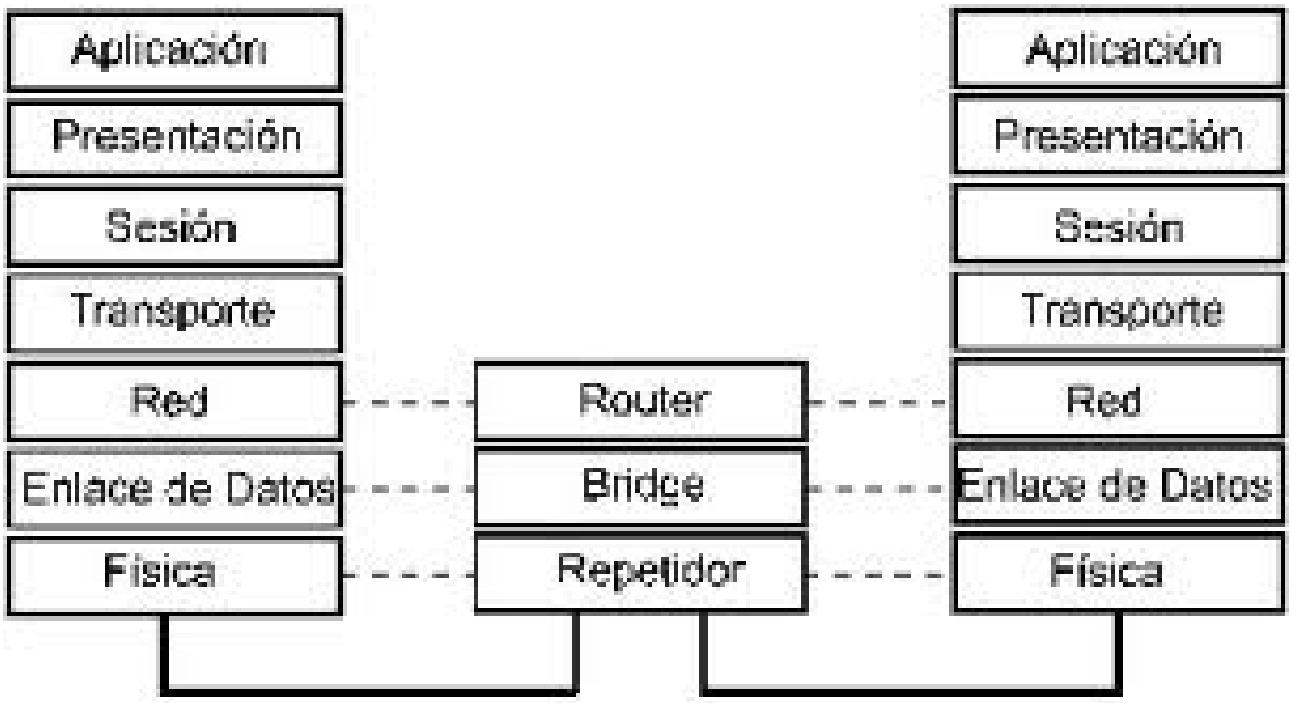
LAN switches L2 y L3 - VLANs - Trunk 802.1q

Logioco Pablo

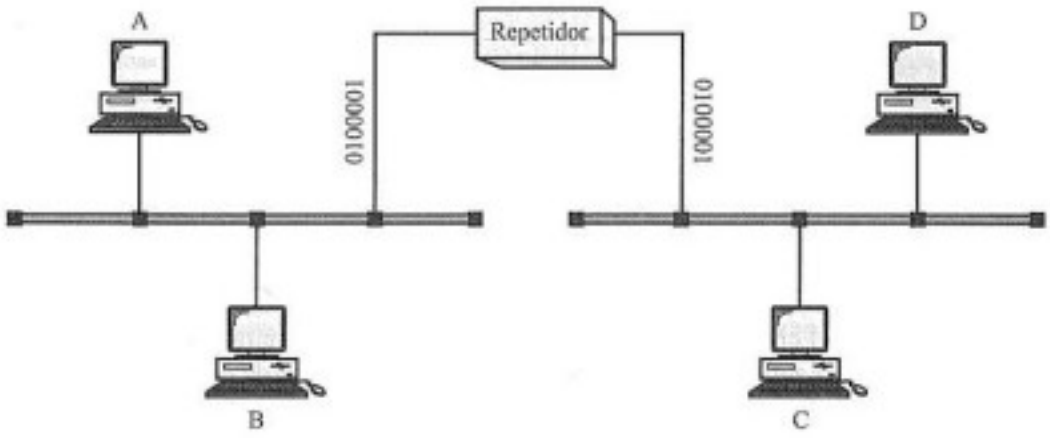
Cardozo Griselda

Los dispositivos de interconexión son usados para interconectar las redes en las diferentes capas de red. Los dispositivos pueden funcionar en:



Repetidores

Uno de los elementos de interconexión de redes es el repetidor.



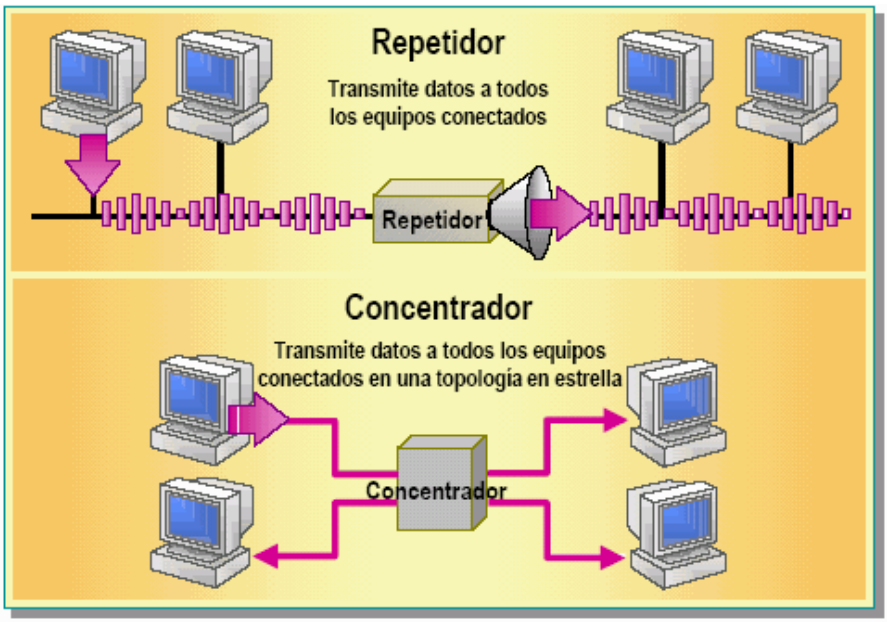
La norma IEEE 802.3 define el repetidor como un dispositivo usado para extender la longitud, topología o interconexión del medio físico, más allá de los límites impuestos por un simple segmento, realizando funciones tales como restaurar la amplitud y forma de la señal. Por tanto, el repetidor actúa solamente sobre la capa física del modelo OSI y su única función es la de regenerar la señal propagada por el medio.

Como los repetidores no discriminan entre los paquetes generados en un segmento y los que son generados en otro segmento, hace que los paquetes lleguen a todos los nodos de la red. Debido a esto existen más riesgo de colisión y más posibilidades de congestión de la red.

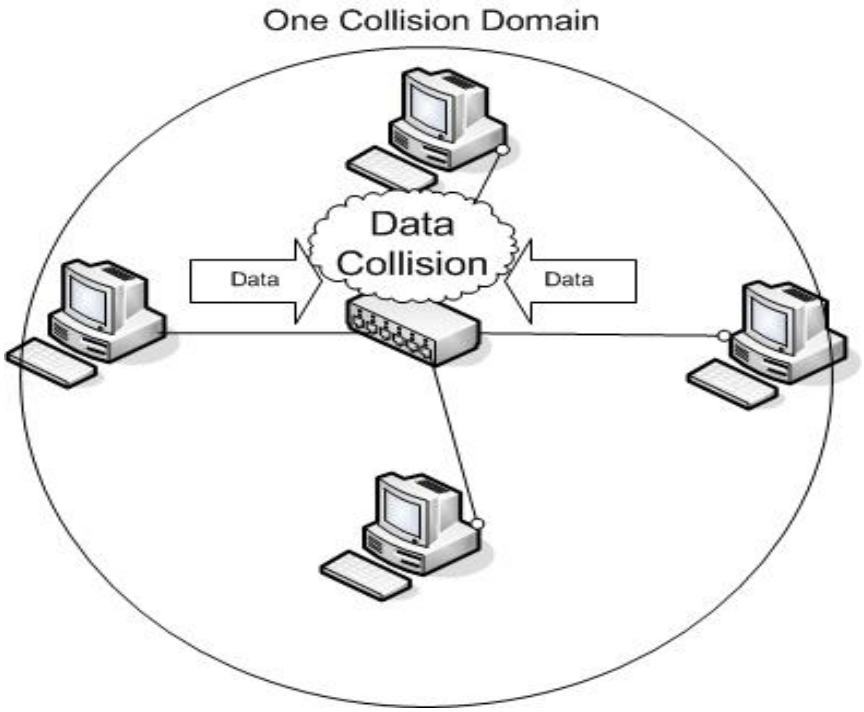
Otra función de los repetidores es monitorizar todos los segmentos conectados para verificar que la red funciona correctamente. Cuando algo falla en un determinado segmento, por ejemplo; se produce una rotura, todos los segmentos Ethernet pueden quedar inoperantes. Los repetidores limitan el efecto de estos problemas, a la sección de cable rota, "segmentando" la red, desconectando el segmento problemático y permitiendo al resto seguir funcionando correctamente. La avería de un segmento en una red punto a punto, habitualmente, sólo desactivará un ordenador, lo que en una topología de bus ocasionaría la desactivación de todos los nodos del segmento.

hubs

El hub es un dispositivo que tiene la función de interconectar las computadoras de una red local. Son múltiples repetidores de puerto.



Los hubs no desempeñan funciones de red tales como dirigir los datos según las direcciones.
Un repetidor recibe una señal digital y la reenvía a todos los puertos activos.
Todos los segmentos LAN de la figura pertenecen al mismo **dominio de colisión;** es decir, cuando dos o más dispositivos en los segmentos LAN transmiten al mismo tiempo, habrá una colisión, entonces se envía una señal de atasco diciendo a los demás dispositivos que no pueden enviar datos.
La utilización de hubs para proporcionar acceso a la red a una mayor cantidad de usuarios reduce el rendimiento para cada usuario, ya que debe compartirse la capacidad fija de los medios entre cada vez más dispositivos.
Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones. Un dominio de colisiones también se denomina segmento de red. Por lo tanto, los hubs y repetidores tienen el efecto de aumentar el tamaño del dominio de colisiones.
La interconexión de los hubs forma una topología física que se denomina estrella extendida. La estrella extendida puede crear un dominio de colisiones notablemente expandido.



Data link layer switching / Conmutación de capa de enlace de datos (2)

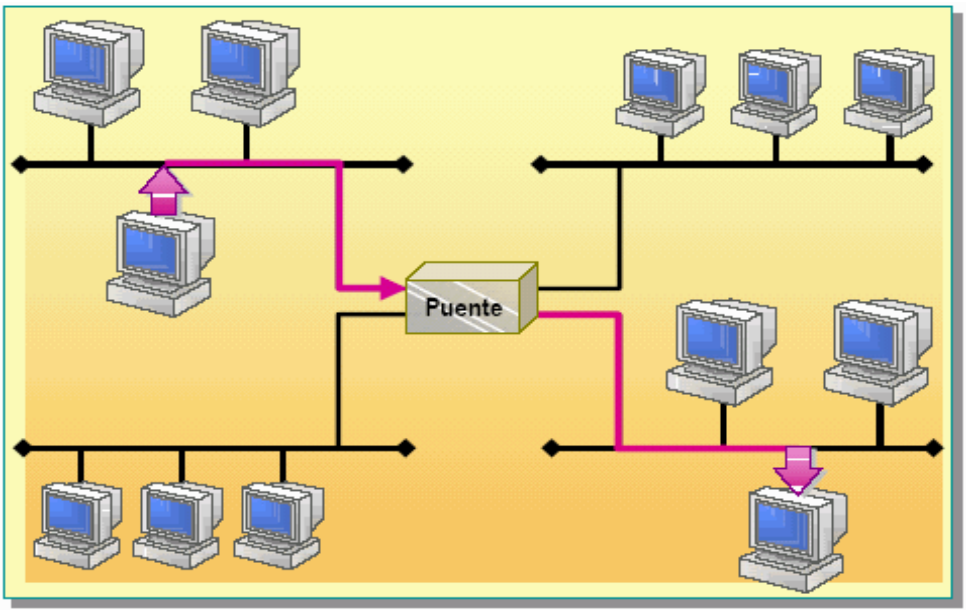
Puentes y Switches LAN

Bridge

Un bridge al igual que un hub sirve para interconectar segmentos de redes LAN . Un **puente de red** o ***bridge*** es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

La figura de abajo muestra cómo cuatro departamentos pueden ser interconectados con un bridge. Cuando los departamentos se interconectan mediante un bridge, la red interconectada

se denomina **LAN**, y cada una de las porciones departamentales de la red como **segmento.** Cada segmento es un dominio de colisión aislado.



Los bridges pueden resolver muchos de los problemas que sufren los hubs.

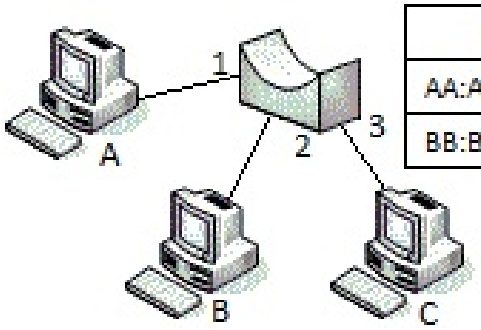
1. - Permiten comunicación interdepartamental mientras mantienen los dominios de colisión aislados para cada departamento.
2. Pueden interconectar diferentes tecnologías LAN
3. No hay un límite respecto al tamaño de una LAN; en teoría, utilizando bridges, es posible construir una LAN que abarque todo el globo

Encaminamiento y filtrado en bridges

Filtrado es la capacidad de un bridge para determinar si un marco debe ser remitido a alguna interfaz o simplemente debe ser dejado. **Encaminamiento** es la capacidad para determinar las interfaces a las que se debiera dirigir un marco, y dirigir, por tanto, el marco a esas interfaces. El filtrado y encaminamiento en bridges se realizan con una **tabla de bridge.**

Dicha tabla contiene entradas para alguno (pero no necesariamente para todos) de los nodos de una LAN. Una entrada en la tabla de bridge contiene

- la dirección LAN del nodo
- la interfaz del bridge que conduce al nodo
- el instante en que se colocó en la tabla la entrada para el nodo



Address	Interface	Time
AA:AA:AA:AA:AA:AA	1	8:12
BB:BB:BB:BB:BB:BB	2	9:45

Para comprender como funciona el filtrado y el encaminamiento de bridge, supongamos que un marco con una dirección de destino DD-DD-DD-DD-DD-DD llega al bridge en la interfaz 1. El bridge se fija en su tabla que la interfaz que conduce a la dirección DD-DD-DD-DD-DD-DD es Y.

- si Y es igual 1, entonces el marco está llegando de un segmento de LAN que contiene al nodo con la dirección MAC DD-DD-DD-DD-DD-DD. No hay necesidad de remitir el marco a ninguna de las demás interfaces; el bridge realiza la función de filtrado desechando el marco.
- si Y es distinto de 1,entonces el marco necesita ser remitido al segmento de LAN unido a la interfaz Y. El bridge realiza su función de remisión poniendo el marco en búfer de salida que precede a la interfaz Y.

Estas reglas sencillas permiten a un bridge mantener dominios de colisión separados para cada uno de los segmentos LAN conectados a sus interfaces, mientras permite que se comuniquen los dominios.

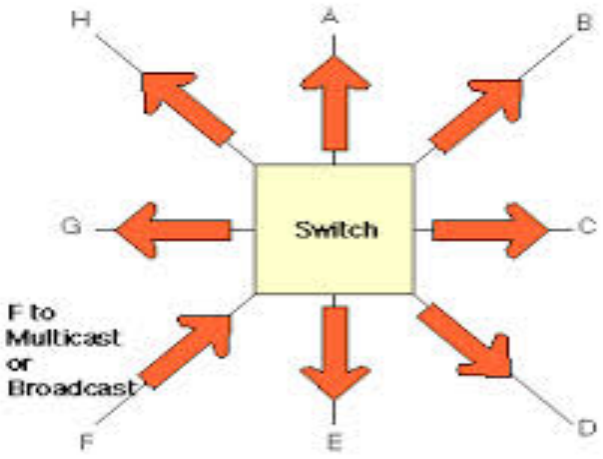
Autoaprendizaje

Un bridge tiene la propiedad de que su tabla se construye automáticamente, dinámicamente y autónomamente. Esta capacidad se lleva a cabo como sigue:

1. La tabla esta vacía inicialmente.
2. Cuando un marco llega una de las interfaces y la dirección de destino del marco no está en la tabla, entonces el bridge remite copias del marco a los búferes de salida que preceden a todas las demás interfaces.
3. Por cada marco recibido, el bridge almacena un su tabla (1) la dirección LAN en el campo de dirección de origen del marco, (2) la interfaz desde que la que llega el marco, y (3) el tiempo actual. De esta forma el bridge registra en su tabla el segmento LAN en el que reside el nodo emisor. Si cada nodo de la LAN envía eventualmente un marco, entonces cada nodo será registrado eventualmente en la tabla.
4. Cuando un marco llega a una de las interfaces y la dirección de destino está en la tabla, entonces el bridge difunde el marco hacia la interfaz apropiada .

5. El bridge borra una dirección en la tabla si no se han recibido marcos con esa dirección como dirección de origen después de cierto periodo de tiempo (**tiempo de envejecimiento**).

De esta forma el administrador no necesita configurar las tablas del bridge en el momento de la instalación o cuando se elimina un host de uno de los segmentos LAN. Como los bridges son del tipo conectar y funcionar, se conocen también como **bridges transparentes.**



Spanning Tree Protocol (STP)

Es un protocolo de red de nivel 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.

Los bucles ocurren cuando hay rutas alternativas hacia un mismo destino (sea una máquina o segmento de red). Estas rutas alternativas son necesarias para proporcionar redundancia y así ofrecer una mayor fiabilidad a la red, dado que en caso de que un enlace falle, los otros puede seguir soportando el tráfico de ésta. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red (bridge) o un conmutador de paquetes Cuando existen bucles en la topología de red, los dispositivos de interconexión de nivel de enlace de datos reenvían indefinidamente las **tramas broadcast y multicast**, creando así un bucle infinito que consume tanto el ancho de banda de la red como CPU de los dispositivos de enrutamiento. Esto provoca que se degrade el rendimiento de la red en muy poco tiempo, pudiendo incluso llegar a quedar inutilizable.

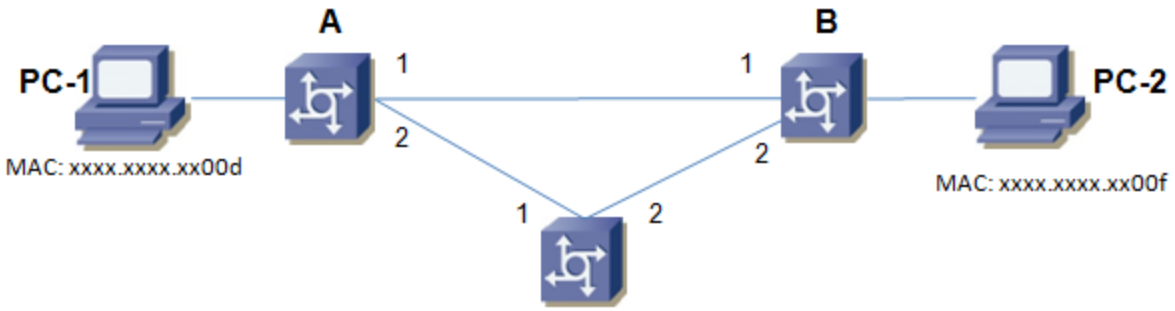
Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN.

¿Por qué son buenas las topologías redundantes?

- **La redundancia permite que las redes sean tolerantes a las fallas.**
- **La redundancia en una red es necesaria para protegerla contra la pérdida de conectividad debido a la falla de un componente individual**

Inconvenientes

- **Bucles de capa 2**
- **Tormenta de Broadcast**
- **Tramas duplicadas**



El detonante es cuando entra en la red una nueva estación de la cual los switches no saben su ubicación. Se genera un ciclo infinito de solicitudes broadcast entre los switches para tratar de encontrar el equipo destino.

Secuencia de eventos. PC-1 envía datos a PC-2

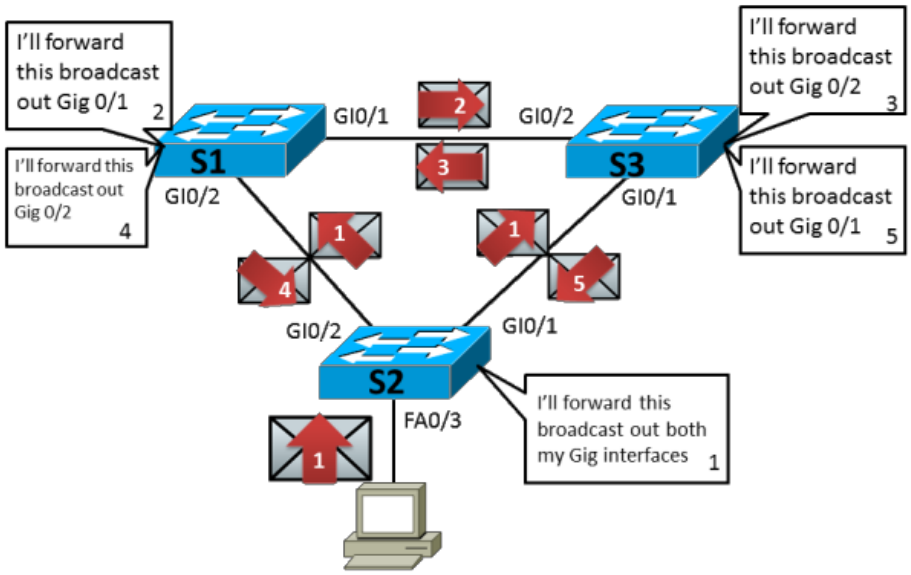
Estado inicial: Ningún switch conoce la ubicación de PC-1 ni PC-2

1.El switch A recibe la trama y no conoce la ubicación del PC-2, entonces emite un mensaje broadcast.
2.El switches B recibe el broadcast y registra la MAC del PC-1 en el puerto 1
3. El switch C recibe el broadcast y registra la MAC del PC-1 en el puerto 1

4.Como B no conoce la MAC del PC-2 hace también un broadcast por todos los puertos menos el puerto por el que recibió la trama
5.Como C no conoce la MAC del PC-2 hace también un broadcast por todos los puertos menos el puerto por el que recibió la trama
6.C recibe entonces un nuevo mensaje indicando que la MAC del PC-1 la encuentra por el puerto 2.
7.B recibe también el nuevo mensaje indicando que la MAC del PC-1 esta en el puerto 2.
8.De nuevo C y B contestan a ese nuevo broadcast pero esta vez el mensaje llega a A.
9.A recibe el broadcast indicando que la MAC del PC-1 la encuentra primero por el puerto 1 y luego por el puerto 2.
10.En algún momento el switch B recibe contestación al mensaje broadcast desde el PC-2 y encuentra la ubicación y la propaga, pero ese mensaje es alterado varias veces en los otros switches debido a los múltiples mensajes broadcast que circulan por la red.

Al cabo de un tiempo, la red se satura de mensajes broadcast y se vuelve indisponible.

La solución a la tormenta de broadcast es utilizar STP. STP es un protocolo utilizado para evitar los bucles en redes con topología redundante. Su funcionamiento se basa en bloquear de forma lógica los enlaces redundantes y levantando el bloqueo cuando se produzcan caídas en los enlaces no bloqueados.

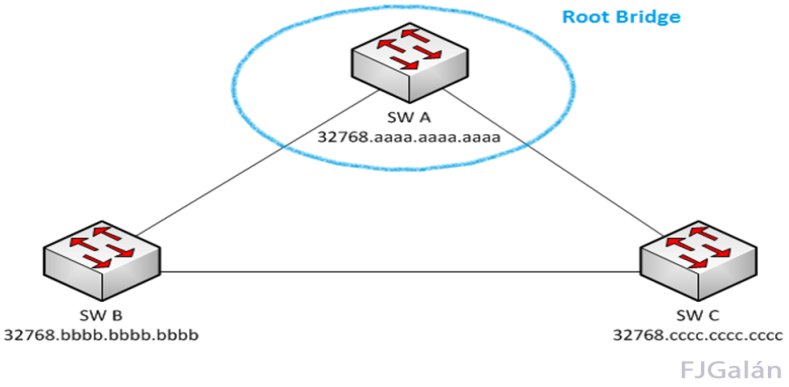


Funcionamiento de STP

Paso 1. Elección del Bridge Raíz

Cada switch tiene asignado un Bridge ID. El switch con menor Bridge ID es elegido como Bridge root o puente raíz.

A continuación se muestra un escenario de tres switches, SW A, SW B y SW C, cuyas direcciones MAC son aaaa.aaaa.aaaa, bbbb.bbbb.bbbb y cccc.cccc.cccc respectivamente. Dado que la prioridad por defecto es la misma para todos los switches, SW A sería elegido como puente raíz.

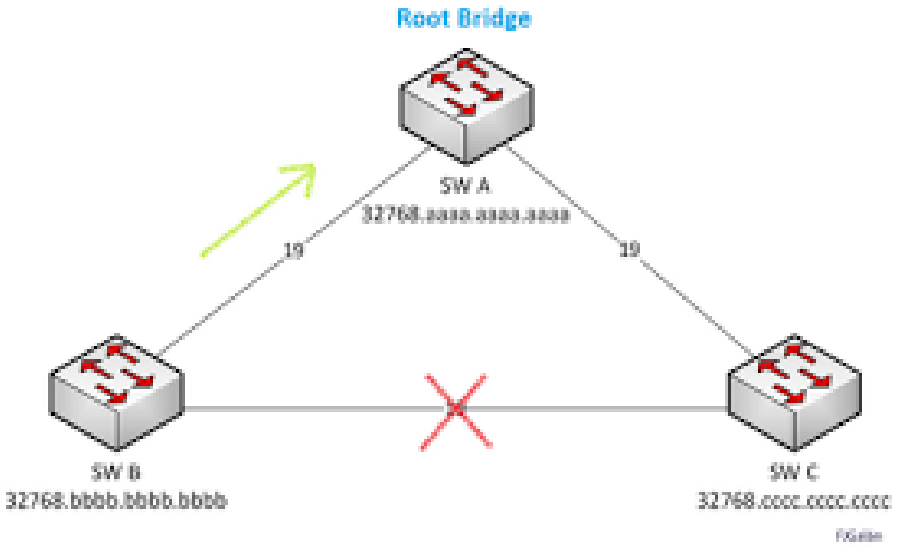


Paso 2. Elección del Root-port

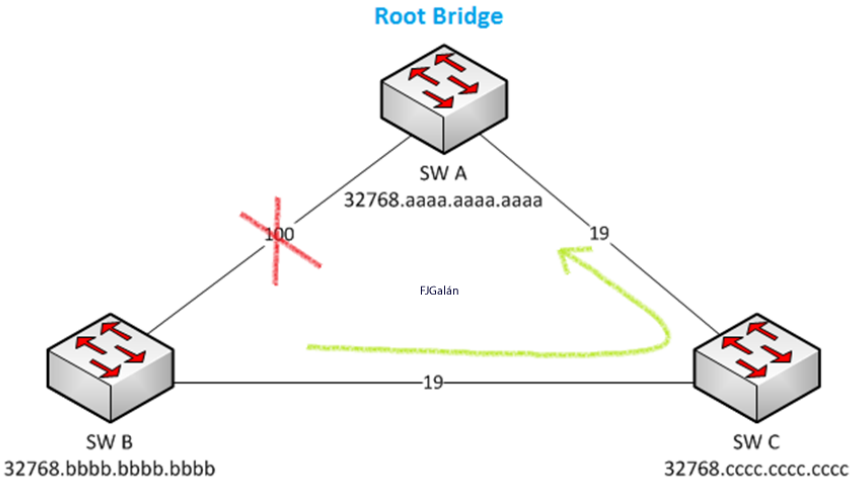
Luego de seleccionar el root bridge, cada switch debe encontrar el mejor camino a ese root. Ese camino es el root-port.
El coste de los enlaces depende de la velocidad de los mismos, y viene especificado para Ethernet por la IEEE en la siguiente tabla.

Velocidad del enlace	Coste
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

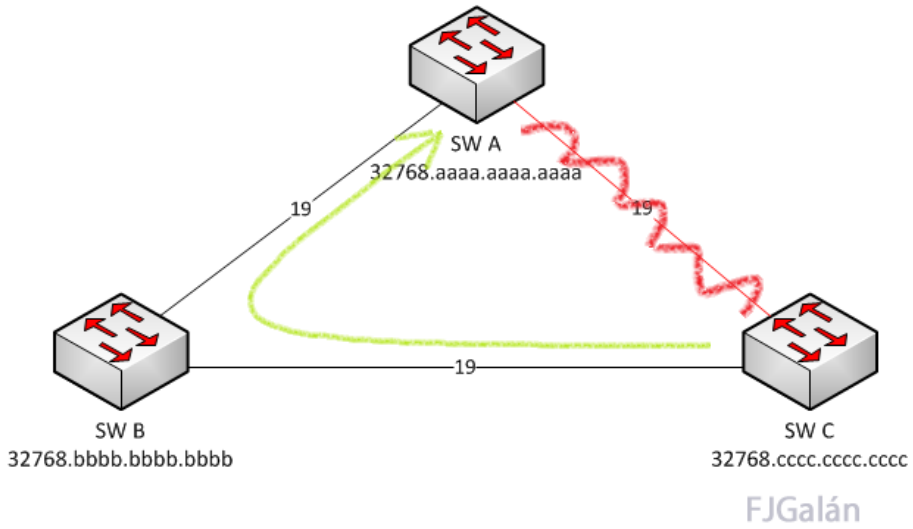
Al igual que en el caso del Bridge ID, un menor valor numérico implica mayor prioridad. De este modo, si todos los enlaces del escenario tienen un costo de 19, SW B elegirá el enlace directo a SW A, ya que el costo de enlace es menor que si va a través de SW C



Sin embargo, si el enlace entre SW B y SW A tiene un costo de 100 y los otros dos siguen siendo de 19, SW B elegirá como camino para llegar al Root Bridge la ruta pasando a través de SW C, ya que 19 + 19 < 100.



Por último, vamos a ver qué sucede cuando un enlace se cae. Evidentemente, la red tiene que seguir funcionando (si no, ¿para qué queremos redundancia?), por lo que los switches recalcularán la mejor ruta hasta el Root Bridge ignorando el enlace caído.



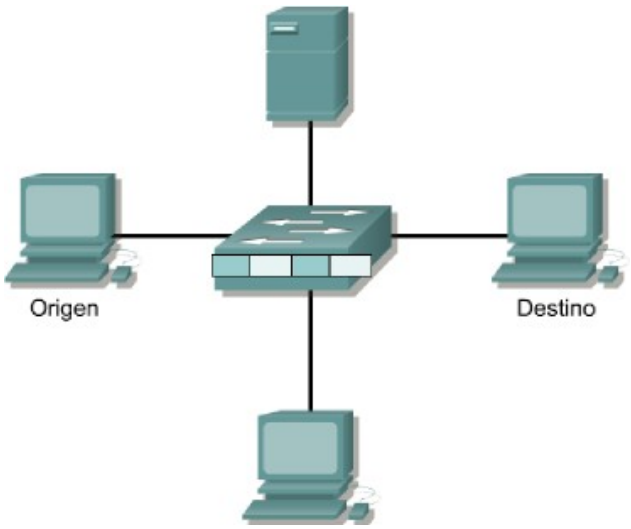
Switch

Los switch son esencialmente bridges multiinterfaz. Como los bridges, reenvían y filtran marcos utilizando las direcciones de destino LAN, y construyen automáticamente tablas de difusión utilizando las direcciones origen de los marcos que atraviesan por ellos.
Los switch ofrecen una conexión de red más directa entre los equipos de origen y destino. Cuando un switch recibe un paquete de datos, crea una conexión interna separada, o segmento, entre dos de sus puertos cualquiera y reenvía el paquete de datos al puerto apropiado del equipo de destino únicamente, basado en la información de la cabecera de cada paquete. Esto aísla la conexión de los demás puertos y da acceso a los equipos origen y destino a todo el ancho de banda de una red.
La diferencia más importante entre un bridge y un switch es que los bridges normalmente tienen un número pequeño de interfaces (de dos a cuatro), mientras que los switches pueden llegar a tener docenas de interfaces.
Otra diferencia importante entre un bridge y un switch es que la mayoría de éstos trabaja también en un modo **full-duplex**, es decir, pueden enviar y recibir marcos al mismo tiempo sobre la misma interfaz.

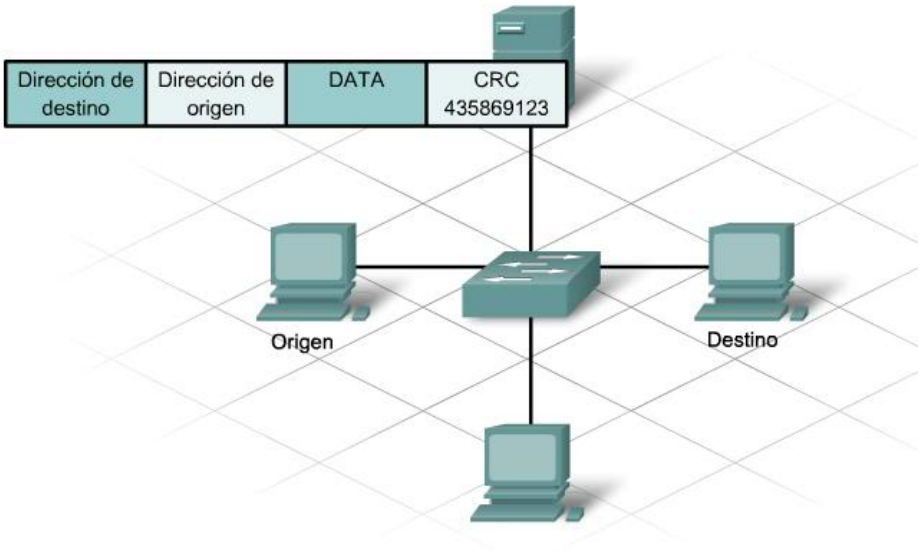
Los switches basados en paquetes suelen usar uno de los siguientes tres métodos para enrutar el tráfico:

- Método de corte
- Almacenamiento y envío
- Libre de fragmentos

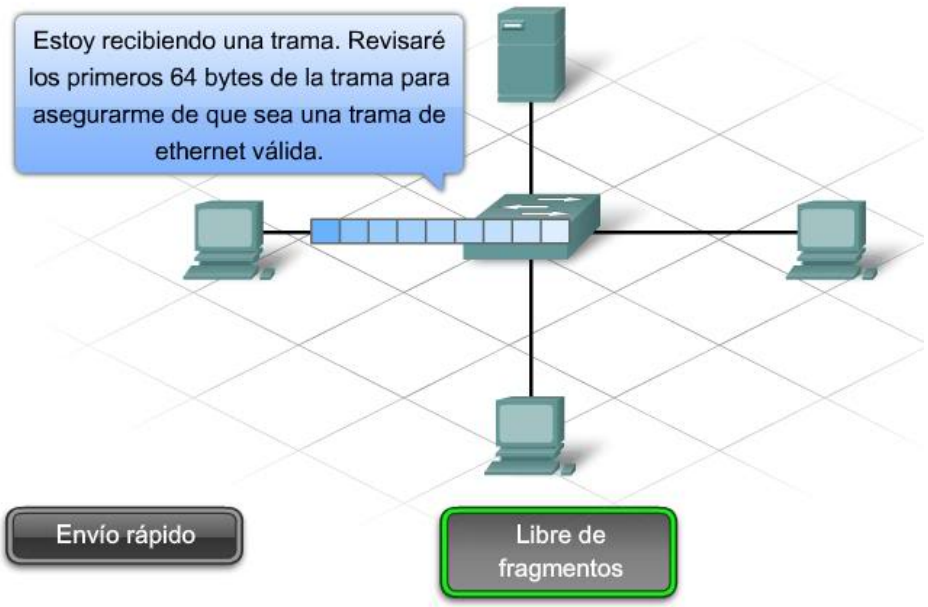
Los switches por **método de corte** leen la dirección Mac tan pronto como el switch detecta el paquete. Después de almacenar los primeros 6 bytes que componen la información acerca de la dirección, inmediatamente comienza a enviar al nodo destino, aunque el resto del paquete esté entrando al switch.



Un switch que utiliza **almacenamiento y envío** guardará el paquete entero en el buffer y verificará que no existan errores CRC u otros problemas. Si el paquete tiene un error, se lo descarta. De otro modo, el switch verifica la dirección MAC y envía el paquete al nodo destino. Aunque este método evita que se conmuten tramas dañadas a otros segmentos de la red, provoca una mayor latencia. Debido a la latencia provocada por el método de almacenamiento y envío, por lo general, sólo se lo utiliza en entornos proclives a producir errores, como los entornos con altas probabilidades de interferencia electromagnética.
Muchos switches combinan ambos métodos utilizando el método de corte hasta alcanzar un determinado nivel de errores, luego cambian a almacenamiento y envío. Muy pocos switches son estrictamente por método de corte ya que este método no proporciona corrección de errores.



Un método menos común es **libre de fragmentos.** Funciona como el método de corte pero almacena los primeros 64 bytes del paquete antes de enviarlo. La razón para ello es que la mayoría de los errores y colisiones tienen lugar durante los 64 bytes iniciales de un paquete.



Conmutación en la capa 3 - capa de Red

ROUTERS

Un router es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante *bridges*), y que por tanto tienen prefijos de red distintos.
La conmutación de la Capa 3 se basa en las direcciones de la capa de red o en las direcciones IP. Al trabajar en la Capa 3 el router puede tomar decisiones basadas en grupos de direcciones de red (Clases) en contraposición con las direcciones MAC de Capa 2 individuales.
Las funciones y la funcionalidad de los switches de Capa 3 y los routers son muy parecidas. La única diferencia importante entre la operación de conmutación de paquetes de un router y de un switch de Capa 3 es la implementación física. En los routers de propósito general, la conmutación de paquetes se produce en el software, mientras que un switch de Capa 3 realiza el envío de paquetes por medio del hardware de circuito integrado de aplicación específica (ASIC).

Funcionamiento

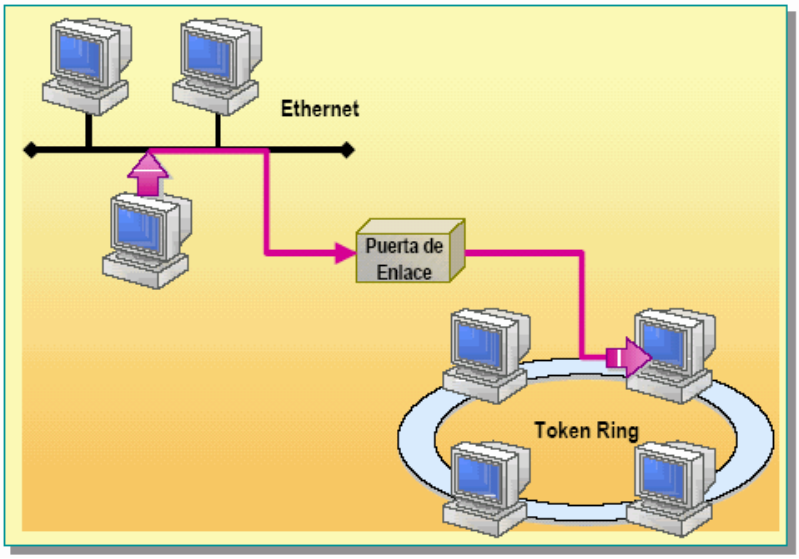
El funcionamiento básico de un *router* (en español 'enrutador' o 'encaminador'), como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. En base a esta información lo reenvían a otro encaminador o al *host* final en una actividad que se denomina 'encaminamiento'. Cada encaminador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto, como protocolos basado en el algoritmo de Dijkstra.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- *Reenvío de paquetes (Forwarding)*: cuando un paquete llega al enlace de entrada de un encaminador, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los encaminadores es que no difunden tráfico difusivo.
- *Encaminamiento de paquetes (routing)*: mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en tomar un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.

Puerta de enlace o gateway



Una **pasarela**, **puerta de enlace** o **gateway** es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.

El gateway o «puerta de enlace» es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a

Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de un gateway (o puerta de enlace) a menudo se parece a 192.168.1.1 ó 192.168.0.1 y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x, que engloban o se reservan a las redes locales. Además se debe notar que necesariamente un equipo que haga de puerta de enlace en una red, debe tener 2 tarjetas de red.

Los gateways incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un bridge o un router, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos. Tienen mayores capacidades que los routers y los bridges porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

Al recibir los datos encapsulados de un protocolo, los gateways se encargan de ir desencapsulándolos hasta el nivel más alto, para luego proceder a encapsular los datos en el otro protocolo, yendo desde el nivel más superior al nivel más inferior, para dejar nuevamente la información en la red tras completarse la traducción. Según el tipo de gateway variará el nivel más bajo de la capa OSI en el que trabajará, pero en general es el nivel de transporte o el físico. Ese es el motivo por el cual muchas puertas de enlace pueden desempeñar además funciones de encaminamiento.

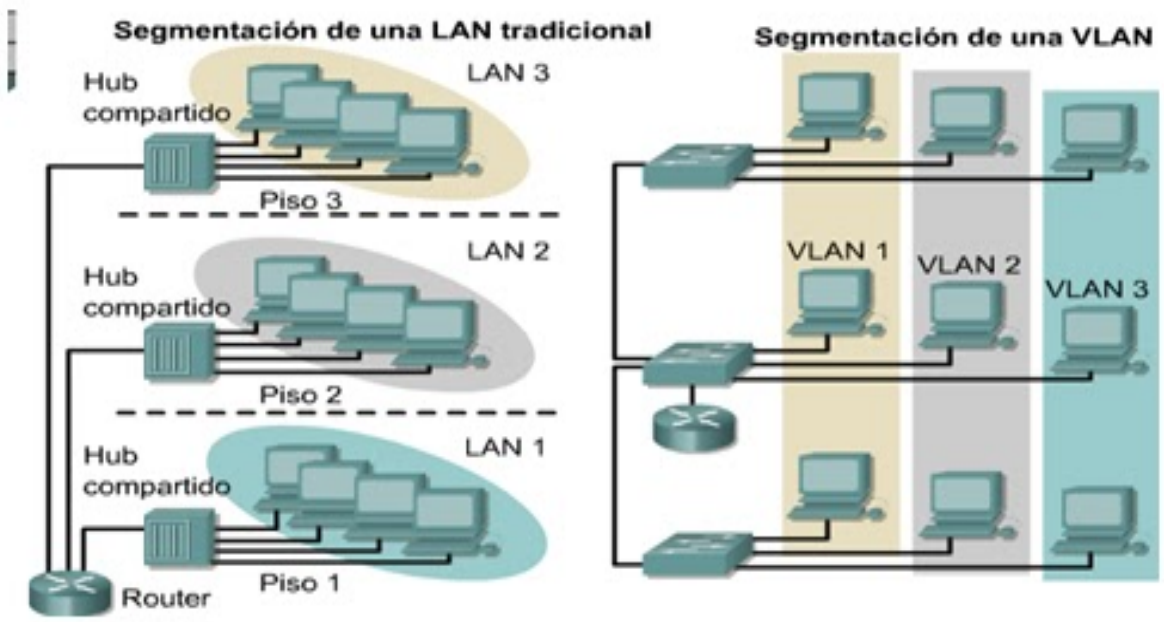
En entornos domésticos se usan los routers ADSL como gateways para conectar la red local doméstica con la red que es Internet, si bien esta puerta de enlace no conecta 2 redes con protocolos diferentes, sí que hace posible conectar 2 redes independientes haciendo uso del ya mencionado NAT.

Vlan (Virtual Lan)

Historia

A principios de la década de 1980 Ethernet ya era una tecnología consolidada que ofrecía una velocidad de 1 Mbits/s, mucho mayor que gran parte de las alternativas de la época.
El diseño de Ethernet no ofrecía escalabilidad, es decir, al aumentar el tamaño de la red disminuyen sus prestaciones o el costo se hace inasumible.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.
Para solucionar estos problemas se inventó el switch Ethernet con auto-aprendizaje, dispositivo de conmutación de tramas de nivel 2. Usar *switches* para interconectar redes Ethernet permite separar dominios de colisión, aumentando la eficiencia y la escalabilidad de la red. Una red tolerante a fallos y con un nivel alto de disponibilidad requiere que se usen topologías redundantes. El principal inconveniente de esta topología lógica de la red es que los *switches* centrales se convierten en cuellos de botella, pues la mayor parte del tráfico circula a través de ellos.
Para 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. 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* sabrán a qué VLAN pertenece cada trama observando la etiqueta VLAN (definida en la norma IEEE 802.1Q).

Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios. El tráfico entre las VLAN está restringido. Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico.



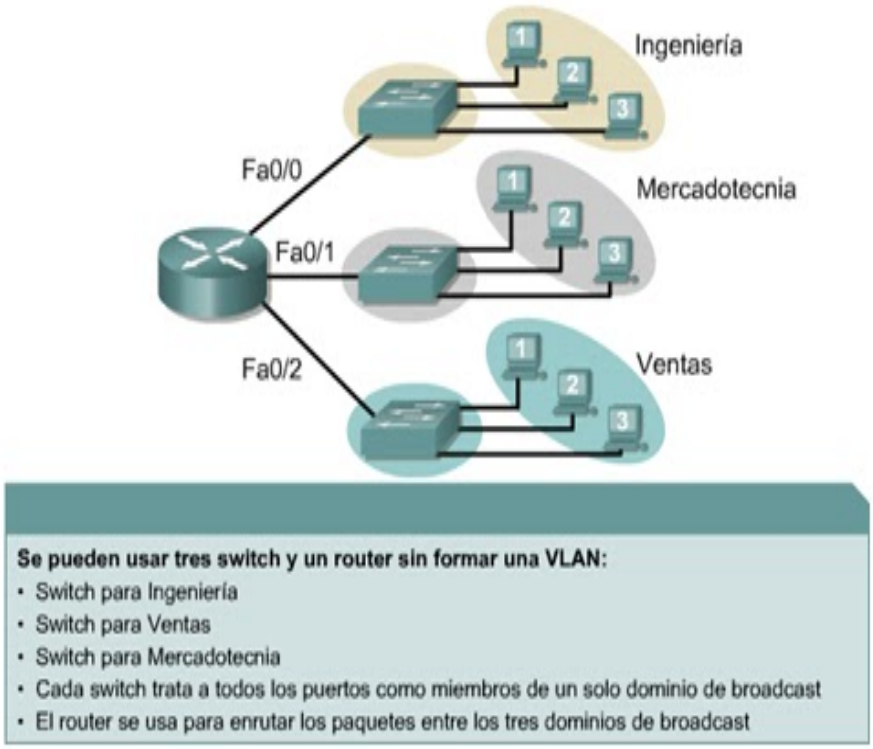
Ventajas de las VLANs

- **Seguridad**: Los datos de dentro de una VLAN no pueden ser accedidos desde otras VLANs, por defecto.
- **Reducción de costes:** EL uso de la red es más eficiente, por lo que no es necesario adquirir nuevo equipamiento más potente.
- **Mejor rendimiento:** Al disminuirse el tamaño de los dominios de broadcast, se reduce el tráfico innecesario que pueda sobrecargar la red.
- **Mejor administración:** Agrupar a los usuarios comunes en una misma VLAN permite que su administración está más controlada y ordenada.

Una VLAN es un dominio de broadcast que se crea en uno o más switches. El diseño de red donde se agrupan los equipos en 3 VLAN requieren de tres dominios de broadcast separados.

El router enruta el tráfico entre las VLAN mediante enrutamiento de Capa 3. El switch envía tramas a las interfaces del router cuando se presentan ciertas circunstancias:

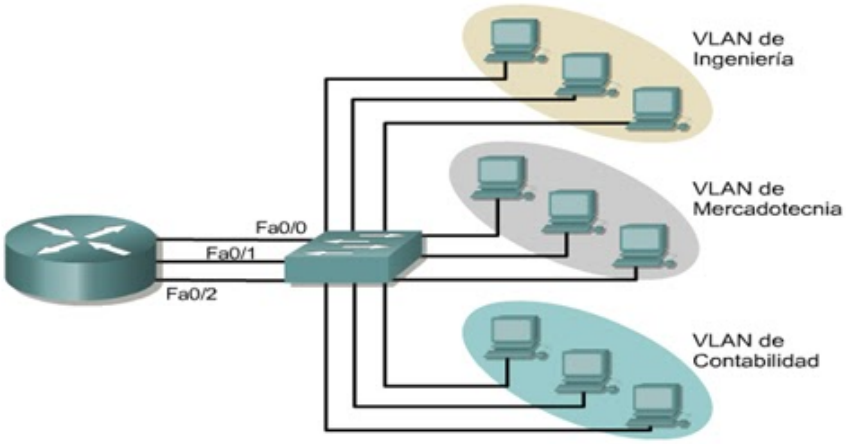
- Si es una trama de broadcast
- Si está en la ruta a una de las direcciones MAC del router

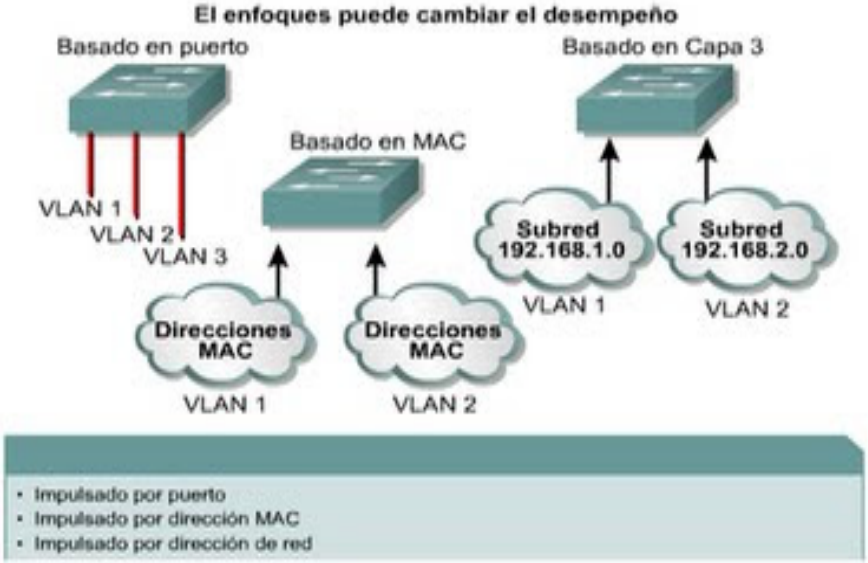


Como decia una VLAN es una agrupación de puertos en un switch o más para formar segmentos de red Ethernet diferentes. Por eso el tráfico en los nodos de una VLAN no pasa hacia otra VLAN sin que haya un dispositivo de capa 3 (router o Switch de capa 3) que interconecte las VLANS

La cantidad de VLAN en un switch varía según diversos factores:

- Patrones de tráfico
- Tipos de aplicaciones
- Necesidades de administración de red
- Aspectos comunes del grupo





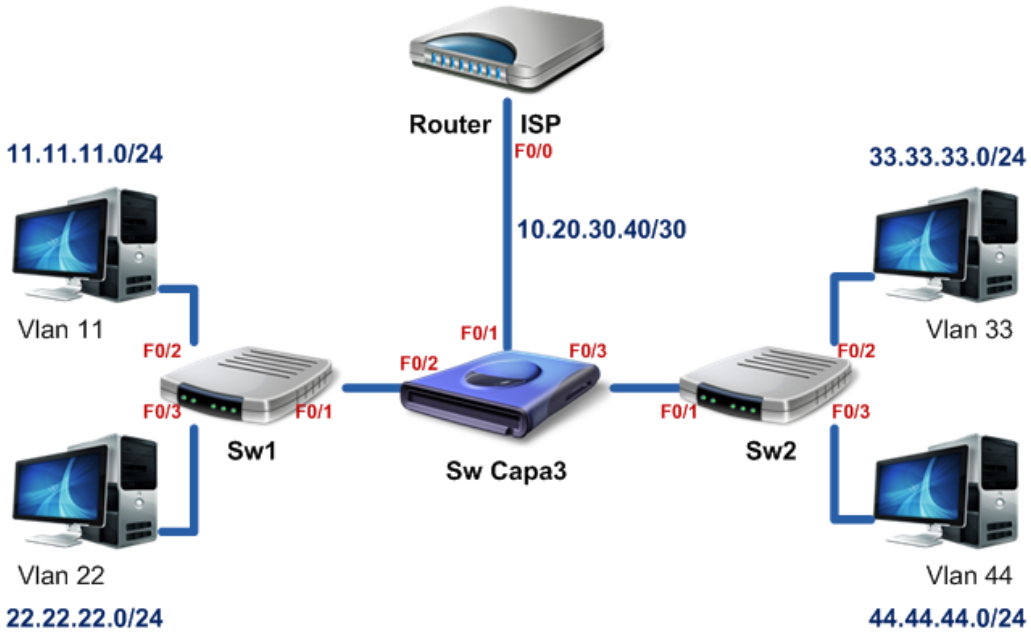
Tipos de VLAN	Descripción
Basado en puerto	• Método de configuración más común • Los puertos se asignan individualmente, en grupos, en filas o en 2 o más switches • Uso sencillo • Se implementa a menudo donde el Protocolo de Control de Host Dinámico (DHCP) se usa para asignar las direcciones IP a los hosts de red
Dirección MAC	• Se implementa con escasa frecuencia hoy en día • Es necesario introducir y configurar cada dirección de forma individual • Los usuarios lo consideran útil • Administración, diagnóstico de fallas y gestión difíciles
Basado en protocolo	• Se configuran como las direcciones MAC, pero usan una dirección lógica o IP • Ya no son comunes debido a DHCP

VLAN de nivel 3

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

- La **VLAN basada en la dirección de red** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

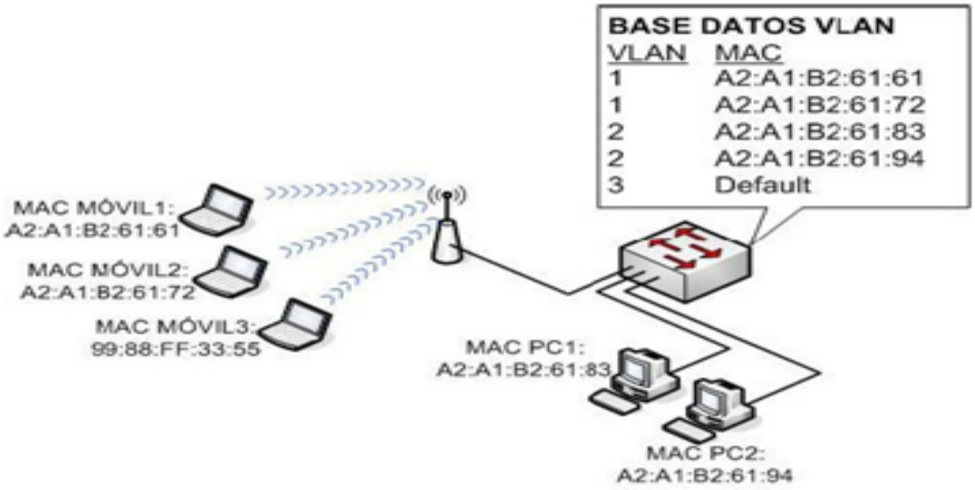
- la VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.



Topology By SE7EN

MAC-based VLANs (VLAN level 2)

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



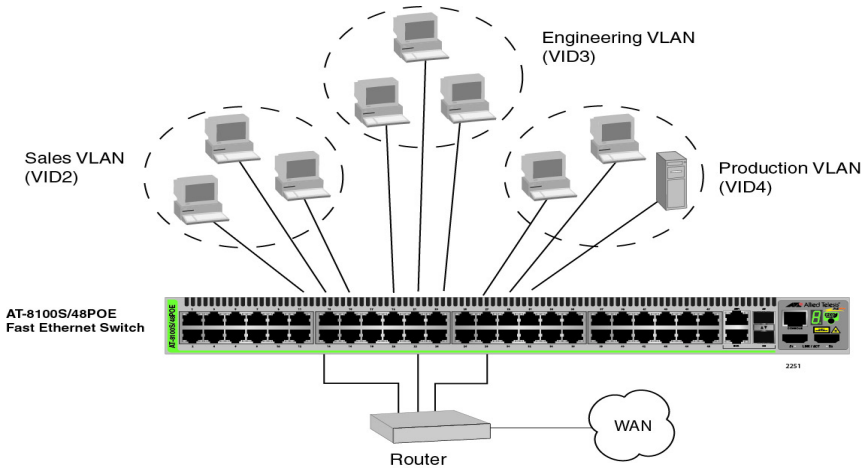
```
S1# show mac address-table interface FastEthernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
10    000c.296a.a21c    DYNAMIC     Fa0/1
10    000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
```

La asignación se realiza mediante paquetes de *software* tales como el CiscoWorks 2000. Con el 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. Se puede consultar el *software* FreeNAC para ver un ejemplo de implementación de un servidor VMPS.

Port-based VLAN (VLAN level 1)

Las **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* 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*.



Las partes necesarias para armar una VLAN:

- Nombre de VLAN
- Identificador de VLAN
- Untagged port
- Identificador de puerto VLAN

Nombre de VLAN

El nombre de la VLAN corresponde al nombre que se le va a asignar en la red. Es recomendable que cada VLAN refleje una seccion.

Identificador VLAN

Es un número único que se le asigna a una VLAN. Este número (VID) es único por cada VLAN y es el identificador en el switch y en la red de la VLAN.

Si una VLAN esta en un mismo switch se le asigna un VID distinto a las otras VLANs de la red. SI se tienen VLANs en diferentes switches se le asigna a una VLAN el mismo VID en los dos switches. Los switches son capaces de reconocer las tramas de una VLAN aunque este en varios switches.

Identificador de puerto VLAN
Todas las redes tienen que tener un identificador de puerto VLAN (PVID). El switch asocia una trama con el PVID. Entonces envía la trama a los PVID asociados a una VLAN. Todos los puertos de una VLAN tienen que tener en el mismo número. El PVID coincide con el VID.

Si se crea una VLAN en un switch y se le asigna el VID 5. Todos los puertos que van a estar en la red 5 en el switch se le asigna el PVID 5.

Untaged port

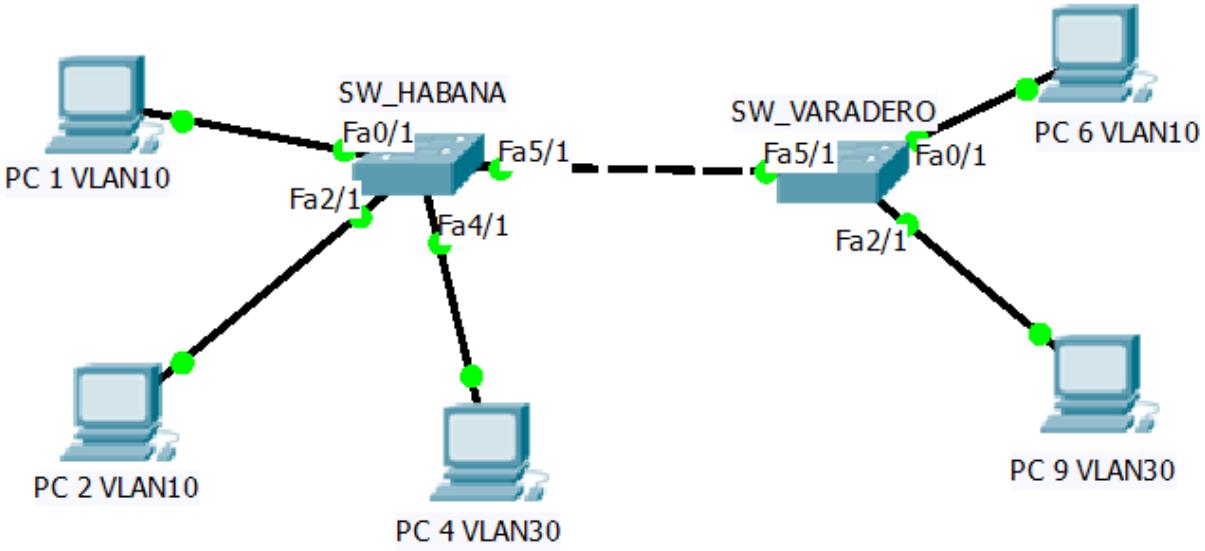
Los puertos 'untagged' son los puertos donde el switch espera que los paquetes no estén marcados con un número de VLAN. El switch asigna la VLAN a los paquetes que entran por ese puerto. Como no tienen una etiqueta (tag) de VLAN, los puertos 'untagged' se pueden asignar únicamente a una VLAN. Normalmente se usan como puertos de acceso, para conectar equipos terminales.

DESPUES DE TENER CREADAS LAS VLANS, ASIGNAREMOS LAS VLANS A LOS PUERTOS DONDEN SE CONECTAN LOS HOST.

SW_HABANA Y SW_VARADERO

PCs 1,2 y 6 VLAN 10(Students)

PC 4 Y 9 VLAN 30(Admin)



Consiste en dos SWITCHES que ya tienen configuradas las VLANs y nosotros tendremos que configurar los puertos a que pertenecen dichas VLANs

En el SW_HABANA tenemos las siguientes lineas de comandos

```
SW_HABANA(config)# interface fastEthernet 0/1
SW_HABANA(config-if)# switchport mode access
SW_HABANA(config-if)# switchport access vlan 10
SW_HABANA(config-if)# interface fastEthernet 2/1
SW_HABANA(config-if)# switchport mode access
SW_HABANA(config-if)# switchport access vlan 10
SW_HABANA(config-if)# interface fastEthernet 4/1
SW_HABANA(config-if)# switchport mode access
SW_HABANA(config-if)# switchport access vlan 30
```

En el SW_ VARADERO tenemos las siguientes lineas de comandos

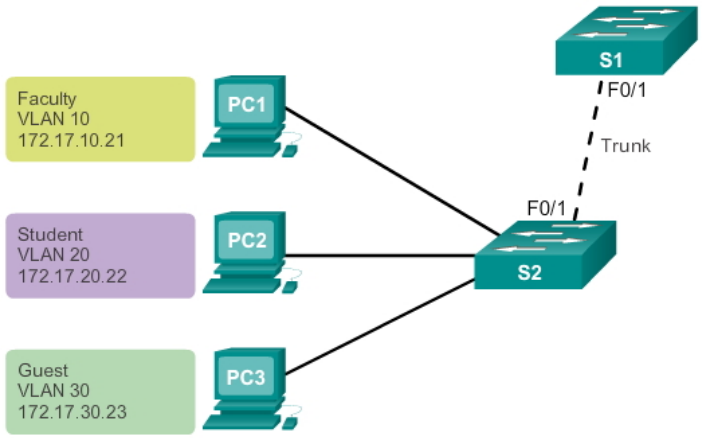
```
SW_ VARADERO (config)# interface fastEthernet 0/1
SW_ VARADERO (config-if)# switchport mode access
SW_ VARADERO (config-if)# switchport access vlan 10
SW_ VARADERO (config-if)# interface fastEthernet 2/1
SW_ VARADERO (config-if)# switchport mode access
SW_ VARADERO (config-if)# switchport access vlan 30
```

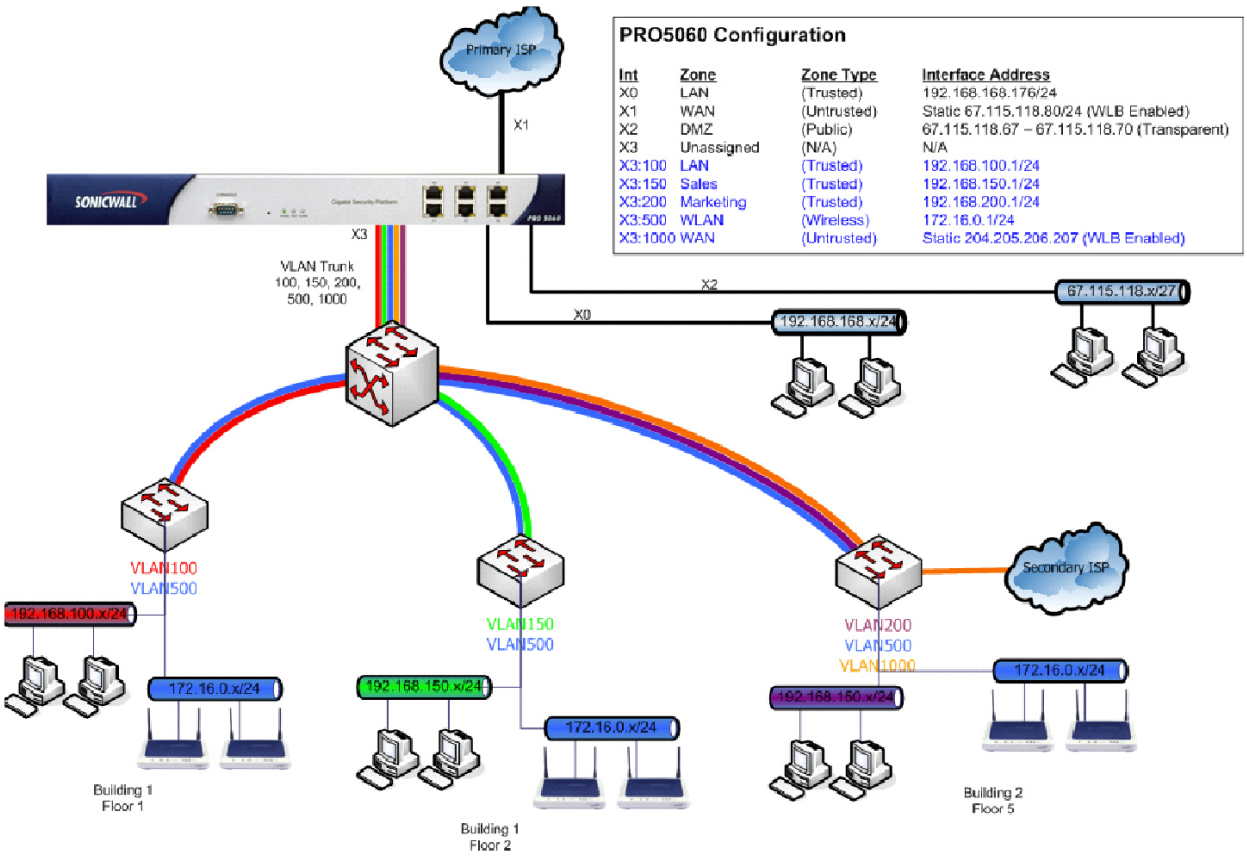
Aquí finaliza la asignacion de VLANs a los puertos de los SWITCHES que se interconectan con los HOTS.

VLANs troncales

Una VLAN troncal es un enlace de capa 2 entre dos switches por donde pasarán los paquetes de, por defecto, todas las VLANs.

De manera predeterminada, un enlace troncal aceptará el tráfico de todas las VLANs, pero esto lo podemos **restringir** indicando únicamente las VLANs que queremos que atraviesen ese troncal





PRO5060 Configuration

Int	Zone	Zone Type	Interface Address
X0	LAN	(Trusted)	192.168.168.176/24
X1	WAN	(Untrusted)	Static 67.115.118.80/24 (WLB Enabled)
X2	DMZ	(Public)	67.115.118.67 – 67.115.118.70 (Transparent)
X3	Unassigned	(N/A)	N/A
X3:100	LAN	(Trusted)	192.168.100.1/24
X3:150	Sales	(Trusted)	192.168.150.1/24
X3:200	Marketing	(Trusted)	192.168.200.1/24
X3:500	WLAN	(Wireless)	172.16.0.1/24
X3:1000	WAN	(Untrusted)	Static 204.205.206.207 (WLB Enabled)

El Vlan trunking protocol (VTP) proporciona un medio sencillo de mantener una configuración de VLAN trunk a través de toda la red conmutada.

VTP

VTP es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

Una trama VTP incluye una cabecera VTP y un mensaje VTP. El contenido de ambos depende del tipo de publicación. La información VTP se inserta en el campo de datos de una trama Ethernet.

la trama Ethernet es encapsulada en una trama 802.1Q tal

VTP opera en 3 modos distintos:

- Servidor
- Cliente
- Transparente

Servidor:

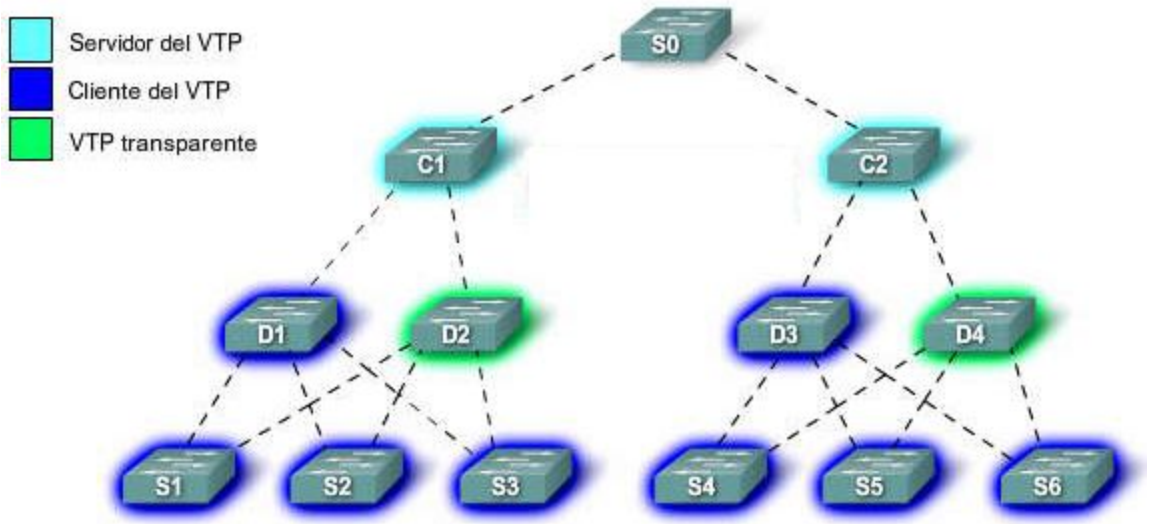
Es el modo por defecto. Desde él se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk. Debe haber al menos un servidor. Se recomienda autenticación MD5.

Cliente:

En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.

Transparente:

Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches. La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio.



Los administradores cambian la configuración de las VLANs en el switch en modo servidor. Después de realizar cambios, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces permitidos en el trunk (VLAN 1, por defecto), lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que

reciben, ni envían las suyas a otros dispositivos. Sin embargo, aquellos que usan la versión 2 del protocolo VTP, enviarán la información que reciban (publicaciones VTP) a otros dispositivos a los que estén conectados con una frecuencia de 5 minutos. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP. En este modo no se podrán crear VLANs, sino que sólo se podrá aplicar la información que reciba de las publicaciones VTP.

Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio. Los switches descartan mensajes de otro dominio VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se deben resetear los números de revisión de todo el dominio VTP para evitar conflictos.

Mensajes VTP

- Petición de aviso o advertisement request.
- Aviso de configuración o subset advertisement
- Resumen de configuración o Summary advertisement.

➔ Un advertisement request o petición de aviso es un mensaje generado por un switch cliente. Un switch configurado como cliente, no memoria la configuración de las VLANs. Entonces cuando arranca se resetea, necesita la configuración existente en su dominio. Entonces es cuando se hace una petición y el switch servidor responde.

➔ Al responder el servidor genera un Aviso de configuración o subset advertisement. La información contenida es los números de VLAN, los nombres y tipos y otra información. }

➔ Cada 5 minutos o 300 segundos, el switch servidor genera un resumen de configuración o Summary advertisement.

Esta información contiene lo siguiente:

- Número y nombre de VLAN
- Tamaño de MTU usado en la VLAN
- Formato de frame usado por la VLAN
- Valor SAID de la VLAN necesitado su es una VLAN 802.10.
- Número de revisión de configuración
- Nombre del dominio VTP.

Una de las funciones de los mensajes VTP es el asegurar que todos los switches tienen la misma versión de configuración de VLAN.
Por defecto se reenvía la información cada 3 minutos aunque contenga la misma configuración que el envío anterior, osea, aunque no haya habido ningún cambio en los últimos 5 minutos.
Para hacer más eficiente este método, existe un número de revisión de configuración, útil para saber cual es la versión mas actualizada. Si la versión del switch es antigua, modificará la configuración con la información recién llegada, y reenviará a los puertos configurados como trunk la ultima versión.
Si la información recibida no contiene todos los datos necesarios para actualizar la versión antigua, este switch generará una petición al switch principal para recibir la versión más moderna.

Seguridad de VLANs

Así como las VLANs mejoran el rendimiento de la red y facilitan su administración, también hay algunas vulnerabilidades que pueden traducirse en ataques. Por ello, es importante conocer por dónde pueden venir estos ataques para aprender a evitarlos.
Los puertos tienen una configuración, por defecto, de dynamic auto (negocian su estado como troncal o acceso según el estado del puerto conectado al otro extremo del cable). Por lo tanto, un atacante podría conectar un dispositivo que simule el funcionamiento de un switch, que encapsule las tramas con 802.1Q y sea capaz de mandar e interpretar mensajes DTP, al igual que hace el switch al que se está conectando, y obtener acceso a las tramas de todas las VLANs que estén permitidas por ese enlace troncal.
Una buena solución, en este caso, sería deshabilitar el protocolo DTP en el switch y configurar únicamente como troncales aquellos puertos que vayan a tener esa función.
Otro posible ataque es una trama a la que se le ha aplicado una segunda etiqueta con la VLAN nativa. Esta etiqueta será suprimida antes de enviarse por un troncal, ya que el switch interpretará que la trama ha sido generada por él mismo. Cuando llegue al otro extremo, el switch enviará la trama a la VLAN “víctima”, la que tenga en la primera etiqueta.
La solución ideal para estas situaciones, aunque no es un ataque que se pueda dar fácilmente, es cambiar la VLAN nativa a otro número que no sea el que viene por defecto y que esta no coincida con ninguna de la VLANs asignadas a PCs cliente.
Otra medida de seguridad ante posibles ataques es configurar varios puertos como PVLAN (Private VLAN). Esto es que un puerto configurado como protegido nunca podrá comunicarse con otro puerto protegido, pero sí con los demás puertos que no estén protegidos. Es decir, dos PCs conectados a puertos protegidos podrían tener una funcionalidad total de red, pero no podrían comunicarse entre ellos.