Wireless Management Interface

Information About Wireless Management Interface

The Wireless Management Interface (WMI) is the mandatory Layer 3 interface on the Cisco Catalyst 9800 Wireless Controller. It is used for all communications between the controller and access points. Also, it is used for all CAPWAP or inter-controller mobility messaging and tunneling traffic.

WMI is also the default interface for in-band management and connectivity to enterprise services, such as, AAA, syslog, SNMP, and so on. You can use the WMI IP address to remotely connect to the device using SSH or Telnet (or) access the Graphical User Interface (GUI) using HTTP or HTTPs by entering the wireless management interface IP address of the controller in the address field of your browser.

The Cisco Catalyst 9800 Series Wireless Controller should be able to use Ethernet Service Port (SP) (Management Interface VRF/GigabitEthernet 0) for the below management/control plane protocols from release 17.6.1 onwards:

- SNMP
- RADIUS (both for user authentication to the box and wireless client authorization)
- TACACS
- Syslog
- NTP
- SSH/NETCONF/HTTPS
- NetFlow

Recommendations for Wireless Management Interface

The Wireless Management Interface is a Layer 3 interface, which can be configured only with a single IP address (IPv4 or IPv6) or using a dual-stack configuration.

It is always recommended to use a wireless management VLAN and configure WMI as a Switched VLAN Interface (SVI). If the uplink port or port-channel to the next-hop switch is configured as a dot1q trunk, the wireless management VLAN would be one of the allowed tagged VLAN on the trunk.

The recommendation is true, independent of the deployment mode of APs (local, FlexConnect, or SDA) with the following exceptions:

- The WMI is configured as an L3 port for Cisco Catalyst 9800 Wireless Controller deployed in a Public Cloud environment.
- The WMI is configured as a loopback interface for embedded wireless controller in Cisco Catalyst 9000 switches.

It is always recommended to statically assign IPv6 address in WMI and not configure using the **ipv6 auto-config** command.

Note The **ipv6 auto-config** command is not supported.

Note You can use only one AP manager interface on Cisco Catalyst 9800 Wireless Controller called the WMI to terminate CAPWAP traffic.

Note There is only one Wireless Management Interface (WMI) on the controller.

Note Layer 3 interface is not supported in Cisco Catalyst 9800-CL Cloud Wireless Controller Guest anchor scenarios.

Instead, it is recommended to use the Layer 2 interfaces and SVI for WMI.

It is recommended to use Layer 3 interface for Public cloud deployments only and not for on-premise as it poses some limitations.

The following are the sample Layer 3 and Layer 2 interface configurations:

Layer 3 interface configuration:

```
interface GigabitEthernet2
no switchport
ip address <ip_address> <mask>
negotiation auto
no mop enabled
no mop sysid
end
```

Layer 2 interface configuration:

```
interface GigabitEthernet2
switchport trunk allowed vlan 25,169,504
switchport mode trunk
negotiation auto
no mop enabled
no mop sysid
end
```

Note To change the WMI interface when RMI is configured, perform the following:

1. Unconfigure the RMI, save the changes using the **write memory** command, and reload the controller.
2. Change the WMI interface.
3. Reconfigure the RMI in the same interface as WMI, save the changes using the **write memory** command, and reload the controller.

Configuring your Controller with Wireless Management Interface (CLI)

You can configure the Wireless Management interface using CLI by directly accessing the physical console (for the Cisco Catalyst 9800 appliances) (or) using the virtual console in case of the Cisco Catalyst 9800-CL Cloud Wireless Controller.

Note The example assumes that:

- You have a Cisco Catalyst 9800-CL Cloud Wireless Controller and the GigabitEthernet 2 is connected to a trunk interface on the uplink switch.
- You want to configure multiple VLANs and dedicate one for Wireless Management interface.

Procedure

Step 1 Access the CLI using VGA or monitor console from the hypervisor of your choice.

Step 2 Terminate the configuration wizard.

```
Would you like to enter the initial configuration dialog? [yes/no]:
no
Would you like to terminate autoinstall? [yes]:
yes
```

Step 3 Enter the configuration mode and add the login credentials using the following command:

```
Device# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# username <name> privilege 15 password <yourpwd>
```

Step 4 (Optional) Set a hostname.

```
Device(config)# hostname C9800
```

Step 5 Configure the VLAN for wireless management interface:

```
Device(config)# vlan 201
Device(config-vlan)# name wireless_management
```

Step 6 Configure the L3 SVI for wireless management interface:

```
Device(config)# int vlan 201
Device(config-if)# description wireless-management-interface
Device(config-if)# ip address 172.16.201.21 255.255.255.192
Device(config-if)# no shutdown
```

Step 7 Configure the interface GigabitEthernet 2 as trunk and allow the wireless management VLAN:

```
Device(config-if)# interface GigabitEthernet2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk allowed vlan 201,210,211
Device(config-if)# shut
Device(config-if)# no shut
```

Note VLANs 210 and 211 are added to the trunk to carry client traffic.

Step 8 Configure a default route (or a more specific route) to reach the device:

```
Device(config-if)# ip route 0.0.0.0 0.0.0.0 172.16.201.1
```

At this point you can use SSH or Telnet, or GUI to access the device, or use the Cisco Catalyst Center or Cisco Prime to continue with the DAY 0 configuration.

Verifying Wireless Management Interface Settings

To verify if the Layer 3 interface is configured correctly, use the following command:

```
Device# show run int vlan 201

Building configuration...

Current configuration : 128 bytes
!
interface Vlan201
 description wireless-management-interface
 ip address 172.16.201.21 255.255.255.0
 no mop enabled
 no mop sysid
end
```

To verify if the wireless management VLAN is active on the uplink to the network, use the following command. In this case the uplink is a trunk interface, so the VLAN needs to be active and forwarding state.

```
Device# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi2         on               802.1q         trunking      1
.....
Port        Vlans allowed on trunk
Gi2         201,210-211
.....
Port        Vlans allowed and active in management domain
Gi2         201,210-211
....
Port        Vlans in spanning tree forwarding state and not pruned
Gi2         201,210-211
....
```

To verify if the wireless management interface is up, use the following command:

```
Device# show ip int brief | i Vlan201
Vlan201   172.16.201.21  YES NVRAM  up  up
```

To verify if the selected interface has been configured as wireless management, use the following command:

```
Device# show wireless interface summary

Wireless Interface Summary

Interface Name Interface Type VLAN ID IP Address     IP Netmask   NAT-IP Address MAC Address
-------------------------------------------------------------------------------------------
Vlan201      Management      201   172.16.201.21  255.255.255.0  0.0.0.0     001e.e51c.a7ff
```

Information About Network Address Translation (NAT)

NAT enables private IP networks that use non-registered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses from the internal network into public addresses. NAT can be configured to advertise to the outside world only few addresses for the entire internal network. This ability provides more security by effectively hiding the private network details.

If you want to deploy your Cisco Catalyst 9800 Wireless Controller on a private network and make it reachable from internet, you need to have the controller behind a router, firewall, or other gateway device that uses one-to-one mapping Network Address Translation (NAT).

To do so, perform the following:

- Configure the NAT device with 1:1 static mapping of the Wireless Management interface IP address (private IP) to a unique external (public) IP address configured on the NAT device.
- Enable the NAT feature on the Wireless Controller and specify its external public IP address. This public IP is used in the discovery responses to APs, so that the APs can then send CAPWAP packets to the right destination.
- Make sure that the external APs discover the public IP of the controller using DHCP, DNS, or PnP.

Note You need not enable NAT if the Cisco Catalyst 9800 Wireless Controller is deployed with a public address. Instead you will need to configure the public IP directly on the Wireless Management Interface (WMI).

Information About CAPWAP Discovery

In a CAPWAP environment, a lightweight access point discovers a wireless controller by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the controller. The controller sends a CAPWAP join response to the access point that allows the access point to join the controller.

If the wireless controller is behind a NAT device, the controller responds to the discovery response in the following ways:

- Using the public IP.
- Using the private IP.
- Using public and private IP.

The Public IP needs to be mapped to the controller's Private IP using static 1:1 NAT configuration on the router or firewall performing the NAT translation.

If your wireless controller manages only Access Points reachable through the public internet (external APs), you need to configure the controller so it responds with only the Public IP in the discovery response.

If your wireless controller manages both internal and external APs, you need to configure the controller so it responds with both Public and Private IPs in the discovery response.

Note In NAT deployments, the APs running internally and externally must use different AP join profiles with CAPWAP Discovery Private and Public enabled separately. This applies to APs upgraded to Cisco IOS XE 17.12.x and later.

Configuring Wireless Management Interface with a NAT Public IP (CLI)

The first step is to configure the controller to use the public NAT IP (this is the public IP that has been configured on the NAT device to statically map 1:1 the WMI's private IP address).

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless management interface** *interface-type interface-number* **Example:** `Device(config)# wireless management interface vlan 20`	Defines the management interface. Here, • *interface-type*—Refers to the VLAN, Gigabit, or loopback types. • *interface-number*—Is the interface number.
Step 3	**public-ip** *external-public-ip* **Example:** `Device(config-mgmt-interface)# public-ip 2.2.2.2`	Defines the external NAT or Public IP.
Step 4	**end** **Example:** `Device(config-mgmt-interface)# end`	Returns to privileged EXEC mode.

Configuring CAPWAP Discovery to Respond Only with Public or Private IP (CLI)

Note By default, if the wireless management interface is configured with a public IP, the controller responds with both Public and Private IP in the CAPWAP discovery response.

The setting to determine the IP (private or public) to include in the discovery response is available in the AP Join profile.

Configuring the Controller to Respond only with a Public IP (CLI)

Configure the Controller to respond only with a Public IP using commands.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**no capwap-discovery private** **Example:** `Device(config-ap-profile)# no capwap-discovery private`	Instructs the controller to not respond with the internal IP. Enables AP to join the controller over Public IP only.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Configuring the Controller to Respond only with a Private IP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**no capwap-discovery public** **Example:** `Device(config-ap-profile)# no capwap-discovery public`	Instructs the controller to not respond with the public IP. Enables AP to join the controller over private IP only.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Verifying NAT Settings

Verify NAT Settings using commands.

```
Device# show wireless interface summary

Wireless Interface Summary

Interface Name Interface Type VLAN ID IP Address     IP Netmask     NAT-IP Address   MAC
Address
-----------------------------------------------------------------------------------------------
Vlan20         Management     20      10.58.20.25    255.255.255.0  2.2.2.2    001e.4963.1cff
```

To verify the settings in the AP join profile, use the following command

```
Device# show run | b ap profile

ap profile default-ap-profile
 no capwap-discovery private
 description "default ap profile"
...
```