烹饪配方：Catalyst 9800的最低引导程序CLI配置

目录

简介
先决条件
配料
配置
网络图
可选：将控制器恢复为出厂默认设置 — 第零天
绕过初始配置向导
引导模板 — 基本设备设置
初始设备配置和带外连接
可选 — 启用CDP
9800-CL — 创建自签名证书
创建 VLAN
配置数据接口 — 设备
配置无线管理接口
配置时区和NTP自动化
VTY访问和其他本地服务
RADIUS 配置
可选 — 每日配置备份
无线配置
可选 — 最佳实践
创建WLAN - WPA2-PSK
创建WLAN - WPA2 — 企业
创建WLAN — 使用本地Web身份验证的访客
创建WLAN — 使用中央Web身份验证的访客
为本地模式AP创建策略
为Flexconnect模式AP创建策略
最终 — 将标记应用到接入点
如何获取AP MAC地址列表
推荐阅读

简介

本文档介绍可用于Catalyst 9800无线局域网控制器(WLC)的“bootstrap”（执行初始配置）的多个选项。 有些可能需要外部进程（PNP或TFTP下载），有些可以通过CLI部分完成，然后通过GUI完成，等等。

本文档将重点介绍“烹饪配方”格式，其中最简化的操作集，以在尽可能短的时间内为基本操作（包括远程管理和最佳实践）配置9800。

提供的模板带有前面带有字符“！”的注释 以说明配置的具体点。此外，必须由您提供的所有值都在下面的“成分”表中标记

此目标为17.3及更高版本

先决条件

- Catalyst 9800控制器“开箱即用”。 基本上，没有任何配置
- 基本了解IOS-XE配置
- 访问控制器的控制台端口。这可以是设备(9800-40、9800-80、9800-L)中的CON物理端口，也可以是通过9800-CL的虚拟机监控程序远程访问客户端
- 对于串行访问，您首选的任何终端客户端应用

配料

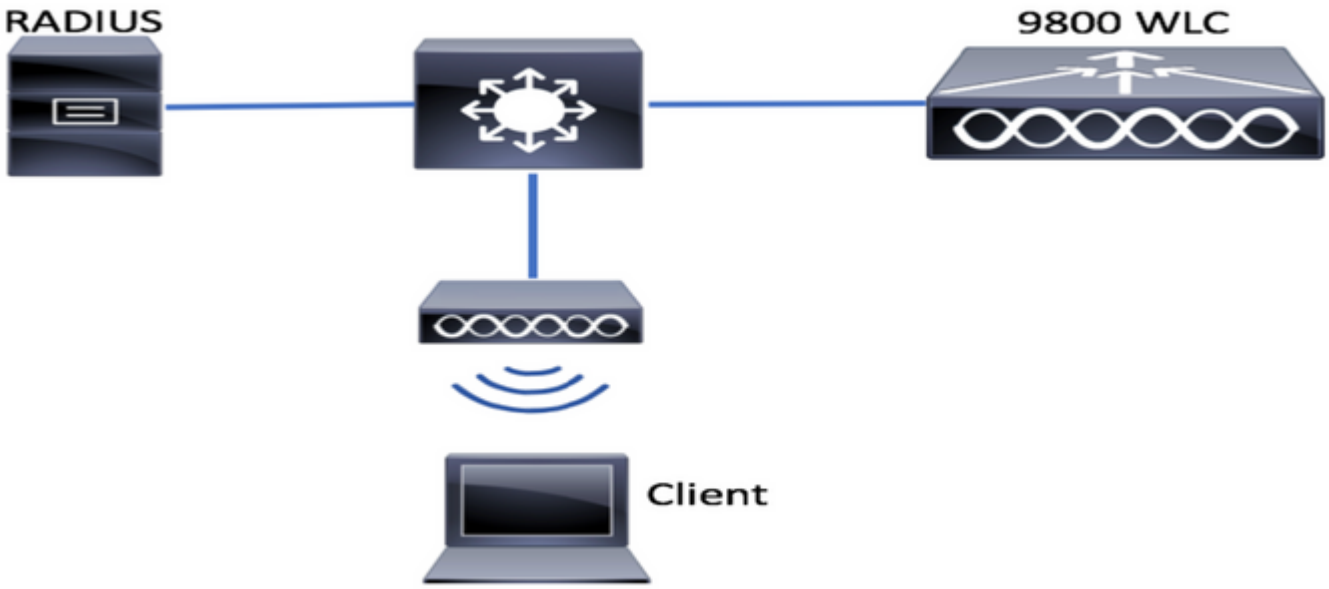
每个大写项都对应于使用配置模板之前必须更改的设置：

所需值	模板中的名称	示例
带外管理IP	[OOM_IP]	192.168.0.25
带外管理默认网关	[OOM_GW]	192.168.0.1
管理员用户名	[管理员]	admin
管理员密码	[密码]	ah1-7k++a1
AP管理员用户名	[AP_ADMIN]	admin
AP CLI密码	[AP_PASSWORD]	alkhb90jlih
AP启用加密	[AP_SECRET]	kh20-9yjh
控制器主机名	[WLC_NAME]	9800-bcn-1
公司域名	[域名]	company.com
客户端VLAN ID	[CLIENT_VLAN]	15
客户端VLAN名称	[VLAN_NAME]	client_vlan
无线管理接口VLAN	[WMI_VLAN]	25
无线管理接口IP	[WMI_IP]	192.168.25.10
无线管理接口掩码	[WMI_MASK]	255.255.255.0
无线管理接口默认GW	[WMI_GW]	192.168.25.1
NTP 服务器	[NTP_IP]	192.168.1.2
Radius服务器IP	[RADIUS_IP]	192.168.0.98
Radius密钥或共享密钥	[RADIUS_KEY]	ThisIsASharedSecret
WLAN SSID WPA2预共享密钥名称	[SSID-PSK]	个人
WLAN SSID WPA2 802.1x身份验证	[SSID-DOT1x]	公司名称
WLAN SSID访客本地Web身份验证	[SSID-LWA]	guest1
WLAN SSID访客本地Web身份验证	[SSID-CWA	guest2

配置

网络图

本文档遵循非常基本的拓扑，其中Calatyst 9800控制器连接到交换机，另外在同一VLAN上连接接入点以用于测试，可选的Radius服务器用于身份验证



可选：将控制器恢复为出厂默认设置 — 第零天

如果您的控制器已配置，并且您想将其移回零日场景，而无需输出任何配置，则可以执行以下可选步骤：

```
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
```

绕过初始配置向导

控制器完成重新加载后，将显示CLI配置向导以执行基本初始配置。在本文档中，我们将绕过此选项，并使用后续步骤中提供的CLI模板配置所有值。

等待控制器完成启动：

```
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
```

按“Enter”键，对初始对话框说“no”，然后按“yes”终止自动安装过程：

```
% 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!
```

引导模板 — 基本设备设置

采用以下配置模板，并修改“配料”(Conterments)表格中显示的值。本文档分为不同的部分，以便于审阅

对于所有部分，请始终从配置模式粘贴内容，按“Enter”键获取提示，然后使用enable和config命令，例如：

```
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
```

初始设备配置和带外连接

在配置模式下使用以下命令。在创建本地密钥后，命令将结束保存配置以确保启用SSH

```
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
```

可选 — 启用CDP

再次在配置模式下输入，然后使用以下命令。对于9800-CL，将接口Te0/0/0和Te0/0/1替换为Gi1和Gi2

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

9800-CL — 创建自签名证书

这只能在9800-CL控制器上执行， 在AP CAPWAP加入的设备型号(9800-80、9800-40、9800-L)上不需要执行

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

创建 VLAN

在配置模式下，根据需要创建尽可能多的客户端vlan，以及与无线管理接口(WMI)对应的VLAN

在大多数情况下，通常至少有2个客户端VLAN，一个用于企业VLAN，一个用于访客接入。大型路由器可根据需要跨越数百个不同的vlan

WMI vlan是大多数管理协议和拓扑访问控制器的点，而且接入点将在此创建其CAPWAP隧道

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

配置数据接口 — 设备

对于9800-L、9800-40、9800-80，在配置模式下，可以使用以下命令为数据平面接口设置基本功能。本示例建议使用LACP，在两个端口上创建信道组。

在交换机端配置匹配的拓扑非常重要。

本部分可能会从提供的示例到真正需要的内容发生重大更改，具体取决于您的拓扑以及是否使用端口通道。请仔细检查。

```
!!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
```

配置无线管理接口

在配置模式下使用以下命令创建WMI。这是关键步骤

```
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]
```

配置时区和NTP自动化

NTP对于多种无线功能至关重要。在配置模式下使用以下命令进行设置：

```
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访问和其他本地服务

遵循最佳实践，这将创建额外的VTY线路，以避免GUI访问问题，并启用基本服务以改进管理接口的TCP会话处理

```
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 配置

这将创建基本设置，以启用与ISE服务器的RADIUS通信

```
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
```

可选 — 每日配置备份

出于安全原因，您可以启用到远程TFTP服务器的自动每日配置备份：

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

无线配置

本节将介绍不同WLAN类型的示例，包括WPA2与预共享密钥、WPA2与802.1x/radius、Central Webauth和Local Webauth的最常见组合。您的部署不应包含所有这些，因此您应根据需要删除和修改

设置country命令至关重要，确保控制器将配置标记为“完成”。 您应修改国家/地区列表以匹配部署位置：

```
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
```

可选 — 最佳实践

这将确保网络符合基本的最佳实践：

- 接入点启用了SSH、非默认凭证和系统日志，以改善故障排除体验。这是使用默认AP加入配置文件，如果添加新条目，应对其应用类似更改
- 启用设备分类，以跟踪连接到网络的客户端类型

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

device classifier
```

创建WLAN - WPA2-PSK

将变量替换为所需的设置。此类WLAN主要用于个人网络、简单场景或支持没有802.1x功能的物联网设备

对于大多数企业方案，这是可选的

```
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
```

创建WLAN - WPA2 — 企业

WPA2 WLAN的最常见方案（使用Radius身份验证）。用于企业环境

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

创建WLAN — 使用本地Web身份验证的访客

用于更简单的访客访问，无ISE访客支持

根据版本，在创建第一个参数映射时可能会收到警告，请回答是，继续

```
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
```

创建WLAN — 使用中央Web身份验证的访客

用于ISE访客支持

```
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
```

为本地模式AP创建策略

本地模式AP是那些将与Catalyst 9800控制器位于同一物理位置的AP，通常位于同一网络上。

现在，我们已经拥有具有基本设备配置的控制器，并创建了不同的WLAN配置文件，是时候将其与策略配置文件结合在一起，并通过标记将它们应用到应广播这些SSID的接入点

有关详细信息，请选中了解Catalyst 9800无线控制器配置模型

```
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
```

为Flexconnect模式AP创建策略

当控制器和AP之间的连接通过WAN完成（因此它们之间的往返延迟增加）时，或者由于拓扑原因，我们需要客户端流量在AP端口本地交换，而不是通过CAPWAP在控制器接口上退出网络时，通常使用Flexconnect模式接入点

配置类似于本地模式，但标记为远程端，具有本地交换流量

```
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
```

最终 — 将标记应用到接入点

最后，我们需要将我们定义的标记应用到每个接入点。您必须将每个AP的以太网MAC地址替换为设备中的AP地址

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

如何获取AP MAC地址列表

您可以使用命令show ap summary获取当前加入的AP的列表

```
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
```

推荐阅读

- Cisco Catalyst 9800系列配置最佳实践
- Catalyst 9800无线LAN控制器的推荐Cisco IOS XE版本
- 无线故障排除工具