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 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 clients can get assigned to one of the configured VLANs. 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. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

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.

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

- The number of VLANs mapped to a VLAN group is not limited by Cisco IOS XE software release. However, if the number of VLANs in a VLAN group exceeds the recommended value of 32, the mobility functionality might not work as expected and in the VLAN group, L2 multicast breaks for some VLANs.

Therefore, it is the responsibility of network administrators to configure 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 device. The static IP client behavior is not supported.

Configuring VLAN Groups

The following sections provide information about the various VLAN Group configuration tasks:

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 recommended number of VLANs 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.

Removing a VLAN Group (GUI)

Procedure

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

Step 2 On the **VLAN** > **VLAN Group** page, check the checkbox adjecent to the VLAN Group you want to delete .

To delete multiple VLAN Groups, select multiple VLAN Groups checkboxes.

Step 3 Click **Delete**.

Step 4 Click **Yes** on the confirmation window to delete the VLAN Group.

Removing 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 recommended number of VLANs in a group is 64.
Step 3	**no vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Device(config)#no vlan group vlangrp1 vlan-list 91-95`	Removes the VLAN group with the given group name (vlangrp1).
Step 4	**end** **Example:** `Device(config)#end`	Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit global configuration mode.

Adding a VLAN Group to a WLAN (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 **Add** to configure the following:

- General
- Access Policies
- QOS and AVC
- Mobility
- Advanced

Step 3 In the **General** tab, proceed as follows:

a) Enter a name and description for the policy profile.
b) To enable the policy profile, set **Status** as *Enabled*.
c) Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.
d) In the **CTS Policy** section, choose the appropriate status for the following:
   - Inline Tagging
   - SGACL Enforcement
e) Specify a default SGT. The valid range is from 2 to 65519.
f) In the **WLAN Switching Policy** section, choose the appropriate status for the following:
   - Central Switching
   - Central Authentication
   - Central DHCP
   - Central Association Enable
   - Flex NAT/PAT
g) Click **Save & Apply to Device**.

Step 4 In the **Access Policies** tab, proceed as follows:

a) Choose the appropriate status for the following:
   - HTTP TLV Caching
   - RADIUS Profiling
   - DHCP TLV Caching
b) Choose a **Local Subscriber Policy Name**.
c) Choose the required **VLAN/VLAN Group**.
d) Specify the multicast VLAN.
e) Choose the required **IPv4 ACL** and **IPv6 ACL**.
f) Choose the required **Pre Auth** and **Post Auth** URL filters.

g) Click **Save & Apply to Device**.

Step 5 In the **QoS and AVC** tab, proceed as follows:

a) Choose the required **Auto QoS**.

b) Specify the **Egress** and **Ingress** details for the following:

- **QoS SSID Policy**
- **QoS Client Policy**
- **Flow Monitor IPv4**
- **Flow Monitor IPv6**

c) In the **SIP-CAC** section, choose the appropriate status for the following:

- Call Snooping
- Send Disassociate
- Send 486 Busy

d) Click **Save & Apply to Device**.

Step 6 In the **Mobility** tab, proceed as follows:

a) Choose the **Export Anchor** check box to enable export anchor, if required.

b) Use the slider to enable or disable **Static IP Mobility**.

c) From the list of **Available** anchors, select the required anchors and move them to the list of **Selected** anchors.

d) Click **Save & Apply to Device**.

Step 7 In the **Advanced** tab, proceed as follows:

a) Specify the following **WLAN Timeout** details:

- Session Timeout
- Idle Timeout
- Idle Threshold
- Client Exclusion Timeout

b) In the **DHCP** section, choose **DHCP Enable** check box and enter the DHCP server IP address.

c) Choose the appropriate status for the following:

- DHCP Option 82 Enable
- DHCP Option 82 ASCII
- DHCP Option 82 RID
- DHCP Option 82 Format
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC

- DHCP AP NAME
- DHCP Policy Tag
- DHCP AP Location
- DHCP VLAN ID

d) In the **AAA Policy** section, choose the appropriate status for the following:
   - Allow AAA Override
   - NAC State

e) Choose the policy name and accounting list.
f) If required, enable **Fabric Profile** and choose from the list of profiles available.
g) From the **Umbrella Parameter Map**, choose an appropriate parameter map.
h) In the **WLAN Flex Policy** section, choose the appropriate status for the following:
   - VLAN Central Switching
   - Split MAC ACL

i) In the **Air Time Fairness Policies** section, choose the appropriate status for the following:
   - 2.4 GHz Policy
   - 5 GHz Policy

j) Click **Save & Apply to Device**.

Adding a VLAN Group to a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**end** **Example:** `Device(config-wlan)#end`	Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit global configuration mode.

Viewing the VLANs in a VLAN Group (CLI)

Command	Description
show vlan group	Displays the list of VLAN groups with name and the VLANs that are available.
show vlan group group-name *group_name*	Displays the specified VLAN group details.