

VLAN partitioning and core switch



Overview

This video was associated with the source search result. Verify technical details against current product documentation and project requirements.

Key Takeaways

VLAN partitioning on a core switch involves creating and managing VLANs to segment network traffic, enhance security, and enable inter-VLAN routing where necessary. Understanding VLAN Partitioning

VLANs (Virtual Local Area Networks) allow you to divide a physical switch into multiple logical broadcast domains, isolating traffic between groups of devices even if they share the same physical infrastructure. This improves network performance, reduces broadcast traffic, and enhances security by limiting access to specific VLANs .

Core Switch Considerations

- **L2 vs L3 Core Switch:** If your core switch operates at Layer 2, you generally need to configure all VLANs on the core to ensure proper traffic forwarding across trunks . For a Layer 3 core switch, VLANs may only need to exist on access/distribution switches if routing is handled elsewhere, but inter-VLAN routing will require VLAN interfaces (SVIs) on the core .
- **Trunking:** Use IEEE 802.1Q trunking to carry multiple VLANs over a single link between the core and distribution/access switches . Proper VLAN filtering ensures that only authorized VLAN traffic passes through each trunk .

- **VLAN Management:** Protocols like VTP (VLAN Trunking Protocol) can help propagate VLAN configurations from the core to other switches, simplifying management in large networks .

Configuration Steps

- **Create VLANs:** Define VLAN IDs on the core switch for each network segment you want to isolate .
- **Assign Ports:** Map physical or logical interfaces to the appropriate VLANs. Access ports connect end devices, while trunk ports carry multiple VLANs to other switches .
- **Configure VLAN Interfaces (SVIs):** On L3 cores, create VLAN interfaces (VLANIF) and assign IP addresses to enable inter-VLAN routing .
- **Bind to VPN Instances (Optional):** For advanced segmentation, VLAN interfaces can be bound to VPN instances to isolate traffic between public and private networks .
- **Enable Routing Protocols:** Configure OSPF or other routing protocols on the core switch if inter-VLAN or external routing is required .

Best Practices

- Plan VLAN IDs carefully to avoid conflicts and simplify management.
- Limit broadcast domains to reduce unnecessary traffic.
- Use SDM templates on Cisco switches to optimize system resources for large numbers of VLANs .
- Monitor STP virtual ports to ensure spanning-tree scalability, especially when many VLANs and trunks exist . By following these steps, VLAN partitioning on the core switch ensures efficient traffic segmentation, secure network boundaries, and scalable inter-VLAN communication.

Article Content

Details of dividing the network | VLAN (Virtual LAN) | N-Study

Divide the network by VLAN If you physically prepare separate Layer 2 switches and divide the Ethernet network, you will need a lot

Related Video Reference

This video was associated with the source search result. Verify technical details against current product documentation and project requirements.

Contact Us

Continue your research online:

Website: <https://thegalleryselfcatering.co.za>

Technical inquiry: <https://thegalleryselfcatering.co.za/contact.html>

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

