VLAN Groups

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the policy profile mapped to the WLAN. In a large venue, such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN group feature uses a single policy profile that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a policy profile to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN.

The system marks VLAN as *Dirty* for 30 minutes when the clients are unable to receive IP addresses using DHCP. 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 non-dirty, new clients in the IP Learn state can get assigned with IP addresses from the VLAN if free IPs are available in the pool and DHCP scope is defined correctly. This is the expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

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 deemed *Dirty* using the Non-Aggressive method, which involves counting one failure per association per client that surpasses the predefined **IP_LEARN_TIMEOUT** duration of 120 seconds. If a client sends a new association request before the **IP_LEARN_TIMEOUT** elapses, it will not be considered a failed client.

In Non-Aggressive method, each client gets a unique hash value derived from its MAC address. This approach ensures that clients belonging to the same vendor, which may differ only by a few bits, do not mistakenly trigger the *Dirty* marking of a VLAN.

Prerequisites for VLAN Groups

- A VLAN should be present in the device for it to be added to the VLAN group.

Restrictions for 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.

  For the VLAN Groups feature to work as expected, the VLANs mapped in a group must be present in the controller.
- The VLAN Groups feature works for access points in local mode.
- The VLAN Groups feature works only in central switching mode and it cannot be used in FlexConnect local switching mode.
- ARP Broadcast feature is not supported on VLAN groups.
- VLAN group Multicast with VLAN group is only supported in local mode AP. Multicast VLAN is required when VLAN group is configured and uses multicast traffic.
- While you configure VLAN groups with multiple VLANs and each VLAN is used by a different subnet, clients having static IP addresses might be assigned to a wrong VLAN if SVIs are not present on the controller. Hence, for every VLAN that belongs to the VLAN group, ensure that you configure an SVI interface with a valid IP address.

Creating a VLAN Group (GUI)

Procedure

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

Step 2 On the **VLAN** > **VLAN** page, click **Add**.

Step 3 Enter the VLAN ID in the **VLAN ID** field.

The valid range is between 2 and 4094.

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

Configure the other parameters if required.

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

Creating a VLAN Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Device(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the maximum number of VLANs supported in a group is 64.

Step 3	**end**
	Example:
	`Device(config)#end`
		Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Adding a VLAN Group to Policy Profile (GUI)

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for the client that is applied on the AP or controller is moved to the policy profile. For example, VLAN, ACL, QOS, Session timeout, Idle timeout, AVC profile, Bonjour profile, Local profiling, Device classification, BSSID QoS, etc. However, all wireless related security attributes and features 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 **Access Policies** tab.

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

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

Adding a VLAN Group to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy my-wlan-policy`	Configures the WLAN policy profile.
Step 3	**vlan** *vlan-group1* **Example:** `Device(config-wireless-policy)# vlan myvlan-group`	Maps the VLAN group to the WLAN by entering the group name.

Step 4	**end**
	Example:
	`Device(config-wlan)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Viewing the VLANs in a VLAN Group

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.

VLAN Group Support for DHCP and Static IP Clients

When a static IP client joins a VLAN group, the controller adds it to a VLAN based on VLAN computation logic. If the client's static IP address isn't part of the VLAN's IP list, the client fails to get internet access, even if the client is authenticated and authorized. The VLAN Group to Support DHCP and Static IP Clients feature aims to handle the network access of such clients. This feature only supports IPv4 clients and is enabled by default. However, ensure that the **ipv4 dhcp required** command is not configured on the wireless policy profile, because this disables the feature, causing the client to be stuck in the IP learn state.

Prerequisites

- Ensure that a switch VLAN interface (SVI) is configured with the IP address.

Restrictions

- FlexConnect local switching and FlexConnect local authentication are not supported. Only Local mode, FlexConnect central switching, and FlexConnect central authentication are supported.
- IPv6 is not supported.
- The peer controller cannot have a VLAN group in the policy profile, because a VLAN group with static IP mobility is not supported.

Supported Features

Table 1: Supported Features

Feature	Support
Guest Anchor	Yes
Mobility	Yes
RLAN	Yes
SVI	Yes Ensure that you configure SVI with an IP address in the same subnet as that of the client's IP address.
IRCM support: Guest AireOS as anchor and Cisco Catalyst 9800 controller as foreign	Yes
IRCM support : Guest AireOS as foreign and Cisco Catalyst 9800 controller as anchor	Yes The client is excluded if there is no match for the SVI.