Cooking Recipe: Minimum Bootstrap CLI configuration for Catalyst 9800

Contents

Introduction

This document describes several options avaialble to "bootstrap" (performing initial configuration) for a Catalyst 9800 Wireless Lan Controller (WLC). Some may need external processes (PNP or TFTP download), some can be done partially over CLI, then complete them over GUI, etc.

This document will focus on a "cooking recipe" format, with the minimum streamlined set of actions, to have a 9800 configured for basic operations, including remote administration, and best practices, on the shortest time possible.

The template provided, has comments prefaced with the character "!" to explain specific points of the configuration. Also, all values that must be provided by you, are marked in the "ingredients" table below

This is targeted towards 17.3 and higher versions

Prerequisites

- Catalyst 9800 Controller "out of the box". Basically, without any configuration
- Basic undestanding of IOS-XE configuration
- Access to the console port of your controller. This can be either the CON physical port in your appliance (9800-40, 9800-80, 9800-L), or via your hypervisor remote access client for 9800-CL
- For serial access, any terminal client application of your preference

Ingredients

Each uppercase item corresponds to a setting you must change before using the configuration template:

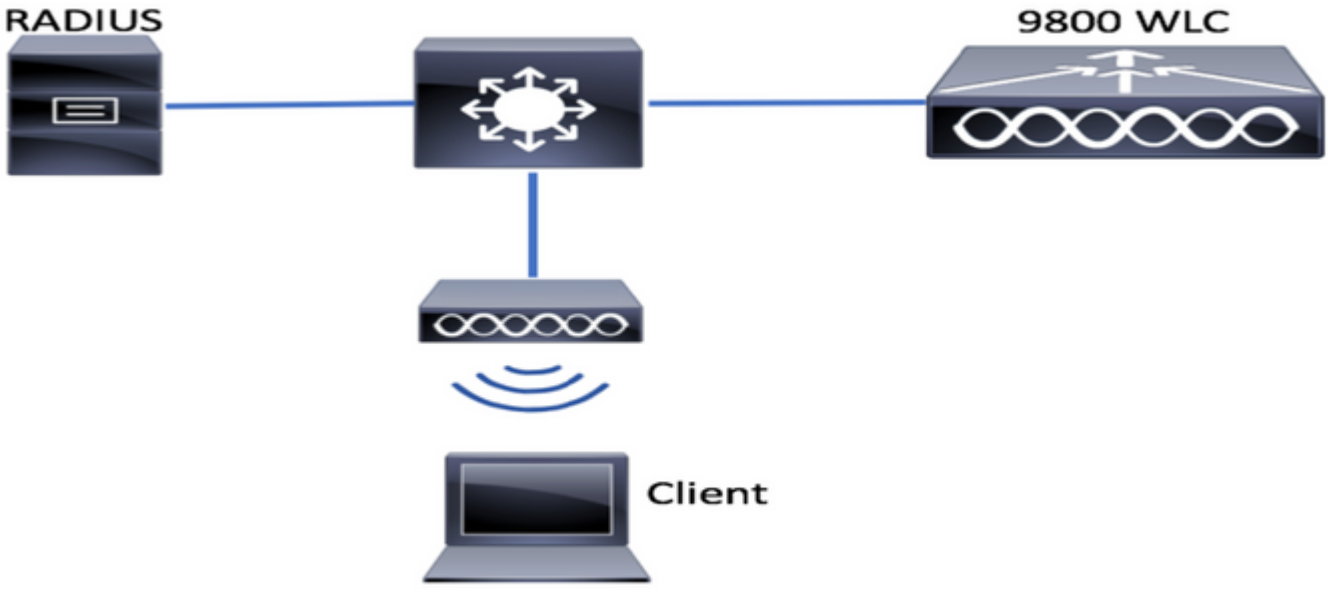
Value Required	Name in Template	Example
Out of Band Management IP	[OOM_IP]	192.168.0.25
Out of Band Management Default Gateway	[OOM_GW]	192.168.0.1
Administrator User Name	[ADMIN]	admin
Administrator Password	[PASSWORD]	ah1-7k++a1
AP Admninistrator User Name	[AP_ADMIN]	admin
AP CLI password	[AP_PASSWORD]	alkhb90jlih
AP Enable Secret	[AP_SECRET]	kh20-9yjh
Controller Host Name	[WLC_NAME]	9800-bcn-1
Company Domain Name	[DOMAIN_NAME]	company.com
Client VLAN ID	[CLIENT_VLAN]	15
Client VLAN Name	[VLAN_NAME]	client_vlan
Wireless Management Interface VLAN	[WMI_VLAN]	25
Wireless Management Interface IP	[WMI_IP]	192.168.25.10
Wireless Management Interface mask	[WMI_MASK]	255.255.255.0
Wireless Management Interface Default GW	[WMI_GW]	192.168.25.1
NTP Server	[NTP_IP]	192.168.1.2
Radius Server IP	[RADIUS_IP]	192.168.0.98
Radius Key or Shared secret	[RADIUS_KEY]	ThisIsASharedSecret

WLAN SSID WPA2 Preshared Key name	[SSID-PSK]	personal
WLAN SSID WPA2 802.1x Authentication	[SSID-DOT1x]	companyname
WLAN SSID Guest Local Web Authentication	[SSID-LWA]	guest1
WLAN SSID Guest Local Web Authentication	[SSID-CWA	guest2

Configure

Network Diagram

This documents follows a very basic topology, with a Calatyst 9800 controller connected to a switch, plus an access point on the same vlan for testing purposes, with optional Radius server for authentication



Optional: Restoring Controller to Factory Defaults - Day Zero

if your controller already has been configured, and you want to move it back to a Day Zero scenario, withtout any configuration, you can perform the following optional procedure:

```
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
```

Bypassing Initial Configuration Wizard

After the controller has finishing reloading, it will present a CLI configuration wizard to perform a basic intiial configuration. In this document, we will bypass this option, and configure all values using the CLI template provided in the next steps.

Wait until the controller has finished booting up:

```
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
```

Press "Enter" key and say "no" to the initial dialog, and "yes", to terminate the autoinstall process:

```
% 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 Template - Basic Device settings

Take the following configuration templates, and modify the values as inidicated on the Ingredients table. This document is split on different sections to facilitate review

For all sections, always paste the content from Config mode, pressing "Enter" key to get prompt, and then using the enable and config commands, for example:

```
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
```

Initial device configuration and out of band connectivity

Use the following commands on Config mode. The commands will end saving the configuration to ensure SSH is enabled, after creating the local key

```
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 - Enable CDP

Enter again in Config mode, and use the following commands. For 9800-CL, Replace interfaces Te0/0/0 and Te0/0/1 with Gi1 and Gi2

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

9800-CL - Create Self Signed Certificate

This is only to be performed on 9800-CL controllers, it is **not** required on the appliance models (9800-80, 9800-40, 9800-L) for AP CAPWAP join

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

Create Vlans

From Config mode, create as many client vlans as required, and the vlan corresponding to the Wireless Management Interface (WMI)

On most scenarios, it is common to have at least 2 client vlans, one for corporate and one for guest access. Large scerarios could span hundreds of different vlans as needed

WMI vlan is the point for access to the controller for most management protocols and topologies, plus that is there the access points will create their CAPWAP tunnels

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

Configure data interfaces - Appliances

For 9800-L, 9800-40, 9800-80, from config mode, you can use the following commands to set basic functionality for the data plane interfaces. This example, is proposing LACP, with channel-group created across both ports.

It is important to configure a matching topology on the switch side.

This is a section that could have singificant changes from the example provided to what is really needed, depending on your toppology and if using port channels. Pleae review carefuly.

```
!!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
```

Configure Wireless Management Interface

Use the following commands from config mode, to create the WMI. This is a critical step

```
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]
```

Configure Time zone and NTP sincronization

NTP is critical for several wireless features. Use the following commands in config mode, to set it up:

```
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 access and other local services

Followng best practices, this will create additional VTY lines, to avoid GUI access issues, and enable basic services to improve TCP session handling for the mangement interfaces

```
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 Configuration

This will create basic settings, to enable radius communications to ISE server

```
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 - Daily Configuration Backup

For security reasons, you can enable an automated daily configuration backup to remote TFTP server:

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

Wireless Configuration

This section will cover an example of different WLAN types, covering the most common combinatios of WPA2 with Preshare Key, WPA2 with 802.1x/radius, Central Webauth and Local Webauth. It is not expected that your deployment will have all of these, so you should remove and modify as needed

It is critifcal to set the country command, to ensure the controller marks the confguration as "complete". You should modify the country list to match your deployment location:

```
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

This will ensure the network is meeting basic best practices:

- Access points have SSH enabled, non-default credentials and syslog, to improve troubleshooting experience. This is using default AP join profile, if adding new entries, you

should apply similar changes to them
- Enable device classification, to track client types connected to the network

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

device classifier
```

Creating WLANs - WPA2-PSK

Replace the variables with your required settings. This type of WLAN is used mostly for personal networks, simple scenarios or to support IOT devices without 802.1x capabilities

This is optional for most Enterprise scenarios

```
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
```

Creating WLANs - WPA2-Enterprise

Most common scenario of WPA2 WLAN with Radius authentication. Used on Enterprise environments

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

Creating WLANs - Guest with Local Web Authentication

Used for simpler Guest access, without ISE guest support

Depending on the version, it is possible to get a warning when creating the first parameter map, please answer yes, to proceed

```
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
```

Creating WLANs - Guest with Central Web Authentication

Used for ISE guest support

```
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
```

Creating policies for local mode APs

Local mode APs are those that will be on the same physical location as the Catalyst 9800 controller, normally over the same network.

Now that we have the controller with basic device configuration, and the different WLAN profiles

created, it is time we glue it all together with the policy profiles and apply them through tags to the access points that should broadcast those SSIDs

For more information, check Understand Catalyst 9800 Wireless Controllers Configuration Model

```
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
```

Creating policies for Flexconnect mode APs

Flexconnect mode Access Points are normally used either when the connection between the controller and the APs is done over a WAN (so there is an increased round trip delay between them), or when for topology reasons, we need the client traffic to be locally switched at the AP port, and not brought through CAPWAP to exit the network at the controller interfaces

The configuration is similar to the local mode, but flagged to be a remote side, with locally switched traffic

```
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 - Apply tags to Access Points

As final step, we need to apply the tags we have defined, to each access point. You must replace the Ethernet mac address of each AP, with the one present in your device

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

How to obtain list of AP mac addresses

You can obtain a list of the currently joined APs, using the command 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
```

Recommended Reading

- Cisco Catalyst 9800 Series Configuration Best Practices
- Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers
- Wireless Troubleshooting Tools