



Configure Network Address Translation for Wireless Management IP

- [Network address translation, on page 1](#)

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 different 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:
<code>Device# configure terminal</code> |
| Step 2 | Configure an AP profile and enter AP profile configuration mode.
Example:
<code>Device(config)# ap profile profile-name</code>
Example:
<code>Device(config)# ap profile xyz-ap-profile</code> |
| Step 3 | Instruct the controller to not respond with the internal IP.
Example:
<code>Device(config-ap-profile)# no capwap-discovery private</code>
Enables AP to join the controller over Public IP only. |
| Step 4 | Return to privileged EXEC mode.
Example:
<code>Device(config-ap-profile)# end</code> |
-

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

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"
...
```