Post 4

Thursday, January 24, 2019 11:11 PM

VLAN BASICS

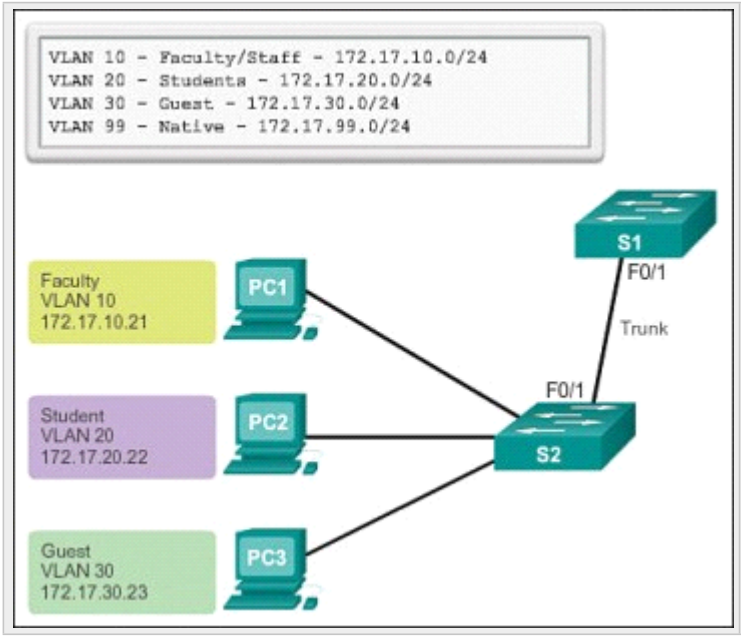
VLAN: Virtual Local Area Network: Allows logical network segmentation: Any port switch can belong to VLAN

- Unicast/multicast/broadcast packets forwarded/flooded to end stations w/in VLAN where sourced

Benefits of VLANS 3.1.1.2

Security	Sensitive data separated from network: Decreased chances of info breach
Cost	Less need for expensive upgrades: More efficient use of BW/uplinks (cheaper)
Performance	• Divides flat L2 networks into multiple logical workgroups (broadcast domains) • Reduces unnecessary traffic: Boosts performances
Shrink Broadcast Domains	Reduces number of devices in broadcast domain (b/c of division)
IT staff efficiency	• Easier to manage network (usrs w/similar reqs share same VLAN) • New switch? Policies configured for VLAN/used when ports assigned • Easy function ID
Simpler project/app mgmt.	• Aggregate usrs/devices to support business/geographic reqs • Separate functions: Project/App managing is easier

Hierarchical network addressing



- Each VLAN corresponds to an IP network
- Network numbers applied to segments/VLANs
- Takes whole network into consideration
- Blocks of addresses reserved on devices in specific areas

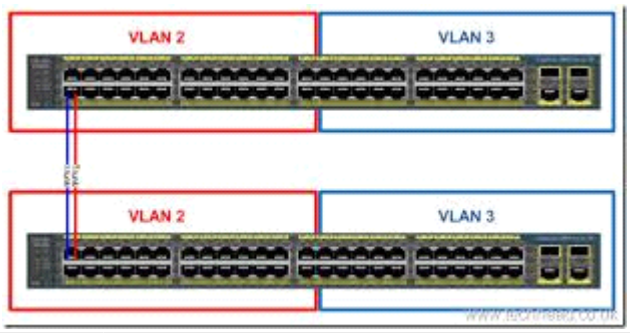
Types of VLANS: Some defined by traffic: Others function they serve

Data (AKA user VLAN)	▪ Config to carry user-generated traffic ▪ Separates network into groups of usrs/devices **NOTE**: Voice/mgmt. traffic NOT data VLAN
Default	▪ All ports part of default VLAN after initial boot of switch (default config) ▪ Part of same broadcast domain ▪ Any device connected to port can communicate w/other devices on other ports

	Default = VLAN 1: Can't be renamed/deleted ▪ All L2 control traffic associated w/VLAN 1 show vlan brief shows current vlan setup
Native	▪ Assigned to 802.1Q trunk port **Trunk port**: Links between switches: Support transmission of traffic w/more than 1 VLAN ○ 802.1Q supports traffic from many VLANs (tagged) ○ Supports traffic that doesn't come from VLANs (untagged) ○ **Tagged traffic**: 4byte tag insert w/in original Ethernet frame header: Specifies VLAN frame belongs to ○ 802.1Q trunk port places untagged traffic on native VLAN (default VLAN 1) ○ Common identifier on opposite ends of trunk link ○ Config native VLAN as unused VLAN instead of VLAN 1
Management	▪ Any VLAN config to access management of switch ▪ VLAN 1 is management VLAN (default) **To create**: SVI (switch virtual interface) of that VLAN is assigned IP/subnet mask ○ Allows switch to be managed via HTTP/Telnet/SSH/SNMP ○ More than 1: Security risk: Increases attack exposure

Voice VLANs 3.1.1.4

VoIP	○ Separate VLANs need to support VoIP traffic ○ Requires: Assured BW: Transmission priority (QoS): Less than 150ms delay: Routing around congestion ○ Networks can be designed to support VoIP (cover more in VoIP class) ○ Specific VLAN designed to carry voice traffic ○ Machine attached to IP phone: Attached to switch



Trunk	• Point-to-point link between 2 devices: Carries more than 1 VLAN: Extends VLAN across a network • Cisco supports IEEE 802.1Q (standards) for trunks on fa/g0/10Gb fa ints (FastEth0/Giga Eth0) • VLANs not as useful w/out trunks • Allow VLAN traffic between switches so devices on same VLAN/diff switches/ can comm w/out intervention of router • Don't belong to specific VLAN: Conduit for multiple VLANs between switches/routers • Could be used between network device/server/other equipped with 801.1Q-capable NIC

Broadcast Domains/VLANs

Without VLANs	• Switch receives a broadcast frame on port: Forwards frame out all ports except ingress • A computer sends out broadcast frame: All switches send out frames out all ports • Entire network receives broadcasts b/c of broadcast domain • Can get traffic intensive
With VLANs	• Segmentation w/VLANs help broadcast frames sent fwd it only to ports configured to support specific VLAN

	• Trunks: Ports that comprise connection between switches • Unicast/multicast/broadcast traffic from host to specific VLAN is restricted to devices in that VLAN

Tagging Eth0 Frames for VLAN ID's /Header Info

- Catalyst 2960 switches: L2 devices: Use eth0 frame header info to forward packets: No routing tables
- Standard headers don't contain info about VLAN in frame: except when placed on trunk (then added)

802.1Q	• **Tags:** Extra information added to VLAN header frames on trunks • **Tagging:** accomplished by IEEE 802.1Q header: Specified in standard • 802.1Q header includes 4byte tag w/in original eth0 frame header specifying which VLAN it belongs to • When switch receives frame on port configured in access mode & assigned a VLAN • Switch inserts VLAN tag in frame header: recalculates FCS: sends tagged frame out of trunk port

VLAN Tag Fields

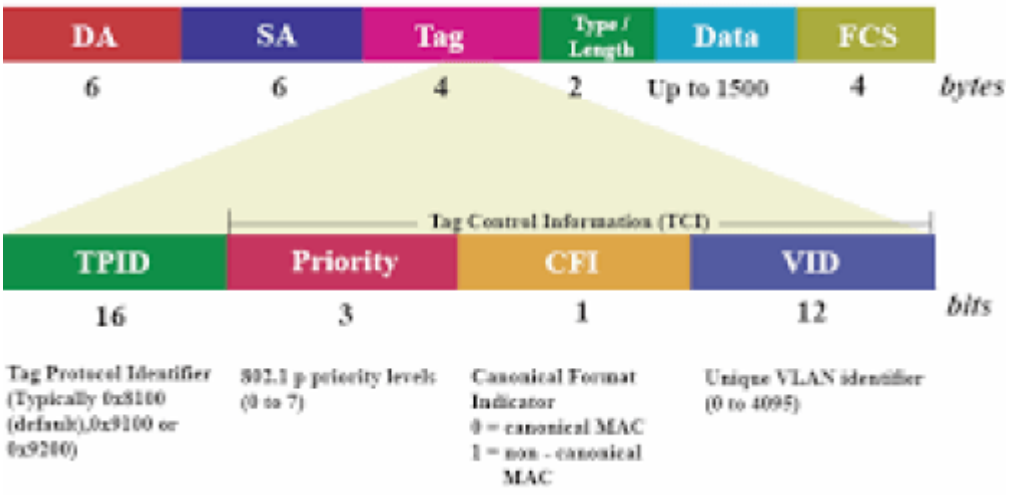
Consists of: Type/Priority/CFI/VLAN ID

Type/TPID value	**Tag Protocol ID**: 2 byte value: For Ethernet, set to hex 0x8100
User priority	• **3-bit value** • Supports level/service implementation
CFI	• **Canonical Format Identifier** • 1-bit identifier • Enables Token Ring frames to be carried across Ethernet links
VID	• **VLAN ID (Virtual LAN)** • 12-bit VLAN ID number • Supports up to 4096 VLAN IDs

How it works:

1. Switch inserts Type/Tag control info fields
2. Recalculates FCS values
3. Inserts new FCS into frame

[Destination Address/Source Address/Frame Check Sequence]



Voice VLAN tagging: Access port used to connect Cisco IP phone can be config to use 2 diff VLANS

- Voice traffic
- Data traffic

Link between switch/IP phone acts as trunk to carry both voice/data VLAN traffic

Contains	Integrated 3-port 10/100 switch: Dedicated connection to devices • Port 1: Connects switch/other VoIP device • Port 2: Internal 10/100 int: Carries phone traffic • Connects PC/device (access port)

Send voice traffic	Access config to send CDP (Cisco Discovery Protocol) packets: Instruct phone to send voice data • **Voice VLAN:** Tagged w/L2 class of service priority value (CoS) • **Access VLAN:** Tagged w/L2 CoS priority value • **Access VLAN:** Untagged (no L2 CoS priority value)