VLAN Groups

- VLAN groups, on page 1
- Prerequisites for VLAN groups, on page 2
- Restrictions for VLAN groups, on page 2
- Create a VLAN Group (GUI), on page 2
- Create a VLAN Group (CLI), on page 3
- Add a VLAN group to policy profile (GUI), on page 3
- Add a VLAN group to a policy profile (CLI), on page 4
- View the VLANs in a VLAN group, on page 5

VLAN groups

A VLAN group is a wireless network configuration feature that

- enables assignment of multiple VLANs to a single policy profile
- dynamically allocates a wireless client to a VLAN within the group based on the client's MAC address, and
- manages VLAN availability and integrity by marking VLANs as *Dirty* when the clients are unable to receive IP addresses using DHCP.

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN associated with the policy profile mapped to the WLAN. In a large venues, such as an auditorium, stadiums, or conference rooms with numerous wireless clients, managing connections using only a single WLAN can be challenging.

The clients can be assigned to one of the configured VLANs. This feature maps a policy profile to a single VLAN or to multiple VLANs using VLAN groups. A VLAN is assigned to the client, and the client receives the IP address from the assigned VLAN.

The system might not clear the *Dirty* flag from the VLAN, even after 30 minutes, for a VLAN group. After 30 minutes, when the VLAN is marked as non-dirty, new clients in the IP Learn state can be assigned IP addresses from the VLAN if available IPs exist in the pool and the DHCP scope is configured correctly. This is expected because the timestamp of each interface must be checked to confirm it exceeds 30 minutes, which results in a 5-minute lag before the global timer expires.

Note The Controller marks the VLAN interface as *Dirty* when three or more clients fail to receive IP addresses through DHCP. The VLAN interface is marked *Dirty* if the VLAN *Dirty* counter increases as a result of an ***IP Learn Failure***, which occurs when a client sends three DHCP discoveries without receiving a response. This occurs before the client is deleted due to an ***IP Learn Timeout***.

Each client receives a unique hash value derived from its MAC address. This approach ensures that clients from the same vendor, which may differ only by a few bits, do not cause incorrect *Dirty* VLAN markings.

Prerequisites for VLAN groups

Review the required condition for VLAN group.

- A VLAN should be present in the device for it to be added to the VLAN group.
- IP MAC binding should be configured on a policy profile that uses a VLAN group.

Restrictions for VLAN groups

Follow these restrictions when configuring VLAN groups:

- If the number of VLANs in a VLAN group exceeds 32, the mobility functionality might not work as expected and Layer 2 multicast might break for some VLANs. Therefore, it is the responsibility of network administrators to configure a feasible number of VLANs in a VLAN group. The VLANs mapped in a group must be present in the controller for the VLAN Groups feature to work as expected.
- The VLAN Groups feature works for APs in local mode.
- The VLAN Groups feature operates only in central switching mode; it cannot be used in FlexConnect local switching mode.
- The ARP Broadcast feature is not supported on VLAN groups.
- Multicast with VLAN group is only supported for access points in local mode. A multicast VLAN is required when a VLAN group is configured and multicast traffic is used.
- When configuring VLAN groups with multiple VLANs, and each VLAN is used by a different subnet, clients with static IP addresses might be assigned to an incorrect VLAN if SVIs are not present on the controller. For every VLAN in the VLAN group, configure an SVI interface with a valid IP address.

Create a VLAN Group (GUI)

Create a VLAN group to assign multiple VLAN IDs efficiently in the network using the GUI.

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN Group**.

Step 2 Click **Add**.

Step 3 Set the **VLAN GROUP** name and the list of **VLANS**.

This can be a range, or a set of comma-separated values.

Step 4 Enter the VLAN name in the **Name** field.

Configure the other parameters if required.

Step 5 Click **Update & Apply to Device**.

Create a VLAN Group (CLI)

Create a VLAN group for network segmentation and traffic management using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a VLAN group with the given group name and add all the VLANs listed in the command.

Example:

```
Device(config)# vlan group vlangrp1 vlan-list 91-95.
```

The VLAN list ranges from 1 to 4096 and the maximum number of VLANs supported in a group is 64.

Step 3 Exit the global configuration mode and return to the privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, press *CTRL-Z* to exit the global configuration mode.

Add a VLAN group to policy profile (GUI)

Assign a VLAN group to an existing policy profile, enabling client traffic association with the specified VLANs using commands.

The policy profile consists mainly of network and switching policies. The policy profile is a reusable entity that can be applied to multiple tags. When you apply a client policy to the AP or controller, the policy profile includes it. Examples are VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, Bonjour profile, local profiling, device classification, and BSSID QoS. However, all security attributes and features related to wireless on the WLAN are grouped under the WLAN profile.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click on a policy profile name.

Step 3 Click on the **Access Policies** tab.

Step 4 Under **VLAN** section, select a a VLAN or VLAN Group from the **VLAN/VLAN Group** drop-down list.

Step 5 Click **Update & Apply to Device**.

Add a VLAN group to a policy profile (CLI)

Map a specific VLAN group to a WLAN policy profile using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN policy profile.

Example:

```
Device(config)# wireless profile policy my-wlan-policy
```

Step 3 Map the VLAN group to the WLAN by entering the group name.

Example:

```
Device(config-wireless-policy)# vlan myvlan-group
```

Step 4 Exit the global configuration mode and return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

View the VLANs in a VLAN group

These commands let you view VLAN group information and VLAN assignments:

Command	Description
show vlan group	Displays the list of VLAN groups with name and the VLANs that are configured.
show vlan group group-name *group_name*	Displays the specified VLAN group details.
show wireless client mac-address *client-mac-addr* **detail**	Displays the VLAN group assigned to the client.
show wireless vlan details	Displays VLAN details.