Wireless Management Interface

- Wireless management interfaces, on page 1
- WMI Configuration Tasks, on page 3
- Network address translation, on page 6

Wireless management interfaces

The Wireless Management Interface (WMI) is a mandatory Layer 3 interface on the controller that

- supports all communications between the controller and access points,
- enables Control And Provisioning of Wireless Access Points (CAPWAP) or inter-controller mobility messaging and tunneling traffic, and
- serves as the default interface for in-band management and connectivity to enterprise services such as AAA, syslog, and SNMP.

You can use the WMI IP address to connect to the device using SSH or Telnet. You can also access the GUI through HTTP or HTTPS by entering the WMI IP address in a browser address field.

Supported Protocols

Starting from Cisco IOS XE Release 17.6.1, the controller can use Ethernet Service Port (SP) (Management Interface VRF or GigabitEthernet 0) for specific management or control plane protocols

Supported protocols for the WMI include:

- Simple Network Management Protocol (SNMP)
- RADIUS (both for user authentication to the controller and wireless client authorization)
- TACACS+
- Syslog
- Network Time Protocol (NTP)
- SSH, Network Configuration Protocol (NETCONF), or HTTPS
- NetFlow

Best practices and restrictions for WMI

Best practices for WMI

- **IP Address Configuration**: Configure the Wireless Management Interface (WMI) with a single IP address, either IPv4 or IPv6. Alternatively, use a dual-stack configuration for flexibility in addressing.
- **IPv6 Recommendations**: Assign a static IPv6 address in WMI. Do not configure the IPv6 address using the **ipv6 auto-config** command for the WMI.
- Always use a dedicated wireless management VLAN and configure the WMI as a Switched VLAN Interface (SVI).
- If you configure the uplink port or port channel to the next-hop switch as a dot1q trunk, ensure the wireless management VLAN is allowed or tagged on the trunk.

This recommendation is applicable to all AP deployment modes (local, FlexConnect, or SDA).

The recommendation is not applicable for certain scenarios:

- The WMI is a Layer 3 port on a controller deployed in a public cloud.
- The WMI is a loopback interface for embedded wireless controller in Cisco Catalyst 9000 switches.

Restrictions

- Only one WMI is allowed on a controller.
- Use only a Layer 2 interface or anA SVI to configure the WMI.
- Do not use a Layer 3 interface for guest anchor scenarios.
- Use a Layer 3 interface for public cloud deployments only.
- Use the WMI to terminate CAPWAP traffic.
- The **ipv6 auto-config** command is not supported.

Change the WMI interface when RMI is configured

Occasionally, you may need to change the Wireless Management Interface (WMI). If Redundant Management Interface (RMI) is configured on your network, this task shows you how to change the WMI interface.

Procedure

Step 1 Remove all RMI configurations.

Step 2 Save the changes using the **write memory** command.

Step 3 Reload the controller.

Step 4 Change the WMI interface.

Step 5 Reconfigure the RMI to use the same interface as the WMI.

Step 6 Save the changes using the **write memory** command.

Step 7 Reload the controller.

The WMI interface is changed, and the RMI is reconfigured to match, maintaining operational consistency.

WMI Configuration Tasks

Migrate VLANs safely for wireless management

Safely migrate from VLAN A to VLAN B for wireless management, ensuring all devices—including those behind Workgroup Bridges (WGB)—continue to correctly receive multicast traffic.

Caution Do not remove VLAN A or SVI A before creating VLAN B or SVI B and associating SVI B with WMI. This sequence is critical to prevent multicast traffic issues.

Procedure

Step 1 Create VLAN B on the relevant network switches.

Step 2 Configure SVI B (Switched Virtual Interface for VLAN B).

Step 3 Associate SVI B with the WMI interface.

Step 4 Verify multicast traffic is flowing correctly to all devices, including those behind WGBs.

Step 5 Once functionality is confirmed, remove VLAN A from the network configuration.

Step 6 Delete SVI A (Switched Virtual Interface for the old VLAN).

Step 7 Document changes and monitor for any multicast or connectivity issues.

The VLANs are migrated, and multicast traffic is properly received by all devices, including those behind WGBs.

Sample interface configuration

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
```

Configure the WMI interface of a controller (CLI)

Configure the WMI interface on a controller using the CLI.

Set up a controller, and assign a dedicated VLAN and interface for wireless management.

The examples assume the GigabitEthernet 2 interface connects to a trunk interface and that you want to configure multiple VLANs and dedicate one of them for the WMI interface.

Before you begin

- Ensure you have physical console access (for the Cisco Catalyst 9800 Series Wireless Controller Appliance) or a virtual console access (Cisco Catalyst 9800 Series Wireless Controller for Cloud).
- Determine your management VLAN, interface IP address, and credentials.

Procedure

Step 1 Access the CLI using Video Graphics Array(VGA) or monitor console from your preferred hypervisor.

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 global configuration mode and configure the login credentials.

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

Step 4 Set a hostname.

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

Step 5 Configure the VLAN for the wireless management interface.

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

Step 6 Configure the Layer 3 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 an interface 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
```

The controller is configured with a dedicated wireless management VLAN and SVI. You can access the device using SSH, telnet, or GUI. You can use the Cisco Catalyst Center or Cisco Prime Infrastructure to continue with the Day 0 configuration.

Verify WMI Settings

Verify if the Layer 3 interface is configured correctly.

```
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
```

Verify if the wireless management VLAN is active on the uplink to the network. 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
....
```

Verify if the wireless management interface is up.

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

Verify if the selected interface has been configured as wireless management.

```
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
```

Network address translation

Network Address Translation (NAT) is a networking mechanism that

- enables private IP networks that use non-registered IP addresses to connect to the Internet
- translates private addresses from the internal network into public addresses before forwarding packets onto another network, and
- provides security by effectively hiding the private network details through advertising only few addresses for the entire internal network.

NAT deployment with Cisco Catalyst 9800 wireless controller

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 these steps:

- 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 Certain ISP routers performing NAT may assign the same public source PORT to different APs. This results in the WLC receiving CAPWAP traffic from same IP:PORT but from different APs. The controller is unable to differentiate the packets are from diffrernent APs, even if packet A is for DATA and Packet B is for CTRL. The controller does not support CAPWAP connections from different APs behind NAT using same SRC IP:PORT.

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).

The IPv6 addresses that are not supported are:

- IPv6 Documentation addresses - 2001:db8::/32
- IPv6 Site Local addresses - fec0::/10
- IPv6 Link Local addresses - fe80::/10
- IPv6 Loopback addresses - ::1
- IPv6 Multicast addresses - FF00::/8

CAPWAP discovery

CAPWAP discovery is a network mechanism that

- enables lightweight access points to discover wireless controllers using CAPWAP discovery mechanisms
- facilitates CAPWAP join requests from access points to controllers, and
- allows controllers to send CAPWAP join responses to access points for joining the controller.

NAT environment response methods

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 behaviour was introduced from the 17.9.5 release and applies to APs upgraded to Cisco IOS XE 17.9.5, 17.9.6, 17.9.m (m>=5), 17.12.n (n>=1) and later releases.

Configure wireless management interface with a NAT public IP (CLI)

Enable the controller to use a public NAT IP address for wireless management interface communication.

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). This configuration allows the wireless management interface to operate in NAT environments where public IP access is required.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Define the management interface.

Example:

```
Device(config)# wireless management interface interface-type interface-number
```

Example:

```
Device(config)# wireless management interface vlan 20
```

- *interface-type*: Refers to the VLAN, Gigabit, or loopback types.
- *interface-number*: Is the interface number.

Step 3 Define the external NAT or Public IP.

Example:

```
Device(config-mgmt-interface)# public-ip external-public-ip
```

Example:

```
Device(config-mgmt-interface)# public-ip 2.2.2.2
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-mgmt-interface)# end
```

The wireless management interface is now configured with the NAT public IP and can communicate through the NAT device using the specified public IP address mapping.

CAPWAP discovery IP response configuration

CAPWAP discovery IP response configuration is a wireless controller setting that controls which IP addresses the controller includes in CAPWAP discovery responses to access points.

CAPWAP discovery response behavior

The controller's IP response behavior in CAPWAP discovery varies based on configuration:

- **Default behavior**: 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.
- **Configurable setting**: The setting to determine the IP (private or public) to include in the discovery response is available in the AP Join profile.

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

Enable APs to join the controller over public IP only by preventing responses with internal IP addresses.

Configure the Controller to respond only with a Public IP using commands when you need to restrict AP discovery to public interfaces only.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile and enter AP profile configuration mode.

Example:

```
Device(config)# ap profile profile-name
```

Example:

```
Device(config)# ap profile xyz-ap-profile
```

Step 3 Instruct the controller to not respond with the internal IP.

Example:

```
Device(config-ap-profile)# no capwap-discovery private
```

Enables AP to join the controller over Public IP only.

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

The controller is now configured to respond only with public IP addresses, ensuring that APs can only join using the public interface.

Configure the controller to respond only with a private IP (CLI)

Configure the controller to respond only with private IP addresses during CAPWAP discovery.

This configuration ensures that access points join the controller using private IP addresses instead of public IP addresses, which is useful in network environments where direct public IP communication should be restricted.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile and enter AP profile configuration mode.

Example:

```
Device(config)# ap profile profile-name
```

Example:

```
Device(config)# ap profile xyz-ap-profile
```

Step 3 Instruct the controller to not respond with the public IP.

Example:

```
Device(config-ap-profile)# no capwap-discovery public
```

Enable AP to join the controller over private IP only.

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

The controller is now configured to respond only with private IP addresses during CAPWAP discovery, ensuring APs join using private network connections.

Verify 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 this command

```
Device# show run | b ap profile

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