This article describes how to troubleshoot VLANs.

Contents

Information 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)

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.
- To apply output VACLs to all outgoing private VLAN traffic, map the secondary VLANs on the Layer 3 VLAN interface of the primary VLAN and then configure the VACLs on the SVI of the primary VLAN.
- 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.
- Because traffic in private VLANs flow in different directions, you can have different VACLs for ingressing traffic and different VACLs for egressing traffic.

Note: We recommend that you keep the same VACLs for the primary VLAN and all secondary VLANs in the private VLAN.

- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.
- You can configure IEEE 802.1X port-based authentication on a private VLAN port, but do not configure 802.1X with port security or per-user ACL on private VLAN ports.
- 802.1X works with private VLANs, but the 802.1X dynamic VLAN assignment or the guest VLAN assignment does not work with private 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.
- Private VLANs support these Switched Port Analyzer (SPAN) features:
    - You can configure a private VLAN port as a SPAN source port.
    - You can use VLAN-based SPAN (VSPAN) on primary, isolated, or community VLANs or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- Do not configure a remote SPAN (RSPAN) VLAN as a private VLAN primary or secondary VLAN.
- A private VLAN host or promiscuous port cannot be a SPAN destination port. If you configure a SPAN destination port as a private VLAN port, the port becomes inactive.
- 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 the user is 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, their MAC address tables are merged into one, shared MAC table.

Initial Troubleshooting 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	Check off
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 private-vlan**
- **show vlan all-ports**
- **show vlan private-vlan**
- **show vlan private-vlan type**
- **show interface vlan** *vlan-id* **private-vlan mapping**
- **show tech-support vlan**

VLAN Issues

This section includes symptoms and solutions for 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.	There are not enough resources in the virtual device context (VDC).	Use the **show vdc resource vlan** command to determine how many unused VLANs that you can configure. If this value is 0, log in as network-admin and use the **limit-resource** command in VDC configuration mode to add more VLAN resources to this VDC.
	You are using a reserved VLAN ID.	VLANs 3968 to 4047 and 4094 are reserved for internal use in each VDC; you cannot change or use these reserved VLANs.

You Cannot Create a PVLAN

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

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

The VLAN Interface is Down

You may 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.
	No interfaces on the VLAN are in the STP forwarding state.	Use the **show vlan internal vlan-info** command to check the operating state of the Spanning Tree Protocol (STP). Configure STP so that at least one interface goes into the STP forwarding state.
	One or more services prevented the VLAN interface from coming up.	Use the **show vlan internal vlan-info** command to determine the state of the VLAN interface. If the state is oper-es, use the **show tech-support interface vlan** command to gather more information.
	The VLAN is a secondary VLAN.	Use the **show vlan internal vlan-info** command to determine the state of the VLAN interface. Change the VLAN to a primary or user VLAN.
	The interface is in the wrong VRF.	Use the **show vrf interface** command to determine the interface that the VLAN interface is assigned to.

See Also

Before Contacting Technical Support

Further Reading

The following links contain further information on this topic from Cisco.com:

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide

External Links

External links contain content developed by external authors. Cisco does not review this content for accuracy.