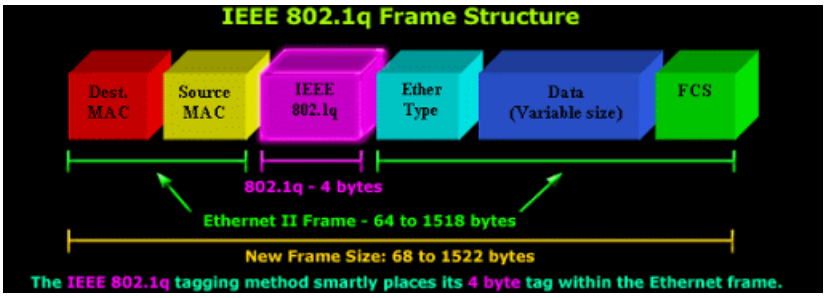
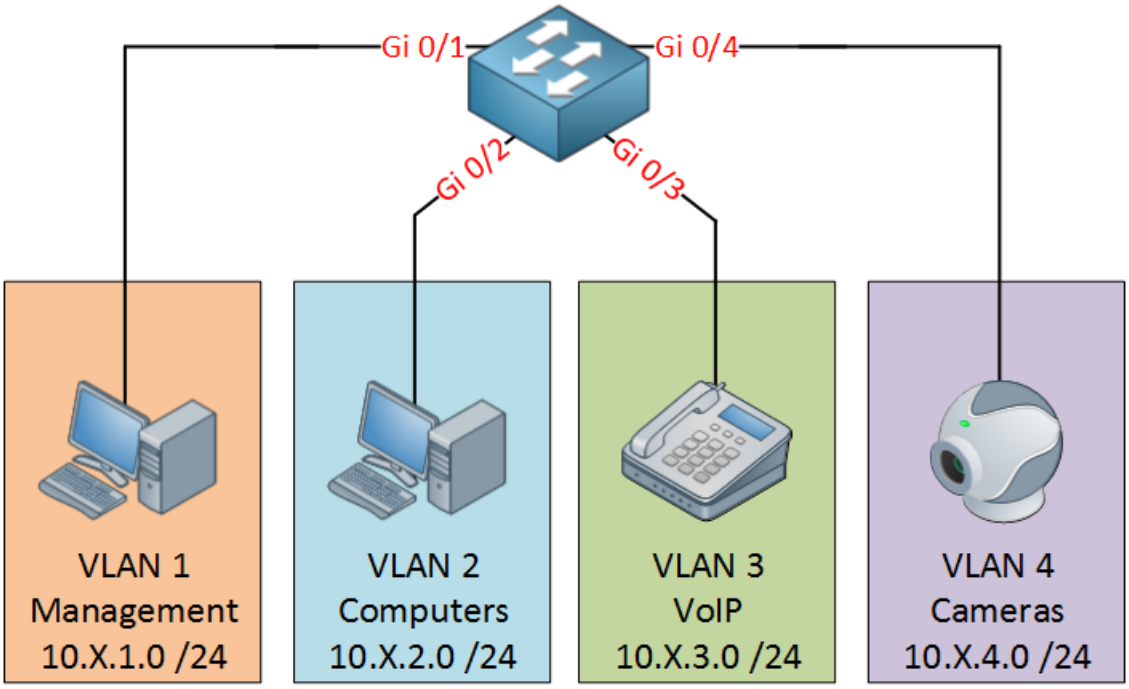
VLAN Overview

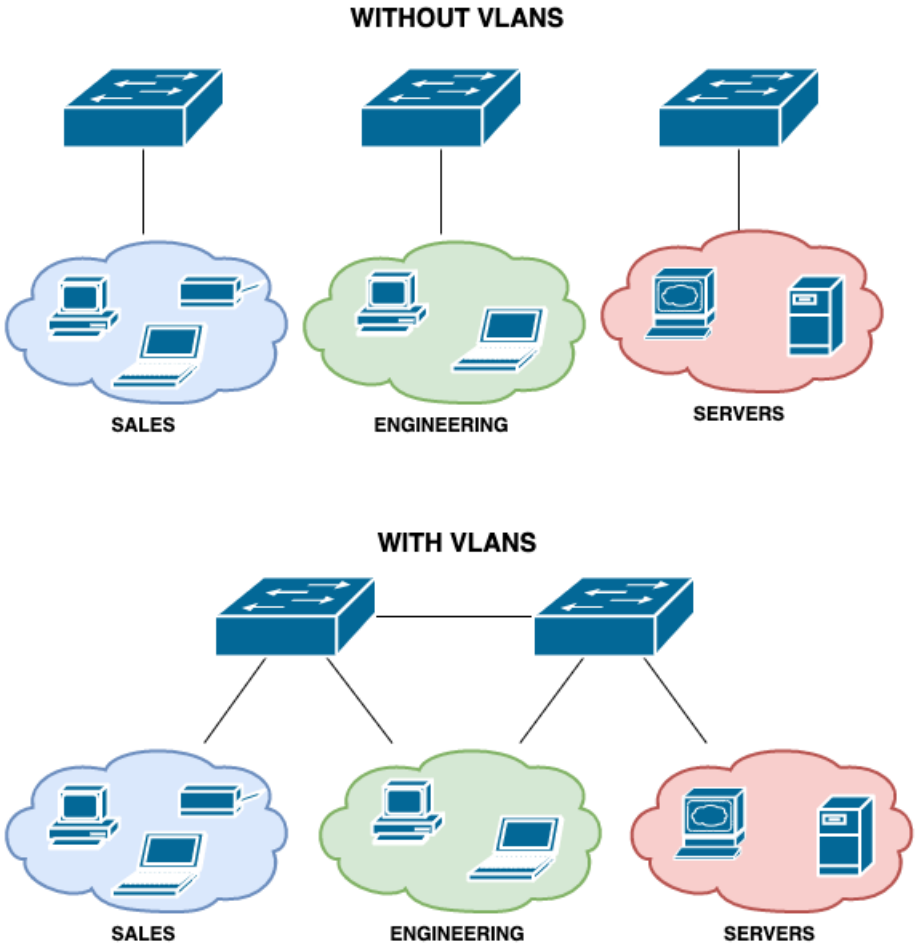
- Everyone in IT should know what a LAN is. A segment of devices locally connected through a shared medium. Think back to circa 2008 and you're playing HALO with your buddies on four different XBOX's. That is a LAN! Famously referred to as a LAN party. Now imagine that through that shared medium you want to separate or segment that traffic at Layer 2.
- Through the use of "Virtual Local Area Networks" you can logically separate Ethernet frames. We do this with a process called "tagging". On the Ethernet frame the switch will add a "VLAN Tag" to the frame to designate that frame is apart of a separate network. What does tagging look like?
- A four-byte tag is inserted in between the source MAC address and the "Ethernet type" field. Through this technology we can separate traffic all locally on one switch, and span that segmentation across even a large Campus Area Network.



- On a single switch you can have multiple VLANs that segment traffic logically.



- Without VLANs we would need a single device to segment traffic logically. Refer to the image below.



Standard VLANs Overview

- Standard range VLANs consist of 1005 VLAN numbers or **"tags"** with 4 default VLANs created out of the box that we can not use to assign to switchports.
- 1 - **Native/Default VLAN** - The untagged VLAN. This VLAN will be used to carry control traffic like **CDP**, **DTP**, **VTP**. The Default VLAN will always be 1, however the **"native"** VLAN can be changed. If changed on one switch it must change on all switches in your LAN.
- 2-1001 - VLANs to be used for ethernet frames; designated by network administrator
- 1002 - Default FDDI VLAN
- 1003 - Default Token Ring TrCRF VLAN
- 1004 - Default FDDI NET VLAN
- 1005 - Default Token Ring TrBRF VLAN
- Standard VLAN are save and stored in a switches **"VLAN Database"**.

Types of standard VLANs

- Access VLANs - **"access"** VLANs are any VLAN tag encapsulated for regular traffic.

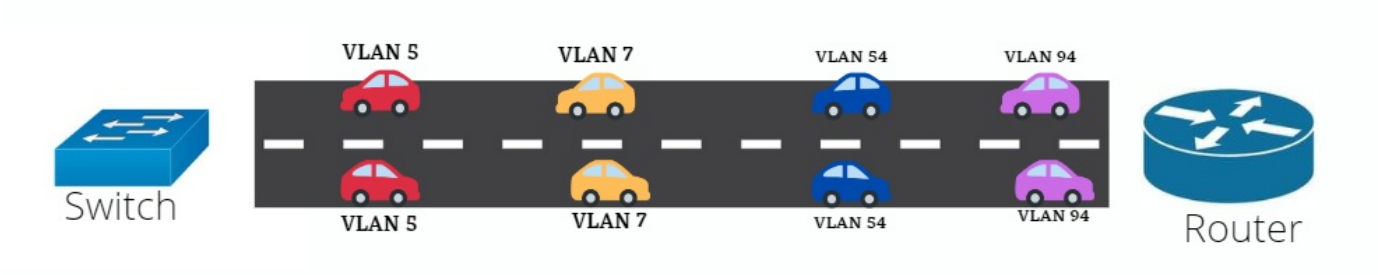
- Voice VLAN - The **Voice** VLAN is a configuration option for Cisco IP Phones so that their VLAN tag can be marked/classified as VoIP traffic and be segmented from the rest of the network. **Voice** VLANs use CDP to communicate that there will be untagged packets from a connected device that will need to be tagged with the native or access VLAN.
- Native VLAN - The **Native** VLAN is the "out of the box" VLAN that will tag all traffic that is not part of a VLAN with a VLAN tag of "1". The **Native** VLAN also carries control plane traffic like **CDP**, **VTP**, **DTP**.
- Black Hole VLAN - This is an unused VLAN that does not belong to any broadcast domain and is used for security purposes.

Extended Range VLANs

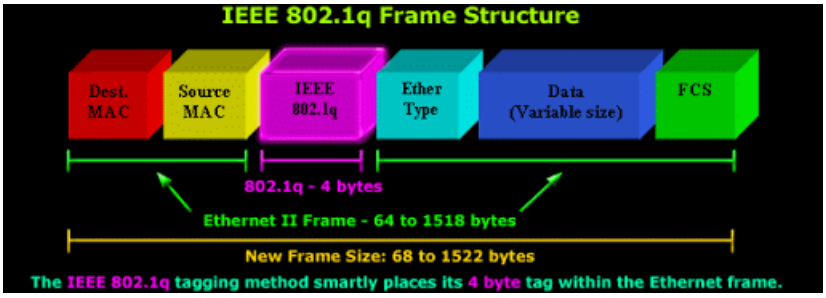
- The extended range for VLANs is **1006 - 4094**
- Extended VLANs are saved in the **NVRAM; "startup-config"** of the switch.

Trunking Overview

- Trunking is the key to all inter-VLAN communication. Think of a trunk as the 6 lane highway that goes both ways. The VLANs are the cars that travel on your highway, the trunk port. They're are multiple different encapsulation methods for creating a trunk link.



- The IEEE encapsulation standard for trunking is 802.1q.



- Like all trunks the 802.1q trunk allows the passing of multiple VLANs to transverse its segment. 802.1q trunks are common place among all LAN, CAN and MAN networks. All Cisco switch hierarchy models require the use of trunks, and 802.1q is the trunking protocol we all use. The 802.1q header is 32-bits and placed in between the source MAC address and the Ethernet type field. 802.1q is also the encapsulation technology utilized in DOT1Q tunneling, and router-on-a-stick.

Switched Virtual Interfaces

- We all know that out of the box switches are Layer 2. Which means they make all forwarding decisions based off MAC addresses and frames. But what if we need to remotely manage a switch? Or what if a small off-site office has an 8 port switch that needs routing? Well we can make a switch do routing a couple of ways. And there are a multitude of reasons why we would need to make a switch do routing, the most common reasons for access level switches is management.
- A SVI or Switched Virtual Interface is a logical Layer 3 interface that allows IP addressing and routing on a Switch.
- SVIs are typically configured at Access switches just for remote management. At the distribution layer SVIs are used as the Default Gateway for all broadcast domains/subnets.