Receta de cocina: Configuración CLI de Bootstrap mínima para Catalyst 9800

Contenido

Introducción

Este documento describe varias opciones disponibles para "bootstrap" (realizar la configuración inicial) para un controlador de LAN inalámbrica (WLC) de Catalyst 9800. Algunos pueden necesitar procesos externos (descarga de PNP o TFTP), algunos se pueden realizar parcialmente a través de CLI, luego completarlos a través de GUI, etc.

Este documento se centrará en un formato de "receta de cocina", con el conjunto mínimo de acciones simplificadas, para que se configure un 9800 para operaciones básicas, incluida la

administración remota, y prácticas recomendadas, en el menor tiempo posible.

La plantilla proporcionada tiene comentarios precedidos del carácter "!" para explicar puntos específicos de la configuración. Además, todos los valores que usted debe proporcionar se marcan en la tabla de "ingredientes" a continuación

Este objetivo es 17.3 y versiones superiores

Prerequisites

- Controlador Catalyst 9800 "listo para usar". Básicamente, sin ninguna configuración
- Introducción básica de la configuración IOS-XE
- Acceso al puerto de la consola del controlador. Puede ser el puerto físico CON en su dispositivo (9800-40, 9800-80, 9800-L) o a través de su cliente de acceso remoto del hipervisor para 9800-CL
- Para el acceso serial, cualquier aplicación cliente terminal de su preferencia

Ingredientes

Cada elemento en mayúscula corresponde a una configuración que debe cambiar antes de utilizar la plantilla de configuración:

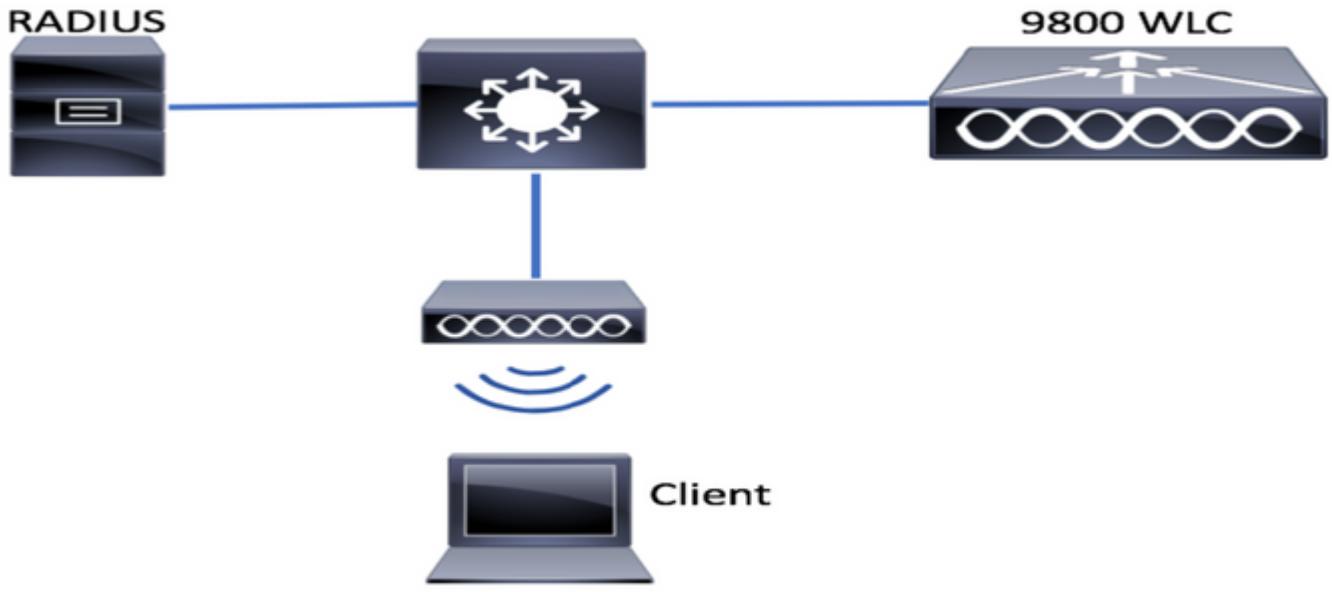
Valor requerido	Nombre de la plantilla	Ejemplo:
IP de administración fuera de banda	[OOM_IP]	192.168.0.25
Gateway predeterminado de administración fuera de banda	[OOM_GW]	192.168.0.1
Nombre de usuario del administrador	[ADMIN]	admin
Contraseña del administrador	[CONTRASEÑA]	ah1-7k++a1
Nombre de usuario del administrador AP	[AP_ADMIN]	admin
Contraseña CLI de AP	[AP_PASSWORD]	alkhb90jlih
AP Enable Secret	[AP_SECRET]	kh20-9yjh
Nombre de host del controlador	[WLC_NAME]	9800-bcn-1
Nombre de dominio de la empresa	[DOMINIO_NOMBRE]	company.com
ID de VLAN del cliente	[CLIENT_VLAN]	15
Nombre de VLAN del cliente	[VLAN_NAME]	client_vlan
VLAN de interfaz de administración inalámbrica	[WMI_VLAN]	25
IP de interfaz de administración inalámbrica	[WMI_IP]	192.168.25.10
Máscara de interfaz de administración inalámbrica	[WMI_MASK]	255.255.255.0
GW predeterminado de la interfaz de gestión inalámbrica	[WMI_GW]	192.168.25.1
Servidor NTP	[NTP_IP]	192.168.1.2

IP del servidor Radius	[RADIUS_IP]	192.168.0.98
Clave Radius o secreto compartido	[RADIUS_KEY]	ThisIsASharedSecret
Nombre de clave precompartida WLAN SSID WPA2	[SSID-PSK]	personal
Autenticación WLAN SSID WPA2 802.1x	[SSID-DOT1x]	nombre de la empresa
Autenticación Web local de invitado WLAN SSID	[SSID-LWA]	guest1
Autenticación Web local de invitado WLAN SSID	[SSID-CWA	guest2

Configurar

Diagrama de la red

Estos documentos siguen una topología muy básica, con un controlador Calatyst 9800 conectado a un switch, más un punto de acceso en la misma vlan para fines de prueba, con un servidor Radius opcional para autenticación



Opcional: Restauración del controlador a los valores predeterminados de fábrica: día cero

si su controlador ya se ha configurado y desea moverlo de nuevo a un escenario de día cero, sin ninguna configuración, puede realizar el siguiente procedimiento opcional:

```
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
```

Omisión del asistente de configuración inicial

Una vez que el controlador haya terminado de recargar, presentará un asistente de configuración CLI para realizar una configuración inicial básica. En este documento, se omite esta opción y se configuran todos los valores mediante la plantilla CLI proporcionada en los siguientes pasos.

Espere hasta que el controlador haya terminado de arrancar:

```
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
```

Pulse la tecla Intro y diga "no" al diálogo inicial y "sí" para finalizar el proceso de instalación automática:

```
% 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!
```

Plantilla de Bootstrap - Configuración básica del dispositivo

Tome las siguientes plantillas de configuración y modifique los valores según se indica en la tabla Ingredientes. Este documento se divide en diferentes secciones para facilitar la revisión

Para todas las secciones, pegue siempre el contenido del modo de configuración, presione la tecla "Intro" para obtener el mensaje y luego use los comandos enable y config, por ejemplo:

```
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
```

Configuración inicial del dispositivo y conectividad fuera de banda

Utilice los siguientes comandos en el modo de configuración. Los comandos terminarán guardando la configuración para asegurarse de que SSH esté habilitado, después de crear la clave local

```
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
```

Opcional: habilitación de CDP

Vuelva a introducirlo en el modo Config y utilice los siguientes comandos. Para 9800-CL, reemplace las interfaces Te0/0/0 y Te0/0/1 con Gi1 y Gi2

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

9800-CL - Crear certificado firmado automáticamente

Esto sólo se debe realizar en controladores 9800-CL, **no** se requiere en los modelos de dispositivos (9800-80, 9800-40, 9800-L) para la unión CAPWAP AP AP

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

Crear VLAN

Desde el modo de configuración, cree tantas vlan de cliente como sea necesario y la vlan correspondiente a la interfaz de administración inalámbrica (WMI)

En la mayoría de los escenarios, es común tener al menos 2 vlan de cliente, una para la empresa y otra para el acceso de invitados. Los grandes escenarios podrían abarcar cientos de vlan diferentes según sea necesario

La vlan de WMI es el punto de acceso al controlador para la mayoría de los protocolos y topologías de administración, además de que allí los puntos de acceso crearán sus túneles CAPWAP

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

Configurar interfaces de datos - Dispositivos

Para 9800-L, 9800-40, 9800-80, desde el modo de configuración, puede utilizar los siguientes comandos para establecer la funcionalidad básica para las interfaces del plano de datos. Este ejemplo, propone LACP, con el grupo de canales creado a través de ambos puertos.

Es importante configurar una topología coincidente en el lado del switch.

Esta es una sección que podría tener cambios significativos del ejemplo proporcionado a lo que

realmente se necesita, dependiendo de su topología y si usa canales de puerto. Revise cuidadosamente.

```
!!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
```

Configuración de la interfaz de gestión inalámbrica

Utilice los siguientes comandos del modo de configuración para crear el WMI. Este es un paso fundamental

```
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]
```

Configurar zona horaria y sincronización NTP

NTP es fundamental para varias funciones inalámbricas. Utilice los siguientes comandos en el modo de configuración para configurarlo:

```
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
```

Acceso VTY y otros servicios locales

Siguiendo las mejores prácticas, esto creará líneas VTY adicionales, para evitar problemas de

acceso a la GUI y habilitar servicios básicos para mejorar el manejo de sesiones TCP para las interfaces de administración

```
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
```

Configuración RADIUS

Esto creará una configuración básica para habilitar las comunicaciones de radio en el servidor ISE

```
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
```

Opcional: copia de seguridad de la configuración diaria

Por razones de seguridad, puede habilitar una copia de seguridad de la configuración diaria automatizada en el servidor TFTP remoto:

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

Configuración inalámbrica

Esta sección tratará un ejemplo de diferentes tipos de WLAN, que abarca las combinaciones más comunes de WPA2 con Preshare Key, WPA2 con 802.1x/radius, Central Webauth y Local Webauth. No se espera que su implementación tenga todas estas características, por lo que debe quitarlas y modificarlas según sea necesario

Es fundamental establecer el comando country, para asegurarse de que el controlador marque la configuración como "completa". Debe modificar la lista de países para que coincida con la ubicación de implementación:

```
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
```

Opcional: Prácticas recomendadas

Esto garantizará que la red cumpla las mejores prácticas básicas:

- Los puntos de acceso tienen SSH habilitado, credenciales no predeterminadas y syslog, para mejorar la experiencia de resolución de problemas. Esto está utilizando el perfil de unión de AP predeterminado, si agrega nuevas entradas, debería aplicarles cambios similares
- Habilite la clasificación de dispositivos para realizar un seguimiento de los tipos de clientes conectados a la red

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

device classifier
```

Creación de WLANs - WPA2-PSK

Reemplace las variables por la configuración necesaria. Este tipo de WLAN se utiliza principalmente para redes personales, escenarios simples o para admitir dispositivos IOT sin capacidades 802.1x

Esto es opcional para la mayoría de los escenarios empresariales

```
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
```

Creación de WLANs - WPA2-Enterprise

Escenario más común de WPA2 WLAN con autenticación Radius. Utilizado en entornos empresariales

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

Creación de WLANs - Invitado con Autenticación Web Local

Se utiliza para un acceso de invitados más sencillo, sin compatibilidad con invitados ISE

Dependiendo de la versión, es posible obtener una advertencia al crear el primer mapa de parámetros, responda sí, para continuar

```
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
```

Creación de WLANs - Invitado con Autenticación Web Central

Se utiliza para el soporte de invitados de ISE

```
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
```

Creación de políticas para AP de modo local

Los AP de modo local son aquellos que estarán en la misma ubicación física que el controlador Catalyst 9800, normalmente a través de la misma red.

Ahora que tenemos el controlador con la configuración básica del dispositivo y los diferentes perfiles WLAN creados, es hora de que lo conectemos todo con los perfiles de políticas y los aplicemos a través de etiquetas a los puntos de acceso que deberían difundir esos SSID

Para obtener más información, consulte Introducción al modelo de configuración de los controladores inalámbricos Catalyst 9800

```
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_local_clients
```

Creación de políticas para los AP del modo Flexconnect

Los puntos de acceso del modo Flexconnect se utilizan normalmente bien cuando la conexión entre el controlador y los AP se realiza a través de una WAN (por lo que hay un mayor retardo de ida y vuelta entre ellos), o bien cuando por razones de topología, necesitamos que el tráfico del cliente se conmute localmente en el puerto AP y no se lleve a través de CAPWAP para salir de la red en las interfaces del controlador

La configuración es similar al modo local, pero marcada como un lado remoto, con tráfico conmutado localmente

```
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
```

Final - Aplicar etiquetas a los puntos de acceso

Como último paso, debemos aplicar las etiquetas que hemos definido a cada punto de acceso. Debe reemplazar la dirección MAC Ethernet de cada AP, por la que está presente en su dispositivo

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

Cómo obtener la lista de direcciones MAC AP

Puede obtener una lista de los APs actualmente unidos, usando el comando show ap summary

```
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
```

Bibliografía recomendada

- Prácticas recomendadas de configuración de Cisco Catalyst serie 9800
- Versiones Cisco IOS XE recomendadas para los controladores de LAN inalámbrica Catalyst 9800
- Herramientas de resolución de problemas inalámbricos