Kochrezepte: Minimale Bootstrap-CLI-Konfiguration für Catalyst 9800

Inhalt

Einleitung

In diesem Dokument werden verschiedene Optionen für "Bootstrap" (Durchführen der Erstkonfiguration) für einen Catalyst 9800 Wireless LAN Controller (WLC) beschrieben. Einige benötigen möglicherweise externe Prozesse (PNP- oder TFTP-Download), andere können teilweise über die CLI ausgeführt werden, sie dann über die Benutzeroberfläche ausführen usw.

Dieses Dokument konzentriert sich auf ein Kochrezeptformat mit minimalen rationalisierten Aktionen, sodass eine 9800 für den Basisbetrieb, einschließlich Remote-Verwaltung und Best

Practices, so schnell wie möglich konfiguriert wird.

Die Vorlage enthält Kommentare, die mit dem Zeichen "!" vorangestellt werden. um spezifische Punkte der Konfiguration zu erläutern. Alle Werte, die Sie angeben müssen, sind in der Tabelle "Zutaten" unten gekennzeichnet

Diese Version ist für Versionen ab Version 17.3 vorgesehen.

Voraussetzungen

- Catalyst 9800-Controller ist sofort einsatzbereit. Grundsätzlich, ohne Konfiguration
- Grundlegendes zur IOS-XE-Konfiguration
- Zugriff auf den Konsolenport des Controllers. Dabei kann es sich entweder um den physischen CON-Port in Ihrer Appliance (9800-40, 9800-80, 9800-L) oder über Ihren Hypervisor-Client für Remote-Zugriff auf 9800-CL handeln.
- Für seriellen Zugriff, jede Terminal-Client-Anwendung Ihrer Präferenz

Inhaltsstoffe

Jedes Großbuchstabe entspricht einer Einstellung, die Sie vor Verwendung der Konfigurationsvorlage ändern müssen:

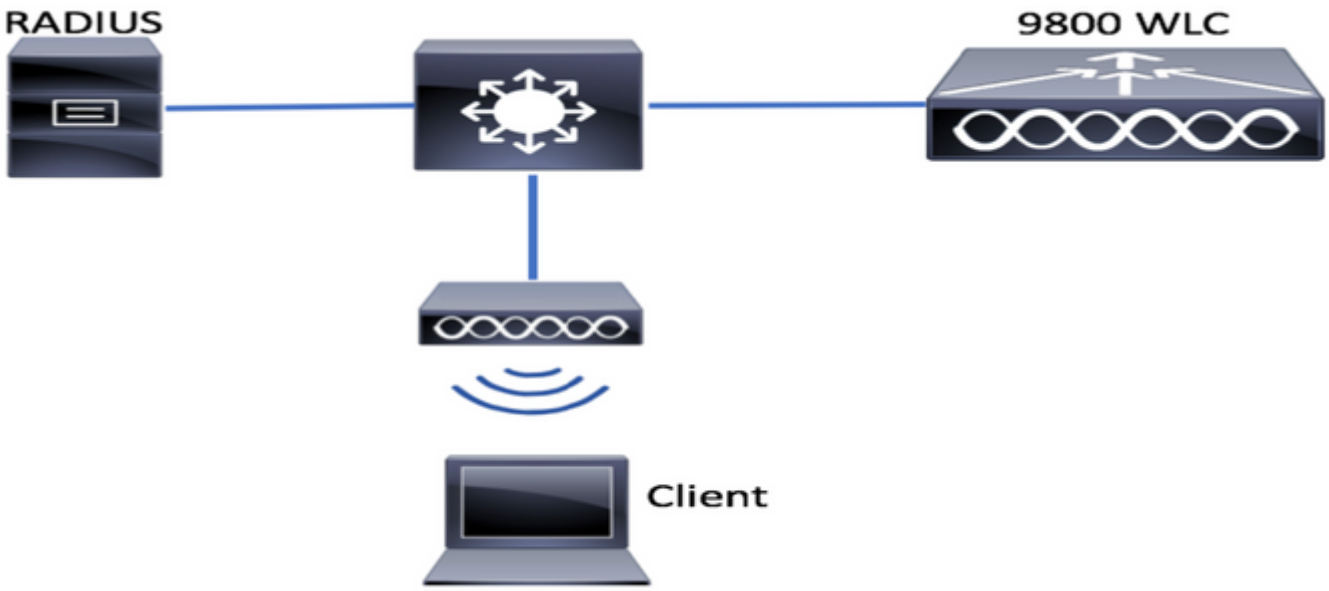
Erforderlicher Wert	Name in Vorlage	Beispiel
Out-of-Band-Management-IP	[OOM_IP]	192.168.0.25
Out-of-Band Management Default-Gateway	[OOM_GW]	192.168.0.1
Administrator-Benutzername	[ADMIN]	Administrator
Administratorkennwort	[KENNWORT]	ah1-7k++a1
Benutzername des AP-Administrators	[AP_ADMIN]	Administrator
AP CLI-Kennwort	[AP_PASSWORT]	Alkhb90jlih
AP - Geheime Aktivierung	[AP_SECRET]	kH20-9 JJH
Name des Controller-Hosts	[WLC_NAME]	9800-bcn-1
Name der Firmendomäne	[DOMÄNE_NAME]	company.com
Client-VLAN-ID	[CLIENT_VLAN]	15
Client-VLAN-Name	[VLAN_NAME]	Client_VLAN
VLAN der Wireless-Management-Schnittstelle	[WMI_VLAN]	25
Wireless Management Interface-IP	[WMI_IP]	192.168.25.10
Wireless Management Interface-Maske	[WMI_MASK]	255.255.255.0
Standard-GW für Wireless-Verwaltungsschnittstelle	[WMI_GW]	192.168.25.1
NTP-Server	[NTP_IP]	192.168.1.2

Radius-Server-IP	[RADIUS_IP]	192.168.0.98
RADIUS-Schlüssel oder gemeinsam genutzter geheimer Schlüssel	[RADIUS_KEY]	ThisIsASharedSecret
WLAN SSID WPA2 Vorläufiger gemeinsamer Schlüsselname	[SSID-PSK]	persönlich
WLAN SSID WPA2 802.1x-Authentifizierung	[SSID-DOT1x]	Firmenname
WLAN-SSID - lokale Webauthentifizierung von Gastbenutzern	[SSID-LWA]	Gast1
WLAN-SSID - lokale Webauthentifizierung von Gastbenutzern	[SSID-CWA]	Gast2

Konfigurieren

Netzwerkdiagramm

Diese Dokumente folgen einer sehr einfachen Topologie, bei der ein Controller der Serie 9800 mit einem Switch verbunden ist, sowie ein Access Point im selben VLAN zu Testzwecken, mit optionalem Radius-Server für die Authentifizierung



Optional: Wiederherstellung des Controllers auf die Werkseinstellungen - Tag Null

Wenn Ihr Controller bereits konfiguriert wurde und Sie ihn ohne Konfiguration auf ein Day Zero-Szenario zurücksetzen möchten, können Sie die folgende optionale Vorgehensweise ausführen:

```
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
```

Assistent zum Umgehen der Erstkonfiguration

Nachdem der Controller das erneute Laden abgeschlossen hat, wird ein CLI-Konfigurationsassistent angezeigt, mit dem eine grundlegende Erstkonfiguration durchgeführt werden kann. In diesem Dokument umgehen wir diese Option und konfigurieren alle Werte mithilfe der in den nächsten Schritten bereitgestellten CLI-Vorlage.

Warten Sie, bis der Controller das Hochfahren abgeschlossen hat:

```
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
```

Drücken Sie die Eingabetaste, und sagen Sie "no" (Nein) zum ersten Dialogfeld, und "yes" (Ja), um den automatischen Installationsvorgang zu beenden:

```
% 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!
```

Bootstrap-Vorlage - Grundlegende Geräteeinstellungen

Verwenden Sie die folgenden Konfigurationsvorlagen, und ändern Sie die Werte, die in der Tabelle "Inhaltsstoffe" angegeben sind. Dieses Dokument ist in verschiedene Abschnitte unterteilt, um die Überprüfung zu vereinfachen.

Fügen Sie in allen Abschnitten den Inhalt immer im Konfigurationsmodus ein, drücken Sie die Eingabetaste, um die Eingabeaufforderung anzuzeigen, und verwenden Sie dann die Befehle enable und config, z. B.:

```
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
```

Erstkonfiguration von Geräten und Out-of-Band-Konnektivität

Verwenden Sie die folgenden Befehle im Konfigurationsmodus. Die Befehle beenden das Speichern der Konfiguration, um sicherzustellen, dass SSH aktiviert ist, nachdem sie den lokalen Schlüssel erstellt haben

```
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
```

Optional - CDP aktivieren

Wechseln Sie erneut in den Konfigurationsmodus, und verwenden Sie die folgenden Befehle. Ersetzen Sie für 9800-CL die Schnittstellen Te0/0/0 und Te0/0/1 durch Gi1 und Gi2.

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

9800-CL - selbstsigniertes Zertifikat erstellen

Dies ist nur für Controller der Serie 9800-CL erforderlich. Es ist **nicht** für die Einheitenmodelle (9800-80, 9800-40, 9800-L) für AP-CAPWAP-Verbindungen erforderlich.

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

VLANs erstellen

Erstellen Sie im Konfigurationsmodus so viele Client-VLANs wie erforderlich, und das VLAN entspricht der Wireless Management Interface (WMI).

In den meisten Szenarien ist es üblich, mindestens zwei Client-VLANs zu verwenden, eines für den Firmenzugriff und eines für den Gastzugriff. Große Szenarien können bei Bedarf Hunderte verschiedener VLANs umfassen.

WMI-VLAN ist der Zugriffspunkt für den Zugriff auf den Controller für die meisten Verwaltungsprotokolle und -topologien. Darüber hinaus erstellen die Access Points ihre CAPWAP-Tunnel.

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

Konfigurieren von Datenschnittstellen - Appliances

Für 9800-L, 9800-40, 9800-80 können Sie im Konfigurationsmodus die folgenden Befehle verwenden, um grundlegende Funktionen für die Datenebenenschnittstellen festzulegen. In diesem Beispiel wird LACP vorgeschlagen, wobei eine Channel-Gruppe für beide Ports erstellt

wird.

Es ist wichtig, auf Switch-Seite eine passende Topologie zu konfigurieren.

In diesem Abschnitt können erhebliche Änderungen vorgenommen werden, von dem bereitgestellten Beispiel bis hin zu dem, was wirklich benötigt wird, je nach Topologie und Verwendung von Port-Channels. Bitte überprüfen Sie sorgfältig.

```
!!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
```

Konfigurieren der Wireless-Verwaltungsschnittstelle

Verwenden Sie die folgenden Befehle aus dem Konfigurationsmodus, um die WMI zu erstellen. Dies ist ein wichtiger Schritt

```
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 somethng like Vlan25, depending on your WMI VLAN ID
wireless management interface Vlan[WMI_VLAN]
```

Zeitzone und NTP-Sincronisierung konfigurieren

NTP ist für verschiedene Wireless-Funktionen von entscheidender Bedeutung. Verwenden Sie die folgenden Befehle im Konfigurationsmodus, um sie einzurichten:

```
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-Zugriff und andere lokale Services

Anhand der Best Practices werden zusätzliche VTY-Leitungen erstellt, Probleme mit dem GUI-Zugriff vermieden und Basisdienste in die Lage versetzt, die TCP-Sitzungsverarbeitung für die Verwaltungsschnittstellen zu verbessern.

```
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-Konfiguration

Dadurch werden grundlegende Einstellungen erstellt, um die Radius-Kommunikation mit dem ISE-Server zu aktivieren.

```
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
```

Optional - Tägliche Konfigurationssicherung

Aus Sicherheitsgründen können Sie ein automatisiertes tägliches Konfigurations-Backup auf den Remote-TFTP-Server aktivieren:

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

Wireless-Konfiguration

In diesem Abschnitt wird ein Beispiel für verschiedene WLAN-Typen beschrieben. Dabei werden die häufigsten Kombinationen von WPA2 mit Preshare Key, WPA2 mit 802.1x/radius, Central Webauth und Local Webauth behandelt. Es wird nicht erwartet, dass Ihre Bereitstellung alle diese Funktionen umfasst. Daher sollten Sie diese nach Bedarf entfernen und ändern.

Es ist wichtig, den Länderbefehl festzulegen, um sicherzustellen, dass der Controller die Konfiguration als "vollständig" markiert. Sie sollten die Länderliste so ändern, dass sie mit Ihrem

Bereitstellungsort übereinstimmt:

```
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
```

Optional - Best Practices

Dadurch wird sichergestellt, dass das Netzwerk die grundlegenden Best Practices erfüllt:

- Access Points verfügen über SSH-aktivierte, nicht standardmäßige Anmeldeinformationen und Syslog, um die Fehlerbehebung zu verbessern. Dies verwendet das Standard-AP-Join-Profil. Wenn Sie neue Einträge hinzufügen, sollten Sie ähnliche Änderungen auf diese anwenden.
- Geräteklassifizierung aktivieren, um mit dem Netzwerk verbundene Client-Typen zu verfolgen

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

device classifier
```

Erstellen von WLANs - WPA2-PSK

Ersetzen Sie die Variablen durch die gewünschten Einstellungen. Diese Art von WLAN wird hauptsächlich für private Netzwerke, einfache Szenarien oder zur Unterstützung von IOT-Geräten ohne 802.1x-Funktionen verwendet.

Dies ist für die meisten Enterprise-Szenarien optional.

```
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
```

Erstellen von WLANs - WPA2-Enterprise

Das häufigste Szenario eines WPA2-WLAN mit Radius-Authentifizierung. Wird in Unternehmensumgebungen verwendet

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

Erstellen von WLANs - Gast mit lokaler Webauthentifizierung

Einfacherer Gastzugriff ohne ISE-Gastsupport

Je nach Version ist es möglich, eine Warnung beim Erstellen der ersten Parameterzuordnung zu erhalten, bitte antworten Sie ja, um fortzufahren

```
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
```

Erstellen von WLANs - Gast mit zentraler Webauthentifizierung

Für ISE-Gastsupport verwendet

```
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
```

Erstellen von Richtlinien für APs im lokalen Modus

APs im lokalen Modus sind APs, die sich am selben physischen Standort wie der Catalyst 9800-Controller befinden, normalerweise über dasselbe Netzwerk.

Jetzt, da der Controller über eine grundlegende Gerätekonfiguration verfügt und verschiedene WLAN-Profile erstellt wurden, ist es an der Zeit, alles mit den Richtlinienprofilen zu verbinden und diese mithilfe von Tags auf die Access Points anzuwenden, die diese SSIDs übertragen sollen.

Weitere Informationen finden Sie unter Konfigurationsmodell der Catalyst 9800 Wireless Controller verstehen.

```
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 3600
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_local_clients
```

Erstellen von Richtlinien für Flexconnect-Modus-APs

Access Points im FlexConnect-Modus werden normalerweise verwendet, wenn die Verbindung zwischen dem Controller und den APs über ein WAN erfolgt (d. h. eine erhöhte Round-Trip-Verzögerung zwischen den Access Points besteht), oder wenn der Client-Datenverkehr aus Topologiegründen lokal am AP-Port geswitcht und nicht über CAPWAP übertragen werden muss, um das Netzwerk an den Controller-Schnittstellen zu verlassen.

Die Konfiguration ähnelt dem lokalen Modus, wird jedoch als Remote-Seite gekennzeichnet und verfügt über lokalen Switch-Verkehr.

```
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 3600
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
```

Endlich - Anwenden von Tags auf Access Points

Als letzten Schritt müssen wir die von uns definierten Tags auf jeden Access Point anwenden. Sie müssen die Ethernet-MAC-Adresse jedes AP durch die im Gerät vorhandene ersetzen.

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

Abrufen einer Liste von AP-MAC-Adressen

Mithilfe des Befehls show ap summary können Sie eine Liste der aktuell verbundenen Access Points abrufen.

```
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
```

Empfohlene Lektüre

- Cisco Catalyst Serie 9800 - Best Practices für die Konfiguration
- Empfohlene Cisco IOS XE-Versionen für Catalyst 9800 Wireless LAN Controller
- Tools zur Fehlerbehebung für Wireless