Red de Área Local Virtual
VLAN

Juan M. Hurtado A., MSc

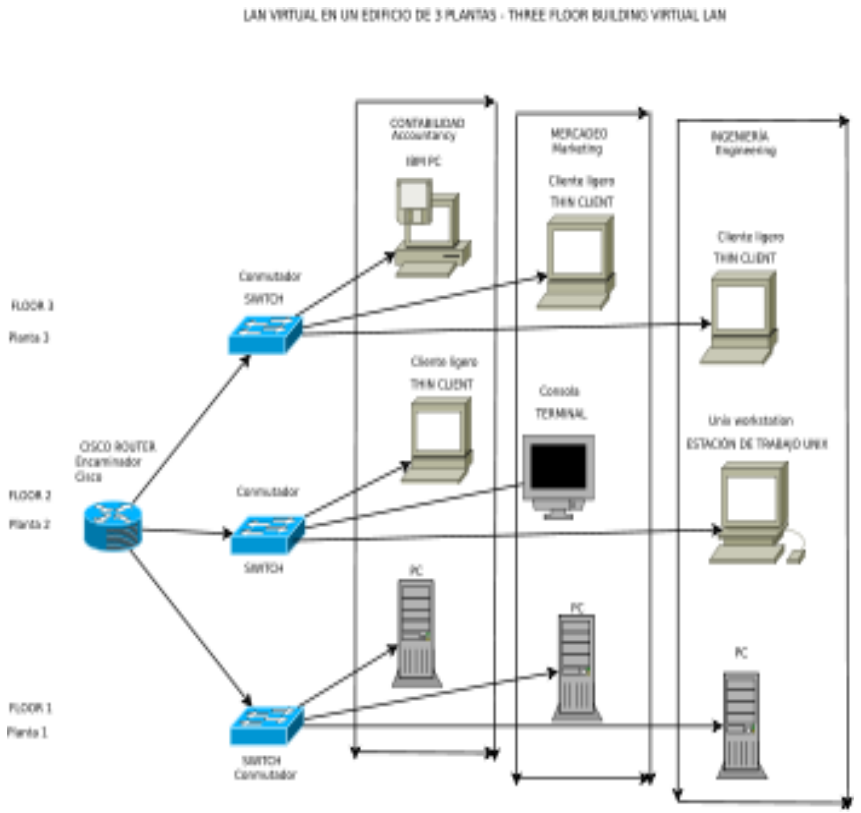
Fuente:
Comunicaciones y Redes de Computadores 7ED
William Stallings

Definición

Una VLAN (acrónimo de virtual LAN, red de área local virtual) es un **método para crear redes lógicas independientes dentro de una misma red física**.

Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, **separando segmentos lógicos de una red de área local** (los departamentos de una empresa) **que no deberían intercambiar datos usando la red local** (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).



Tomado de: http://es.wikipedia.org/wiki/VLAN

Antecedente Histórico

Ethernet era, una red de difusión; cuando dos estaciones transmiten simultáneamente se producen colisiones y se desperdicia ancho de banda en transmisiones fallidas (80´s)
Al aumentar el tamaño de la red, disminuyen sus prestaciones o el costo se hace inasumible. CSMA/CD, impone de por sí limitaciones en cuanto al ancho de banda máximo y a la máxima distancia entre dos estaciones.

Conectar múltiples redes Ethernet era por aquel entonces complicado, y aunque se podía utilizar un Router para la interconexión, estos eran caros y requería un mayor tiempo de procesado por paquete grande, aumentando el retardo.



Tomado de: http://es.wikipedia.org/wiki/VLAN

Antecedente Histórico

W. Kempf inventó el *bridge*, dispositivo software para interconectar dos LANs. 90´s

Kalpana desarrolló el *switch* Ethernet, puente multipuerto implementado en hardware.

Sincoskie consiguió aliviar la sobrecarga de los *switches* inventando LAN virtuales al añadir una etiqueta a las tramas Ethernet con la que diferenciar el tráfico. Al definir varias LAN virtuales cada una de ellas tendrá su propio spanning tree y se podrá asignar los distintos puertos de un *switch* a cada una de las VLAN

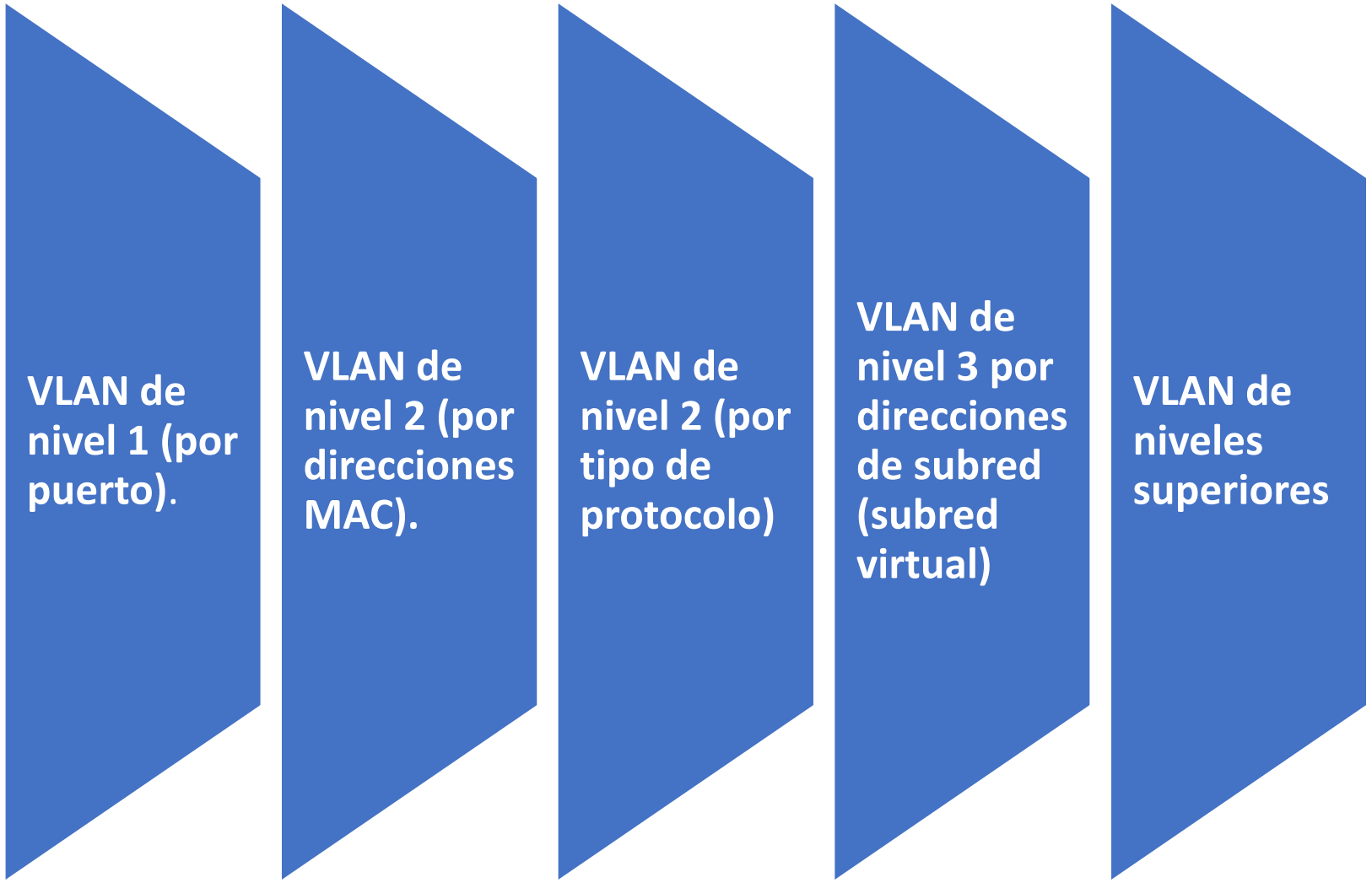
Al definir varias LAN virtuales se podrá asignar los distintos puertos de un *switch* a cada una de las VLAN

Para unir VLAN que están definidas en varios *switches* se puede crear un enlace especial llamado *trunk*, por el que fluye tráfico de varias VLAN

Los *switches* saben a qué VLAN pertenece cada trama observando la etiqueta VLAN (definida en la norma IEEE 802.1Q)

Tomado de: http://es.wikipedia.org/wiki/VLAN

Clasificación de las Vlans



Tomado de: http://es.wikipedia.org/wiki/VLAN

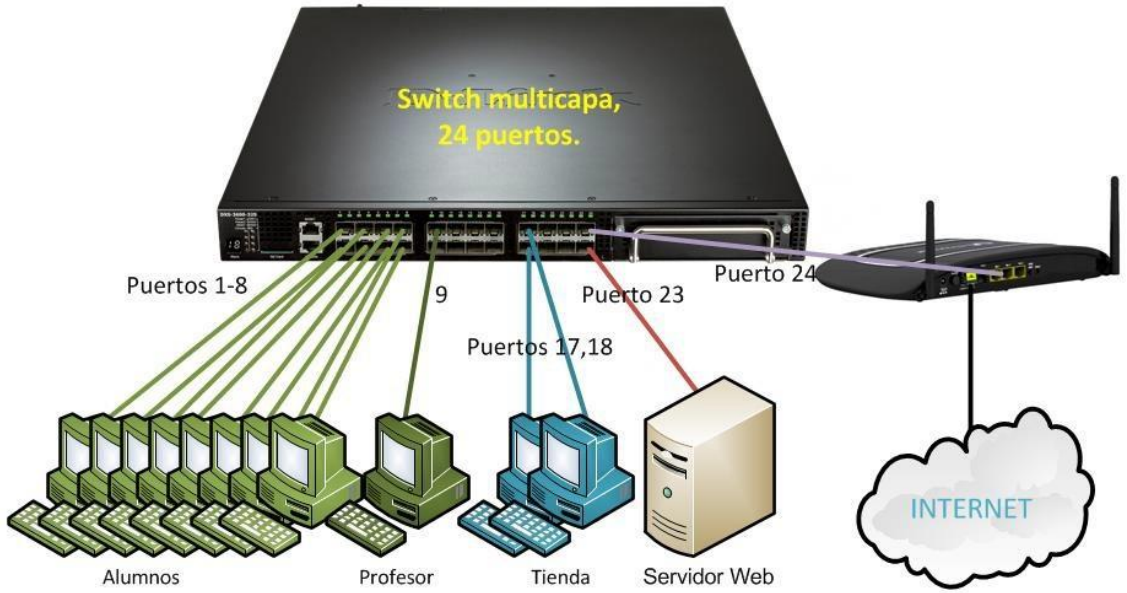
Clasificación de las Vlans

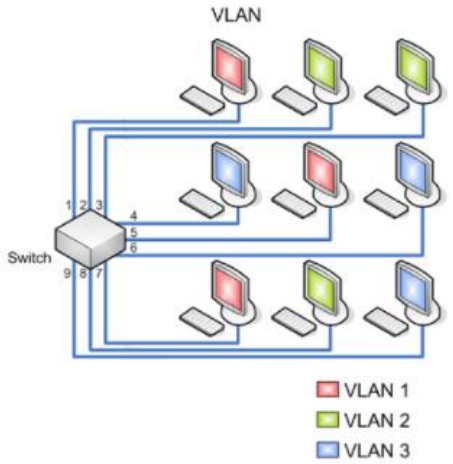
VLAN de nivel 1 (por puerto).
También conocida como “port switching” o Vlan Estáticas.

Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos.

No permite la movilidad de los usuarios, habría que reconfigurar las VLANs si el usuario se mueve físicamente.

Es la más común





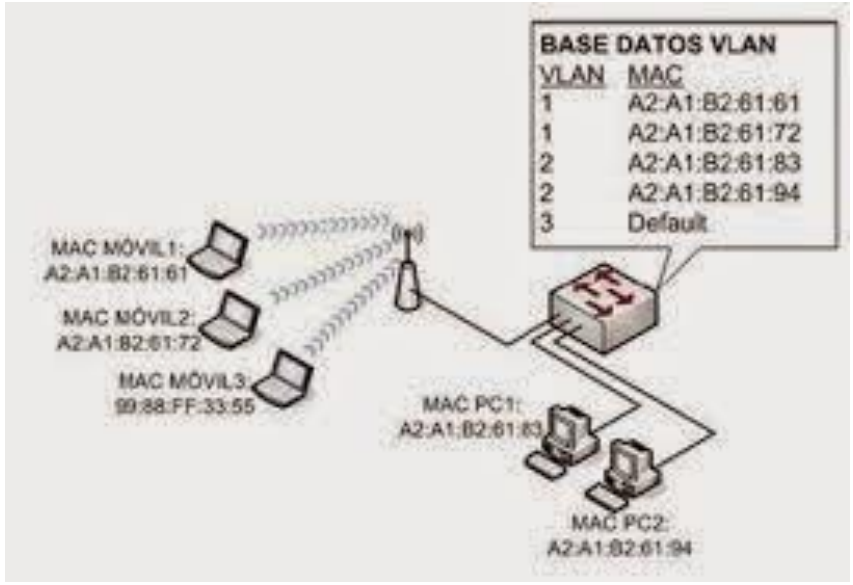
Tomado de: http://es.wikipedia.org/wiki/VLAN

Clasificación de las Vlans

VLAN de nivel 2 por direcciones MAC.
Se asignan hosts a una VLAN en función de su dirección MAC.

Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo.

El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.

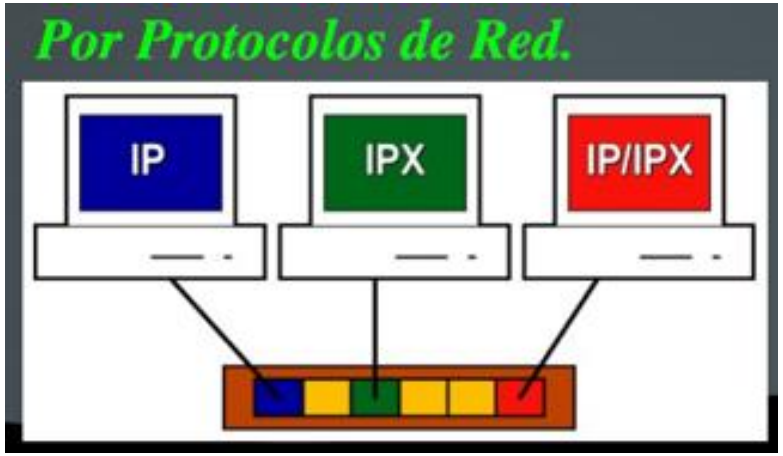


Tomado de: http://es.wikipedia.org/wiki/VLAN

Clasificación de las Vlans

VLAN de nivel 2 por tipo de protocolo.

La VLAN queda determinada por el contenido del campo *tipo de protocolo* de la trama MAC.



Por ejemplo, se asociaría VLAN 1 al protocolo IPv4,

VLAN 2 al protocolo IPv6,

VLAN 3 a AppleTalk,

VLAN 4 a IPX...

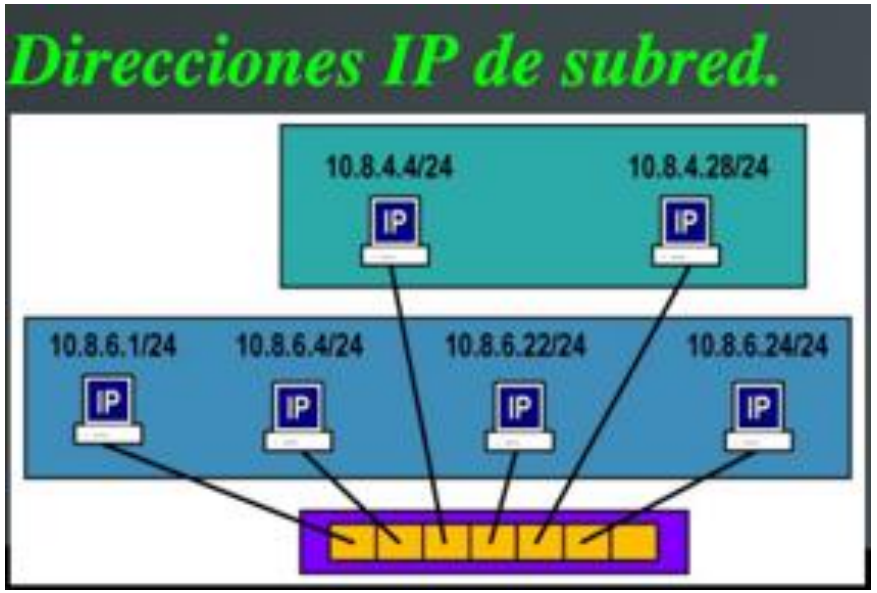
Tomado de: http://es.wikipedia.org/wiki/VLAN

Clasificación de las Vlans

VLAN de nivel 3 por direcciones de subred (subred virtual). La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece.

En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN.

Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLANs



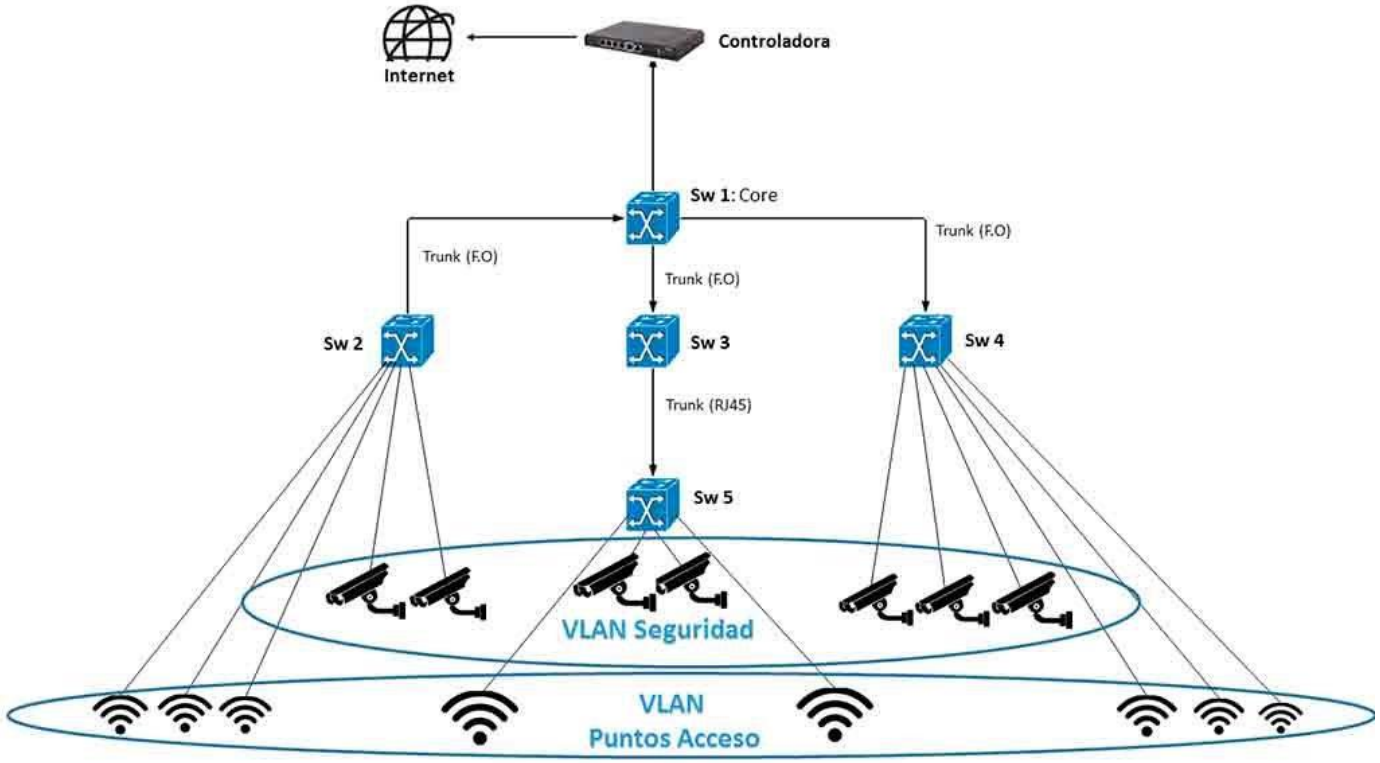
Tomado de: http://es.wikipedia.org/wiki/VLAN

Clasificación de las Vlans

VLAN de niveles superiores.

Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico.

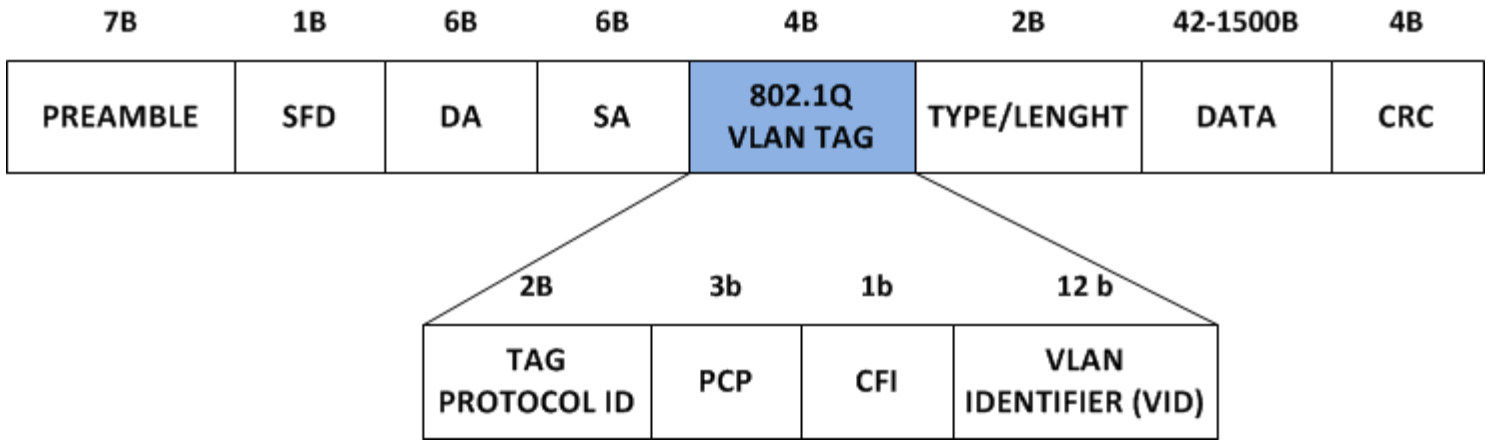
La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo.



Tomado de: http://es.wikipedia.org/wiki/VLAN

Protocolos

Protocolo IEEE 802.1Q)



El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN

Tomado de: http://es.wikipedia.org/wiki/VLAN

Gestión de pertenencia a una Vlan.

VLAN estáticas
También se denominan VLAN basadas en el puerto.
Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un *switch* o conmutador a dicha VLAN.
Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto.
Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el *switch*



Tomado de: http://es.wikipedia.org/wiki/VLAN

Gestión de pertenencia a una Vlan.

VLAN dinámicas

La asignación se realiza mediante paquetes de *software* VMPS (acrónimo en inglés de *VLAN Management Policy Server* o Servidor de Gestión de Directivas de la VLAN).

El administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo.

En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN



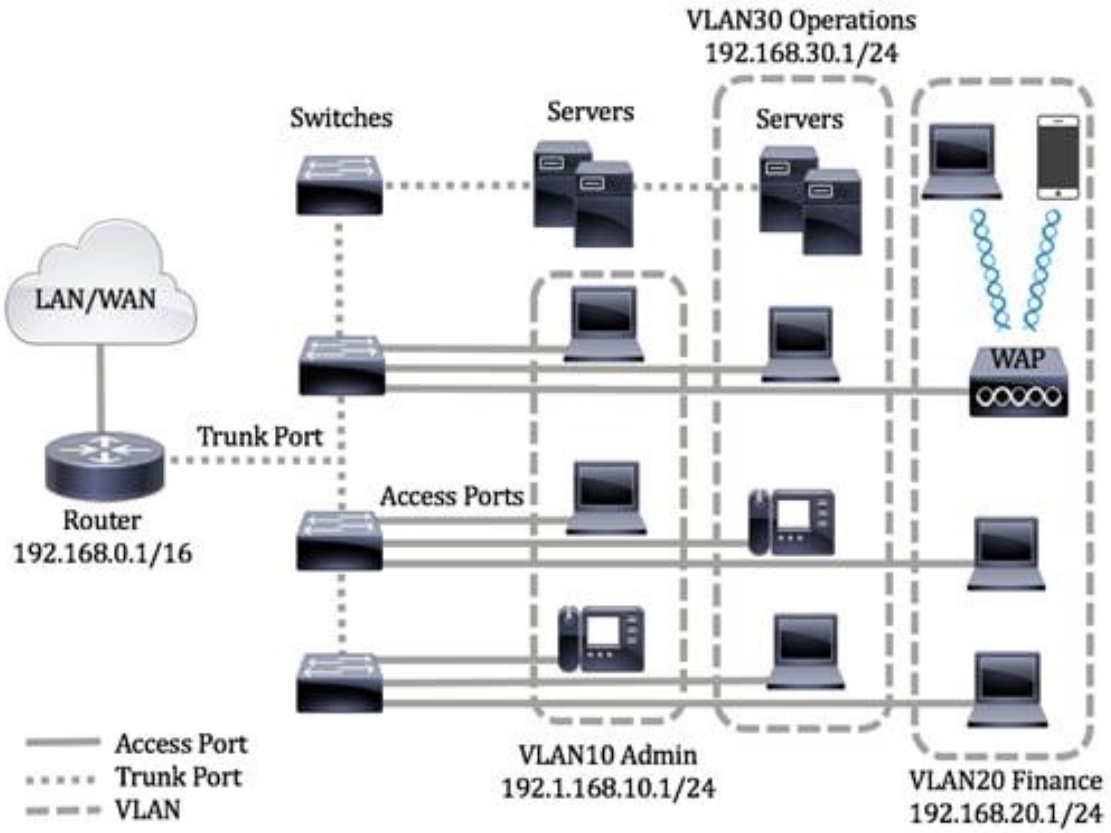
Tomado de: http://es.wikipedia.org/wiki/VLAN

Vlan basado en puerto de conexión

Tipos de puertos

Access port: solamente una VLAN puede estar asociada a este puerto. Las tramas nunca serán etiquetadas.

(switchport mode access)



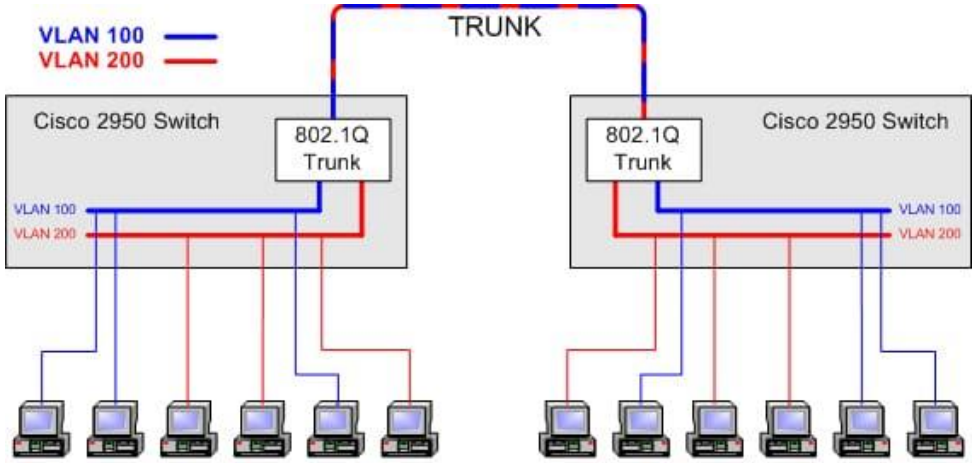
Tomado de: https://sites.google.com/site/tuxnots/materias-de-la-facu/gnu-linux/redesvirtualesvlans

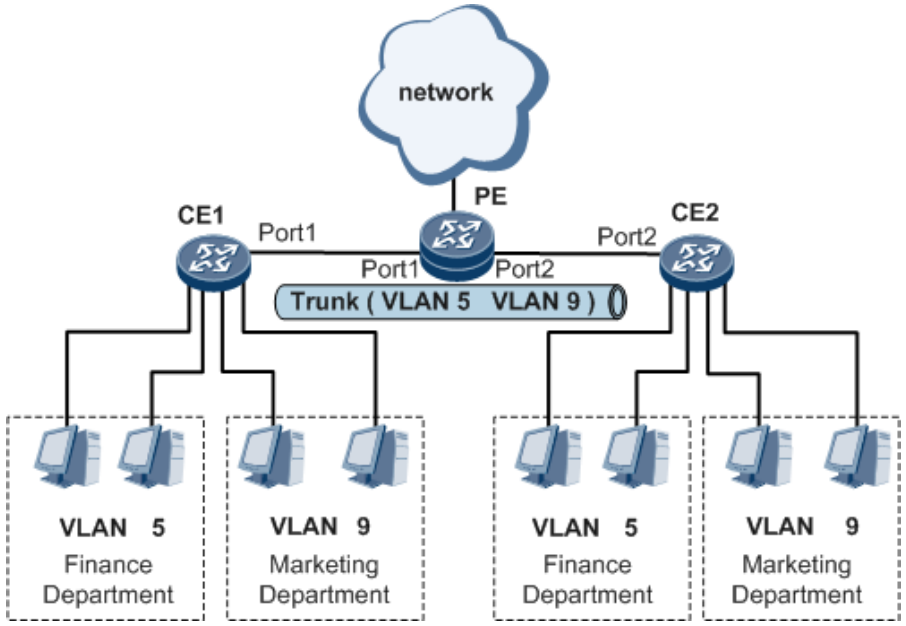
Vlan basado en puerto de conexión

Tipos de puertos

Trunk port: todas las VLAN's podran estar asociadas a este puerto. Las tramas siempre deberan ser etiquetadas.

(switchport mode trunk)





Tomado de: https://sites.google.com/site/tuxnots/materias-de-la-facu/gnu-linux/redesvirtualesvlans

Diseño de Vlans

Caso Universidad

La red institucional de un campus universitario suele separar los usuarios en tres grupos: alumnos, profesores y administración. Cada uno de estos grupos constituye un dominio de difusión, una VLAN, y se suele corresponder asimismo con una subred IP diferente. De esta manera la comunicación entre miembros del mismo grupo se puede hacer en nivel 2, y los grupos están aislados entre sí, sólo se pueden comunicar a través de un router.

Imagine que la universidad tiene una red con un rango de direcciones IP del tipo 192.16.XXX.0/24, cada VLAN, definida en la capa de enlace de datos (nivel 2 de OSI), se corresponderá con una subred IP distinta:

VLAN 10. Administración. Subred IP 192.16.10.0/24

VLAN 20. Profesores. Subred IP 192.16.20.0/24

VLAN 30. Alumnos. Subred IP 192.16.30.0/24

En cada edificio de la universidad hay un switch denominado de acceso, porque a él se conectan directamente los sistemas finales. Los switches de acceso están conectados con enlaces trunk (enlace que transporta tráfico de las tres VLANs) a un switch troncal, de grandes prestaciones, típicamente Gigabit Ethernet o 10-Gigabit Ethernet. Este switch está unido a un router también con un enlace trunk, el router es el encargado de llevar el tráfico de una VLAN a otra.

Tomado de: http://es.wikipedia.org/wiki/VLAN