Setup
  
- Recommended: power up the second unit only after a first 5760 is deployed
- Use `Controller# switch 1 Priority 15` on the first unit to prevent having the second unit become active and wipe out your config …
# Wireless Best Practices – IOS-XE

<table>
<thead>
<tr>
<th><strong>WIRELESS / RF</strong></th>
<th><strong>INFRASTRUCTURE</strong></th>
</tr>
</thead>
</table>
| • Enable Band Select  
• Enable Fast ssid change  
• Disable Low data rates  
• Enable Platinum QoS for Voice WLAN  
• Enable RRM(DCA and TPC) to be auto  
• Configure WebAuth best practices  
• Enable CleanAir  
• Enable DFS Channels  
• Limit the number of SSIDs to 3 | • Upgrade to recommended software version  
• Configure GUI Settings  
• Apply right-to-use licenses  
• Configure default gateway  
• Enable NTP/Time  
• Enable ap capwap multicast  
• Configure DHCP Snooping  
• Configure LAG for port redundancy  
• Enable Local Profiling  
• Enable AVC(Application Visibility and Control) |

<table>
<thead>
<tr>
<th><strong>SECURITY</strong></th>
<th><strong>HA</strong></th>
</tr>
</thead>
</table>
| • Enable 802.1x and WPA/WPA2 on WLAN/SSID  
• Change advanced EAP timers  
• Enable client exclusion  
• Enable rogue classification  
• Enable “Max Concurrent Logins for a user name”  
• Enable strong password policies  
• Enable ACL on your WLAN | • Full ring setup for stack cable redundancy  
• Connect powered down 5760 when pairing WLCs  
• Same HW and SW version on both WLCs  
• Upgrade the HA Pair instead of individual WLCs  
• Add APs when Permanent count WLC is Active  
• HA-SKU Standby handles APSSO for 1000 APs  
• Provision for Standby 5760  
• Set switch priority for deterministic Active election |

Prime Infrastructure
CA šablony a workflow
Cisco PI 2.2 – Converged Access Templates

Overview

WLAN: 4 SSID Support – WPA2-Ent/WPA2-Personal/Open/Guest-CWA, 802.11 AC, Captive Bypass-Portal, Fast SSID-Change etc.

Application Experience: Wireless Flexible Netflow, Application Visibility and Per-SSID BW allocation

Security: Radius, TACACS+, 802.1X, CWA, AAA-Override, Client Timeout, NAC, DHCP Snooping, ARP Insp., Clear Passwd Encryption etc.

Wireless Best Practices: Band-Select, RRM, CleanAir, DCA Channel, Radius Timeout, WiFi Direct Policy etc.

Platforms: 3x50 / 4500E-Sup8E
Single-Device CA Design:
- Single Sub-Domain
- No SPG

Platforms: 3x50 / 4500E-Sup8E
Multi-Device CA Design:
- Single or Multi Sub-Domain
- Mobility, MA and SPG

Platforms: 3x50 / 4500E-Sup8E / 5760
Multi-Device CA Design:
- Single or Multi Sub-Domain
- Mobility, MA and SPG

Platforms: 5760
IOS-XE Centralized Design:
- Single or Multi Sub-Domain
- Centralized Wireless Mobility
Cisco PI 2.2 – Converged Access Templates
Example - WLAN Design

Enterprise WLAN Design:
- Three WLAN design support
- Any number can be deployed in single instance
- Any WLAN security permutation can be selected

- Preset WLAN IDs. User can customize if needed
- Flexible and scalable provisioning approach with VLAN name on each WLANs
- Global configuration across all selected devices
Converged Access Workflow (Template Based)

Step 1

Deploy Distributed Wireless using Converged Access and Prime from scratch in minutes.
Converged Access Workflow (Template Based)

Step 2

Select the right deployment mode

Small Branch Environment

This is normally a small site such as a satellite office or a chain store. There is typically no onsite IT support. Network reliability is critical because most network services and resources are located at the central headquarters. Any simplification and efficiency improvements at a single branch office can translate into significant savings for companies when multiplied by their large number of sites. Converged access for a small branch site can be implemented by a single stack of Cisco Catalyst 3850 switches to support local LAN and wireless needs. No dedicated WLC is needed.

Features:
- Advanced QoS, NetFlow, other services for wireless and wired traffic, Layer 3 visibility, and WAN efficiency.

Benefits:
- Management simplicity, good availability due to mobility agent/mobility controller redundancy within the Cisco Catalyst 3850 switch stack, optimized multicast, mobile device onboarding, BYOD and wireless continuity with either WAN outage or switch failure within the stack. These benefits are also shared with environments described next.

Availability: The Cisco Catalyst 3850 switch stack serves as wireless mobility agent and mobility controller to support up to 50 access points and 2000 wireless clients.
Converged Access Workflow (Template Based)

**Step 3**

Select devices where converged access needs to be enabled.
## Converged Access Workflow (Template Based)

### Step 4

#### Values filled in the ‘ALL Selected Devices’ will be used for each device. Any device-specific value filled in per device, will override the value provided under ‘ALL Selected Devices’. ‘APPLY’ does not check mandatory parameters for ‘ALL Selected Devices’. It is applicable only for individual devices.

<table>
<thead>
<tr>
<th>Devices</th>
<th>Name</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All Selected Devices</td>
<td>Only one WLAN and Guest are mandatory</td>
</tr>
<tr>
<td></td>
<td>Edition-225</td>
<td>For most deployments, this will be mandatory</td>
</tr>
<tr>
<td></td>
<td>Edition-226</td>
<td>Basic IP information for Guest Controller/Anchor (GA)</td>
</tr>
<tr>
<td></td>
<td>Edition-227</td>
<td>If your infrastructure already has existing AAA server, you can integrate that with CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you are wanting to turn on AVC, check the box to enable it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mainly for a large branch for peering between MA/MC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is mandatory and will be applicable for all type of branches.</td>
</tr>
</tbody>
</table>
Converged Access Workflow (Template Based)

Step5

VIOLA !! Preview CLI’s before deploying Converged Access
Demo – Prime Infra CA Workflow
Troubleshooting
Troubleshooting – IOS-XE WLC Config Analyzer

• Now works on the IOS based Controllers
• You need “show tech-support” and “show tech-support wireless”
• It checks for Best Practices Configurations

• Link https://supportforums.cisco.com/document/7711/wlc-config-analyzer
<table>
<thead>
<tr>
<th>Fail Check</th>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>230001</td>
<td>General: Controller with non recommended code version.</td>
</tr>
<tr>
<td>Yes</td>
<td>230057</td>
<td>General: Disabling low data rates/11b can help to optimize the channel utilization on the 2.4 band. Depending on RF coverage, or if using legacy clients, this is highly recommended.</td>
</tr>
<tr>
<td>No</td>
<td>230058</td>
<td>General: Multicast unicast mode is suboptimal transport for networks with IPv6, mDNS, etc. Multicast mode is recommended. To use it, you also need multicast enabled.</td>
</tr>
<tr>
<td>No</td>
<td>230064</td>
<td>General: EAP request timeout larger than 400ms. EAP requests may benefit for faster recovery, and better behavior on bad RF, by using higher counts, lower retry time.</td>
</tr>
<tr>
<td>Yes</td>
<td>230065</td>
<td>General: EAP request retries lower than 3. EAP requests may benefit for faster recovery, and better behavior on bad RF, by using higher counts, lower retry time.</td>
</tr>
<tr>
<td>No</td>
<td>230067</td>
<td>General: Minimum Rogue RSSI detection threshold should be set to -80 or higher, unless mandated by your security policies.</td>
</tr>
<tr>
<td>No</td>
<td>230069</td>
<td>General: At least one Autocontain policy is enabled. Rogue contention has severe impact on client serving time, it should be avoided unless mandated by your security policies.</td>
</tr>
<tr>
<td>Yes</td>
<td>230070</td>
<td>General: AVC visibility is recommended.</td>
</tr>
<tr>
<td>No</td>
<td>230071</td>
<td>General: Fast SSID enabled is recommended for networks that may have Apple IOS client devices.</td>
</tr>
<tr>
<td>No</td>
<td>230072</td>
<td>General: CleanAir detection is highly recommended if your current AP HW types support the feature.</td>
</tr>
<tr>
<td>Yes</td>
<td>230081</td>
<td>General: BandSelect is recommended on WLAN for better client experience.</td>
</tr>
<tr>
<td>Yes</td>
<td>230082</td>
<td>General: Load Balance is recommended on WLAN for better client experience.</td>
</tr>
<tr>
<td>Yes</td>
<td>230083</td>
<td>General: DHCP Snooping is recommended both globally and on each vlan. Please make sure the dhcp trust is enabled on upstream port of the controller as well.</td>
</tr>
<tr>
<td>Yes</td>
<td>230084</td>
<td>General: Radius load balancing is recommended for better performance.</td>
</tr>
<tr>
<td>Yes</td>
<td>230085</td>
<td>General: Web Authentication is recommended on WLAN.</td>
</tr>
</tbody>
</table>
**IOS XE - Traces vs Debugs**

- Traces are not displayed on console/terminal, but stored in a circular buffer
- Traces are “always-on”, you can change the level and filtering options
- Traces are less impactful on system performance
- **Traces are preferred for troubleshooting wireless issues!**

Example - Set the trace level to debug for the trace we want to collect

```
3850-1#set trace capwap ap event level debug
  debug  Debug-level messages (7)
  default Unset Trace Level Value
  err    Error conditions (3)
  info   Informational (6)
  warning Warning conditions (4)
```

- To turn off the trace debugging, set the level back to default
Using Traces

- To view unfiltered output:
  - `show trace message <feature>`

- To view filtered output:
  - `show trace sys-filtered-traces`
  - `show trace messages <feature> filtered`

- Several macros are available to enable sets of traces, example:
  - `set trace group-wireless-secure level debug`

- Clear a trace
  - `set trace control <feature> clear`

- Redirect the output to a file for easier offline analysis:
  - `show trace message <feature> | redirect tftp:...`
  - `show trace message <feature> | tee tftp:...`

Feature list:
- `show trace all-buffer settings`

3.3+

File only

Console + File
Capturing Traffic – CA Wireshark

- To Analyze what is Wrong in the Air, your First Step is to See the Air
- On Converged Access Switches, you can Wireshark directly from the switch

<table>
<thead>
<tr>
<th>Interface type</th>
<th>Capture Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 port (physical port)</td>
<td>Yes</td>
</tr>
<tr>
<td>L3 port (routed/physical port)</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN</td>
<td>Yes</td>
</tr>
<tr>
<td>L2 / L3 Etherchannel, Tunnels (GRE an others)</td>
<td>No</td>
</tr>
<tr>
<td>SVI</td>
<td>Yes</td>
</tr>
<tr>
<td>CAPWAP tunnel</td>
<td>Yes (via CAPWAP tunnel)</td>
</tr>
<tr>
<td>Wireless Client</td>
<td>Yes (via CAPWAP tunnel)</td>
</tr>
<tr>
<td>Wireless SSID</td>
<td></td>
</tr>
</tbody>
</table>

3850-T#monitor capture mycap1 interface capwap 0 in
3850-T#monitor capture mycap1 file location flash:mycap.pcap
3850-T#monitor capture mycap1 file buffer-size 1
3850-T#monitor capture mycap1 start
3850-T#

*Nov 13 07:05:02.000: %BUFCAP-6-ENABLE: Capture Point mycap1 enabled.*

I just want to see what is received

In MB, nice to have to limit flash overload
Wireshark on CA – Example Wireless Capture

3850-T#show monitor capture file flash:/mycap.pcap detailed | section Frame 17
Frame 17: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
   Arrival Time: Nov 13, 2014 07:05:48.552965000 UTC
   Epoch Time: 1415862348.552965000 seconds
   [Time delta from previous captured frame: 1.556023000 seconds]
   [Time delta from previous displayed frame: 1.556023000 seconds]
   [Time since reference or first frame: 44.498983000 seconds]
Frame Number: 17
Frame Length: 122 bytes (976 bits)

3850-T#copy flash:mycap.pcap usbflash0:mycap.pcap
Destination filename [mycap.pcap]?
Copy in progress...CC
68174 bytes copied in 0.240 secs (284058 bytes/sec)

export is usually better -> PC
CA - Sniffer Mode vs Packet Dump vs CLI Wireshark
Which one to Use

- **CLI Wireshark** captures all traffic from the AP
  - Including CAPWAP traffic, on all radios
  - Nice to have a view “from the AP vantage point”

- **Use Packet dump** to target a specific issue that you identified clearly
  - E.g. client does not get an IP
  - Do not use packet dump for “Wi-Fi does not work well” kind of issue

- **Both CLI Wireshark and Packet dump miss a critical element:**
  - the radiotap header
  - Sniffer mode has a form of radiotap information

```
3850-T# config ap packet-dump ftp serverip 172.29.129.56 path / username cisco password cisco
3850-T# config ap packet-dump start 78:7e:61:76:00:d3 APa80c.0dd2.218c
3850-T# ap name AP44d3.ca42.5961 sniff dot11a 48 172.29.129.56
```
Závěr
An Evolutionary Advance to Cisco’s Wired + Wireless Portfolio, to address device and bandwidth scale, and services demands ....
Converged Access Deployment Examples

INTEGRATED CONTROLLER OPTIONS

DMZ
- Prime
- ISE

Optional Guest Anchor

WAN

Small Controller-less BRANCH
- Up to 25 APs with 3650 (50 APs w3850/4K)
- Up to 1000 Clients per branch with 3650
- All WAN Services Available (local termination)

Large Controller-less BRANCH
- 50 Access Points with only 3650s
- 100 Access Points with 3650s / 4K
- Up to 2000 Clients with only 3650s (4000 w/3850 / 4K)
- Visibility, Control and resiliency

Large Layer 3 roaming domains

CAMPUS with 2x 5760 acting as MCs / Controllers
- Up to 2 000 Access Points
- Up to 24 000 wireless clients
- Large Layer 3 roaming domains

EXTERNAL MOBILITY CONTROLLER

ISE
- Prime

Mobility Controller

Mobility Agent

5760 External Controller

Any CA 3K

Traditional
3K/4K
Q & A

Prosíme, ohodnoťte tuto přednášku - TECH-WLAN P2

Děkujeme