Transparencias

de

Redes de Ordenadores

Tema 5

Switched LAN (Puentes)

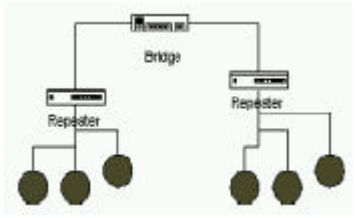
Uploaded by

IngTeleco

http://ingteleco.iespana.es
ingtelecoweb@hotmail.com

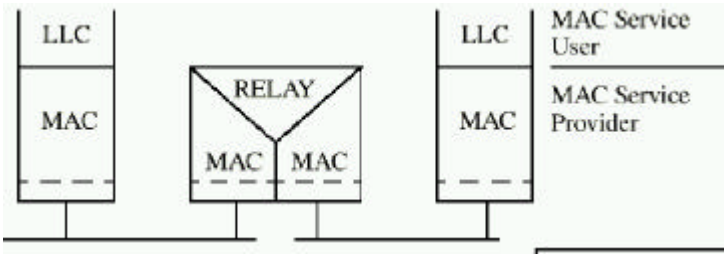
PUENTES (BRIDGES)

- Medio compartido:
  - Todos los nodos "comparten" la red
  - Sólo una máquina puede transmitir cada vez
  - Limitaciones de distancia: (pe. 205m para 100Base-T)
  - Rendimiento total limitado
  - Un único dominio de colisión
- Puentes:
  - Conectan redes compartidas separadas
  - Traducción de tramas/encapsulamiento
  - Reduce el tráfico unicast
  - Permiten múltiples conversaciones



PUENTES (BRIDGES)

- Dispositivos que operan en el nivel 2.
- Analizan cada trama que reciben y la reenvían selectivamente.
  - Analizan direcciones MAC.
  - Reenvían las tramas en función de la dirección MAC de destino.
  - Permiten aplicar filtros.
- Situaciones donde son necesarios:
  - Interoperabilidad
  - Distancia
  - Número de ordenadores
  - Tráfico
  - Fiabilidad
  - Seguridad



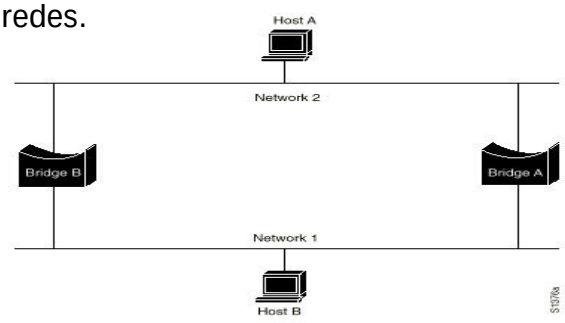
PUENTES TRANSPARENTES

- Presencia y operación transparente a los nodos de la red.
  - Aprende la topología de la red analizando la dirección de origen de las tramas que recibe.
    - Si recibe una trama procedente de A a través del puerto 1 concluye que a través del puerto 1 se alcanza dicho nodo.
  - Crea una tabla, utilizada para el reenvío:
  - Cuando se recibe una trama se extrae la dirección de destino:
    - Si aparece en la tabla se reenvía por el puerto correspondiente.
    - Si no aparece, se reenvía por todos los puertos salvo por el que llegó.
    - Las tramas multicast y broadcast se reenvían por todos los puertos.

Entry	MAC Addr	Port	active
1	0800900A2580	1	yes
2	002034987AB1	1	yes
3	0600A1987C00	2	yes
4	00503222A001	2	yes
5			
6			
7			
8			
9			
10			
11			
12			

PUENTES Y BUCLES

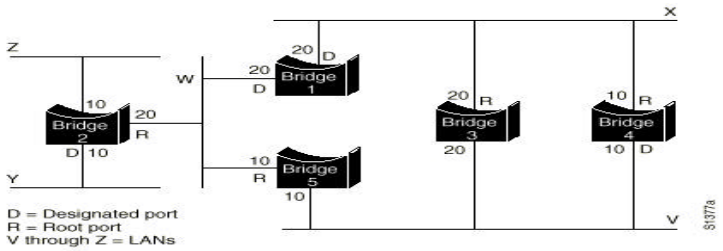
- El protocolo falla cuando hay varios caminos alternativos entre dos redes.



  - A envía un mensaje a B
  - B recibe dos veces el mensaje
  - Los Bridges anotarán a A sucesivamente en la Red 2 y la 1 (en algunos casos).
    - La contestación de B se descarta.
- Solución: Spanning Tree

SPANNING TREE: 802.1D

- Crea un subconjunto de la topología libre de bucles
  - Bloquea algunos puertos.
  - Tolerancia a fallos: los enlaces redudantes se consideran backups y pueen desbloquearse si se produce algún fallo.



  - Asigna un identificador único a cada puente: dirección MAC/prioridad.
  - Cada puerto se identifica con su dirección MAC y se le asigna un costo.

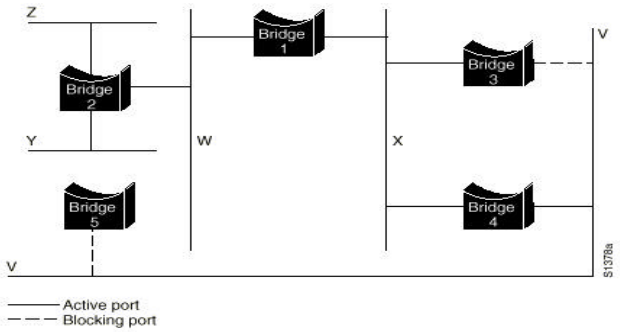
SPANNING TREE (ii)

- Autoconfiguración
  - Asigna un identificador único a cada puente: dirección MAC/prioridad.
  - Cada puerto se identifica con su dirección MAC y se le asigna un costo.
  - Selección del **puente raíz**: Identificador más bajo.
  - Selección del **puerto raíz** de cada puente: El que conduce al puente raíz con un costo agregado menor.
  - Selección de puentes y puertos designados para cada red.
  - Se realiza cuando se conecta el puente por primera vez y cada vez que se detecta un cambio de topología.
- Puente designado de red:
  - El que conduce al puente raíz con menor costo (dirección MAC en caso de igualdad).
  - El único que reencamina tramas hacia la red.
- Puerto designado:
  - Conecta con el puente designado a una red

SPANNING TREE (iii)

- Mensajes de configuración: BPDU
  - Se envían cada 4 segundos.

2	1	1	1	8	4	8	2	2	2	2	2
Protocol identifier	Version	Message type	Flags	Root ID	Root path cost	Bridge ID	Port ID	Message age	Maximum age	Hello time	Forward delay



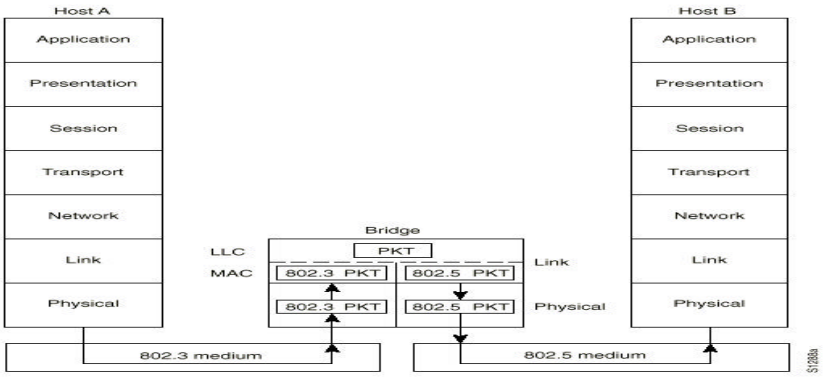
PUENTES REMOTOS

- Conectan dos LAN remotas.
- El puente está constituido por dos 'medios puentes' interconectados por una línea dedicada, o un enlace X.25, Frame Relay, ...

- También utiliza Spanning tree:
  - Topológicamente el enlace punto a punto se considera como una LAN con un puente en cada extremo.
- No hay un estándar: la interoperabilidad solo es posible entre equipos del mismo fabricante.
  - Las tramas LAN se encapsulan normalmente en tramas HDLC.

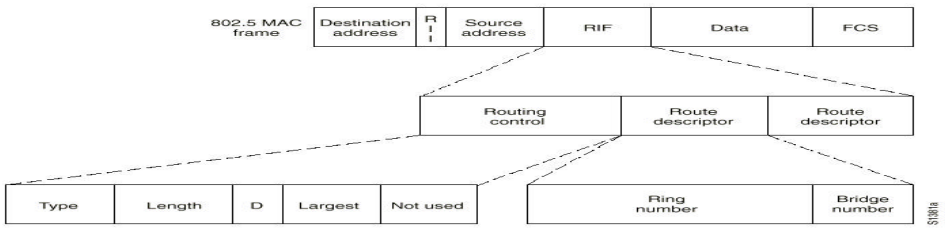
PUENTES TRADUCTORES

- Interconecta dos LAN con diferentes protocolos MAC
  - Reformateo de la trama**.**
  - Campos inexistentes.
  - Diferente velocidad.
  - Acuse de recibo.
  - Diferente tamaño de trama máximo.



Encamimamiento desde el origen

- La estación que emite una trama indica la ruta que debe seguir hasta su destino.
  - Campo adicional de la trama, detrás del campo dirección origen.
  - La presencia de información de routing se indica poniendo a 1 el primer bit de la dirección origen.
  - Secuencia de números de puente, LAN, puente, LAN, etc.,
    - Las LANs se numeran con direcciones de 12 bits únicas en toda la red.
    - Los puentes con direcciones de 4 bits únicas en el contexto de las LANs que interconectan.

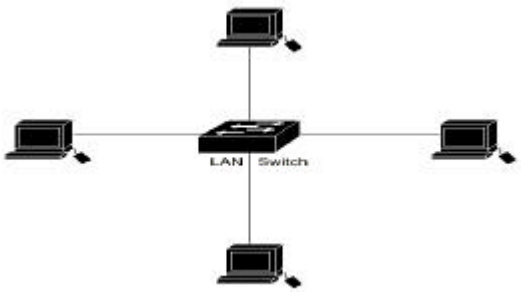


Encamimamiento desde el origen (ii)

- Descarta las tramas que no tienen 1 en el primer bit de la dirección origen.
- Análisis:
  - Busca del nº de LAN por la que ha llegado, si va seguido por su propio nº de puente, reenvía la trama a la LAN que le sigue en la secuencia.
- Información sobre la topología de la red:
  - Trama de descubrimiento (discovery frame).
    - Enviada en todas direcciones y retransmitida por todos los puentes en todas las LANs.
    - La estación de destino responde con una trama de acuse de recibo que viaja en orden inverso, cada puente anota en la trama de respuesta su propio número y el número de la LAN por la que la emite.
    - La estación de origen recibe una o varias tramas que le indican todas las rutas posibles hacia el destino especificado.
    - Elige la que considera óptima y la incluye en su tabla de rutas para poder utilizarla en posteriores envíos a dicha estación.

Switches

- Origen:
  - Problemas de Ancho de Banda
- Bridge multipuerto:
  - Dividen un *"dominio de broadcast"* en *"dominios de colisión"*
    - Aislan el tráfico.
  - Inspeccionan la dirección MAC de destino y reenvían la trama por el puerto adecuado.
  - Las tramas broadcast se envían por todos los puertos.
  - Utilizan procedimientos de aprendizaje y "spanning tree".



Switches: Taxonomía

- Modos de operación:
  - CUT THROUGH
    - La trama se reenvía sin recibirla completa.
    - Almacenan los primeros 512 bits hasta asegurarse de que no hay colisión.
    - Baja latencia (1/20 de S&F)
  - STORE AND FORWARD
    - Almacena la trama, comprueba el CRC y se reenvía.
    - Necesario en algunos casos (diferentes velocidades, puerto de salida ocupado)
- Buffering:
  - INPUT BUFFERING
    - Buffer en cada pto. de entrada, retransmisión cuando el pto. de salida está libre
    - *"Head-of-line blocking"*
  - OUTPUT BUFFERING
    - Buffer en cada puerto de salida.
    - Acceso denegado a un puerto si otro envía un tráfico a dicho destino.
  - PATH BUFFERING
    - Hay buffer en el puerto de entrada y de salida
- Blocking - non-blocking
  - Colisiones internas o no.

Switches: nivel de conmutación

- NIVELES
  - **Capa 2**
    - Bridge multipuerto: Más barato, mejor rendimiento, full-duplex.
    - Identifican el destino por la dirección MAC.
    - Crean dominios de colisión separados.
    - Transparentes.
  - **Capa 3**
    - Bridge + Router (sin funciones de acceso a través de WAN).
    - Mejor rendimiento que el router
      - un orden superior (varios millones - millón).
      - Basados en hardware.
    - Identifican el destino por la dirección de red.
      - No diferencian aplicaciones.
    - Packet by Packet (PPL3) Y Cut-trough (CTL3)
      - CTL3: Analiza el destino del primer paquete de una serie, establecen una conexión y conmutan a nivel 2 (+ Rendimiento).
    - Ventajas:
      - Usan protocolos de red (RIP y OSPF) para para procesar rutas externas al switch.
      - PPL3: análisis de la trama IP.
      - Priorización, filtros a nivel de red, autenticación.

Switches: nivel de conmutación (ii)

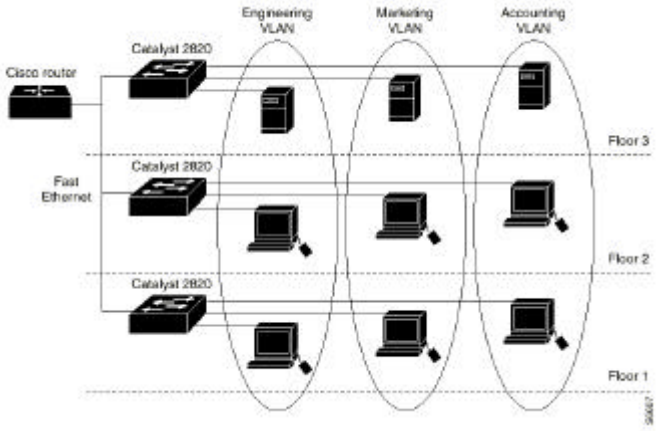
- **Capa 4**
  - Conecta directamente origen y destino y permite identifica la aplicación de origen
  - Generar calidades de servicio en función de las aplicaciones.
  - Filtros de seguridad.
    - Ya introducidos por los router, pero a base de reducir el rendimiento por el uso de sw y BD.
    - En los switches se consigue el mismo efecto con mejor rendimiento.
  - Arquitectura
    - Crossboard
      - » Esquemas complejos de buffering.
      - » Priorización por flujos.
    - Memoria compartida y cola de salida
      - » Múltiples niveles de prioridad
      - » Se reserva una capacidad de memoria para cada tipo de tráfico
    - Colas por flujos
      - » Una cola por flujo
      - » El espacio por cola y el total de colas (y de flujos está limitado)

VLAN

- LAN tradicionales:
  - Nodos conectados mediante hub.
    - Propaga todos los datos entrantes por la red, incluidas las colisiones.
    - Dominio de colisión o segmento de LAN.
  - Bridges o switches para mejorar rendimiento:
    - Evita que se propaguen las colisiones.
    - Retransmitirán todas las tramas de broadcast o multicast que reciban.
    - Dominio de broadcast o LAN.
  - Routers para separar la red en diferentes dominios de broadcast.
- Los nodos que pertenecen a una LAN deben estar próximos:
  - La definición se realiza a través de la conexión física.
- Las VLAN se desarrollan como:
  - Alternativa al uso de routers.
  - Liberación de la servidumbre de la ubicación.

VLAN (ii)

- Resultan difíciles de definir:
  - Un dominio de broadcast.
  - Un grupo de estaciones, quizás sobre varios segmentos LAN, que no están constreñidos por su localización física y pueden comunicarse como si estuvieran en una LAN común.
- Vista física / lógica



VLAN: Ventajas

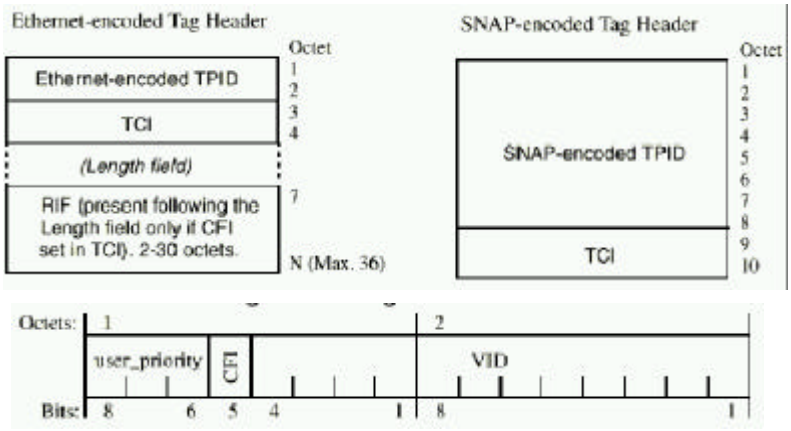
- Rendimiento
  - Donde el tráfico de broadcast y multicast sea importante.
  - Los switches son más rápidos que los routers, lo que se aprecia a medida que el tráfico aumenta.
- Formación de Grupos de Trabajo Virtuales
  - Crear grupos temporales sin desplazar físicamente a los miembros.
- Administración simplificada
  - El 70% del costo de la red se debe a las ampliaciones, movimientos, cambios de usuarios.
  - Evitar recablear y reconfigurar hubs y routers.
- Costo Reducido
  - Los switches son mucho más baratos que los routers.
- Seguridad
  - Periódicamente, pueden difundirse por la red datos sensibles.
  - Se restringe el acceso a esta información a los usuarios autorizados.

VLAN: estandares y conceptos básicos

- Estándares:
  - 802.1 Q
    - Define un método de establecimiento de VLANs
    - Establede el etiquetado de tramas (Tagged Frames)
    - Proporciona un medio para mantener información de prioridad a través de LANs.
  - GVRP (GARP VLAN Registration Protocol)
    - Propaga el registro a una VLAN por la red
- Conceptos básicos:
  - Tagged Frames: Se inserta en la trama información VLAN Id y prioridad.
  - Trunk Links: Permite que varias VLANs atraviesen un enlace.
  - Access Links: Extremo de la red, donde conectar los dispositivos antiguos
  - VID: Identificador de la VLAN

Tagged Frames

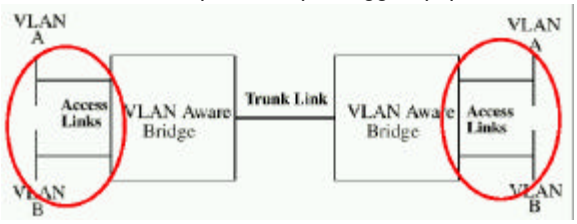
- 4 bytes insertados tras las direcciones de Emisión y Destino
- Tagged Protocol Identifier (TPID)=2 bytes (x8100)
- Tagged Control Information (TCI)=2 bytes



Trunk y Access Links

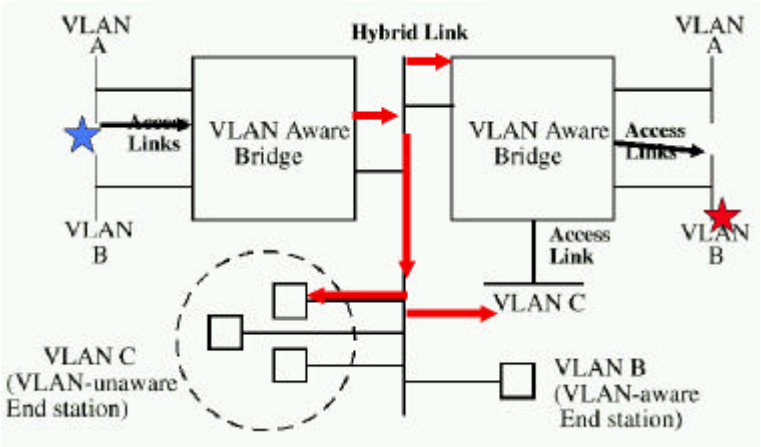
- *Enlace "Trunk"*
  - Enlace entre dispositivos "VLAN-aware".
  - Las tramas que circulan son etiquetadas ("tagged frames").

- *Enlace de acceso*
  - Conecta a un dispositivo "VLAN-unaware" a un puerto de un "switch VLAN-aware".
  - Las tramas no deben estar etiquetadas ("untagged"), pertenencia ser implícita.



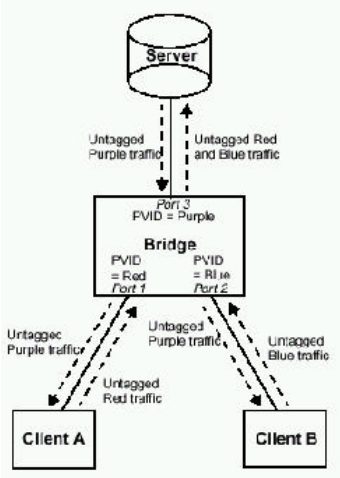
Hybrid Links

- *Enlace híbrido*
  - Combinación de los dos anteriores.
  - Existen tanto dispositivos "VLAN-aware" como dispositivos "VLAN-unaware".
  - Puede contener tanto tramas etiquetadas como no, pero todas las tramas de una VLAN específica deben ser del mismo tipo.



Tablas

- MFD (Multiple forwarding databases):
  - Aprendizaje independiente
  - Cada VLAN direcciones MAC independientemente, duplicando las direcciones MAC si es preciso
- SFD (Single forwarding databases:
  - Aprendizaje compartido
  - No duplica las direcciones MAC
  - Son posibles las VLAN asimétricas
- VLAN asimétricas
  - Los servidores heredados (legacy) pueden comunicarse con clientes heredados mediante un enlace físico
  - Los clientes heredados no pueden comunicarse entre sí.

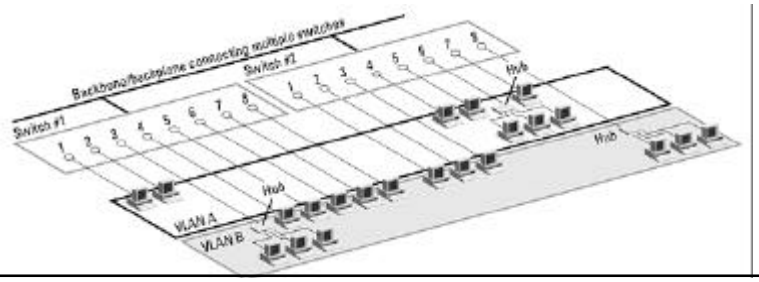


Operación de VLAN

- IEEE 802.1Q
- Un switch recibe una trama:
  - Identificar la VLAN de la que procede
    - Por el puerto de entrada, la dirección MAC de origen, …
    - El switch mantiene una BD con la equivalencia entre cada VLAN y los campos utilizados para indicar su pertenencia.
  - Determinar dónde debe enviarse la trama (según la operación normal de la LAN)
  - Determinar si la trama de reenviarse o no
    - Base de Datos de filtrado.
  - Determinar si es preciso incluir el identificador de la VLAN o no en la trama.
    - Identificación implícita de la VLAN (Nº de puerto, dirección MAC, ...)
    - Identificación explícita con una etiqueta (tag) añadida en la cabecera de la trama.
      - Dispositivos capaces de gestionar "tags": VLAN-aware.

Tipos de VLAN

- ***VLAN Nivel 1: Pertenencia por Puerto***
  - Se agrupan puertos de un switch (pe, puertos 1, 2, 3, 7, y 8 componen la VLAN A, mientras los puertos 4, 5, y 6 componen VLAN B).
  - En la 1ª generación de switches la creación de VLAN quedaba restringida a un solo switch.
  - La 2ª generación soporta VLAN que se extienden a varios switches (Figura)
  - Sigue siendo el método más habitual para crear VLAN
  - Inconvenientes:
    - No permite que varias VLAN compartan el mismo segmento físico (puerto)
    - Tampoco permite movilidad de los usuarios.



Tipos de VLAN (ii)

- *VLAN Nivel 2: Pertenencia por la dirección MAC*
  - El switch mantiene una tabla con las direcciones MAC que pertenecen a cada VLAN.
  - Como la dirección MAC es característica de cada estación, este tipo de definición de la pertenencia a una VLAN puede considerarse basada en el usuario.
  - Cuando un nodo se mueve no se necesita ninguna reconfiguración de la VLAN.
  - Inconvenientes:
    - La pertenencia a la VLAN debe asignarse desde el principio.
    - Cuando se usan portátiles con "docking stations" la dirección MAC está asociada con éstas y no con el portátil,.
    - Si varias VLAN comparten medio físico pueden presentar problemas de degradación de rendimiento y seguridad.
    - La información intercambiada entre estos switches es de tal calibre (cuando la red es amplia) que también puede resentirse el rendimiento.

Tipos de VLAN (iii)

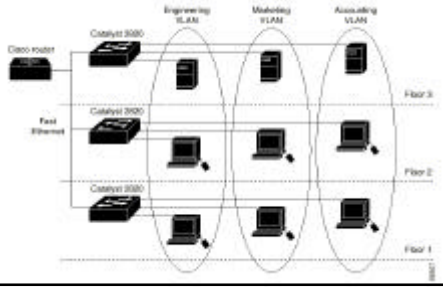
- *VLAN Nivel 3 : Pertenencia por Tipo de Protocolo*
  - Tipo de protocolo de red indicado en al cabecera de la trama MAC.
- *VLAN Nivel 3 : Pertenencia por Dirección IP*
  - La dirección IP (subred) puede utilizarse para clasificar la pertenencia a una VLAN.
  - No debe confundirse con las funciones de los router, las direcciones IP se utilizan sólo como un método para determinar la pertenencia o no a una VLAN.
  - Algunos vendedores incorporan capacidades de nivel 3 en los switches, añadiendo funciones normalmente asociadas con el routing, con el reencaminamiento de datagramas incorporado en chips ASIC con la consiguiente mejora de rendimiento.
  - Ventajas:
    - Permite dividir la red por tipo de protocolo utilizado (en VLANs con orientación al servicio o a la aplicación).
    - Desplazamientos sin reconfiguraciones.
    - No necesita etiquetar tramas, la información de la VLAN va en la propia trama.
  - Inconveniente:
    - Resulta más lento inspeccionar la cabecera de red que la cabecera MAC.
    - Los switches de nivel 3 resultan más lentos que los de nivel 2.

TIPOS DE VLAN (iv)

- *VLAN de niveles superiores (Nivel 4)*
  - Definir la pertenencia a una VLAN basándose en aplicaciones, servicios o combinaciones de estas.
  - Puede utilizarse el tipo de protocolo de transporte o bien campos de la cabecera de transporte para realizar la definición de la pertenencia a un grupo (TCP o UDP, puertos de origen destino, ...)
  - Ventajas:
    - Permite dividir la red por atendiendo específicamente a la aplicación o servicio, independientemente del usuario (estación final).
    - Desplazamientos sin reconfiguraciones.
  - Inconveniente:
    - La inspección es la más lenta de todas.
- 802.1Q define sólo VLAN de nivel 1 y de nivel 2 basadas en tipo de protocolo, el resto son soluciones propietarias.

Componentes de una VLAN

- Switches
  - Segmentan lógicamente estaciones conectadas a ellos.
    - Puntos de entrada a la VLAN para las estaciones finales
    - Agrupan usuarios, puertos o direcciones lógicas en comunidades de interés.
    - Pueden utilizarse varios switches conectados agrupar en comunidades.
    - Emplean el identificador de trama, o etiquetado (tagging) para agrupar lógicamente a los usuarios en VLANs administrativamente definidas.
- Routers
  - Proporcionan comunicaciones entre grupos de trabajo
    - Gestión de broadcast y procesamiento de rutas.
    - Comunicación entre VLAN y acceso a recursos compartidos.
    - Porporcionan acceso a sitios remotos a través de enlaces WAN.



Comunicación de la pertenencia a una VLAN

- Los switches deben disponer de un modo para saber a qué VLAN pertenece el tráfico procedente de otros switches.
  - Las VLAN de nivel 2 deben comunicar la pertenencia explícitamente, en el resto la comunicación es implícita.
- Comunicación entre switches de información de la VLAN:
  - *Mantenimiento de tablas mediante señalización:*
    - Al recibir la primera trama de una estación, el switch resuelve la dirección MAC o el puerto de entrada con su pertenencia a la VLAN y la guarda en tabla.
    - Difunde esta información constantemente a todos los demás switches.
    - Si la red es grande, la señalización de actualización de las tablas puede congestionar el backbone: no es escalable.
  - *Etiquetado de Tramas.*
    - Se inserta una cabecera en cada trama en los tramos entre switches para identificar la VLAN a la pertenece una trama de nivel MAC.
  - *TDM*
    - El método menos utilizado es multiplexar en el tiempo, reservando canales para cada VLAN.
    - Se eliminan los problemas de sobrecarga, pero dr desperdicia ancho de banda debido a los slots no utilizados.