





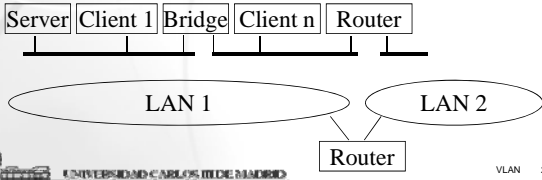
VLAN: Redes Locales Virtuales

Prof. Dr. Jose Ignacio Moreno Novella

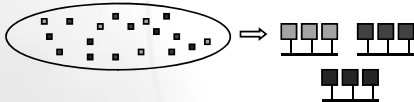
Concepto de LAN

- LANs:
 - Son redes donde se comparte el mismo dominio de difusión
 - Formadas por uno o más segmentos LAN
 - Dispositivos físicamente conectados mediante cableado, repetidores, hubs, bridges o switches
 - Separadas/Interconectadas mediante el uso de routers



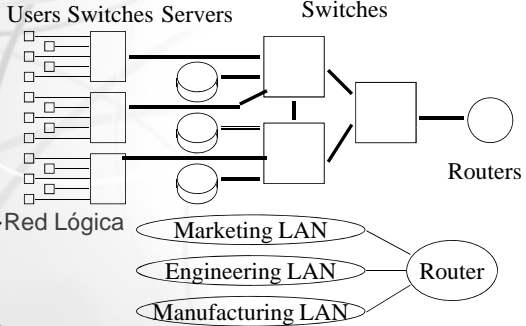
Concepto VLAN

- VLANs: "LANs especiales"
 - Los miembros de la LAN están definidos por el administrador de la red: "VIRTUAL".
 - Tráfico multicast y broadcast alcanza únicamente miembros de la red.
 - Independiente de situación geográfica y de donde se conecten los miembros.
 - Separadas mediante el uso de routers



Concepto de VLAN

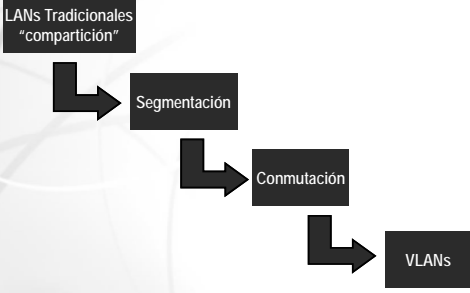
- Red Física
 - Users Switches Servers Switches Routers
- Red Lógica
 - Marketing LAN
 - Engineering LAN
 - Manufacturing LAN
 - Router



VLANs

- VLAN: *formación de grupos de trabajo (LANs) independientemente de su posición geográfica que comparten un dominio de colisión.*
 - LAN Física
 - LAN Virtual
- Tipos de VLAN
 - basada en puertos
 - basada en direcciones MAC
 - basada en protocolo nivel 3
 - basada en aplicaciones

Evolución

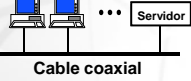


LANs Tradicionales "compartición" → Segmentación → Conmutación → VLANs



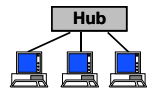
Evolución (I)

◆Cableados tradicionales:



Cable coaxial

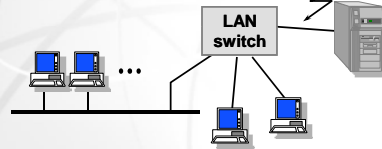
◆ Hub básico:



Cableado en estrella

Evolución (II)

◆LANs conmutadas:

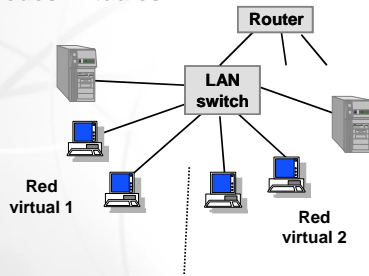


Cableado en estrella

- Más ancho de banda:
- Ethernet duplex
 - FDDI
 - 100VGAnyLAN
 - ATM ...

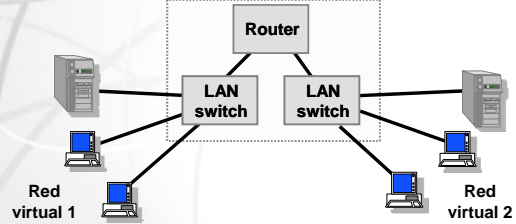
Evolución (III)

◆Redes virtuales:



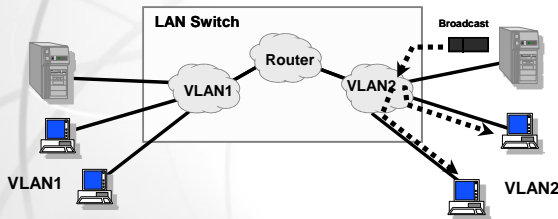
Evolución (IV)

◆Router + Switch:

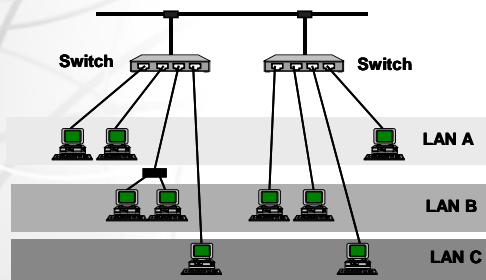


Evolución (V)

◆Red virtual = Dominio de Broadcast



Escenario



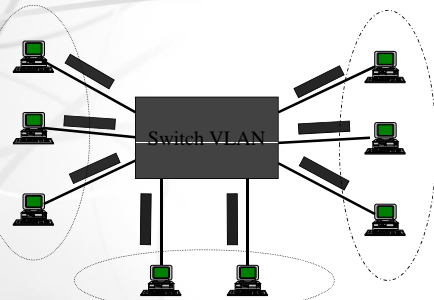
Ventajas de las VLANs

- ◆ Prestaciones:
 - ❖ Reduce el envío de tráfico de difusión y multicast a destinos no implicados mediante la construcción de VLANs específicas.
- ◆ Formación de grupos virtuales.
 - ❖ Sin necesidad de desplazar a las personas
 - ❖ Por tiempo adaptado al grupo
 - ❖ Problemas
 - ✓ Recursos compartidos: impresoras
 - ✓ Servidores vs granjas de servidores
- ◆ Administración
 - ❖ 70 % del coste de red se debe a añadir, mover o reconfigurar usuarios en la red. VLANs simplifican este proceso.
 - ❖ Necesario establecer una gestión de grupos virtuales.
- ◆ Reducción de costes
- ◆ Seguridad
 - ❖ Información crítica sólo es difundida a los usuarios que pueden acceder a ella.

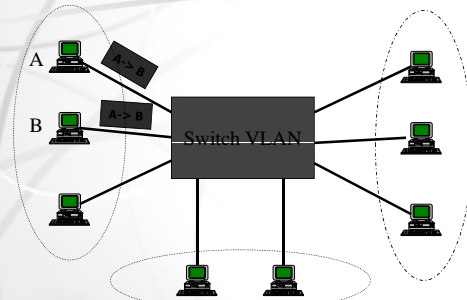
Funcionamiento de las VLANs

- ◆ Marcado explícito
 - ❖ origen
- ◆ Marcado implícito
 - ❖ Puerto
 - ❖ MAC origen
 - ❖ IP origen
 - ❖ Tipo de protocolo
- ◆ El marcado requiere que los bridges/switches mantengan información de filtrado.
- ◆ Si las VLANs se forman en base a puertos debe mantenerse que puertos pertenecen a que VLAN.
- ◆ Todos los bridges de la red deben tener la misma visión.
- ◆ Una vez que el bridge ha decidido donde debe encaminar la trama, esta se encamina como en el caso de redes LAN tradicionales. Si los dispositivos destinatarios son capaces de manejar tramas marcadas (VLAN-aware), el marcado se mantiene. En caso contrario el bridge elimina el marcado.

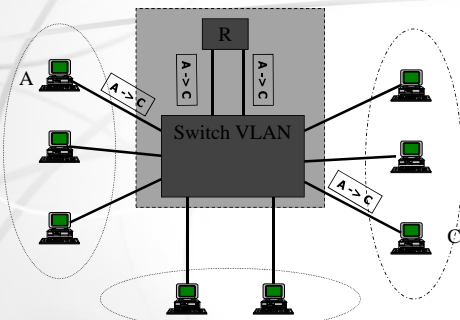
Funcionamiento. Difusión



Funcionamiento. Unicast Interno



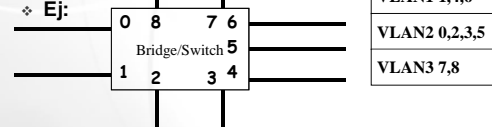
Funcionamiento. Traf.entre VLAN



Tipos de VLANs

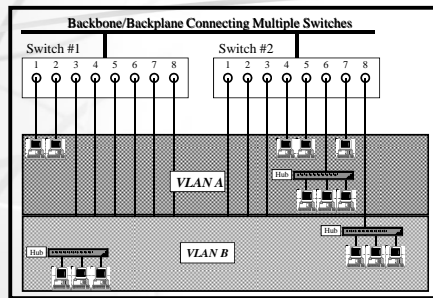
- ◆ VLAN de nivel 1: Por puerto
 - ❖ Los miembros de la VLAN se especifican en base al puerto en el cual se encuentran conectados a los dispositivos de interconexión.
 - ❖ Requiere reconfigurar las VLANs si el usuario se mueve físicamente.

◆ Ej:





VLAN por puerto



VLAN 19

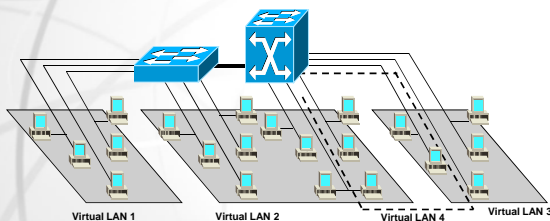
Tipos de VLANs

- ◆ VLAN de nivel 2: Por dirección MAC
 - ❖ Los miembros de una VLAN dependen de la dirección MAC de las estaciones
 - ❖ No requiere reconfiguración si las estaciones se mueven físicamente a puertos distintos
 - ❖ Los miembros de la VLAN deben asignarse inicialmente. Problemas si existen decenas o cientos de usuarios
 - ❖ Problemas para identifica a terminales que poseen varios direcciones MAC

VLAN1	11:22:33:44:55:66
VLAN2	22:33:44:55:66:77
VLAN3	33:44:55:66:77:88
VLAN1	00:22:33:44:55:66
VLAN3	33:44:55:66:77:99
VLAN3	00:11:55:66:77:88

VLAN 20

VLAN por dirección MAC



VLAN 21

Tipos de VLANs

- ◆ VLANs nivel 2: Por tipo de protocolo
 - ❖ Basado en el campo tipo de protocolo del nivel 2

VLAN1	IP
VLAN2	IPX

- ◆ VLANs nivel 3: Direcciones de Subred
 - ❖ Basado en la cabecera de nivel 3

VLAN1	138.43
VLAN2	163.117.139

- ❖ No tiene nada que ver con routing la cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece.
- ❖ Requiere más retardo debido a procesamiento.
- ◆ VLANs nivel n
 - ❖ Basados en otros niveles. Ej: VLAN para ftp,....

VLAN 22

IEEE 802.1q

- ◆ Estándar internacional
- ◆ Define VLANs de nivel 1 y 2 y niveles superiores
- ◆ Compatible con bridges y switches sin capacidad de VLAN.
- ◆ Soporte de medio compartido y LANs conmutadas
- ◆ Soporte de configuración estática y dinámica
- ◆ Otros:
 - ❖ CISCO ISL: Inter Link Switch
 - ❖ 3COM Virtual LAN Trunking

VLAN 23

Tipos de enlaces

- ◆ Enlaces de acceso (usuarios)
 - ❖ Los switches aprenden o tienen configurados por gestión a que VLAN pertenece dicho enlace
- ◆ Enlace de interconexión (interswitches)
 - ❖ Utilizan un mecanismo de marcado para intercambiar tráfico de VLANs
 - ❖ Los switches deben saber que enlaces soportan marcado y cuales no.

VLAN 24



VLAN Tagging

Dest. Addr	Src. Addr	VLAN Tag	Prot. Type
------------	-----------	----------	------------

- ◆ First switch adds tag containing VLAN id to all incoming packets
- ◆ Intermediate switches do not recompute the VLAN id
- ◆ Last switch removes tags from all outgoing packets
- ◆ Tag is not swapped at every hop like VC Id or labels

UNIVERSIDAD CARLOS III DE MADRID

VLAN 25

Escenario

UNIVERSIDAD CARLOS III DE MADRID

VLAN 26

IEEE 802.1Q: Features

- ◆ Allows up to 4095 VLANs
- ◆ Allows port based, MAC address based, and higher-layer VLANs
- ◆ Upward compatible with existing VLAN-unaware hubs and bridges
- ◆ Supports both shared-media and switched LANs
- ◆ Allows mixing legacy bridges and VLAN-aware bridges
- ◆ Retains plug and play mode of current LAN bridges

UNIVERSIDAD CARLOS III DE MADRID

VLAN 27

Features (Cont)

- ◆ Extends 802.1p priority mechanism to priority based on VLAN membership
- ◆ Allows priority associated with each VLAN
- ◆ VLAN-based priority takes precedence over other priority considerations
- ◆ Allows signaling priority information on non-priority (CSMA/CD) LANs
- ◆ Allows both local/universal MAC addresses
- ◆ Operation with/without explicit VLAN header in the frame

UNIVERSIDAD CARLOS III DE MADRID

VLAN 28

Features (Cont)

- ◆ Supports static and dynamic configurations for each VLAN
- ◆ Allows intermixing different IEEE 802 MACs and FDDI
- ◆ Allows signaling source routing information on CSMA/CD LANs
- ◆ Each VLAN is a subset of a "single" physical spanning tree
Does not preclude future extensions to multiple spanning trees

UNIVERSIDAD CARLOS III DE MADRID

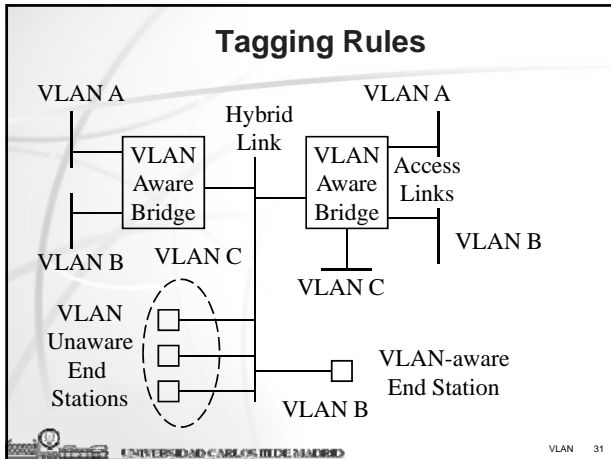
VLAN 29

Features (Cont)

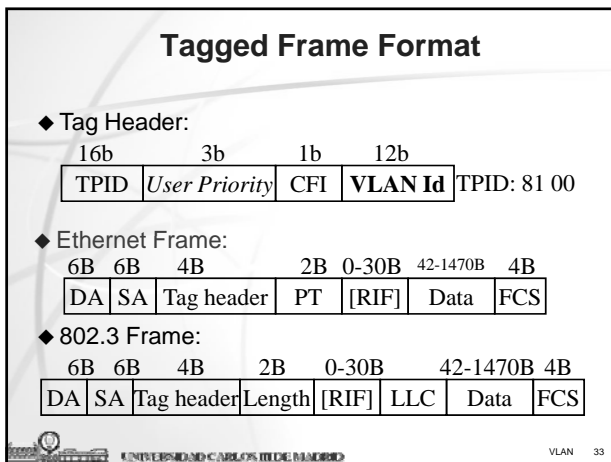
- ◆ Overlapping VLANs:
 - ❖ Multiple stations with same individual address
 - ❖ One station with multiple interfaces using the same address
 - ❖ Restriction: One station or interface per VLAN

UNIVERSIDAD CARLOS III DE MADRID

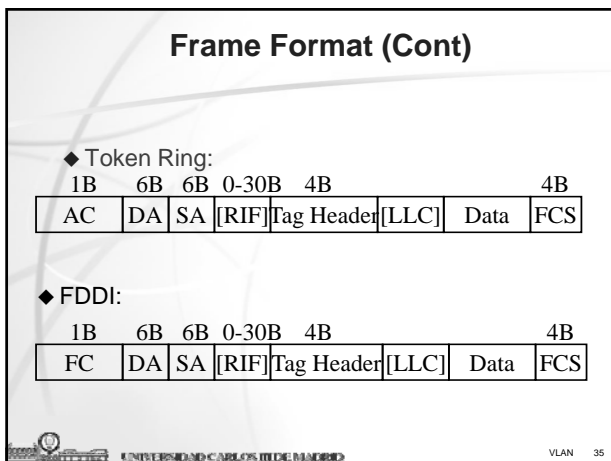
VLAN 30



- ### Tagging Rules (Cont)
- ◆ On a given LAN segment for a given VLAN, all frames should be either implicitly or explicitly tagged.
 - ◆ Different VLANs on the same segment may use different options.
 - ◆ Access Link: Contain VLAN unaware devices
All frames on access links are untagged
 - ◆ Hybrid Link: Contains both VLAN-aware and VLAN-unaware devices
 - ❖ All frames for some VLANs are tagged
 - ❖ All frames for other VLANs are untagged
- VLAN 32



- ### Frame Format (Cont)
- ◆ TPID = Tag Protocol ID
 - ◆ CFI = Canonical Format Indicator
= Bit order of address info in TR/FDDI frames
= Presence/absence of RIF in 802.3/Ethernet frames
 - ◆ RIF = Routing Information Field
 - ❖ New routing type: 01 = Transparent frame
⇒ No routing info.
 - ◆ DA = Destination Address, SA = Source Address
PT = Protocol Type, LLC = Logical Link Control
FCS = Frame Check Sequence
 - ◆ Largest data size = 1470 on 802.3
- VLAN 34



- ### GVRP
- ◆ GARP VLAN registration protocol
 - ◆ GARP = Generic attribute registration protocol
 - ◆ Register VLAN Ids and port filtering modes
 - ◆ Both end-stations and bridges can be GARP participants
 - ◆ GARP Participants issue/revoke membership declaration ⇒ Creates entries in the databases
 - ◆ VLAN-aware bridges propagate VLAN membership changes on all active ports
- VLAN 36



GVRP (Cont)

- ◆ VLAN-aware end stations can "source prune" traffic for VLANs that have no other members
- ◆ Initially, all ports on all bridges are set to a default "Port VLAN ID"

GMRP in VLANs

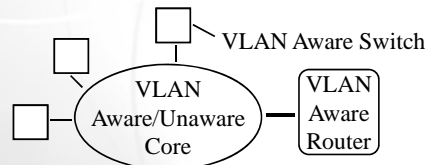
- ◆ Original GMRP is designed for one LAN ⇒ One one context or base spanning tree context
- ◆ With VLANs, multicast addresses are registered a particular VLAN context ⇒ Filtering behavior in a VLAN does not affect other VLANs

VLAN Filtering Database

- ◆ Two Types of Entries:
 - ❖ VLAN Registration entries
 - ❖ Group Registration entries
- ◆ Both types can static or dynamic
 - ❖ Static VLAN Entries: via Management
 - ❖ Dynamic Filtering Entry:
 - ✓ via learning or registration
 - ✓ Learnt entries are aged out
- ◆ Port Map for each VLAN: Whether frames should be tagged or untagged

Communication Between VLANs

- ◆ Need routers
- ◆ Can use 1-armed VLAN-aware router
- ◆ VLAN-aware switches can route between VLANs
- ◆ Such switches can be placed in the core, in the edges, or everywhere



802.1Q Architecture

