VLAN overview

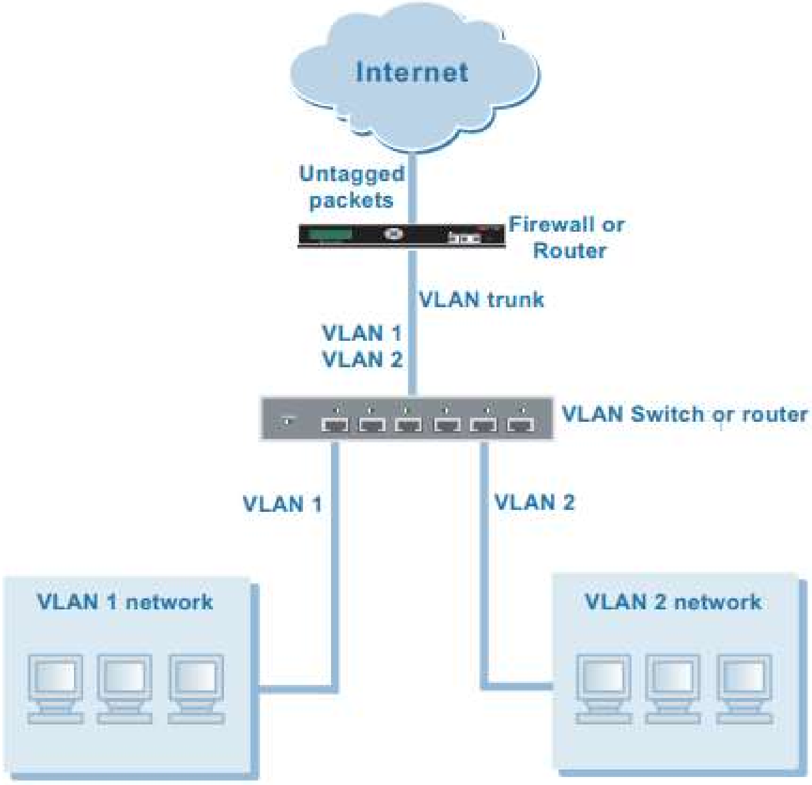
Ver 1.0

A VLAN is group of PCs, servers, and other network devices that communicate as if they were on the same LAN segment, even though they may not be. For example, the workstations and servers for an accounting department could be scattered throughout an office, connected to numerous network segments, but they can still belong to the same VLAN (see Figure 1).

A VLAN segregates devices logically instead of physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. The communication among devices on a VLAN is independent of the physical network.

A VLAN segregates devices by adding 802.1Q VLAN tags to all of the packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information. VLANs allow highly flexible, efficient network segmentation, enabling users and resources to be grouped logically, regardless of physical locations

Figure 1: Basic VLAN topology

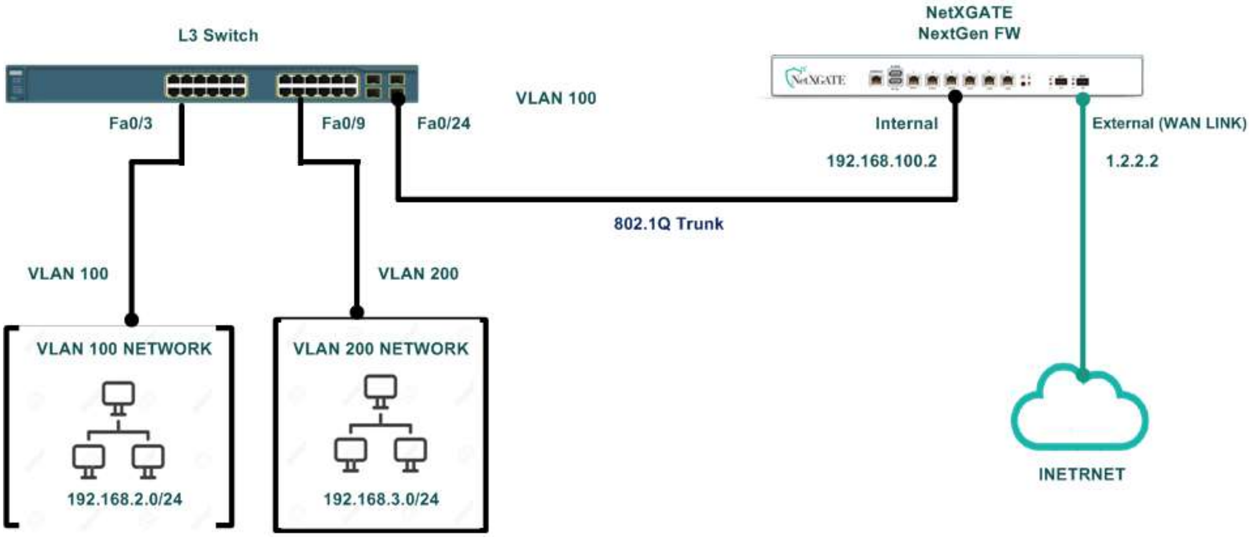


NetXGATE units and VLANs

In a typical VLAN configuration, 802.1Q-compliant VLAN layer-2 switches or layer-3 routers or firewalls add VLAN tags to packets. Packets passing between devices in the same VLAN can be handled by layer 2 switches. Packets passing between devices in different VLANs must be handled by a layer 3 device such as router, firewall, or layer 3 switch. Using VLANs, a single NetXGATE unit can provide security services and control connections between multiple security domains. Traffic from each security domain is given a different VLAN ID. The NetXGATE unit can recognize VLAN IDs and apply security policies to secure network. The NetXGATE unit can also apply authentication, content filtering, and AV protection for network and VPN traffic that is allowed to pass between security domains.

Evaluation-grade VLANs in NAT/Route mode

In this example, the NetXGATE NextGen-FW unit operates in NAT/Route mode. The internal interface –LAN 1 connects to a Cisco 2900 switch using an 802.1Q trunk and is configured with two VLAN sub interfaces (VLAN 100 and VLAN 200). The external interface-WAN1 connects to the Internet. The external interface is not configured with VLAN sub interfaces. When the Cisco switch receives packets from VLAN 100 and VLAN 200, it applies VLAN ID tags and forwards the packets to local ports and across the trunk to the NetXGATE FW. The NetXGATE has policies that allow traffic to flow between the VLANs and from the VLANs to the external network.



Configuring the Cisco switch

Add a configuration file to the Cisco Catalyst 2900 Ethernet switch. The file defines the VLAN sub interfaces and the 802.1Q trunk interface on the switch.

To configure the VLAN sub interfaces and the trunk interfaces

Add this file to the Cisco switch:

```
!
 interface FastEthernet0/3
    switchport access vlan 100
! interface FastEthernet0/9
    switchport access vlan 200
! interface FastEthernet0/24
   switchport trunk encapsulation dot1q
   switchport mode trunk
!
```

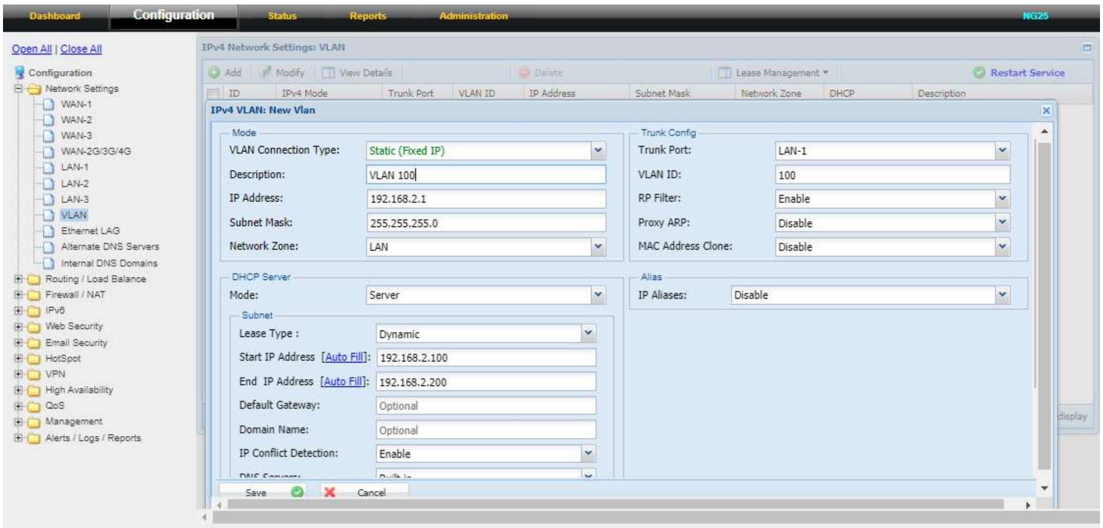
The switch has the following configuration:

Port 0/3 VLAN ID 100

Port 0/9 VLAN ID 200

Port 0/24 802.1Q trunk

Note: To complete the setup, configure devices on VLAN 100 and VLAN 200 with default gateways. The default gateway for VLAN 100 network is the NetXGATE VLAN 100 IP Address.



IPv4 VLAN: New Vlan

Mode

VLAN Connection Type: Static (Fixed IP)

Description: VLAN 100

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Network Zone: LAN

Trunk Config

Trunk Port: LAN-1

VLAN ID: 100

RP Filter: Enable

Proxy ARP: Disable

MAC Address Clone: Disable

DHCP Server

Mode: Server

Subnet

Lease Type : Dynamic

Start IP Address [Auto Fill]: 192.168.2.100

End IP Address [Auto Fill]: 192.168.2.200

Default Gateway: Optional

Domain Name: Optional

IP Conflict Detection: Enable

Alias

IP Aliases: Disable