

요리 방법: Catalyst 9800의 최소 부트스트랩 CLI 구성

목차

[소개](#)

[사전 요구 사항](#)

[재료](#)

[구성](#)

[네트워크 다이어그램](#)

[선택 사항: 컨트롤러를 공장 기본값으로 복원 - 근무일 0](#)

[초기 구성 마법사 우회](#)

[부트스트랩 템플릿 - 기본 디바이스 설정](#)

[초기 디바이스 컨피그레이션 및 대역 외 연결](#)

[선택 사항 - CDP 활성화](#)

[9800-CL - 자체 서명 인증서 생성](#)

[VLAN 생성](#)

[데이터 인터페이스 구성 - 어플라이언스](#)

[무선 관리 인터페이스 구성](#)

[표준 시간대 및 NTP 동기화 구성](#)

[VTY 액세스 및 기타 로컬 서비스](#)

[Radius 컨피그레이션](#)

[선택 사항 - 매일 구성 백업](#)

[무선 구성](#)

[선택 사항 - 모범 사례](#)

[WLAN 생성 - WPA2-PSK](#)

[WLAN 생성 - WPA2-엔터프라이즈](#)

[WLAN 생성 - 로컬 웹 인증을 사용하는 게스트](#)

[WLAN 생성 - 중앙 웹 인증을 사용하는 게스트](#)

[로컬 모드 AP에 대한 정책 생성](#)

[Flexconnect 모드 AP에 대한 정책 생성](#)

[최종 - 액세스 포인트에 태그 적용](#)

[AP MAC 주소 목록을 가져오는 방법](#)

[권장 읽기](#)

소개

이 문서에서는 Catalyst 9800 WLC(Wireless Lan Controller)에 대해 "부트스트랩"(초기 컨피그레이션 수행)할 수 있는 여러 옵션에 대해 설명합니다. 일부 프로세스에는 외부 프로세스(PNP 또는 TFTP 다운로드)가 필요할 수 있으며, 일부는 CLI를 통해 부분적으로 수행한 다음 GUI를 통해 완료할 수도 있습니다.

이 문서에서는 가능한 최단 시간에 원격 관리 및 모범 사례를 비롯한 기본 작업을 위해 9800을 구성할 수 있도록 최소한의 간소화된 작업 집합과 함께 "요리 조리법" 형식에 중점을 둡니다.

제공된 템플릿에 "!" 문자가 앞에 있는 주석이 있습니다. 를 클릭하여 컨피그레이션의 특정 지점을 설명합니다. 또한 사용자가 제공해야 하는 모든 값은 아래 "재료" 테이블에 표시됩니다.

17.3 이상 버전을 대상으로 합니다.

사전 요구 사항

- Catalyst 9800 Controller "즉시 사용 가능" 기본적으로 컨피그레이션 없음
- IOS-XE 컨피그레이션의 기본 이해
- 컨트롤러의 콘솔 포트에 액세스합니다. 어플라이언스의 CON 물리적 포트(9800-40, 9800-80, 9800-L) 또는 9800-CL용 하이퍼바이저 원격 액세스 클라이언트를 통한 수 있습니다.
- 직렬 액세스의 경우, 원하는 터미널 클라이언트 애플리케이션을 선택합니다.

재료

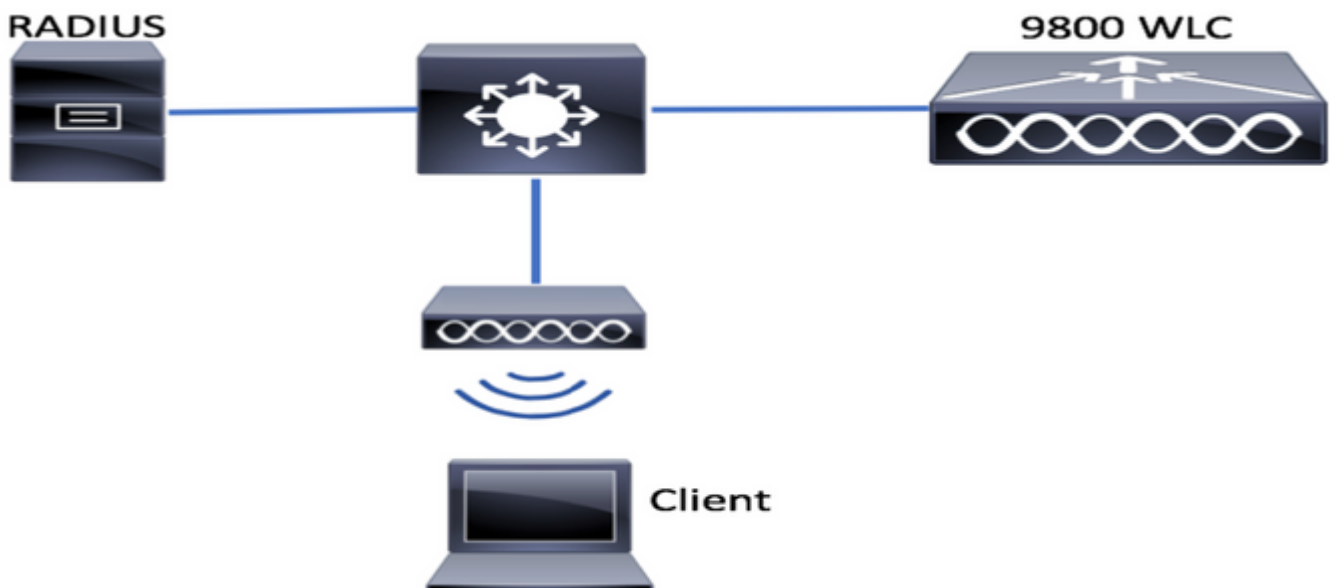
각 대문자 항목은 구성 템플릿을 사용하기 전에 변경해야 하는 설정에 해당합니다.

| 필요한 값 | 템플릿의 이름 | 예 |
|---------------------------|---------------|---------------|
| 대역 외 관리 IP | [OOM_IP] | 192.168.0.25 |
| 대역 외 관리 기본 게이트웨이 | [OOM_GW] | 192.168.0.1 |
| 관리자 사용자 이름 | [관리] | 관리자 |
| 관리자 비밀번호 | [암호] | 아1-7k++a1 |
| AP 관리자 사용자 이름 | [AP_ADMIN] | 관리자 |
| AP CLI 비밀번호 | [AP_PASSWORD] | 알크브90질리 |
| AP 암호 사용 | [AP_SECRET] | kh20-9yjh |
| 컨트롤러 호스트 이름 | [WLC_이름] | 9800-bcn-1 |
| 회사 도메인 이름 | [도메인 이름] | company.com |
| 클라이언트 VLAN ID | [클라이언트_VLAN] | 15 |
| 클라이언트 VLAN 이름 | [VLAN_NAME] | 클라이언트_vlan |
| 무선 관리 인터페이스 VLAN | [WMI_VLAN] | 25 |
| 무선 관리 인터페이스 IP | [WMI_IP] | 192.168.25.10 |
| 무선 관리 인터페이스 마스크 | [WMI_MASK] | 255.255.255.0 |
| 무선 관리 인터페이스 기본 GW | [WMI_GW] | 192.168.25.1 |
| NTP 서버 | [NTP_IP] | 192.168.1.2 |
| RADIUS 서버 IP | [RADIUS_IP] | 192.168.0.98 |
| Radius 키 또는 공유 암호 | [RADIUS_KEY] | 공유 암호 |
| WLAN SSID WPA2 사전 공유 키 이름 | [SSID-PSK] | 개인 |
| WLAN SSID WPA2 802.1x 인증 | [SSID-DOT1x] | 회사 이름 |
| WLAN SSID 게스트 로컬 웹 인증 | [SSID-LWA] | 게스트1 |

구성

네트워크 다이어그램

이 문서는 매우 기본적인 토폴로지를 따릅니다. 이 토폴로지는 Calatyst 9800 컨트롤러가 스위치에 연결되고, 테스트를 위해 동일한 VLAN에 액세스 포인트가 추가되며, 인증을 위해 RADIUS 서버(옵션)가 제공됩니다.



선택 사항: 컨트롤러를 공장 기본값으로 복원 - 근무일 0

컨트롤러가 이미 구성되어 있고 컨피그레이션 없이 Day Zero 시나리오로 다시 이동하려는 경우 다음 선택적 절차를 수행할 수 있습니다.

```

DAO2#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Sep 7 10:09:31.141: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
DAO2#reload

System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

Sep 7 10:10:55.318: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
Chassis 1 reloading, reason - Reload command
  
```

초기 구성 마법사 우회

컨트롤러가 다시 로드를 마치면 CLI 컨피그레이션 마법사가 나타나 기본 초기 컨피그레이션을 수행합니다. 이 문서에서는 이 옵션을 건너뛰고 다음 단계에 제공된 CLI 템플릿을 사용하여 모든 값을

구성합니다.

컨트롤러 부팅이 완료될 때까지 기다립니다.

```
Installation mode is INSTALL
```

```
No startup-config, starting autoinstall/pnp/ztp...
```

```
Autoinstall will terminate if any input is detected on console
```

```
Autoinstall trying DHCPv4 on GigabitEthernet0
```

```
Autoinstall trying DHCPv6 on GigabitEthernet0
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0: Machine Check: 0 Bank 9: ee2000000003110a
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0 ADDR ff007f00 MISC 228aa040101086
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR 0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0: Machine Check: 0 Bank 10: ee2000000003110a
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0 ADDR ff007fc0 MISC 228aa040101086
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR 0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0: Machine Check: 0 Bank 11: ee2000000003110a
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0 ADDR ff007f80 MISC 228aa040101086
```

```
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR 0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
```

```
Autoinstall trying DHCPv4 on GigabitEthernet0,Vlan1
```

```
Autoinstall trying DHCPv6 on GigabitEthernet0,Vlan1
```

```
Acquired IPv4 address 192.168.10.105 on Interface GigabitEthernet0
```

```
Received following DHCPv4 options:
```

```
domain-name : cisco.com
```

```
dns-server-ip : 192.168.0.21
```

```
OK to enter CLI now...
```

```
pnp-discovery can be monitored without entering enable mode
```

```
Entering enable mode will stop pnp-discovery
```

```
Guestshell destroyed successfully
```

"Enter" 키를 누르고 초기 대화 상자에 "no"를 입력하고 "yes"를 눌러 자동 설치 프로세스를 종료합니다.

```
% Please answer 'yes' or 'no'.
```

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Would you like to terminate autoinstall? [yes]: yes
```

Press RETURN to get started!

부트스트랩 템플릿 - 기본 디바이스 설정

다음 구성 템플릿을 사용하여 재료 테이블에 표시된 대로 값을 수정합니다. 이 문서는 검토를 용이하게 하기 위해 서로 다른 섹션에 분할됩니다.

모든 섹션의 경우 항상 Config 모드에서 내용을 붙여넣고, 프롬프트를 표시하려면 "Enter" 키를 누른 다음 enable 및 config 명령을 사용합니다. 예를 들면 다음과 같습니다.

```
WLC>enable
WLC#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
WLC(config)#hostname controller-name
```

초기 디바이스 컨피그레이션 및 대역 외 연결

구성 모드에서 다음 명령을 사용합니다. 로컬 키를 생성한 후 SSH가 활성화되도록 컨피그레이션 저장을 종료합니다.

```
hostname [WLC_NAME]

int gi0
ip add [OOM_IP] 255.255.255.0
exit
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 [OOM_GW]

no ip domain lookup

username [ADMIN] privilege 15 password 0 [PASSWORD]

ip domain name [DOMAIN_NAME]

aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
aaa authorization network default local

line con 0
privilege level 15
login authentication CONSOLE
exit
crypto key generate rsa modulus 2048
ip ssh version 2
end
wr
```

선택 사항 - CDP 활성화

구성 모드에서 다시 입력하고 다음 명령을 사용합니다. 9800-CL의 경우 Te0/0/0 및 Te0/0/1 인터페이스를 Gi1 및 Gi2로 바꿉니다.

```
cdp run
int te0/0/0
```

```
cdp ena
int te0/0/1
cdp ena
```

9800-CL - 자체 서명 인증서 생성

이는 9800-CL 컨트롤러에서만 수행되며 AP CAPWAP 조인에 대해 어플라이언스 모델(9800-80, 9800-40, 9800-L)에는 필요하지 않습니다.

```
wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 [CHANGEPASSWORD]
```

VLAN 생성

구성 모드에서 필요한 만큼 클라이언트 VLAN을 만들고 WMI(Wireless Management Interface)에 해당하는 VLAN을 만듭니다.

대부분의 시나리오에서 기업 VLAN과 게스트 액세스를 위한 클라이언트 VLAN이 각각 2개 이상 있는 것이 일반적입니다. 필요한 경우 수백 개의 서로 다른 VLAN을 포괄할 수 있는 대형 시나리오

WMI VLAN은 대부분의 관리 프로토콜과 토폴로지에 대한 컨트롤러에 액세스하는 지점이며, 액세스 포인트에서 CAPWAP 터널을 생성합니다

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]
```

```
vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

데이터 인터페이스 구성 - 어플라이언스

9800-L, 9800-40, 9800-80의 경우 컨피그레이션 모드에서 다음 명령을 사용하여 데이터 평면 인터페이스에 대한 기본 기능을 설정할 수 있습니다. 이 예에서는 두 포트 모두에서 생성된 채널 그룹이 있는 LACP를 제안합니다.

스위치 측에서 매칭 토폴로지를 구성하는 것이 중요합니다.

이 섹션은 토폴로지와 포트 채널을 사용하는 경우에 따라 제공된 예제에서 실제로 필요한 것으로 변경된 내용이 있을 수 있는 섹션입니다. 신중하게 검토하십시오.

```
!!Interfaces. LACP if standalone or static (channel-group 1 mode on) on if HA before 17.1.
```

```
interface TenGigabitEthernet0/0/0
description You should put here your switch name and port
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no negotiation auto
channel-group 1 mode active
```

```
interface TenGigabitEthernet0/0/1
description You should put here your switch name and port
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no negotiation auto
channel-group 1 mode active
```

```
no shut

int po1
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no shut

!!Configure the same in switch and spanning-tree portfast trunk
port-channel load-balance src-dst-mixed-ip-port
```

무선 관리 인터페이스 구성

구성 모드에서 다음 명령을 사용하여 WMI를 만듭니다. 이는 매우 중요한 단계입니다.

```
int vlan [WMI_VLAN]
ip add [WMI_IP] [WMI_MASK]
no shut

ip route 0.0.0.0 0.0.0.0 [WMI_GW]

!! The interface name will normally be something like Vlan25, depending on your WMI VLAN ID
wireless management interface Vlan[WMI_VLAN]
```

표준 시간대 및 NTP 동기화 구성

NTP는 여러 무선 기능에 매우 중요합니다. 컨피그레이션 모드에서 다음 명령을 사용하여 설정합니다.

```
ntp server [NTP_IP]
!!This is European Central Time, it should be adjusted to your local time zone
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
```

VTY 액세스 및 기타 로컬 서비스

모범 사례를 따르면, GUI 액세스 문제를 방지하기 위해 추가 VTY 라인을 생성하고 기본 서비스를 사용하여 관리 인터페이스에 대한 TCP 세션 처리를 개선할 수 있습니다.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service tcp-keepalives-in
service tcp-keepalives-out
logging buffered 512000

line vty 0 15
transport input ssh

line vty 16 50
transport input ssh
```

Radius 컨피그레이션

이렇게 하면 ISE 서버에 대한 RADIUS 통신을 활성화하는 기본 설정이 생성됩니다.

```
radius server ISE
address ipv4 [RADIUS_IP] auth-port 1645 acct-port 1646
key [RADIUS_KEY]
automate-tester username dummy probe-on
```

```
aaa group server radius ISE_GROUP
server name ISE
```

```
aaa authentication dot1x ISE group ISE_GROUP
```

```
radius-server dead-criteria time 5 tries 3
radius-server deadtime 5
```

선택 사항 - 매일 구성 백업

보안상의 이유로 원격 TFTP 서버에 대한 자동화된 일일 컨피그레이션 백업을 활성화할 수 있습니다.

```
archive
path tftp://TFTP_IP/lab_configurations/9800-config.conf
time-period 1440
```

무선 구성

이 섹션에서는 WPA2와 Preshare Key, WPA2 및 802.1x/radius, Central Webauth 및 Local Webauth의 가장 일반적인 조합을 다루는 다양한 WLAN 유형의 예를 살펴봅니다. 구축에 이러한 모든 기능이 포함될 것으로 예상되지 않으므로 필요에 따라 제거하고 수정해야 합니다.

컨트롤러가 컨피그레이션을 "완료"로 표시하려면 country 명령을 설정해야 합니다. 배포 위치와 일치하도록 국가 목록을 수정해야 합니다.

```
ap dot11 24ghz cleanair
ap dot11 5ghz cleanair
no ap dot11 5ghz SI
```

```
!!Important: replace country list with to match your location
!!These commands are supported from 17.3 and higher
wireless country ES
wireless country US
```

선택 사항 - 모범 사례

이를 통해 네트워크가 다음과 같은 기본적인 모범 사례를 충족할 수 있습니다.

- 액세스 포인트는 문제 해결 환경을 개선하기 위해 SSH를 활성화하고, 기본 자격 증명이 아닌 자격 증명 및 syslog를 사용합니다. 이는 기본 AP 가입 프로파일을 사용하는 것으로, 새 항목을 추가할 경우 유사한 변경 사항을 적용해야 합니다
- 디바이스 분류 활성화, 네트워크에 연결된 클라이언트 유형 추적

```
ap profile default-ap-profile
mgmtuser username [AP_ADMIN] password 0 [AP_PASSWORD] secret 0 [AP_SECRET]
ssh
syslog host [AP_SYSLOG]
```

```
device classifier
```


WLAN 생성 - WPA2-PSK

변수를 필수 설정으로 바꿉니다. 이 유형의 WLAN은 대부분 개인 네트워크, 단순한 시나리오 또는 802.1x 기능 없이 IOT 장치를 지원하는 데 사용됩니다.

대부분의 엔터프라이즈 시나리오에 대해 선택 사항입니다.

```
wlan wlan_psk 1 [SSID-PSK]
security wpa psk set-key ascii 0 [WLANPSK]
no security wpa akm dot1x
security wpa akm psk
no shutdown
```

WLAN 생성 - WPA2-엔터프라이즈

RADIUS 인증을 사용하는 WPA2 WLAN의 가장 일반적인 시나리오입니다. 엔터프라이즈 환경에서 사용

```
wlan wlan_dot1x 2 [SSID-DOT1X]
security dot1x authentication-list ISE
no shutdown
```

WLAN 생성 - 로컬 웹 인증을 사용하는 게스트

ISE 게스트 지원 없이 더 간단한 게스트 액세스에 사용

버전에 따라 첫 번째 매개변수 맵을 만들 때 경고를 받을 수 있습니다. 계속하려면 예(yes)로 응답하십시오.

```
parameter-map type webauth global
yes ! this may not be needed depending on the version
virtual-ip ipv4 192.0.2.1
virtual-ip ipv6 1001::1
```

```
aaa authentication login WEBAUTH local
aaa authorization network default local
```

```
wlan wlan_webauth 3 [SSID-WEBAUTH]
peer-blocking drop
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no security ft
no security wpa wpa2
security web-auth
security web-auth authentication-list WEBAUTH
security web-auth parameter-map global
no shu
```

WLAN 생성 - 중앙 웹 인증을 사용하는 게스트

ISE 게스트 지원에 사용

```
aaa authentication network default local
aaa authorization network MACFILTER group ISE_GROUP
```

```
aaa accounting identity ISE start-stop group ISE_GROUP
```

```
aaa server radius dynamic-author  
client [RADIUS_IP] server-key [RADIUS_KEY]
```

```
ip access-list extended REDIRECT  
10 deny icmp any any  
20 deny udp any any eq bootps  
30 deny udp any any eq bootpc  
40 deny udp any any eq domain  
50 deny ip any host [RADIUS_IP]  
55 deny ip host [RADIUS_IP] any  
60 permit tcp any any eq www
```

```
wlan wlan_cwa 5 [SSID-CWA]  
mac-filtering MACFILTER  
no security wpa  
no security wpa wpa2 ciphers aes  
no security wpa akm dot1x  
no security ft  
no security wpa wpa2  
no shutdown
```

!! we will create two policy profiles, to be used later depending if the APs are local or flex mode

```
wireless profile policy local_vlanclients_cwa  
aaa-override  
accounting-list ISE  
ipv4 dhcp required  
nac  
vlan [CLIENT_VLAN]  
no shutdown
```

```
wireless profile policy policy_flex_cwa  
no central association !!Ensure to disable central-assoc for flexconnect APs  
no central dhcp  
no central switching  
aaa-override  
accounting-list ISE  
ipv4 dhcp required  
nac  
vlan [CLIENT_VLAN]  
no shutdown
```

로컬 모드 AP에 대한 정책 생성

로컬 모드 AP는 일반적으로 동일한 네트워크를 통해 Catalyst 9800 컨트롤러와 동일한 물리적 위치에 있는 AP입니다.

이제 기본 디바이스 컨피그레이션이 포함된 컨트롤러와 여러 WLAN 프로파일이 생성되었으므로, 이제 정책 프로필과 함께 이 모든 디바이스를 연결하고 이러한 SSID를 브로드캐스트해야 하는 액세스 포인트에 태그를 통해 적용할 차례입니다

자세한 내용은 [Understand Catalyst 9800 Wireless Controllers Configuration Model\(Catalyst 9800 무선 컨트롤러 컨피그레이션 모델 이해\)](#)을 참조하십시오.

```
wireless profile policy policy_local_clients  
description local_vlan  
dhcp-tlv-caching  
http-tlv-caching
```

```

radius-profiling
session-timeout 86400 !!Ensure to not use 0 since 0 means no pmk cache
idle-timeout 300
vlan [CLIENT_VLAN]
no shutdown

wireless tag site site_tag_local
description local

wireless tag policy policy_tag_local
description "Tag for APs on local mode"
!! Include here only the WLANs types from previous sections, that you have defined and are
interesting for your organization
!! For guest WLANS (CWA/LWA), it is common to use a different policy profile, to map to a
different VLAN
wlan wlan_psk policy policy_policy_local_clients
wlan wlan_dot1x policy policy_policy_local_clients
wlan wlan_webauth policy policy_policy_local_clients
wlan wlan_cwa policy policy_policy_local_clients

```

Flexconnect 모드 AP에 대한 정책 생성

Flexconnect 모드 액세스 포인트는 일반적으로 컨트롤러와 AP 간의 연결이 WAN을 통해 수행될 때 (따라서 AP 간의 왕복 지연 시간이 증가함) 또는 토폴로지를 이유로 인해 클라이언트 트래픽이 AP 포트에서 로컬로 스위칭되어야 하며 컨트롤러 인터페이스에서 네트워크를 종료하기 위해 CAPWAP를 통해 전달되지 않아야 합니다.

컨피그레이션은 로컬 모드와 비슷하지만 로컬에서 스위칭된 트래픽이 있는 원격 측으로 플래그가 지정되었습니다.

```

wireless profile flex flex_profile_native
acl-policy REDIRECT
central-webauth
arp-caching
!! Replace 25 with the VLAN native on your AP L2 topology
native-vlan-id 25
vlan-name [VLAN_NAME]
vlan-id [CLIENT_VLAN]

wireless tag site site_tag_flex
flex-profile flex_profile_native
no local-site

wireless profile policy policy_flex_clients
no central association !!Ensure to disable central-assoc for flexconnect APs
no central dhcp
no central switching
dhcp-tlv-caching
http-tlv-caching
idle-timeout 300
session-timeout 86400 !!Ensure to not use 0 since 0 means no pmk cache
vlan [CLIENT_VLAN]
no shutdown

wireless tag policy policy_tag_flex
description "Profile for Flex mode APs"
!! Include here only the WLANs types from previous sections, that you have defined and are
interesting for your organization
!! For guest WLANS (CWA/LWA), it is common to use a different policy profile, to map to a
different VLAN

```

```
wlan wlan_psk policy policy_flex_clients
wlan wlan_dot1x policy policy_flex_clients
wlan wlan_webauth policy policy_flex_clients
wlan wlan_cwa policy policy_flex_cwa
```

최종 - 액세스 포인트에 태그 적용

마지막 단계에서는 정의한 태그를 각 액세스 포인트에 적용해야 합니다. 각 AP의 이더넷 MAC 주소를 디바이스에 있는 MAC 주소로 교체해야 합니다.

```
!!Tag assignment using static method. Replace mac with your device
ap F4DB.E683.74C0
policy-tag policy_tag_local
site-tag site_tag_local
```

AP MAC 주소 목록을 가져오는 방법

show ap summary 명령을 사용하여 현재 연결된 AP 목록을 얻을 수 있습니다

```
Gladius1#sh ap summ
Number of APs: 1
```

```
AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address State
-----
-----
9130E-r3-sw2-g1012 3 9130AXE 0c75.bdb6.28c0 0c75.bdb5.7e80 Test123 ES 192.168.25.139 Registered
```

권장 읽기

- [Cisco Catalyst 9800 Series 구성 모범 사례](#)
- [Catalyst 9800 Wireless LAN Controller용 권장 Cisco IOS XE 릴리스](#)
- [무선 문제 해결 도구](#)