

Understanding Private VLANs on EX-series Switches

The private VLAN (PVLAN) feature on EX-series switches allows an administrator to split a broadcast domain into multiple isolated broadcast subdomains, essentially putting a VLAN inside a VLAN. Just like regular VLANs, PVLANs are isolated on Layer 2 and require that a Layer 3 device be used to route traffic among them. Private VLANs are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts.

In a private VLAN, one VLAN is designated the primary VLAN, and other VLANs are nested inside that VLAN as secondary VLANs.

- **Primary**—A VLAN used to forward frames downstream to isolated and community VLANs.
- **Isolated**—A secondary VLAN that receives packets only from the primary VLAN and forwards frames upstream to the primary VLAN.
- **Community**—A secondary VLAN that transports frames among community interfaces within the same community and forwards frames upstream to the primary VLAN.

Private VLANs provide IP address conservation and efficient allocation of those IP addresses. In a typical network, VLANs usually correspond to a single IP subnet. In private VLANs, the hosts in all the secondary VLANs still belong to the same IP subnet as the subnet allocated to the primary VLAN. Hosts within the secondary VLAN are numbered out of IP subnets associated with the primary VLAN, and their IP subnet masking information reflects that of the primary VLAN subnet. Any primary routed VLAN interfaces (RVIs) perform functions similar to proxy ARP to enable communication between hosts that are members of a different secondary VLAN.

Related Topics

- Understanding Bridging and VLANs on EX-series Switches
- Example: Configuring a Private VLAN on an EX-series Switch
- Creating a Private VLAN (CLI Procedure)

