

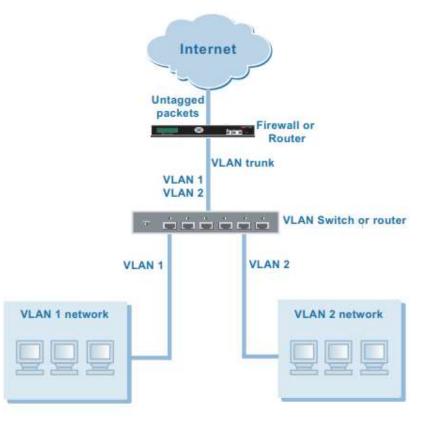
# **VLAN overview**

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



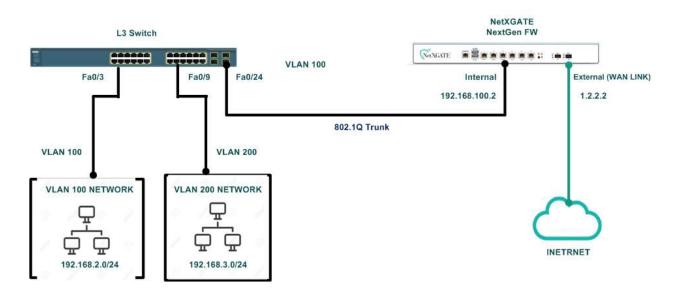
#### Figure 1: Basic VLAN topology

### **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:

i

interface FastEthernet0/3

switchport access vlan 100

! interface FastEthernet0/9

switchport access vlan 200

! interface FastEthernet0/24

switchport trunk encapsulation dot1q

switchport mode trunk

i

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.

| Namonk Satings   ID   IPv4 Mode   Truk Port   VLAN ID   IP Address   Submet Mask   Description     WAN-2   | stration NG26   | orts Administration | ON Status Repo                | Dashboard Configurat       |
|--|---|---------------------|-------------------------------|----------------------------|
| ID   Bout Mode   Trunk Port   VLAN ID   IP Address   Subnet Mask   Network Zone   DHCP   Description     WAN-3   WAN-3   Wode   Trunk Port   VLAN ID   IP Address   Subnet Mask   Network Zone   DHCP   Description     WAN-3   Wan-3   Wode   Trunk Port   VLAN ID   IP Address   IP   |   |                     | IPv4 Network Settings: VLAN   | en All   Close All         |
| V Wak-1 I Dow Mode I Dake Pote V CAN LD IP Address Down Mode   V Wak-23 V Wak-23 Mode Turk Config Turk Config   V Wak-23 V Wak-23 Mode Turk Config   V Wak-23 V Wak-23 Description: V LAN 100   LAN-1 VLAN 100 VLAN 100 VLAN 100   LAN-2 IP Address: 192.168.2.1 VLAN 100   MANA Subnet Mask: 255.255.0 Proxy ARP: Disable   MARA Subnet Mask: 255.255.0 Proxy ARP: Disable   MARA Network Zone: LAN MAC Address Clone: Disable   MARA Subnet Pricewall /NS Proxy ARP: Disable   Prow ARP: Disable MAC Address Clone: MAC Address Clone: MARA   IP Address: Subnet Subnet Subnet Alias   IP Address Clone: Disable MARA   VPN End IP Address (Lato Ell): 192.168.2.00   UPN High Availability Default Gateway: Optional   Dorand Default Gateway: Optional Disable   | 😑 Delete 🔄 Lease Management * 📀 Restart Servi             | etails 👘            | 🗘 Add 📝 Modify 🛄 View De      | Configuration              |
| WAN-2     WAN-3     WAN-2     LAN-1     LAN-1     Description:     VLAN 100     Prov ARP:     Bable     WAN-2     MARM     Subnet Mask:     25.255.255.0     Prov ARP:     Disable     MAC Address Clone:     MAC Address Clone:     Disable     MAC Address Clone:     Prova ARP:     Disable     MAC Address Clone:     Prova ARP:     Disable     MAC Address Clone:     Disable     Mala     Prova ARP:     Disable     Prova ARP:     Disable<  | N ID IP Address Subnet Mask Network Zone DHCP Description | Trunk Port VLAN ID  | ID IPv4 Mode                  |                            |
| WAN-3 Wode Turk Config.   WAN-20/30/46 VLAN Connection Type: Static (Fixed IP) Turk Port: LAN-1   LAN-1 Description: VLAN 100  VLAN 100   LAN-3 IP Address: 192.168.2.1 RP Filter: Enable   VARN Subnet Mask: 255.255.255.0 RP Filter: Enable   MARM Material DNS Domains Network Zone: LAN MAC Address Clone: Disable   Routing / Load Stance DHCP Sarver Alias Alias   Routing / Load Stance DHCP Sarver Alias   Proval / NAT Bescrify Lesse Type : Dynamic   Helsoet Statit IP Address (Lator Fill): 192.168.2.100   VPN End IP Address (Lator Fill): 192.168.2.200   UPA Default Gateway: Optional   Ocs Default Gateway: Optional   | ×   |                     | IPv4 VLAN: New Vlan           |                            |
| LAN-1 Description: VLAN 100   LAN-2 IP Address: 192.168.2.1   MARN Subnet Mask: 255.255.255.0   Marking Subnet Mask: 255.255.255.0   Proxy ARP: Disable   Marking Description: Web Servers   Internal DNS Domains DHCP Server MAC Address Clone:   Routing / Load Baance DHCP Server Alias   Friewall NNAT Mode: Server   Pix0 Subnet Lease Type :   Dynamic VPN   High Availability End IP Address (Latto Fill):   QoS Default Gateway:   Optional Descriptional  | Trunk Config  |                     | Mode                          |                            |
| LAN-2 Description: VLAY 100 VUAY 10: 100   LAN-3 IP Address: 192.168.2.1 RP Filter: Enable   WAK Subnet Mask: 255.255.0 Proxy ARP: Disable   Bement LAG Network Zone: LAN MAC Address Clone: Disable   Atternate DNS Dervers Network Zone: LAN MAC Address Clone: Disable   Prevail /NAT Mode: Server V   IP/0 Subnet Subnet Macro   Web Security Subnet Lase Type : Dynamic   Hofsort Start IP Address [Autor Fil]: 192.168.2100   VFN Hof IP Address [Autor Fil]: 192.168.2100   VFN End IP Address [Autor Fil]: 192.168.2100   Optional Domain onto Domain onto  | Trunk Port: LAN-1   | Static (Fixed IP)   | VLAN Connection Type:         |                            |
| D LAN-3 IP Address: 192.168.2.1 RP Filter: Enable MAX   MARK Subnet Mask: 255.255.255.0 Proxy ARP: Disable MAC Address Clone: Mac Ad | VLAN ID: 100  | VLAN 100            | Description:                  |                            |
| Ethemat LAG Subnet Mask: 255.255.255.0 Provy APP: Disable M   Atlanata DNS Sorvers Network Zone: LAN V MAC Address Clone: Disable V   Rocking/ Load Balance OHCP Server MAC MAC Address Clone: Disable V   Provy APP: Disable V MAC Address Clone: Disable V   Provy APP: Disable V MAC Address Clone: Disable V   Provy APP: Disable V MAC Address Clone: Disable V   Provy APP: Disable V MAC Address Clone: Disable V   Provy APP: Disable V MAC Address Clone: Disable V   Provy APP: Disable V MAC Address Clone: Disable V   Web Security Subnet Lease Type : Dynamic V   Web Security Start IP Address [Little Fill]: 192.168.2100 Disable V   VPN End IP Address [Little Fill]: 192.168.2100 Disable V   VPN Default Gateway: Optional Disable Disable   | RP Filter: Enable   | 192.168.2.1         | IP Address:                   |                            |
| Alternate DNS Servers Network Zone: LAN MAC Address Glone: Disable   Internal DNS Domains DHCP Server Alternal DNS Machines   Firewall / NAT Mode: Server   IP/d Submet IP Alterses (Late Fill):   Web Security Lease Type : Dynamic   Email Security Start IP Address (Late Fill): 192.168.2.100   VPN Hold Foress (Late Fill): 192.168.2.00   VPN End IP Address (Late Fill): 192.168.2.00   Optional Management Domain Name   | Proxy ARP: Disable  | 255.255.255.0       | Subnet Mask:                  |                            |
| Routing / Load Balance PDHCP Server Allas   Finewall / NAT Mode: Server IP Allases:   Disable v   Prevail / NAT Subset   Web Security Lesse Type : Dynamic   Holspot Ven   Holspot Start IP Address (Autor Fill):   VPN End IP Address (Autor Fill): 192.168.2.100   VPN End IP Address (Autor Fill): 192.168.2.200   Oc5 Default Gateway: Optional   Optional Domain of Name  | ✓ MAC Address Clone: Disable ✓                            | LAN                 | Network Zone:                 |                            |
| Fiewall NAT Mode: Server IP Alases: Disable   IP Alases: Disable V   Web Security Lesse Type : Dynamic V   Halspot Start IP Address [Auto Fill]: 192.168.2100 V   VPN Hold Factors [Auto Fill]: 192.168.2200 Default Gateway:   Optional Optional Default Management   | Aller   |                     | DUCP Server                   |                            |
| Web Security Submit   Email Security Lease Type : Dynamic   HolSpot Start IP Address [Auto Fill]: 192.168.2.100   VPN End IP Address [Auto Fill]: 192.168.2.200   VPN End IP Address [Auto Fill]: 192.168.2.200   OoS Default Gateway: Optional  |   | Server              |                               |                            |
| Email Security Lease Lype : Dynamic   Horspot Start IP Address [Auto Fill]: 192.168.2.100   VPN End IP Address [Auto Fill]: 192.168.2.200   OoS Default Gateway: Optional   Management Domain Name: Default Gateway:   |   |                     | - Subnet                      | Pv6                        |
| HotSpot     Start IP Address     [Auto Fill]:     192.168.2.100       VPN     End IP Address     [Auto Fill]:     192.168.2.200       High Availability     End IP Address     [Auto Fill]:     192.168.2.200       CoS     Default Gateway:     Optional       Management     Domain Name:     Ontional   | ¥   | Dynamic             | Lease Type :                  |                            |
| High Availability     Eind ar Address     Lean Zall       GoS     Default Gateway:     Optional       Management     Domain Name:     Optional   |   | 192.168.2.100       | Start IP Address [Auto Fill]: |                            |
| OoS     Default Gateway:     Optional       Management     Domain Name:     Optional   |   | 192.168.2.200       | End IP Address [Auto Fill]:   |                            |
|  |   | Optional            | Default Gateway:              | QoS                        |
|  |   | Optional            | Domain Name:                  | Alerts / Logs / Reports    |
| IP Conflict Detection: Enable 🗠  |   | Enable              | IP Conflict Detection:        | - contra i coga i redporta |
| DHC Comment  |   | nula ta             | DMC Conserve                  |                            |