

How To Guide

XRoads Networks

Edge Network Appliance How To Guide:

EdgeXOS VLANs

VLAN Overview

This document provides an overview of what a VLAN is and how it is configured on the EdgeXOS platform. Use the step-by-step guide below to configure a VLAN on the Edge appliance and see how it is configured with other devices.

What Is A VLAN?

IEEE 802.1Q (also known as VLAN Tagging) was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e. trunking). IEEE 802.1Q is also the name of the standard issued by this process, and in common usage the name of the encapsulation protocol used to implement this mechanism over Ethernet networks.

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Ports on a switch can be grouped into VLANs in order to limit traffic flooding since it is limited to ports belonging to that VLAN and its trunk ports. Any switch port can belong to a VLAN. Packets are forwarded and flooded only to stations in the same VLAN. Each VLAN is a logical network, and packets destined for stations that do not belong to the same VLAN must be forwarded through a routing device. Each VLAN can also run a separate instance of the spanning-tree protocol (STP).

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

How To Configure A VLAN:

The following steps should be used when configuring a VLAN on the EdgeXOS platform:

- 1) Select the Interfaces tab – This is the tab at the top of the web GUI titled Interfaces.
- 2) Select VLAN Tagging – Navigate to the drop-down menu and select the VLAN Tagging menu option.
- 3) Enter the VLAN Network – Type in the network address to be used for this VLAN. This must essentially be the gateway address which the VLAN will be using.
- 4) Subnet Mask – Enter the correct subnet mask in '/' notation. Example: A Class C network is a /24.
- 5) Enter the VLAN Tag ID – This is the identifier for this specific VLAN. All packets coming in using this VLAN will be tagged with this ID.

The following screen demonstrates the initial VLAN configuration screen:

The screenshot shows the 'VLAN Tags' configuration page. On the left is a dark blue sidebar with three sections: 'VLAN Tags: ?' (with a help icon), 'Add VLAN: ?' (with a help icon), and 'VLAN Interface: ?' (with a help icon). The main content area has a top navigation bar with five tabs: 'Select', 'VLAN Interface Address', 'Netmask (Slash Notation)', 'VLAN ID', and 'VLAN Interface'. Below the tabs are three input fields: a dotted IP address field with the placeholder '(Enter the VLAN IP Address and Subnet)', a VLAN ID field with the placeholder '(Enter the VLAN ID)', and a dropdown menu currently set to 'LAN'. At the bottom are three buttons: '<< Back', 'Add VLAN', and 'Delete VLAN'.

Example:

For example if we are terminating a VLAN using ID 2, and the network on this VLAN was using 10.0.0.0/24 with the gateway being 10.0.0.1.

This screenshot shows the same 'VLAN Tags' configuration page as above, but with example values entered. The IP address field contains '10 . 0 . 0 . 1' and the subnet mask field contains '24', with the placeholder '(Enter the VLAN IP Address and Subnet)' to the right. The VLAN ID field contains '2' and the placeholder '(Enter the VLAN ID)' to the right. The 'Add VLAN' button is highlighted with a red rectangular border.

How To Configure With A Cisco:

Cisco conf to configure the port you want to use as the trunk:

```
conf t
interface FastEthernet0/2 (it doesn't have to be 0/2)
duplex full
speed 100
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2
switchport mode trunk
```

This conf will do the following:

Set the port to full duplex mode; force the port to 100Mb mode;
Set the port VLAN encapsulation to support 802.1Q;
Tell the switch that the port is allowed to run VLANs through (even if you set just VLAN 2, Cisco will automatically add VLAN 1 and VLAN 1002-1005) to the port and set the port to trunk mode as well.

Important: Trunk mode tells the switch that a number of VLANS can go through it. This last line is usually the mother of all screw-ups. If you forget that, you won't get your VLAN working.

Now configure some other port to be used as the destination for the VLAN:

```
conf t
interface FastEthernet0/1
duplex half
speed 10
switchport access vlan 2
end
```

Here we tell the switch to force the port 1 to half duplex 10Mb mode (normal 10 Mb NIC) and only traffic from interface VLAN 2 can go through this port. also you can use a number of ports with VLAN 2, like a HUB)

You should now connect some other device to port 1.

Let it have an IP of 10.0.0.2 mask 255.255.255.0 GW 10.0.0.1

Then attempt a ping to the gateway to confirm that the VLAN is working.

```
ping -s 100 10.0.0.1
ping -s 1476 10.0.0.1
```

If both pings work then everything should work fine, if the first ping works, but the second does not, contact XRoads Networks support.

Firewall Issues With A VLAN:

The easiest way to setup VLANs is with no firewall enabled. However if you want security between VLAN networks, then the firewall must be enabled. The image below shows how the Firewall is enabled under the Firewall > L7 Firewall Control menu:

Firewall Enabled Firewall Disabled (Disabling will turn off all perimeter security)

If you want to allow all VLAN access out to the WAN, but control VLAN access between each other, then the following example is a good place to start.

In this example we have two networks, 192.168.25.0/24 and 192.168.27.0/24 on VLANs 2 and 3 respectively. In order to block access between these VLANs we add the following rules (see image).

<input type="radio"/>	VLANtest	WANx	192.168.25.0/24	192.168.27.0/24	ANY ANY	DROP	Off
<input type="radio"/>	VLANtest	WANx	192.168.25.0/24	ANY	ANY ANY	ACCEPT	Off
<input type="radio"/>	VLANtest	WANx	192.168.27.0/24	192.168.25.0/24	ANY ANY	DROP	Off
<input type="radio"/>	VLANtest	WANx	192.168.27.0/24	ANY	ANY ANY	ACCEPT	Off

We MUST use the WAN+ designator as the LAN designator is only used for the primary LAN interface, not the VLANs.

Troubleshooting:

Some users have reported issues when connecting to certain switches, if you are experiencing an issue, try setting the LAN interface to 0.0.0.0 and using a DMZ port for management, this has been found to fix certain switch issues.