Troubleshooting VLANs

- About Troubleshooting VLANs, on page 1
- Guidelines and Limitations for Troubleshooting VLANs, on page 1
- Initial Troubleshooting VLANs Checklist, on page 2
- Troubleshooting VLAN Issues, on page 3

About Troubleshooting VLANs

VLANs provide a method of isolating devices that are physically connected to the same network but are logically considered to be part of different LANs that do not need to be aware of one another.

You should use only the following characters in a VLAN name:

- a through z or A through Z
- 0 through 9
- - (hyphen) or _ (underscore)

Guidelines and Limitations for Troubleshooting VLANs

Follow these guidelines when configuring VLANs:

- Keep user traffic off the management VLAN; keep the management VLAN separate from user data.
- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.
- VACLs that apply to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.
- If you do not map the secondary VLAN to the Layer 3 VLAN interface of the primary VLAN, you can have different VACLs for primary and secondary VLANs.
- IGMP runs only on the primary VLAN and uses the configuration of the primary VLAN for all secondary VLANs.
- Any IGMP join request in the secondary VLAN is treated as if it is received in the primary VLAN.

- A destination SPAN port cannot be an isolated port. (However, a source SPAN port can be an isolated port.)
- You can configure SPAN to span both primary and secondary VLANs or, alternatively, to span either one if you are interested only in ingress or egress traffic.
- A MAC address learned in a secondary VLAN is placed in the shared table of the primary VLAN. When the secondary VLAN is associated to the primary VLAN, its MAC address tables are merged into one shared MAC table.
- You can configure a private VLAN (PVLAN) port as a SPAN source port.
- A PVLAN host or promiscuous port cannot be a SPAN destination port.
- TFTP download to Cisco Nexus 9000 Series switches is not supported when the transfer is done when you are using In-band Management, for example, VLAN SVI that is in default or custom VRF. The TFTP transfer times out and fails. CoPP for TFTP traffic only matches the TFTP connections on the ports and it does not match the concurrent data transfers that are on the dynamic ports. All the other TFTP traffic after an initial connection is placed in default class and it is dropped.

  Possible workarounds for the download are:

  - Use the management port for TFTP as the management VRF does not participate in CoPP.
  - Use FTP or another file transfer protocol to transfer the files. (It is sorted into the management class of CoPP and it is not sorted in the default class.)
  - Edit the CoPP policy to accommodate the TFTP traffic from the TFTP server that is to be grouped into another CoPP class as displayed in the following example:

    1. Create an ACL permitting only TFTP server address:

       ```
       switch# show ip access-lists copp_udp
       IP access list copp_udp
               10 permit udp x.x.x.x/32 any <-- TFTP server address
       ```

    2. Copy the CoPP policy and apply the ACL in the management class:

       ```
       switch(config)# copp copy profile strict suffix udp-customized
       switch(config)# class-map type control-plane match-any
       copp-class-management-udp-customized
       switch(config-cmap)# match access-group name copp_udp
       ```

    3. Apply the new CoPP policy to the Cisco Nexus 9000 Series switch:

       ```
       switch(config)# control-plane
       switch(config-cp)# service-policy input copp-policy-strict-udp-customized
       ```

    4. Verify that your applied CoPP policy contains the ACL in the management class:

       ```
       switch(config-cp)# show policy-map interface control-plane | b tftp prev 10
       ```

Initial Troubleshooting VLANs Checklist

Troubleshooting a VLAN problem involves gathering information about the configuration and connectivity of individual devices and the entire network. Begin your troubleshooting VLAN issues by checking the following issues first:

Checklist	Done
Verify the physical connectivity for any problem ports or VLANs.	
Verify that you have both end devices in the same VLAN.	

The following CLI commands are used to display VLAN information:

- **show vlan** *vlan-id*
- **show vlan all-ports**
- **show tech-support vlan**
- **show vlan private-vlan** [*type*]
- **show interface vlan** *vlan-id* **private-vlan mapping**

Troubleshooting VLAN Issues

You Cannot Create a VLAN

You may have a problem when creating a VLAN.

Symptom	Possible Cause	Solution
You cannot create a VLAN	You are using a reserved VLAN ID.	VLANs 3968 to 4047 and 4094 are reserved for internal use; you cannot change or use these reserved VLANs.

You Cannot Create a PVLAN

You may experience issues when creating a private VLAN (PVLAN).

Symptom	Possible Cause	Solution
You cannot create a PVLAN.	The PVLAN feature is not enabled.	Use the **feature private-vlan** command to enable the PVLAN feature.

The VLAN Interface is Down

You might have a problem when configuring VLAN interfaces.

Symptom	Possible Cause	Solution
The VLAN interface is down.	The VLAN does not exist.	Use the **show vlan** command to determine if the VLAN exists. Use the **vlan** command to create the VLAN.
	The interface is in the wrong VRF.	Use the **show vrf interface** command to determine the interface to which the VLAN interface is assigned.