Information About NAT Support

Network Address Translation (NAT) allows a device to act as an agent between the Internet (public) and a local network (private). It maps the controller's intranet IP addresses to a corresponding external address. The AP-manager interface of the controller must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

The master AP in an Embedded Wireless Controller (EWC) network performs NAT on the wireless client traffic. This is achieved by translating the public and private IP addresses of the clients. Depending on the placement and number of NATs, the translation may be required at one or both ends of the tunnel.

The master AP performs NAT for the guest WLAN. However, this is not required for the employee WLAN. The IP address for the clients connected to the guest WLAN is provided by the internal DHCP server running on the master AP, whereas the clients connected to the employee WLAN gets the IP address from an external DHCP server.

The master AP acts as a gateway to the traffic coming from the clients connected to the NAT-ed WLAN and performs address translation. The clients connected to the non NAT-ed WLAN uses the gateway provided by the external DHCP server to send the traffic.

For centralized NAT WLANs, the controller provisions the VLAN mapping to the specific WLAN. When performing NAT, both the private IP address (address in the network before the NAT device) and the public IP address (address in the public network) has to be configured.

The external DHCP server provides the IP addresses for the APs. The master AP requires two IP addresses, one for the internal AP and one for when it is acting as a wireless controller. The internal DHCP server is not used to assign IP addresses to the APs connected to the network. The external DHCP server is used to provide the IP address to the clients on non- NAT-ed WLANs.

Restrictions for NAT Support

- When centralized NAT is enabled, wired to wireless client traffic on the same VLAN is not supported.

- The WLAN, where centralized NAT is enabled, must also be provisioned on the master AP.

- Client DHCP server must run on the EWC for centralized NAT to work. External DHCP servers are not supported.

Enabling Centralized NAT on a VLAN

Procedure

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

Step 2	**wireless ewc-ap centralized-nat vlan** *vlan-id*
	
	Example:
	`Device(config)# wireless ewc-ap`
	`centralized-nat`
	`test-vlan 10`
		Enables centralized NAT on a VLAN.

Step 3	(Optional) **wireless ewc-ap centralized-nat vlan** *vlan-id* **peer-blocking**
	
	Example:
	`Device(config)# wireless ewc-ap`
	`centralized-nat`
	`test-vlan 10 peer-blocking`
		Configures peer to peer blocking.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying NAT Support

To view the history of the AP datapath programming for centralized NAT, use the below command:

```
Device# show wireless mob-exp centralized-nat history

Centralized NAT Global event history:
Timestamp Event RC Context
------------------------- ----------- ---- -------
06/17/2019 05:28:39.962760 Route add 0 100.100.100.0/255.255.255.0 0.0.0.0 2
06/17/2019 05:28:39.961794 VLAN update 0 0-4095 0,10 1,100 1
06/17/2019 05:28:39.961162 Route add 0 10.10.10.0/255.255.255.0 0.0.0.0 1
Centralized NAT AP DP plumbing client event history:
Timestamp Event RC Context
------------------------- ----------- ---- -------
06/17/2019 05:37:55.827602 Client del 0 10.10.10.3
06/17/2019 05:37:55.826296 Client del 0 10.10.10.3
06/17/2019 05:37:32.160737 Client add 0 MAC b8:27:eb:27:f3:f6, IP 10.10.10.4, WLAN 2
06/17/2019 05:37:31.454851 Client del 0 10.10.10.4
06/17/2019 05:37:31.453479 Client del 0 10.10.10.4
06/17/2019 05:36:25.659639 Client add 0 MAC b8:27:eb:27:f3:f6, IP 10.10.10.4, WLAN 1
06/17/2019 05:35:52.513500 Client add 0 MAC b8:27:eb:be:08:ea, IP 10.10.10.3, WLAN 1
```

To view the NAT status, use the below command on the AP:

```
Device# show flexconnect ewc-ap nat status
Programmed WLC IP
9.9.71.50
Programmed Vlan Config
output 0: vlan 0-9,11-4095
output 1: vlan 10
Programmed Route Table
0.0.0.0/0 1.1.1.1                          0
10.10.10.0/24 -                           2
NAT and P2P Block Status:
WLAN    NAT-Enabled        P2P-Block
  0       false              false
  1       true               false
```