ENTERPRISE WIRELESS

# WLSI 300-120

*Complete Learning Guide*

UNOFFICIAL STUDY GUIDE

**FREE SAMPLE · FIRST 40 PAGES**

JOZEF BAROŠ

# Implementing Cisco Wireless Advanced Solutions

**WLSI 300-120 v1.2 — Complete Learning Guide**

A complete study guide for the Implementing Cisco Wireless Advanced Solutions exam, built around the Catalyst 9800 controller running IOS XE, with AireOS equivalents where they aid engineers migrating an existing estate.

Covering FlexConnect, quality of service, multicast, location services, advanced location services, security for wireless client connectivity, monitoring and device hardening — with 265 knowledge-check questions, 57 diagrams and ten worked cases from production networks.

# Disclaimer

This book is an independent study guide. It is not affiliated with, authorised by, endorsed by, or sponsored by Cisco Systems, Inc. Cisco, Catalyst, IOS XE, FlexConnect, CleanAir, Cisco Spaces, Catalyst Center and Identity Services Engine are trademarks or registered trademarks of Cisco Systems, Inc. All other trademarks are the property of their respective owners, and are used here for identification purposes only.

The configuration examples in this book are written for teaching. They are drawn from published documentation and production experience, but they are illustrative rather than deployment-ready: addresses, credentials, VLAN numbers and profile names are examples, and any configuration should be reviewed against your own design, your own software release and Cisco's current documentation before being applied to a production network.

Command syntax, feature availability and platform behaviour change between IOS XE releases. Where a detail matters to your deployment, verify it against the configuration guide for the specific release you are running. Neither the author nor any contributor accepts liability for loss or damage arising from the use of the material in this book.

Exam topics are those published by Cisco for Implementing Cisco Wireless Advanced Solutions v1.2 (300-120). Cisco may revise the blueprint at any time without notice, and the current version should be confirmed on Cisco's own website before you sit the exam.

# About This Book

This book was written for the engineer who can already build a wireless network and now has to make it work properly — at forty branches, under an audit, during an outage, for users who do not care why. That is the level the WLSI 300-120 exam is pitched at, and it is the level the material here assumes.

## What it assumes you already know

A working knowledge of wireless fundamentals: how 802.11 associates and authenticates, what a CAPWAP tunnel is, how an access point joins a controller, and the basics of RF. If you hold a CCNA-level wireless certification or have run a campus wireless network, you have the foundation this book builds on. Where a concept from that level is decisive — the DTIM beacon, the four-way handshake, PIM sparse mode — it is restated briefly rather than assumed.

## How each section is built

Every sub-section follows the same shape, deliberately:

- **Explanation from first principles**, because a mechanism you understand is one you can reason about under exam pressure, and a mechanism you have memorised is not.
- **Diagrams** where a relationship is spatial or sequential — data paths, decision trees, protocol exchanges.
- **Complete configurations** for the Catalyst 9800, written as you would type them, with verification commands alongside.
- **Four kinds of margin note**: an Exam Tip where something is directly testable, a Common Pitfall where deployments reliably go wrong, a Did You Know for the detail that makes a mechanism make sense, and From the Field for what actually happens in production.
- **A summary and key takeaways**, written so the takeaways alone are a usable revision pass.
- **Five knowledge-check questions** with a full explanation of why the correct answer is correct — and, where it matters, why the plausible wrong answer is wrong.

## How to use it

For a **first pass**, read a section end to end and attempt its questions without looking back. The questions are written to be answerable from the section, so a wrong answer identifies a specific gap rather than a general weakness.

For **revision**, the key takeaways and the summaries are designed to be read alone. Reading only the takeaways from all eight sections takes about ninety minutes and is a reasonable final-week exercise.

For **practical reference**, the configuration blocks are self-contained and the verification commands after each are the ones worth committing to memory. Section 6.9, Section 7.6 and the troubleshooting sub-sections in each domain are written to be usable during an actual incident.

The **ten cases** at the end are best left until the sections are complete. They deliberately cross domain boundaries, and their value is in recognising which domain a symptom belongs to — which requires having the domains in place first.

## A note on the platform

Configurations are given for the **Catalyst 9800** running IOS XE, because that is the platform Cisco expects candidates to configure. Where a concept has a well-known AireOS equivalent — FlexConnect groups, metal QoS profiles, CPU ACLs — the mapping is given, both because engineers migrate estates and because the exam occasionally frames a question in terms an AireOS engineer would recognise.

## How This Book Maps to the Exam

The eight sections correspond one to one with the eight domains of the published blueprint, and the depth given to each reflects its weighting. The table below maps every blueprint topic to the sub-section that covers it.

| Blueprint topic | Weight | Section |
|---|---|---|
| 1.0 FlexConnect | 15% | |
| 1.1 Switching and operating modes | | 1.1 |
| 1.2a FlexConnect groups and roaming | | 1.3 |
| 1.2b Split tunnelling and fault tolerance | | 1.4 |
| 1.2c VLAN-based central switching and Flex ACL | | 1.5 |
| 1.2d Smart AP image upgrade | | 1.6 |
| 1.3 Office Extend | | 1.7 |
| 2.0 QoS on a Wireless Network | 10% | |
| 2.1 QoS schemes, wired to wireless mapping | | 2.1, 2.4 |
| 2.2 QoS for wireless clients | | 2.2, 2.3 |
| 2.3 AVC | | 2.5 |
| 3.0 Multicast | 10% | |
| 3.1 Multicast components | | 3.1 |
| 3.2 Effect on wireless networks | | 3.2 |
| 3.3 Multicast on a WLAN | | 3.3 |
| 3.4 mDNS | | 3.4 |
| 3.5 Multicast Direct | | 3.5 |

| Blueprint topic | Weight | Section |
|---|---|---|
| 4.0 Location Services | 10% | |
| 4.1 Deploy CMX and Cisco Spaces | | 4.3, 4.4 |
| 4.2 Implement location services | | 4.1, 4.2, 4.5 |
| 5.0 Advanced Location Services | 10% | |
| 5.1a-b Detect and Locate, Analytics | | 5.1, 5.2 |

| Blueprint topic | Weight | Section |
|---|---|---|
| 5.1c-e Presence, captive portals, connectors | | 5.2, 5.3 |
| 5.2 Location-aware guest services | | 5.4 |
| 5.3 Troubleshoot location accuracy | | 5.5 |
| 5.4 Troubleshoot connector high availability | | 5.6 |
| 5.5 wIPS using Cisco Catalyst Center | | 5.7 |
| 6.0 Security for Wireless Client Connectivity | 20% | |
| 6.1 Client profiling on WLC and ISE | | 6.2 |
| 6.2a CWA using ISE, self-registration | | 6.3 |
| 6.2b LWA using ISE or WLC | | 6.4 |
| 6.2c Native supplicant provisioning | | 6.5 |
| 6.2d Certificate provisioning on the controller | | 6.6 |
| 6.3 Client security on different architectures | | 6.7 |
| 6.4 Identity-Based Networking | | 6.8 |

| Blueprint topic | Weight | Section |
|---|---|---|
| 7.0 Monitoring | 15% | |
| 7.1 Reports on Cisco Catalyst Center | | 7.2 |
| 7.2 Alarms and rogues (WLC, Catalyst Center) | | 7.3, 7.4 |
| 7.3 RF interferers (WLC, Catalyst Center) | | 7.5 |
| 7.4 Troubleshoot client connectivity | | 7.6, 7.7 |
| 8.0 Device Hardening | 10% | |
| 8.1 Device access controls, RADIUS and TACACS+ | | 8.1 |
| 8.2 Access point authentication, 802.1X | | 8.2 |
| 8.3 Control Plane ACLs on the controller | | 8.3 |

Two sub-sections have no direct blueprint entry and are included because the exam assumes them: **6.1**, which establishes the 802.1X, EAP and WPA vocabulary that Domain 6 is written in, and **7.1**, which explains how monitoring data leaves the controller at all. **8.4** consolidates hardening measures introduced across several domains into a single checklist.

> ✅ **Exam Tip — Weighting is a guide to depth, not to question count**

A 20 percent domain will not necessarily produce exactly one question in five, and a 10 percent domain can still decide a marginal pass. Use the weightings to allocate study time — Domains 6 and 7 together are more than a third of the exam — but do not treat the smaller domains as optional. Device hardening is 10 percent, and its content is short enough to master completely, which makes it some of the cheapest marks available.

# About This Free Sample

This is a **free sample of the complete guide**. It contains the front matter, the full blueprint mapping, and the first four sub-sections of Section 1, and the start of the fifth, — the FlexConnect domain — reproduced exactly as it appears in the book, including its diagrams, configurations, callouts and knowledge-check questions.

Nothing here is abridged. What you read in these pages is what every one of the 334 pages looks like, so you can judge the depth, the tone and the level of detail before deciding whether the full guide is right for you.

## What is in this sample

- **About This Book** — how the material is structured and how to use it.
- **How This Book Maps to the Exam** — every blueprint topic mapped to its sub-section.
- **Section 1 overview** — the FlexConnect domain and what it is worth.
- **1.1 FlexConnect Components, Switching Modes and Operating Modes** — complete.
- **1.2 The Catalyst 9800 Configuration Model for FlexConnect** — complete.
- **1.3 FlexConnect Groups and Roaming** — complete.
- **1.4 Split Tunnelling and Fault Tolerance** — complete.
- **1.5 VLAN-Based Central Switching and Flex ACLs** — the opening, where the sample breaks off.

## What is in the full guide

| Section | Domain | Weight | Pages |
|---|---|---|---|
| 1 | FlexConnect | 15% | 47 |
| 2 | QoS on a Wireless Network | 10% | 36 |
| 3 | Multicast | 10% | 32 |
| 4 | Location Services | 10% | 28 |
| 5 | Advanced Location Services | 10% | 34 |
| 6 | Security for Wireless Client Connectivity | 20% | 50 |
| 7 | Monitoring | 15% | 36 |
| 8 | Device Hardening | 10% | 23 |
| — | Ten cases from the field | — | 31 |
| — | Front matter, glossary and wrap-up | — | 17 |

Every one of the 63 sub-sections follows the same structure you are about to see: explanation from first principles, diagrams, complete Catalyst 9800 configurations with verification commands, four kinds of margin note, a summary, key takeaways, and five knowledge-check questions with full explanations.

> ✅ **Exam Tip — The questions explain themselves**
> Every knowledge-check answer includes a full explanation of why the correct option is correct and, where it matters, why the most plausible wrong option is wrong. A question you get wrong should identify a specific gap, not leave you guessing.

# Section 1 — FlexConnect

Every wireless design eventually meets the same wall: the controller lives in a data centre, the users do not. A branch office, a retail store, a clinic, or a home office is connected to that data centre by a WAN link that is slower, more expensive, and less reliable than the LAN. **FlexConnect** is Cisco's answer to that problem. It lets an access point keep its brain in the central controller while keeping its user traffic — and, when the WAN fails, part of its decision-making — at the branch.

On the WLSI 300-120 exam FlexConnect carries **15%** of the score, the joint-largest weighting after wireless client security. That weighting is not accidental: FlexConnect touches switching, VLANs, ACLs, authentication, roaming, and software upgrades all at once, so it is fertile ground for scenario questions. Almost every FlexConnect question you will see is really asking one of two things: *where does this packet get switched?* and *what still works when the WAN goes down?*

This section builds the answer from the ground up. We start with the two independent choices that define FlexConnect — switching mode and operating mode — then translate them into the Catalyst 9800 configuration model of tags and profiles. From there we work outward through groups and fast roaming, split tunneling and fault tolerance, VLAN mapping and Flex ACLs, efficient image upgrade, and OfficeExtend, closing with a disciplined troubleshooting method you can use on a real branch at 2 a.m.

| Sub-section | Focus | What the exam asks |
|---|---|---|
| 1.1 Fundamentals | Switching and operating modes | Where traffic is switched, what survives a WAN cut |
| 1.2 The 9800 model | Tags, flex profile, policy profile | Which object holds which setting |
| 1.3 Groups and roaming | Key caching, 802.11r, OKC | Why a roam is slow and how to fix it |
| 1.4 Split tunneling | Split ACLs, fault tolerance, local auth | Which traffic stays local; what breaks offline |
| 1.5 VLANs and Flex ACLs | VLAN mapping, AAA override, ACL enforcement | Which VLAN a client lands in and why |
| 1.6 Image upgrade | Efficient / smart image upgrade | How to upgrade a branch over a thin WAN |
| 1.7 OfficeExtend | OEAP, DTLS, personal SSID | Teleworker design and its ports |
| 1.8 Troubleshooting | A repeatable triage order | Reading show output under pressure |

> ✅ **Exam Tip — Two questions answer most FlexConnect items**
> Before you read the options, ask yourself: (1) is this WLAN **centrally switched** or **locally switched**? (2) is the AP in **connected** or **standalone** mode? Nearly every FlexConnect scenario resolves once you have answered both. Options that mix the two — "the AP switches locally but the client is dropped because the WLC is unreachable" — are usually the distractors.

# 1.1 FlexConnect Components, Switching Modes and Operating Modes

An access point that has joined a controller normally does very little thinking. It builds a **CAPWAP** tunnel — Control And Provisioning of Wireless Access Points, the standard protocol an AP uses to talk to its controller — and hands every user frame to the controller inside that tunnel. The controller applies policy, decrypts, and places the frame on a VLAN. This is called **local mode**, and it is an excellent design when the AP and the controller sit on the same campus LAN.

Put a WAN link in the middle and local mode becomes expensive. A user printing to a printer three metres away would send that traffic across the country to the data centre and back — a phenomenon engineers call *hairpinning* or *tromboning*. Worse, if the WAN drops, the AP loses its controller and the branch loses its wireless entirely. FlexConnect solves both problems by moving the **data plane** to the AP while leaving the **control plane** in the controller.

## Two independent choices

FlexConnect is defined by two settings that people constantly conflate. They are independent, and the exam loves the combinations.

- **Switching mode** — where the user's data frame is placed on a wire. *Central switching* sends it through the CAPWAP data tunnel to the controller. *Local switching* has the AP bridge it directly onto the local switch port, tagged into a VLAN.
- **Authentication mode** — where the client's identity is checked. *Central authentication* means the controller (and behind it, a RADIUS server such as Cisco ISE) does the checking. *Local authentication* means the AP itself terminates the EAP exchange, using either a locally configured RADIUS server or its own local EAP database.

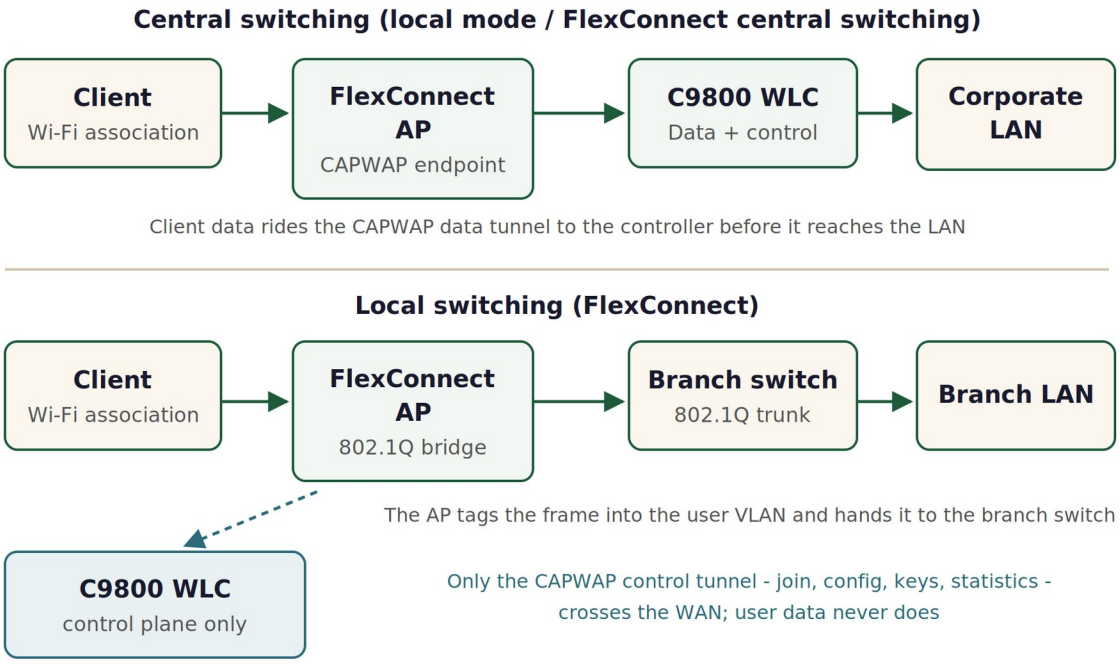


*Figure 1.1 — Central switching sends every frame to the controller; local switching bridges it onto the branch VLAN and keeps only the control tunnel across the WAN.*

The two choices give four combinations, and each one behaves differently when the WAN fails. Memorise this table — it is the single densest source of FlexConnect exam questions.

| Combination | Typical use | Behaviour if the WAN drops |
|---|---|---|
| Central switching + central auth | Small branch, DC-bound traffic only | WLAN is torn down; clients disconnect |
| Local switching + central auth | The common branch design | Existing clients keep working; new joins fail |
| Local switching + local auth | Resilient branch, WAN often unstable | New clients can still authenticate on the AP |
| Central switching + local auth | Not supported / not used | N/A — a classic distractor |

> ⚠️ **Common Pitfall — "Local switching" does not mean "local authentication"**
>
> A locally switched WLAN with central 802.1X still needs the controller for every **new** association, because the EAP exchange is relayed over CAPWAP. If a question says the WAN is down and asks whether a **new** user can connect, the answer is no — unless local authentication (or a locally configured RADIUS server in the flex profile) is present.

## Connected and standalone: the operating modes

The second dimension is the AP's **operating mode**, which is not something you configure — it is a state the AP falls into. While the CAPWAP control tunnel is up and heartbeats are being acknowledged, the AP is in **connected mode**. When the AP misses its heartbeats (by default it retries every 5 seconds and gives up after roughly 30 seconds of silence), it declares the controller unreachable and enters **standalone mode**.

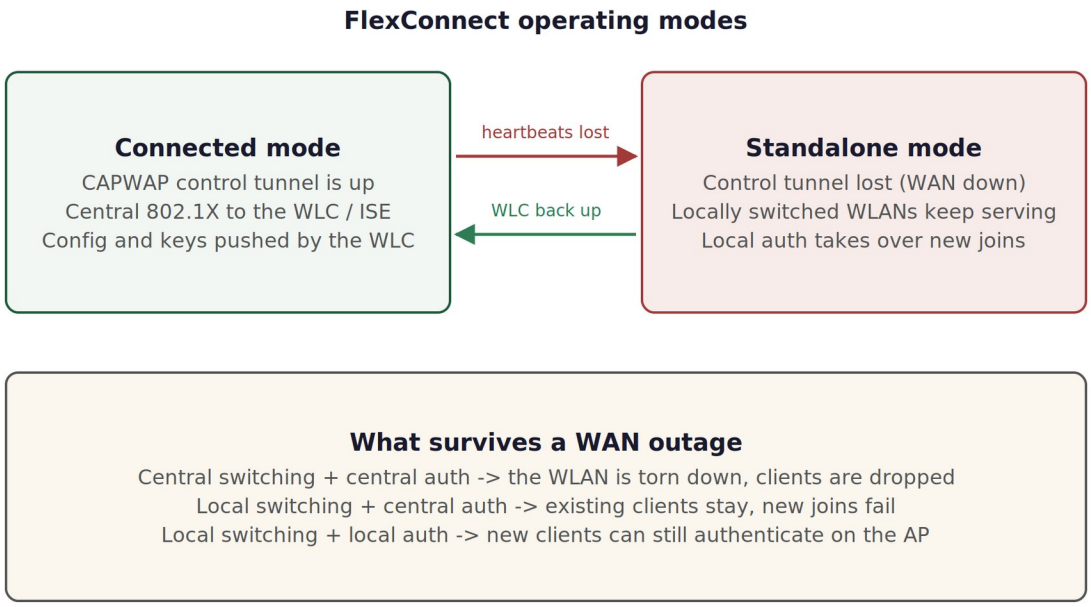


*Figure 1.2 — Connected and standalone mode, and what each combination of switching and authentication survives.*

In standalone mode the AP keeps serving locally switched WLANs from the configuration it already holds in flash. It cannot learn anything new: no configuration changes, no new WLANs, no controller-driven RRM decisions, and no CAPWAP-relayed authentication. Centrally switched WLANs are disabled outright, because their only path to the network was the tunnel that just died.

> 💡 **Did you know? — Standalone is not the same as autonomous**
>
> An *autonomous* AP has no controller at all and is configured through its own IOS CLI. A *standalone* FlexConnect AP is still a controller-managed AP — it is simply running on the last configuration it was given, waiting for the controller to come back. You cannot log into it and reconfigure WLANs; when the tunnel returns, the controller's configuration wins.

## Where FlexConnect fits among the AP modes

On a Catalyst 9800 an AP's mode determines what software role it plays. Only a handful matter for this exam.

| AP mode | Data plane | Typical role |
|---|---|---|
| Local | CAPWAP to the WLC | Campus AP on a LAN, RTT under 100 ms |
| FlexConnect (flex) | Local bridge or CAPWAP, per WLAN | Branch AP across a WAN, RTT up to 300 ms |
| Flex + Bridge | Local bridge with mesh backhaul | Outdoor or mesh branch deployments |
| Monitor | None — receive only | Location, rogue and wIPS scanning |
| Sniffer | Forwards captures to a sniffer | Over-the-air packet capture |
| Sensor | None — runs synthetic tests | Catalyst Center assurance testing |

> ✅ **Exam Tip — Round-trip time is the design boundary**
> A **local-mode** AP tolerates about **100 ms** of round-trip latency to its controller. A **FlexConnect** AP tolerates up to **300 ms**. When a scenario mentions a satellite link, a long-haul MPLS circuit, or a VPN over the public Internet, that latency figure is usually the reason FlexConnect is the correct answer.

## Converting an AP to FlexConnect on the Catalyst 9800

Changing an AP's mode causes it to reboot and rejoin, so it is done during a change window. The mode can be set per AP from the controller CLI:

*Putting a single AP into FlexConnect mode (the AP reboots)*

```
WLC# ap name AP-BR1-01 mode flex submode none
Changing the AP's mode will cause the AP to reboot. Continue? (y/n): y

WLC# show ap name AP-BR1-01 config general | include Mode|Site Tag|IP
AP Mode                                         : FlexConnect
AP Submode                                      : Not Configured
Site Tag Name                                   : ST-BRANCH01
IP Address Configuration                        : DHCP
IP Address                                      : 10.10.11.21
```

For a whole site you rarely set the mode AP by AP. Instead the **AP join profile** attached to the site tag carries the mode, and every AP that inherits that site tag adopts it on join. That is the subject of sub-section 1.2.

*Verifying that a WLAN is locally switched for a given AP*

```
WLC# show wireless profile policy detailed PP-BRANCH-USERS | include switching|
dhcp|VLAN
Central Switching                       : DISABLED
Central Authentication                  : ENABLED
Central DHCP                            : DISABLED
VLAN                                    : 20
```

```
WLC# show ap name AP-BR1-01 config general | include FlexConnect
FlexConnect Local Switching              : Enabled
FlexConnect Local Authentication         : Disabled
FlexConnect VLAN Support                 : Enabled
FlexConnect Native VLAN                  : 10
```

🌍 **From the Field — The trunk is the other half of the design**

A FlexConnect AP that switches locally is, from the branch switch's point of view, a device that sends 802.1Q-tagged frames. The switch port must be a **trunk**, its native VLAN must match the AP's native VLAN, and every user VLAN you intend to map must be allowed on that trunk. In practice more branch "wireless outages" are caused by a missing VLAN on the trunk than by anything happening over the air.

*The matching branch switch port — the piece people forget*

```
Switch(config)# interface GigabitEthernet1/0/12
Switch(config-if)#  description AP-BR1-01
Switch(config-if)#  switchport mode trunk
Switch(config-if)#  switchport trunk native vlan 10
Switch(config-if)#  switchport trunk allowed vlan 10,20,30,40
Switch(config-if)#  spanning-tree portfast trunk
Switch(config-if)#  power inline auto
```

## The AireOS equivalent

Many production networks still run AireOS controllers (5520, 8540, 3504), and the exam may show either syntax. The concepts are identical; only the objects differ. AireOS configures FlexConnect on the **AP** and on the **WLAN**, while the 9800 configures it on **profiles** that are bound to APs by tags.

*AireOS: the same result in three commands*

```
(WLC) > config ap mode flexconnect AP-BR1-01
(WLC) > config wlan flexconnect local-switching 5 enable
(WLC) > config ap flexconnect vlan native 10 AP-BR1-01
(WLC) > show ap config general AP-BR1-01
```

**Summary**

FlexConnect separates the data plane from the control plane so that a branch AP can bridge user traffic locally while the controller, across the WAN, keeps configuration and policy. Two independent settings define its behaviour: switching mode (central or local) and authentication mode (central or local). The AP is in connected mode while its CAPWAP control tunnel is alive and falls into standalone mode when heartbeats fail, at which point centrally switched WLANs go down and locally switched ones keep running on cached configuration. FlexConnect also relaxes the controller latency budget from roughly 100 ms to 300 ms of round-trip time, which is what makes a WAN-attached branch practical.

**Key Takeaways**

- **Central switching** tunnels user data to the WLC; **local switching** bridges it onto the branch VLAN.
- **Central auth** needs the WLC for every new association; **local auth** lets the AP authenticate on its own.
- **Connected vs standalone** is a state, not a setting — it follows the health of the CAPWAP control tunnel.
- In standalone mode, **centrally switched WLANs are dropped** and locally switched ones keep serving.
- Latency budget: **100 ms** for local mode, **300 ms** for FlexConnect.
- A locally switching AP needs a **trunk port** with the right native VLAN and allowed VLAN list.

### Knowledge Check — 1.1

**Q1.** A branch WLAN is configured for local switching with central 802.1X authentication. The WAN link fails. What happens to a user who is already associated and to a user who now tries to connect?

**A.** Both users are disconnected immediately
**B.** Both users continue to work normally
**C.** The associated user keeps working; the new user cannot authenticate
**D.** The associated user is disconnected; the new user connects using cached credentials

**Correct answer: C.** Traffic for an already-authenticated client is bridged locally by the AP and needs no controller, so that session survives. A new association requires the EAP exchange to be relayed to the controller, which is unreachable, so the join fails unless local authentication is configured.

**Q2.** Which statement about a FlexConnect AP in standalone mode is correct?

**A.** It continues to serve locally switched WLANs using its cached configuration
**B.** It converts itself to an autonomous AP and can be configured over SSH
**C.** It continues to serve centrally switched WLANs by buffering traffic
**D.** It reboots every 30 seconds until the controller returns

**Correct answer: A.** A standalone AP runs on the configuration it already holds and keeps locally switched WLANs alive. It is still a controller-managed AP, it cannot be reconfigured locally, and centrally switched WLANs are disabled because their data path is gone.

**Q3.** What is the maximum round-trip time Cisco supports between a FlexConnect AP and its controller?

**A.** 100 ms
**B.** 20 ms
**C.** 1 000 ms
**D.** 300 ms

**Correct answer: D.** FlexConnect is designed for WAN-attached sites and supports up to 300 ms of round-trip latency. 100 ms is the figure for a local-mode AP, which is why a high-latency circuit points to FlexConnect as the design answer.

**Q4.** A locally switched WLAN maps clients into VLAN 30, but clients receive no DHCP address. The AP is joined, the WLAN is up, and the flex profile lists VLAN 30. What should you check first?

- **A.** That the controller has an SVI in VLAN 30
- **B.** That VLAN 30 is allowed on the trunk port connecting the AP to the branch switch
- **C.** That the AP is running the same software version as the controller
- **D.** That central DHCP is enabled on the policy profile

**Correct answer: B.** With local switching, the AP tags the frame and hands it to the branch switch; the controller is not in the data path and needs no SVI. If the trunk does not allow VLAN 30, the tagged frames are discarded and DHCP never reaches the server.

**Q5.** Which combination of switching and authentication is NOT a supported FlexConnect design?

- **A.** Central switching with local authentication
- **B.** Local switching with central authentication
- **C.** Local switching with local authentication
- **D.** Central switching with central authentication

**Correct answer: A.** Local authentication exists so that a branch can keep authenticating clients when the controller is unreachable. That only makes sense when the data path is also local, so central switching with local authentication is not a valid design and appears in exam questions purely as a distractor.

## 1.2 The Catalyst 9800 Configuration Model for FlexConnect

If you learned wireless on AireOS, the Catalyst 9800 feels inside-out at first. On AireOS you configured an AP, then a WLAN, then a FlexConnect group, and each object carried its own settings. On the 9800 you configure **profiles** — reusable bundles of settings — and then bind them to APs with **tags**. Nothing is configured on an AP directly except which tags it wears.

This is worth the adjustment, because it is what lets one controller run 500 branches without 500 separate configurations. It is also examinable in its own right: a large share of 9800 questions are really asking *which object holds this setting?*

### Three tags, and what each one carries

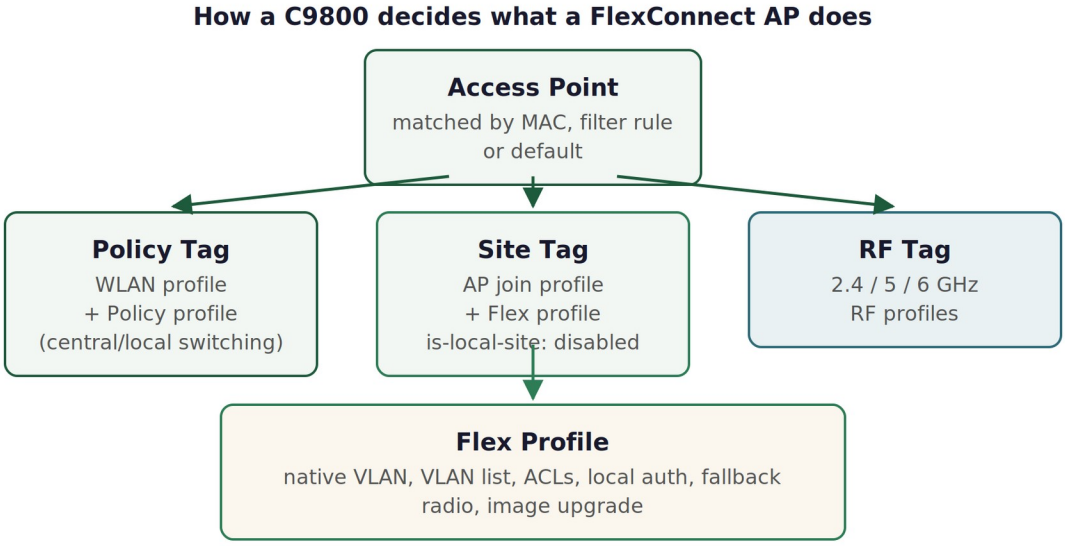


*Figure 1.3 — An AP wears three tags. For FlexConnect, the site tag and the policy tag do the work.*

| Tag | Contains | FlexConnect relevance |
|---|---|---|
| Policy tag | WLAN profile + policy profile pairs | Sets central vs local switching, VLAN, ACLs |
| Site tag | AP join profile + flex profile | Makes the site remote; carries branch settings |
| RF tag | 2.4 / 5 / 6 GHz RF profiles | Radio behaviour only — no FlexConnect role |

The **site tag** is the FlexConnect switch. A site tag with `local-site` configured describes a campus site whose APs run in local mode. A site tag with `no local-site` describes a **remote** site: its APs run in FlexConnect mode, and the site tag may then reference a **flex profile** holding the branch-specific settings.

> ✅ **Exam Tip — `no local-site` is the FlexConnect trigger**
>
> On the 9800 you do not tick a box called "FlexConnect" on the WLAN. You mark the **site tag** as not local (`no local-site`), which puts every AP wearing that tag into FlexConnect mode, and then you turn off central switching on the **policy profile** for the WLANs that should bridge locally. Two objects, two settings — exam questions frequently give you one and ask for the other.

## Building a branch from scratch

The order below is the one to memorise, because each object references the previous one. Build the flex profile first, then the site tag that uses it, then the policy profile, then the policy tag, and finally tag the APs.

### Step 1 — the flex profile

The **flex profile** holds everything that is specific to the branch's wiring and offline behaviour: the native VLAN the AP's own management traffic uses, the list of user VLANs the AP may bridge into, any Flex ACLs, local authentication settings, and the image-upgrade knobs.

*A complete flex profile for a branch*

```
WLC(config)# wireless profile flex FLEX-BRANCH01
WLC(config-wireless-flex-profile)#  description "Branch 01 - Bratislava"
WLC(config-wireless-flex-profile)#  native-vlan-id 10
WLC(config-wireless-flex-profile)#  arp-caching
WLC(config-wireless-flex-profile)#  vlan-name USERS
WLC(config-wireless-flex-vlan)#      vlan-id 20
WLC(config-wireless-flex-vlan)#      exit
WLC(config-wireless-flex-profile)#  vlan-name VOICE
WLC(config-wireless-flex-vlan)#      vlan-id 30
WLC(config-wireless-flex-vlan)#      exit
WLC(config-wireless-flex-profile)#  vlan-name GUEST
WLC(config-wireless-flex-vlan)#      vlan-id 40
WLC(config-wireless-flex-vlan)#      acl-name FLEX-GUEST-ACL
WLC(config-wireless-flex-vlan)#      exit
WLC(config-wireless-flex-profile)#  predownload
WLC(config-wireless-flex-profile)#  ip overlap                ! allow overlapping
IPs across sites
WLC(config-wireless-flex-profile)#  exit
```

> 💡 **Did you know? — Why the native VLAN matters twice**
>
> The native VLAN in a flex profile is the untagged VLAN the AP itself uses — the one carrying its CAPWAP tunnel and DHCP request. It must match `switchport trunk native vlan` on the branch switch. If the two disagree, the AP either never joins or joins on the wrong subnet, and every downstream symptom looks like a mysterious VLAN problem.

### Step 2 — the AP join profile and the site tag

The **AP join profile** carries controller-facing settings for the AP: CAPWAP timers, the AP's login credentials, syslog and TFTP destinations, and — importantly for branches — the primary and secondary controller names the AP should fall back to.

*AP join profile plus a remote site tag*

```
WLC(config)# wireless profile ap-join APJ-BRANCH
WLC(config-ap-profile)#  description "Branch AP join profile"
WLC(config-ap-profile)#  capwap retransmit timeout 5
WLC(config-ap-profile)#  capwap retransmit count 5
WLC(config-ap-profile)#  syslog host 10.1.50.20
WLC(config-ap-profile)#  exit

WLC(config)# wireless tag site ST-BRANCH01
WLC(config-site-tag)#  description "Remote site - Branch 01"
WLC(config-site-tag)#  ap-profile APJ-BRANCH
WLC(config-site-tag)#  flex-profile FLEX-BRANCH01
WLC(config-site-tag)#  no local-site
WLC(config-site-tag)#  exit
```

> ⚠️ **Common Pitfall — Changing an AP's site tag reboots the AP**
>
> A site tag change moves the AP between AP-join profiles and, potentially, between local and FlexConnect mode. The AP must reload to apply it. Policy-tag and RF-tag changes are disruptive to clients but do **not** reboot the AP. Plan site-tag work in a maintenance window; treat policy-tag work as a client-impacting change.

### Step 3 — the WLAN, policy profile and policy tag

The **WLAN profile** defines the SSID and its security. The **policy profile** defines what happens to a client once it has joined: which VLAN, which QoS, and — the setting that matters here — whether traffic is switched centrally.

*WLAN, policy profile and the policy tag that pairs them*

```
WLC(config)# wlan WLAN-CORP 5 CORP-BR
WLC(config-wlan)#  security dot1x authentication-list AAA-DOT1X
WLC(config-wlan)#  security wpa psk set-key ascii 0 <none>      ! WPA2-Enterprise,
no PSK
WLC(config-wlan)#  no shutdown
WLC(config-wlan)#  exit

WLC(config)# wireless profile policy PP-BRANCH-USERS
WLC(config-wireless-policy)#  description "Branch users - locally switched"
WLC(config-wireless-policy)#  no central switching
WLC(config-wireless-policy)#  no central dhcp
WLC(config-wireless-policy)#  central authentication              ! 802.1X still
relayed to ISE
```

```
WLC(config-wireless-policy)#  vlan USERS                          ! the name from
the flex profile
WLC(config-wireless-policy)#  session-timeout 86400
WLC(config-wireless-policy)#  no shutdown
WLC(config-wireless-policy)#  exit

WLC(config)# wireless tag policy PT-BRANCH01
WLC(config-policy-tag)#  wlan WLAN-CORP policy PP-BRANCH-USERS
WLC(config-policy-tag)#  exit
```

✅ **Exam Tip — Name, not number, in a flex policy profile**

On a locally switched policy profile you normally reference the **VLAN name** defined in the flex profile (`vlan USERS`), not a numeric VLAN ID. The name lets one policy profile serve many branches whose VLAN numbering differs — branch 1 maps USERS to VLAN 20, branch 2 maps it to VLAN 120, and neither needs its own WLAN.

### Step 4 — tagging the access points

Tags reach an AP in one of three ways: statically per AP, through an **AP filter** that matches on the AP name with a regular expression, or from the default tags if nothing else matches. At scale, filters are how you avoid touching each AP.

*Static tagging, then the scalable alternative*

```
! Option A - per AP, by Ethernet MAC
WLC(config)# ap 00a2.891c.4400
WLC(config-ap-tag)#  policy-tag PT-BRANCH01
WLC(config-ap-tag)#  site-tag   ST-BRANCH01
WLC(config-ap-tag)#  rf-tag     RF-BRANCH
WLC(config-ap-tag)#  exit

! Option B - match every AP whose name starts with AP-BR1
WLC(config)# ap filter name FLT-BRANCH01
WLC(config-ap-filter)#  ap-name-regex ^AP-BR1-.*
WLC(config-ap-filter)#  tag policy PT-BRANCH01
WLC(config-ap-filter)#  tag site   ST-BRANCH01
WLC(config-ap-filter)#  tag rf     RF-BRANCH
WLC(config-ap-filter)#  exit
WLC(config)# ap filter priority 1 filter-name FLT-BRANCH01
```

🌍 **From the Field — Name your APs before you deploy them**

AP filters are only as good as your naming convention. Teams that agree on something like `AP-<site>-<floor>-<number>` can onboard an entire branch by racking APs and letting the regex do the tagging. Teams that let APs keep their factory names end up tagging by MAC address forever.

## Verifying the build

*The four commands that confirm a FlexConnect site is correct*

```
WLC# show ap tag summary
AP Name          AP Mac          Site Tag      Policy Tag     RF Tag
Misconfigured
---------------- --------------- ------------- -------------- ------------
-------------
AP-BR1-01        00a2.891c.4400  ST-BRANCH01   PT-BRANCH01    RF-BRANCH    No
AP-BR1-02        00a2.891c.5100  ST-BRANCH01   PT-BRANCH01    RF-BRANCH    No

WLC# show wireless tag site detailed ST-BRANCH01
Site Tag Name       : ST-BRANCH01
AP Profile          : APJ-BRANCH
Local-site          : DISABLED
Flex Profile        : FLEX-BRANCH01

WLC# show wireless profile flex detailed FLEX-BRANCH01
Flex Profile Name   : FLEX-BRANCH01
Native Vlan Id      : 10
ARP Caching         : ENABLED
VLAN Name  VLAN Id   ACL
---------- --------- --------------------
USERS      20        -
VOICE      30        -
GUEST      40        FLEX-GUEST-ACL

WLC# show wireless client summary
MAC Address     AP Name      Type  State        Protocol  Method    Role
--------------- ------------ ----- ------------ --------- --------- --------
b826.d4a1.7e02  AP-BR1-01    WLAN  Run          11ax(5)   Dot1x     Local
```

⚠️ **Common Pitfall — A "Misconfigured: Yes" in `show ap tag summary` is not cosmetic**

It means the AP is wearing a tag that references a profile that does not exist, or a combination the controller cannot apply — for example a site tag marked `no local-site` whose flex profile was deleted. The AP falls back to default tags, which almost always means local mode and central switching, and the branch quietly starts tunnelling all of its traffic across the WAN.

**Summary**

The Catalyst 9800 configures FlexConnect through profiles bound by tags rather than through per-AP settings. The site tag decides whether a site is local or remote — `no local-site` puts its APs into FlexConnect mode — and points at a flex profile carrying the native VLAN, the user VLAN list, Flex ACLs, and local authentication settings. The policy profile decides, per WLAN, whether traffic is centrally or locally switched and which VLAN name the client lands in. Build the objects in order (flex profile, AP join profile, site tag, WLAN, policy profile, policy tag), then attach the tags to APs statically or through an AP-name filter, and verify with `show ap tag summary`.

**Key Takeaways**

- **Site tag + `no local-site`** turns APs into FlexConnect APs; the **flex profile** holds the branch settings.
- **Policy profile** holds `no central switching` — that is what makes a WLAN switch locally.
- Reference VLANs by **name** in the flex profile so one policy profile serves many branches.
- A **site tag change reboots the AP**; policy and RF tag changes do not.
- **AP filters** with name regexes are how tags scale beyond a handful of sites.
- `show ap tag summary` reporting **Misconfigured: Yes** means the AP has silently fallen back to default tags.

### Knowledge Check — 1.2

**Q1.** Which object on a Catalyst 9800 determines that an access point operates in FlexConnect mode?

**A.** The policy profile, when central switching is disabled
**B.** The site tag, when it is configured with `no local-site`
**C.** The RF tag assigned to the AP
**D.** The WLAN profile's security settings

**Correct answer: B.** A site tag marked as not local describes a remote site, and every AP wearing that tag joins in FlexConnect mode. Disabling central switching on the policy profile is a separate step that decides how a particular WLAN's traffic is forwarded.

**Q2.** An engineer changes the site tag on 40 production branch APs during business hours. What is the most likely consequence?

**A.** Only clients on centrally switched WLANs are affected
**B.** The change is applied without any client impact
**C.** The APs move to the default policy tag but keep serving clients
**D.** All 40 APs reboot and clients are disconnected until they rejoin

**Correct answer: D.** A site tag change can move an AP between AP-join profiles and between local and FlexConnect mode, so the AP must reload to apply it. Policy-tag and RF-tag changes disrupt clients but do not force a reboot.

**Q3.** Where is the list of user VLANs that a FlexConnect AP is allowed to bridge into configured?

**A.** In the flex profile referenced by the site tag
**B.** In the AP join profile
**C.** In the WLAN profile
**D.** On the AP itself, using the AP console

**Correct answer: A.** The flex profile carries the branch's data-plane settings: native VLAN, the VLAN name-to-ID list, Flex ACLs, and local authentication. The AP join profile carries controller-facing settings such as CAPWAP timers and syslog.

**Q4.** Why does a locally switched policy profile usually reference a VLAN **name** rather than a VLAN ID?

**A.** Because the 9800 does not support numeric VLAN IDs in policy profiles

**B.** Because VLAN names are required for AAA override to work

**C.** So that one policy profile can serve branches that use different VLAN numbers for the same purpose

**D.** Because names are resolved by the RADIUS server rather than the AP

**Correct answer: C.** The flex profile maps a name such as USERS to whatever VLAN ID that branch happens to use. Referencing the name lets a single WLAN and policy profile be reused across hundreds of sites with different numbering.

**Q5.** `show ap tag summary` shows Misconfigured: Yes for several APs. What does this indicate?

**A.** The APs are running an older software version than the controller

**B.** The APs have lost their CAPWAP tunnel and are in standalone mode

**C.** The APs are joined to the wrong RF group

**D.** A tag on those APs references a profile that does not exist or cannot be applied, so default tags are in effect

**Correct answer: D.** The misconfigured flag means the tag binding is invalid — a missing flex profile, for example. The controller falls back to the default tags, which typically means local mode and central switching, so branch traffic starts crossing the WAN unnoticed.

## 1.3 FlexConnect Groups and Roaming

A single FlexConnect AP is easy. A branch with twelve APs, a warehouse scanner that walks the length of the building, and a WAN link with 120 ms of latency is where the design gets interesting. Everything in this sub-section exists for one reason: to stop a roam from having to cross the WAN.

### Why a roam is expensive

When a client first joins a WPA2-Enterprise or WPA3-Enterprise WLAN it runs a full **802.1X** exchange: the supplicant on the laptop talks EAP to the authenticator (the AP or controller), which relays it as RADIUS to the authentication server. Depending on the EAP method that is anywhere from four to a dozen round trips, each one crossing the WAN. The result is a shared secret called the **PMK** (Pairwise Master Key), from which the AP and client derive the keys that actually encrypt frames.

If every roam repeated that exchange, a voice call would drop every time the user turned a corner. A roam has a budget of roughly **150 ms** before voice quality suffers audibly, and a full 802.1X exchange over a WAN link can easily take ten times that. Fast, secure roaming exists to reuse the PMK instead of re-deriving it.

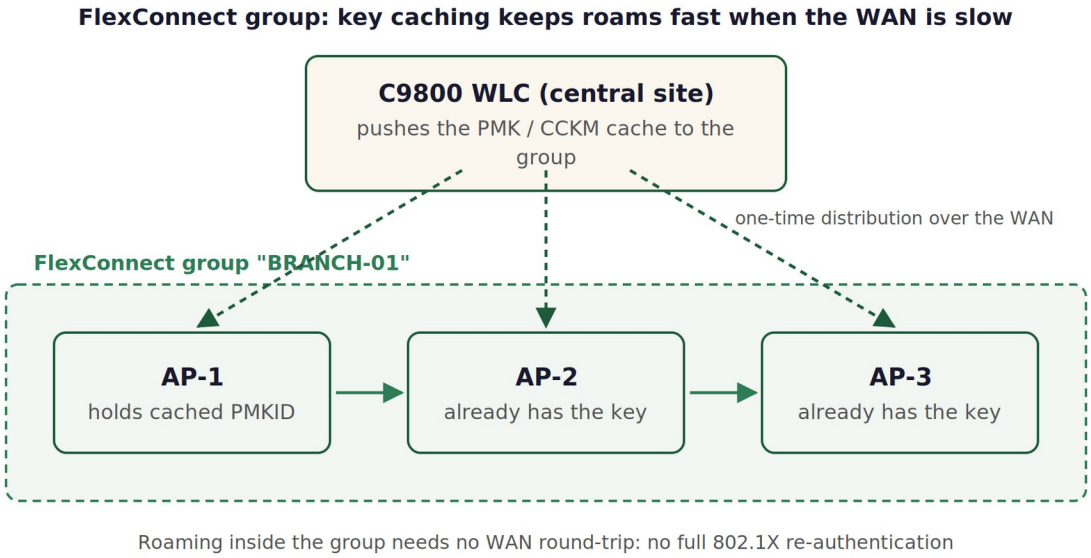


*Figure 1.4 — Key material is distributed once to every AP in the group, so a roam inside the branch needs no WAN round trip.*

### What a FlexConnect group actually is

On AireOS, a **FlexConnect group** is an explicit object: you create it, add APs to it, and configure group-wide settings. On the Catalyst 9800 the same job is done by the **site tag** — every AP wearing the same site tag is, in effect, in the same FlexConnect group, and the flex profile referenced by that

site tag holds the group-wide settings. If the exam gives you AireOS wording, translate it: *FlexConnect group* = *site tag + flex profile*.

| Function | AireOS object | Catalyst 9800 object |
|---|---|---|
| Group membership | FlexConnect group | Site tag |
| Group-wide settings | FlexConnect group tabs | Flex profile |
| Key caching domain | FlexConnect group | Site tag |
| Local RADIUS / local EAP | FlexConnect group > Local Auth | Flex profile local-auth |
| WLAN–VLAN mapping | AP or FlexConnect group | Flex profile + policy profile |
| Efficient image upgrade | FlexConnect group > Image Upgrade | Flex profile predownload |

> ✅ **Exam Tip — The group is the roaming domain**
> Fast roaming without a WAN round trip only works **within** a FlexConnect group (site tag). A client roaming from an AP in site tag ST-BRANCH01 to an AP in ST-BRANCH02 performs a **full authentication**, even if the two APs are ten metres apart. Splitting one physical site across two site tags is a classic self-inflicted roaming problem.

## The three fast-roaming mechanisms

Three mechanisms can shorten a roam, and they are frequently confused. Learn them by what they standardise and who supports them.

| Mechanism | Standard | How it saves time |
|---|---|---|
| CCKM | Cisco proprietary | AP holds a cached key; used by Cisco voice handsets |
| OKC / PMK caching | De-facto, not in 802.11 | The PMK is shared with neighbouring APs in advance |
| 802.11r Fast Transition | IEEE 802.11r | Key hierarchy and over-the-air/over-the-DS handshake |

**802.11r** is the standards-based option and the one to design with today. It introduces a key hierarchy in which the controller holds a top-level key and each AP derives a per-AP key, so the client can authenticate to the new AP with a four-message exchange and no RADIUS traffic at all. The catch is legacy clients: some older supplicants refuse to associate to an SSID that advertises FT. **Adaptive 802.11r** solves this by advertising FT only to clients that understand it.

*Enabling 802.11r Fast Transition on a WLAN (Catalyst 9800)*

```
WLC(config)# wlan WLAN-CORP 5 CORP-BR
WLC(config-wlan)#  shutdown
WLC(config-wlan)#  security ft                          ! enable Fast Transition
WLC(config-wlan)#  security ft over-the-ds               ! optional: FT over the
distribution system
```

```
WLC(config-wlan)#  security wpa akm ft dot1x            ! advertise the FT-802.1X
AKM
WLC(config-wlan)#  security wpa akm dot1x               ! keep plain 802.1X for
legacy clients
WLC(config-wlan)#  security pmf optional
WLC(config-wlan)#  no shutdown
WLC(config-wlan)#  exit

! Adaptive FT - advertise FT only to clients that support it
WLC(config)# wlan WLAN-CORP 5 CORP-BR
WLC(config-wlan)#  security ft adaptive
```

⚠️ **Common Pitfall — Over-the-air or over-the-DS — pick deliberately**

**Over-the-air FT** has the client talk directly to the target AP before it roams. **Over-the-DS** has the client send the request through its current AP, which forwards it over the wired network. Over-the-DS is the better choice on congested channels but is poorly supported by some mobile operating systems; Apple devices in particular prefer over-the-air. Turning on over-the-DS "because it sounds more efficient" is a common cause of mysterious roaming failures on iPhones.

## Voice, roaming and the branch

Voice clients are where roaming design earns its keep. A handset roams far more aggressively than a laptop, and it does so while a call is in progress. In a FlexConnect branch three things must line up: all APs the handset can reach must share one site tag, the WLAN must offer a fast-roaming AKM the handset supports, and the user VLAN must exist on every AP's trunk so the client keeps its IP address after the roam.

🌍 **From the Field — The roam that broke the warehouse**

A distribution centre reported that barcode scanners lost their session halfway down each aisle. The APs were fine and the RF was fine. The cause was that the site had been built in two phases, and the second phase of APs had been given a new site tag because "the flex profile needed a new VLAN." Every scanner crossing the invisible boundary between phase 1 and phase 2 performed a full 802.1X authentication over a 90 ms WAN link. Merging the site tags and adding the VLAN to the original flex profile fixed it in one change window.

## Verifying roaming behaviour

*Confirming that fast roaming is actually being used*

```
WLC# show wireless client mac-address b826.d4a1.7e02 detail | include Roam|Policy|
AKM|Site
Client State                    : Associated
Policy Profile                  : PP-BRANCH-USERS
AP Name                         : AP-BR1-04
```

```
Site Tag                         : ST-BRANCH01
Wireless LAN Name                : CORP-BR
AKM                              : FT-802.1X
Roaming Type                     : Fast Roam - 11r
Last Roam Time                   : 08/24/2026 09:41:22

WLC# show wireless client mac-address b826.d4a1.7e02 mobility history
Time                  AP Name        Roam Type        Duration(ms)
--------------------  -------------  ---------------  -------------
09:41:22              AP-BR1-04      11r over-the-air  38
09:33:07              AP-BR1-02      11r over-the-air  41
09:28:55              AP-BR1-01      Full auth         612
```

✅ **Exam Tip — Read the roam duration, not the client's complaint**

A roam of 30–50 ms is healthy. A roam that consistently shows several hundred milliseconds and a type of *Full auth* means fast roaming is not happening — either the client does not support the AKM, the target AP is in a different site tag, or the WLAN is not advertising FT.

**Summary**

Fast roaming exists to avoid repeating the full 802.1X exchange every time a client moves, which on a WAN-attached branch is the difference between a 40 ms roam and a dropped call. On the Catalyst 9800 the roaming domain is the site tag — the equivalent of an AireOS FlexConnect group — and key material is distributed once to all of its APs. CCKM is the Cisco-proprietary option used by older voice handsets, OKC pre-distributes the PMK to neighbouring APs, and 802.11r Fast Transition is the standards-based mechanism you should design with, using adaptive FT when legacy clients are present. Roams between site tags are always full authentications.

**Key Takeaways**

- A **FlexConnect group** on AireOS equals a **site tag plus flex profile** on the 9800.
- Fast roaming works **inside** a group; crossing site tags forces a **full 802.1X** authentication.
- **CCKM** is proprietary, **OKC** pre-shares the PMK, **802.11r** is the IEEE standard — know which is which.
- **Adaptive 802.11r** advertises FT only to capable clients, protecting legacy supplicants.
- **Over-the-air vs over-the-DS** FT is a compatibility decision, not a performance one.
- A healthy roam is **tens of milliseconds**; repeated *Full auth* roams point at a design fault.

## Knowledge Check — 1.3

**Q1.** On a Catalyst 9800, which object defines the FlexConnect roaming domain in which key caching applies?

**A.** The site tag
**B.** The policy tag
**C.** The RF tag

**D.** The AP join profile

**Correct answer: A.** The site tag groups APs into what AireOS called a FlexConnect group, and the flex profile it references carries the group-wide settings. Key caching applies within that group; a roam to an AP wearing a different site tag is a full authentication.

**Q2.** Voice handsets at a branch report audible gaps when users walk between two halves of the same warehouse. Roams inside each half are fast. What is the most likely cause?

**A.** The handsets do not support WPA3
**B.** The APs in one half are running an older RF profile
**C.** The two halves of the warehouse use different site tags
**D.** Central DHCP is enabled on the policy profile

**Correct answer: C.** Fast roaming is confined to a site tag. If the two halves were built with separate site tags, every crossing triggers a full 802.1X exchange over the WAN, which is long enough to be audible on a call.

**Q3.** Which fast-roaming mechanism is defined by an IEEE standard rather than by Cisco?

**A.** CCKM
**B.** 802.11r Fast Transition
**C.** OKC
**D.** PMK caching by AP name

**Correct answer: B.** 802.11r is the IEEE standard that defines the FT key hierarchy and handshake. CCKM is Cisco proprietary and OKC is a widely implemented but non-standardised optimisation.

**Q4.** Why would an engineer configure adaptive 802.11r instead of plain 802.11r?

**A.** To allow 802.11r to work without a RADIUS server
**B.** To let clients roam between different site tags without re-authenticating
**C.** To reduce the number of spatial streams needed for a roam
**D.** To advertise Fast Transition only to clients that support it, so legacy clients can still associate

**Correct answer: D.** Some legacy supplicants refuse to associate to an SSID advertising FT. Adaptive FT keeps the SSID usable for those clients while still offering fast transition to modern ones.

**Q5.** A client's mobility history shows repeated roams of type 'Full auth' lasting over 500 ms. Which check is LEAST useful?

**A.** Confirming the target APs share the same site tag
**B.** Confirming the WLAN advertises an AKM the client supports
**C.** Verifying the RF profile's data rates on the 2.4 GHz radio
**D.** Confirming that fast transition is enabled on the WLAN

**Correct answer: C.** Data rates influence throughput and cell size but do not decide whether a roam reuses cached key material. The roaming domain, the advertised AKM, and whether FT is enabled are the three things that turn a full authentication into a fast roam.

# 1.4 Split Tunneling and Fault Tolerance

So far a WLAN has been either centrally switched or locally switched. Split tunneling breaks that binary: it lets a **single SSID** send some traffic down the CAPWAP tunnel and bridge the rest locally, based on an access control list. Fault tolerance, the second half of this sub-section, is about what the branch can still do for itself when the tunnel is gone.

## How split tunneling decides

Split tunneling is most commonly used with OfficeExtend APs, where a teleworker needs to reach both the corporate data centre and the printer in the next room. You define an IP ACL and attach it to the policy profile as a **split MAC ACL**. The AP evaluates every client packet against it.

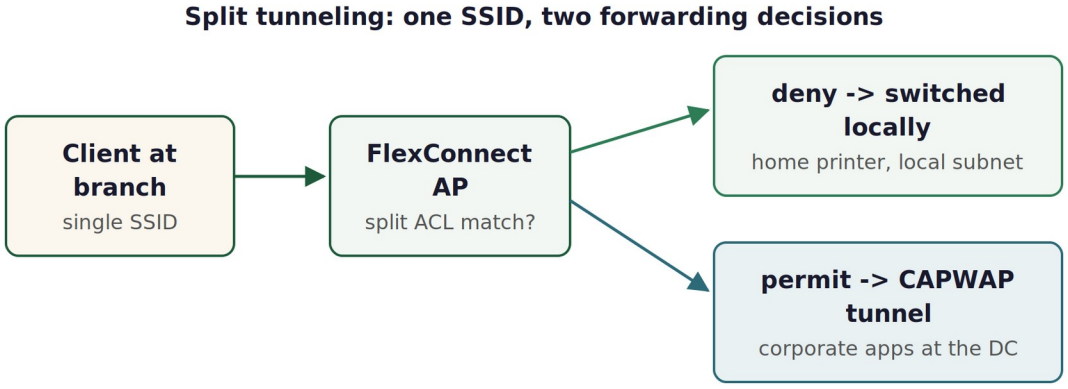


*Figure 1.5 — One SSID, two forwarding decisions. In a split ACL the denied traffic is what stays local.*

> ⚠️ **Common Pitfall — The ACL logic is inverted from what you expect**
>
> In a split-tunnel ACL, a **deny** entry means "do not tunnel this — switch it locally," and a **permit** entry means "send this through the CAPWAP tunnel to the controller." Engineers who read it as a normal firewall ACL configure it backwards and end up tunnelling the home network while leaking corporate traffic locally. Write the local subnets as `deny`, then finish with `permit ip any any`.

*Split tunneling on a Catalyst 9800 — the ACL keeps the home subnet local*

```
WLC(config)# ip access-list extended SPLIT-HOME-ACL
WLC(config-ext-nacl)#  10 deny   ip any 192.168.1.0 0.0.0.255      ! home LAN -
switch locally
WLC(config-ext-nacl)#  20 permit ip any any                        ! everything
else - tunnel it
WLC(config-ext-nacl)#  exit
```

```
WLC(config)# wireless profile flex FLEX-TELEWORKER
WLC(config-wireless-flex-profile)#  acl-policy SPLIT-HOME-ACL
WLC(config-wireless-flex-profile)#  office-extend
WLC(config-wireless-flex-profile)#  exit

WLC(config)# wireless profile policy PP-TELEWORKER
WLC(config-wireless-policy)#  no central association
WLC(config-wireless-policy)#  aaa-override
WLC(config-wireless-policy)#  flex split-mac-acl SPLIT-HOME-ACL
WLC(config-wireless-policy)#  flex vlan-central-switching
WLC(config-wireless-policy)#  ipv4 dhcp required
WLC(config-wireless-policy)#  vlan default
WLC(config-wireless-policy)#  no shutdown
WLC(config-wireless-policy)#  exit
```

*The AireOS equivalent, applied per AP and WLAN*

```
(WLC) > config flexconnect acl create SPLIT-HOME-ACL
(WLC) > config flexconnect acl rule add SPLIT-HOME-ACL 1
(WLC) > config flexconnect acl apply SPLIT-HOME-ACL
(WLC) > config ap local-split enable 5 acl SPLIT-HOME-ACL AP-OEAP-01
```

💡 **Did you know? — Split tunneling and central DHCP are related**

Locally split traffic leaves the AP on the local subnet, so the client needs an address that is routable there — which is why OfficeExtend split-tunnel designs usually keep DHCP and the client's IP address central and rely on the AP to translate. When you see `flex vlan-central-switching` together with a split MAC ACL, that combination is what makes the two worlds coexist on one SSID.

## Fault tolerance: keeping the branch alive

Fault tolerance is the set of behaviours that keep a FlexConnect site usable when the controller is unreachable. There are four layers, and a good branch design uses all of them.

### 1. Session persistence

Already-authenticated clients on locally switched WLANs keep working when the AP goes standalone — their traffic never needed the controller. This is automatic and requires no configuration, but it is worth stating explicitly because exam questions test it directly.

### 2. Local authentication on the AP

For **new** clients to join while the WAN is down, the AP itself must be able to authenticate them. The flex profile can point the AP at a locally reachable RADIUS server (a branch server, or a Cisco ISE node at the site) or turn the AP itself into a small authentication server using **local EAP**, typically EAP-FAST.

*Local authentication in the flex profile*

```
! An EAP profile describing which methods the AP may terminate
WLC(config)# eap profile EAP-FLEX-LOCAL
WLC(config-eap-profile)#  method fast
WLC(config-eap-profile)#  exit

! A RADIUS server the branch AP can reach without the WAN
WLC(config)# radius server BRANCH-ISE
WLC(config-radius-server)#  address ipv4 10.10.11.50 auth-port 1812 acct-port 1813
WLC(config-radius-server)#  key 0 <shared-secret>
WLC(config-radius-server)#  exit

WLC(config)# wireless profile flex FLEX-BRANCH01
WLC(config-wireless-flex-profile)#  local-auth ap eap-fast EAP-FLEX-LOCAL
WLC(config-wireless-flex-profile)#  local-accounting-radius
WLC(config-wireless-flex-profile)#  exit

! And on the WLAN's policy profile, tell it not to depend on the controller
WLC(config)# wireless profile policy PP-BRANCH-USERS
WLC(config-wireless-policy)#  no central authentication
WLC(config-wireless-policy)#  no central switching
WLC(config-wireless-policy)#  no shutdown
```

### 3. Fallback controllers

Before an AP declares itself standalone it will try to join another controller. The AP join profile carries a primary, secondary and tertiary controller; a branch design should always populate at least two, pointing at controllers in different data centres.

*Giving branch APs somewhere else to go*

```
WLC(config)# ap name AP-BR1-01 controller primary WLC-DC1 10.1.10.10
WLC(config)# ap name AP-BR1-01 controller secondary WLC-DC2 10.2.10.10
WLC(config)# ap name AP-BR1-01 controller tertiary WLC-DR 10.3.10.10

WLC# show ap name AP-BR1-01 config general | include Controller
Primary Cisco Controller Name        : WLC-DC1
Primary Cisco Controller IP Address  : 10.1.10.10
Secondary Cisco Controller Name      : WLC-DC2
Secondary Cisco Controller IP Address: 10.2.10.10
```

### 4. Ethernet fallback

A subtler failure is an AP whose wired uplink dies while its radios stay up: clients associate to an AP that leads nowhere. **FlexConnect Ethernet fallback** shuts the radios when the Ethernet link goes down and brings them back when it recovers, with a configurable delay to stop the radios flapping on an unstable port.

*Shutting the radio when the uplink fails*

```
WLC(config)# wireless profile flex FLEX-BRANCH01
WLC(config-wireless-flex-profile)#  fallback-radio-shut
WLC(config-wireless-flex-profile)#  exit

WLC# show wireless profile flex detailed FLEX-BRANCH01 | include Fallback
Fallback Radio Shut                  : ENABLED
```

🌍 **From the Field — Design for the outage you will actually have**

In most branch networks the WAN does not fail cleanly; it degrades. Latency climbs, packets are lost, and the AP oscillates between connected and standalone. Two settings blunt this: generous CAPWAP retransmit timers in the AP join profile, and local authentication so that a brief flap does not lock out every user trying to join. Engineers who tune only for the total-outage case are surprised by the brownout case.

**Summary**

Split tunneling lets one SSID forward some traffic locally and tunnel the rest, driven by an ACL whose deny entries mark the traffic to keep local. On the Catalyst 9800 it is configured as an ACL policy in the flex profile plus a split MAC ACL on the policy profile, and it is most often paired with OfficeExtend. Fault tolerance is layered: already-associated clients survive automatically on locally switched WLANs, local authentication lets new clients join while the WAN is down, primary and secondary controllers give the AP somewhere else to join, and Ethernet fallback shuts the radios when the AP's own uplink fails.

**Key Takeaways**

- In a split-tunnel ACL, **deny = switch locally**, **permit = send through the tunnel**.
- 9800 configuration: `acl-policy` in the flex profile, **`flex split-mac-acl`** on the policy profile.
- **Existing clients** on locally switched WLANs survive a WAN outage with no configuration at all.
- **Local authentication** (local EAP or a branch RADIUS server) is what lets *new* clients join offline.
- Always configure **primary and secondary controllers** for branch APs.
- **`fallback-radio-shut`** prevents clients associating to an AP whose wired uplink is dead.

## Knowledge Check — 1.4

**Q1.** In a FlexConnect split-tunnel ACL, what does a `deny` entry cause the AP to do with matching traffic?

**A.** Drop it silently
**B.** Send it through the CAPWAP tunnel to the controller
**C.** Forward it only after the client re-authenticates
**D.** Switch it locally instead of sending it through the CAPWAP tunnel

**Correct answer: D.** Split-tunnel ACL logic is inverted compared with a firewall ACL: deny marks traffic that must not be tunnelled, so the AP bridges it onto the local network. Permitted traffic is what rides the CAPWAP tunnel.

**Q2.** Which Catalyst 9800 policy-profile command attaches a split-tunnel ACL to a WLAN?

- **A.** acl-policy <acl-name>
- **B.** flex split-mac-acl <acl-name>
- **C.** ipv4 acl <acl-name>
- **D.** flex vlan-central-switching

**Correct answer: B.** The policy profile uses `flex split-mac-acl` to apply the split ACL to clients on that WLAN. `acl-policy` is the flex-profile command that makes the ACL available to the AP in the first place.

**Q3.** A branch uses local switching with central authentication and no local authentication. The WAN fails for two hours. What is true during the outage?

- **A.** All clients are disconnected within 30 seconds
- **B.** New clients can join because the AP caches credentials for 24 hours
- **C.** Clients already associated keep working; no new client can authenticate
- **D.** The AP converts the WLAN to open authentication automatically

**Correct answer: C.** Local switching keeps existing sessions alive because their data path does not involve the controller. Without local authentication there is nothing at the branch able to complete an 802.1X exchange, so new joins fail for the duration of the outage.

**Q4.** What problem does FlexConnect Ethernet fallback (`fallback-radio-shut`) solve?

- **A.** Clients associating to an AP whose wired uplink has failed and therefore has no path to the network
- **B.** APs joining the wrong controller after a WAN outage
- **C.** Excessive multicast traffic on the branch trunk
- **D.** Clients failing to roam between site tags

**Correct answer: A.** If the AP's Ethernet port goes down but its radios stay up, clients happily associate to an AP that leads nowhere. Ethernet fallback shuts the radios until the uplink recovers, with a delay timer to avoid flapping on an unstable port.

**Q5.** Which configuration is required for a new client to complete 802.1X at a branch while the controller is unreachable?

- **A.** Central DHCP enabled on the policy profile
- **B.** Local authentication on the AP, using local EAP or a locally reachable RADIUS server
- **C.** A secondary controller configured in the AP join profile
- **D.** 802.11r Fast Transition enabled on the WLAN

**Correct answer: B.** A secondary controller helps only if it is reachable, and fast roaming does not help a brand-new client. Only local authentication puts an authenticator at the branch itself, whether that is the AP running local EAP or a RADIUS server on the local subnet.

# 1.5 VLAN-Based Central Switching and Flex ACLs

Two features share this sub-section because they answer the same question from different angles: *what happens to a client's traffic once the AP has decided to switch it locally?* VLAN-based central switching decides **which** traffic is bridged locally and which is tunnelled, based on the VLAN a client is assigned. Flex ACLs then filter what that locally switched client may reach.

## The VLAN a client lands in

On a locally switched WLAN, several sources can decide a client's VLAN, and they are evaluated in a fixed order. Knowing that order is the difference between confidently answering a scenario question and guessing.

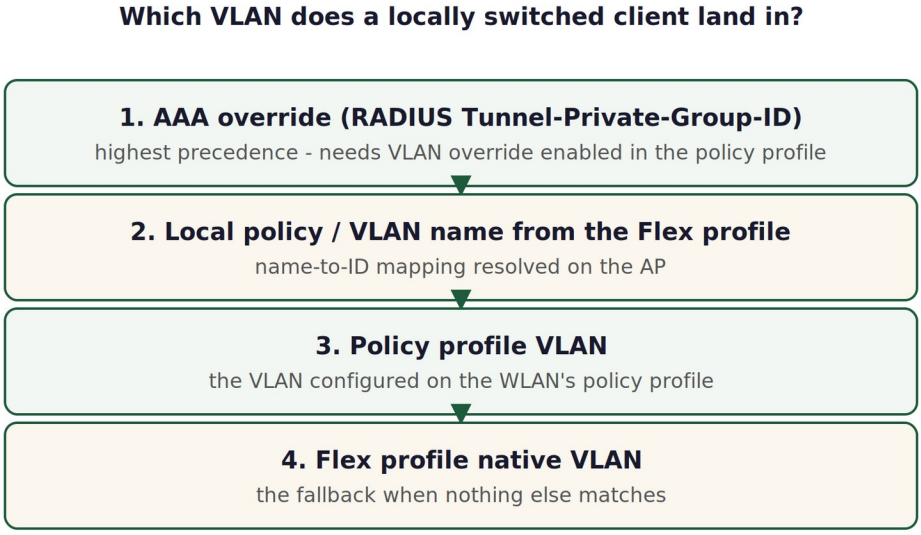


*Figure 1.6 — VLAN assignment precedence on a locally switched WLAN.*

The **AAA override** at the top is the RADIUS server — typically Cisco ISE — returning a VLAN in its Access-Accept. It arrives as the classic trio of RADIUS attributes: Tunnel-Type (13, VLAN), Tunnel-Medium-Type (6, 802), and Tunnel-Private-Group-ID (the VLAN name or ID). For it to be honoured, the policy profile must have `aaa-override` enabled.

*Accepting a VLAN from ISE on a locally switched WLAN*

```
WLC(config)# wireless profile policy PP-BRANCH-USERS
WLC(config-wireless-policy)#  aaa-override
WLC(config-wireless-policy)#  aaa-override vlan fallback      ! use the profile
VLAN if the override is invalid
WLC(config-wireless-policy)#  no central switching
WLC(config-wireless-policy)#  vlan USERS
WLC(config-wireless-policy)#  no shutdown
```

```
WLC# show wireless client mac-address b826.d4a1.7e02 detail | include VLAN|Override
VLAN                            : 30
Override VLAN                   : 30
AAA Override                    : Enabled
```

⚠️ **Common Pitfall — An overridden VLAN that the AP does not know**

If ISE returns VLAN 30 but the flex profile never mapped a name to VLAN 30, the AP has no sub-interface for it and the client is stranded — associated, but with no path off the AP. Either add every VLAN ISE can return to the flex profile, or configure `aaa-override vlan fallback` so an unknown override falls back to the policy-profile VLAN instead of black-holing the client.

## VLAN-based central switching

**VLAN-based central switching** is the feature that lets a single locally switched WLAN send *some* clients' traffic centrally, decided by the VLAN the RADIUS server returned. If the returned VLAN exists in the flex profile, the client is switched locally into it. If it does not exist locally, the client's traffic is tunnelled to the controller and placed on that VLAN centrally.

*Enabling VLAN-based central switching on the policy profile*

```
WLC(config)# wireless profile policy PP-BRANCH-MIXED
WLC(config-wireless-policy)#  no central switching             ! locally switched
by default
WLC(config-wireless-policy)#  aaa-override
WLC(config-wireless-policy)#  flex vlan-central-switching      ! unknown AAA VLANs
go central
WLC(config-wireless-policy)#  vlan USERS
WLC(config-wireless-policy)#  no shutdown

WLC# show wireless profile policy detailed PP-BRANCH-MIXED | include central
Central Switching                       : DISABLED
Central Authentication                  : ENABLED
Flex Central Switching                  : ENABLED
```

🌍 **From the Field — One SSID for staff and contractors**

A retailer used a single corporate SSID at every store. Staff were placed by ISE into the store's local VLAN and broke out to the Internet locally, keeping the WAN free. Contractors were placed into a VLAN that existed only in the data centre, so their traffic was tunnelled back and inspected by the central firewall. One WLAN, one policy profile, two very different data paths — decided entirely by what ISE returned.

✅ **Exam Tip — Match the feature to the symptom**

If a question describes clients on a locally switched WLAN whose traffic unexpectedly appears at the controller, look for **VLAN-based central switching** plus an AAA-returned VLAN that is missing from the flex profile. That is the designed behaviour, not a fault.

## Flex ACLs: filtering locally switched traffic

With central switching, an ACL applied on the controller sees every client packet. With local switching the controller sees nothing, so filtering must happen on the AP. A **FlexConnect ACL** (Flex ACL) is an IP ACL that the controller pushes to the AP, where it is applied to a VLAN or to a client session.

There are two places a Flex ACL can be attached, and the exam expects you to know the difference:

- **VLAN ACL** — attached to a VLAN inside the flex profile. Every client in that VLAN on that AP is filtered, in both directions. Use it for broad segmentation such as guest VLANs.
- **Client (policy) ACL** — returned by ISE per user, or set on the policy profile. Applies to that client's session only. Use it for role-based access such as contractors or quarantined devices.

*A guest Flex ACL applied to a VLAN in the flex profile*

```
WLC(config)# ip access-list extended FLEX-GUEST-ACL
WLC(config-ext-nacl)#  10 permit udp any any eq 53          ! DNS
WLC(config-ext-nacl)#  20 permit udp any any eq 67          ! DHCP
WLC(config-ext-nacl)#  30 deny   ip any 10.0.0.0 0.255.255.255    ! no internal
networks
WLC(config-ext-nacl)#  40 deny   ip any 192.168.0.0 0.0.255.255
WLC(config-ext-nacl)#  50 permit ip any any                 ! Internet is fine
WLC(config-ext-nacl)#  exit

WLC(config)# wireless profile flex FLEX-BRANCH01
WLC(config-wireless-flex-profile)#  acl-policy FLEX-GUEST-ACL
WLC(config-wireless-flex-profile)#  vlan-name GUEST
WLC(config-wireless-flex-vlan)#      vlan-id 40
WLC(config-wireless-flex-vlan)#      acl-name FLEX-GUEST-ACL
WLC(config-wireless-flex-vlan)#      exit
```

*Verifying that the AP actually received and installed the ACL*

```
WLC# show wireless profile flex detailed FLEX-BRANCH01 | begin VLAN
VLAN Name    VLAN Id   ACL Name
------------ --------- --------------------
USERS        20        -
VOICE        30        -
GUEST        40        FLEX-GUEST-ACL

! From the AP itself (console or SSH)
AP-BR1-01# show ip access-lists
Extended IP access list FLEX-GUEST-ACL
    10 permit udp any any eq domain
    20 permit udp any any eq bootps
    30 deny ip any 10.0.0.0 0.255.255.255
    40 deny ip any 192.168.0.0 0.0.255.255
```

```
    50 permit ip any any

AP-BR1-01# show capwap client rcb | include Name|Mode
   Name              : AP-BR1-01
   Mode              : FlexConnect
```

⚠️ **Common Pitfall — An ACL policy that was never allowed on the AP**

On the 9800 an ACL must be listed under `acl-policy` in the flex profile before the AP will download it. Mapping an ACL name to a VLAN without that `acl-policy` line produces a configuration that looks complete on the controller but never installs on the AP — and the traffic you meant to block flows freely. Always confirm with `show ip access-lists` on the AP itself.

💡 **Did you know? — Flex ACLs are not the same as central ACLs**

A Flex ACL is enforced by the access point's own dataplane, which is why it supports a smaller feature set than an ACL on the controller: no logging in some releases, limited entry counts, and no support for object groups. Keep them short and purposeful. If you need rich policy, consider returning a downloadable ACL from ISE or using SGT-based policy, covered in Section 6.

**Summary**

On a locally switched WLAN the client's VLAN comes from, in order, an AAA override, a VLAN name resolved through the flex profile, the policy profile's VLAN, and finally the flex profile's native VLAN. VLAN-based central switching uses that decision to route traffic two different ways on one WLAN: VLANs known to the AP are bridged locally, while VLANs that exist only centrally are tunnelled to the controller. Because the controller is not in the local data path, filtering must be done on the AP with Flex ACLs, attached either to a VLAN in the flex profile or to an individual client session, and the ACL must be listed as an `acl-policy` before the AP will install it.

**Key Takeaways**

- VLAN precedence: **AAA override > flex VLAN name > policy profile VLAN > native VLAN**.
- `aaa-override vlan fallback` stops an **unknown AAA VLAN** from stranding a client.
- **`flex vlan-central-switching`** tunnels clients whose AAA VLAN does not exist at the branch.
- **Flex ACLs are enforced on the AP** — the controller never sees locally switched traffic.
- Attach a Flex ACL to a **VLAN** for segmentation or to a **client session** for role-based access.
- An ACL must appear under **`acl-policy`** in the flex profile or the AP never downloads it.

## Knowledge Check — 1.5

**Q1.** A client on a locally switched WLAN is assigned VLAN 55 by ISE, but VLAN 55 is not defined in the flex profile and VLAN-based central switching is not enabled. What is the result?

**A.** The client is placed in the native VLAN automatically

**B.** The client's traffic is tunnelled to the controller and placed in VLAN 55 centrally

**C.** The client associates but has no data path, because the AP has no sub-interface for VLAN 55

**D.** The client is denied association by the AP

# Continue Reading

The sample breaks off part-way through Section 1, four sub-sections into a book of sixty-three. The section continues with the rest of VLAN-based central switching and Flex ACLs, then efficient AP image upgrade, OfficeExtend access points, and a full troubleshooting sub-section — and seven more domains follow after it.

## The complete guide

| | |
|---|---|
| Pages | 334 |
| Sections | 8, matching the eight blueprint domains |
| Sub-sections | 63, each with its own knowledge check |
| Questions | 260, with full explanations |
| Diagrams | 57, drawn for this book |
| Field cases | 10 worked investigations crossing domain boundaries |
| Also included | Blueprint mapping, glossary, hardening checklist |

## Where to get it

**leanpub.com/wlsi**

Leanpub delivers PDF and EPUB, with free updates for the life of the edition — so a revised blueprint or an updated configuration reaches you at no additional cost.

## Other guides in this series

Guides written to the same structure exist for other exams — enterprise wireless, security, automation, data centre and cybersecurity operations — at **leanpub.com/u/prodigitalj**.

**Thank you for reading, and good luck with the exam.**