Receita de Cozimento: Configuração de CLI de bootstrap mínima para o Catalyst 9800

Contents

Introduction

Este documento descreve várias opções disponíveis para "bootstrap" (executando a configuração inicial) para um Catalyst 9800 Wireless Lan Controller (WLC). Alguns podem precisar de processos externos (download de PNP ou TFTP), alguns podem ser parcialmente realizados via CLI, depois concluídos via GUI, etc.

Este documento se concentrará em um formato de "receita de cozinha", com o conjunto mínimo de ações simplificadas, para ter um 9800 configurado para operações básicas, incluindo

administração remota e melhores práticas, no menor tempo possível.

O modelo fornecido tem comentários com precedência sobre o caractere "!" para explicar pontos específicos da configuração. Além disso, todos os valores que devem ser fornecidos por você estão marcados na tabela "ingredientes" abaixo

Destina-se às versões 17.3 e superior

Prerequisites

- Controlador Catalyst 9800 "pronto para uso". Basicamente, sem nenhuma configuração
- Compreensão básica da configuração do IOS-XE
- Acesso à porta de console do seu controlador. Pode ser a porta física do CON no dispositivo (9800-40, 9800-80, 9800-L) ou através do cliente de acesso remoto do hipervisor para 9800-CL
- Para acesso serial, qualquer aplicativo cliente terminal de sua preferência

Ingredientes

Cada item em maiúsculas corresponde a uma configuração que você deve alterar antes de usar o modelo de configuração:

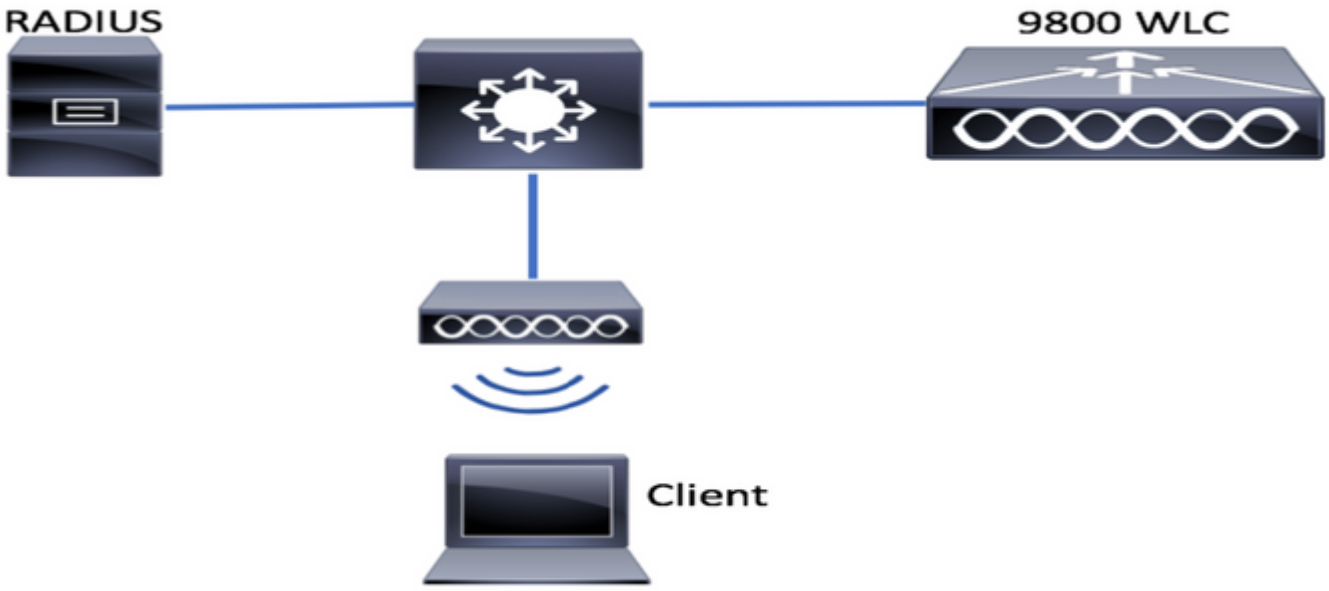
Valor obrigatório	Nome no modelo	Exemplo
IP de gerenciamento fora de banda	[OOM_IP]	192.168.0.25
Gateway padrão fora da banda	[OOM_GW]	192.168.0.1
Nome de usuário do administrador	[ADMIN]	admin
Senha do administrador	[SENHA]	ah1-7k++a1
Nome de usuário do administrador do AP	[AP_ADMIN]	admin
senha de CLI de AP	[AP_PASSWORD]	alkhb90jlih
Segredo de ativação de AP	[AP_SECRET]	kh20-9yjh
Nome do host da controladora	[WLC_NAME]	9800-bcn-1
Nome de domínio da empresa	[DOMAIN_NAME]	company.com
ID da VLAN do cliente	[CLIENT_VLAN]	15
Nome da VLAN do cliente	[VLAN_NAME]	client_vlan
VLAN da interface de gerenciamento sem fio	[WMI_VLAN]	25
IP da interface de gerenciamento sem fio	[WMI_IP]	192.168.25.10
Máscara da interface de gerenciamento sem fio	[WMI_MASK]	255.255.255.0
GW padrão da interface de gerenciamento sem fio	[WMI_GW]	192.168.25.1
Servidor NTP	[NTP_IP]	192.168.1.2

IP do servidor Radius	[RADIUS_IP]	192.168.0.98
Chave RADIUS ou segredo compartilhado	[RADIUS_KEY]	EsteÉOSegredoCompartilhadc
WLAN SSID WPA2 Nome da chave pré-compartilhada	[SSID-PSK]	pessoal
Autenticação WPA2 802.1x de SSID da WLAN	[SSID-DOT1x]	nome da empresa
Autenticação da Web local de convidado do SSID da WLAN	[SSID-LWA]	convidado1
Autenticação da Web local de convidado do SSID da WLAN	[SSID-CWA	convidado2

Configurar

Diagrama de Rede

Esses documentos seguem uma topologia muito básica, com um controlador Calatyst 9800 conectado a um switch, além de um ponto de acesso na mesma vlan para fins de teste, com servidor Radius opcional para autenticação



Opcional: Restauração do controlador para os padrões de fábrica - Dia zero

se o controlador já tiver sido configurado e você quiser movê-lo de volta para um cenário de Dia Zero, sem nenhuma configuração, você poderá executar o seguinte procedimento 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
```

Ignorando o Assistente de Configuração Inicial

Depois que o controlador terminar de recarregar, ele apresentará um assistente de configuração da CLI para executar uma configuração inicial básica. Neste documento, ignoraremos essa opção e configuraremos todos os valores usando o modelo CLI fornecido nas próximas etapas.

Aguarde até que o controlador termine a inicialização:

```
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
```

Pressione a tecla "Enter" e diga "não" à caixa de diálogo inicial e "sim" para encerrar o processo de autoinstalação:

```
% 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!
```

Modelo de bootstrap - Configurações básicas do dispositivo

Pegue os seguintes modelos de configuração e modifique os valores conforme indicado na tabela Ingredientes. Este documento é dividido em diferentes seções para facilitar a revisão

Para todas as seções, sempre cole o conteúdo do modo de configuração, pressionando a tecla "Enter" para obter o prompt e, em seguida, usando os comandos enable e config, por exemplo:

```
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
```

Configuração inicial do dispositivo e conectividade fora da banda

Use os seguintes comandos no modo de configuração. Os comandos terminarão salvando a configuração para garantir que o SSH esteja ativado, após a criação da chave 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 - Habilitar CDP

Entre novamente no modo de configuração e use os seguintes comandos. Para o 9800-CL, substitua as interfaces Te0/0/0 e Te0/0/1 por Gi1 e Gi2

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

9800-CL - Create Self Signed Certificate (Criar certificado autoassinado)

Isso só deve ser executado em controladores 9800-CL, **não** é necessário nos modelos de dispositivo (9800-80, 9800-40, 9800-L) para a união AP CAPWAP

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

Criar VLANs

No modo Config, crie quantas vlans de cliente forem necessárias e a vlan correspondente à interface de gerenciamento sem fio (WMI)

Na maioria dos cenários, é comum ter pelo menos duas vlans de cliente, uma para corporativo e outra para acesso de convidado. Grandes cenários podem abranger centenas de vlans diferentes conforme necessário

A vlan WMI é o ponto de acesso ao controlador para a maioria dos protocolos e topologias de gerenciamento, além de que lá os pontos de acesso criarão seus túneis CAPWAP

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

Configurar interfaces de dados - Dispositivos

Para 9800-L, 9800-40, 9800-80, no modo de configuração, você pode usar os seguintes comandos para definir a funcionalidade básica para as interfaces do plano de dados. Este exemplo está propondo LACP, com channel-group criado em ambas as portas.

Éimportante configurar uma topologia correspondente no lado do switch.

Esta é uma seção que pode ter alterações significativas do exemplo fornecido para o que é realmente necessário, dependendo da topologia e se estiver usando canais de porta. Por favor, reveja 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
```

Configurar a interface de gerenciamento sem fio

Use os seguintes comandos do modo de configuração para criar a WMI. Esta é uma etapa crítica

```
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 o fuso horário e sincron NTP

O NTP é essencial para vários recursos sem fio. Use os seguintes comandos no modo de configuração para configurá-lo:

```
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
```

Acesso VTY e outros serviços locais

Seguindo as práticas recomendadas, isso criará linhas VTY adicionais, para evitar problemas de acesso à GUI e permitir que serviços básicos melhorem o tratamento da sessão TCP para as interfaces de gerenciamento

```
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
```

Configuração de RADIUS

Isso criará configurações básicas para habilitar as comunicações de raio para o 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 - Backup de configuração diário

Por motivos de segurança, você pode habilitar um backup de configuração diário automatizado para o servidor TFTP remoto:

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

Configuração sem fio

Esta seção cobrirá um exemplo de diferentes tipos de WLAN, abrangendo as combinações mais comuns de WPA2 com Preshare Key, WPA2 com 802.1x/radius, Central Webauth e Local Webauth. Não se espera que sua implantação tenha todos esses itens, portanto, você deve remover e modificar conforme necessário

Éfundamental definir o comando country para garantir que o controlador marque a configuração como "completa". Você deve modificar a lista de países para corresponder ao seu local de implantação:

```
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 - Práticas recomendadas

Isso garantirá que a rede esteja atendendo às melhores práticas básicas:

- Os pontos de acesso têm credenciais e syslog SSH ativados, não padrão, para melhorar a experiência de solução de problemas. Isso está usando o perfil de associação de AP padrão, se adicionar novas entradas, você deve aplicar alterações semelhantes a elas
- Habilitar classificação de dispositivos para rastrear tipos de clientes conectados à rede

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

device classifier
```

Criando WLANs - WPA2-PSK

Substitua as variáveis pelas configurações necessárias. Esse tipo de WLAN é usado principalmente para redes pessoais, cenários simples ou para suportar dispositivos IOT sem recursos 802.1x

Isso é opcional para a maioria dos cenários empresariais

```
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
```

Criando WLANs - WPA2-Empresa

O cenário mais comum de WPA2 WLAN com autenticação Radius. Usado em ambientes empresariais

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

Criando WLANs - Convidado com Autenticação da Web Local

Usado para acesso mais simples para convidados, sem suporte para convidados do ISE

Dependendo da versão, é possível obter um aviso ao criar o primeiro mapa de parâmetros. Responda sim 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
```

Criando WLANs - Convidado com Autenticação da Web Central

Usado para suporte de convidado 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
```

Criando políticas para APs de modo local

Os APs no modo local são aqueles que estarão no mesmo local físico que o controlador Catalyst 9800, normalmente na mesma rede.

Agora que temos o controlador com a configuração básica do dispositivo, e os diferentes perfis de WLAN criados, é hora de colar tudo com os perfis de política e aplicá-los por meio de tags aos pontos de acesso que devem transmitir esses SSIDs

Para obter mais informações, consulte Compreender o Modelo de Configuração dos Controladores Sem Fio 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
```

Criando políticas para APs do modo Flexconnect

Os access points do modo Flexconnect são normalmente usados quando a conexão entre o controlador e os APs é feita em uma WAN (portanto há um maior atraso de ida e volta entre eles), ou quando, por razões de topologia, precisamos que o tráfego do cliente seja comutado localmente na porta do AP e não trazido através do CAPWAP para sair da rede nas interfaces do controlador

A configuração é semelhante ao modo local, mas sinalizada para ser um lado remoto, com tráfego comutado 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 - Aplique marcas aos pontos de acesso

Como etapa final, precisamos aplicar as marcas que definimos para cada ponto de acesso. Você deve substituir o endereço MAC Ethernet de cada AP pelo endereço presente no 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
```

Como obter uma lista de endereços MAC AP

Você pode obter uma lista dos APs atualmente associados, usando o 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
```

Leitura Recomendada

- Práticas recomendadas de configuração do Cisco Catalyst 9800 Series
- Versões recomendadas do Cisco IOS XE para controladores de LAN sem fio Catalyst 9800
- Ferramentas de solução de problemas sem fio