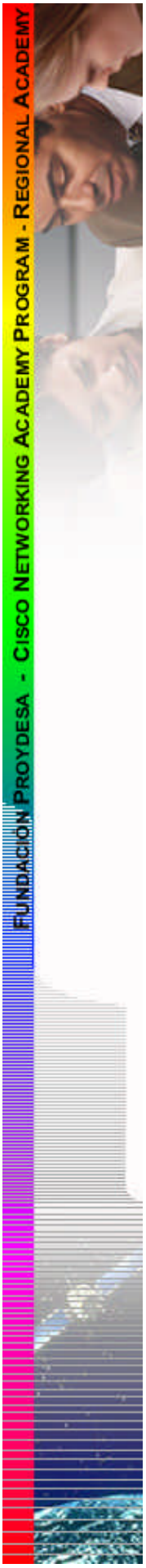


CÓMO FUNCIONAN LOS SWITCHES LAN

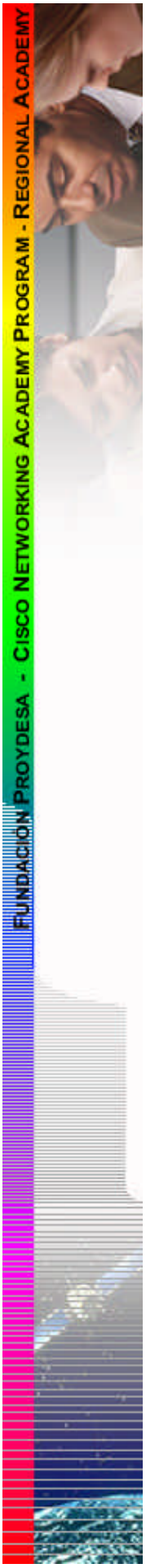
Contenidos

Introducción

Una red típica consta de nodos (computadoras), un medio de conexión (por medio de cableado o inalámbrico), y equipamiento de redes especializado como routers o hubs. En el caso de la Internet, todas estas piezas funcionando juntas le permiten a su computadora enviar información a otra computadora, ¡que podría estar al otro lado del mundo!

Los **switches** son una parte fundamental de la mayoría de las redes. Éstos hacen posible que varios usuarios envíen información a través de una red al mismo tiempo sin hacerse disminuir la velocidad de transmisión entre sí. Al igual que los routers permiten a diferentes redes comunicarse entre sí, los switches permiten a diferentes **nodos** (un punto de conexión de la red, típicamente una computadora) de una red comunicarse directamente entre sí de manera pareja y eficiente.

Imagen cortesía de Cisco Systems, Inc.
Ilustración de un switch Cisco Catalyst.



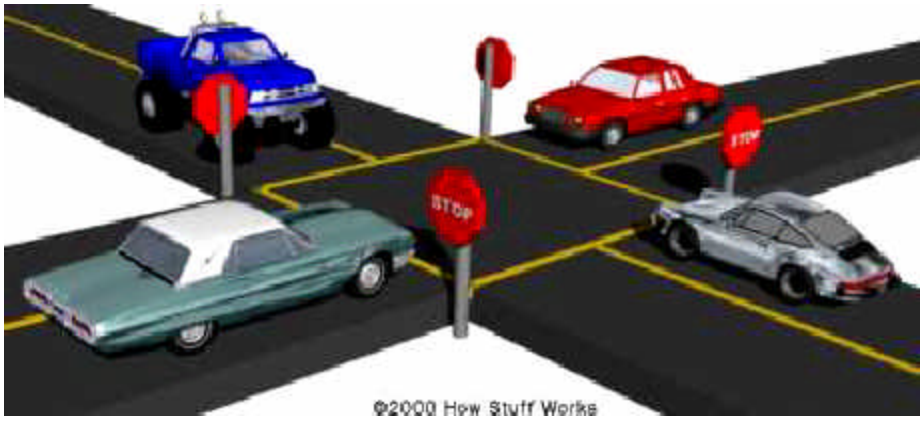
Existen muchos tipos diferentes de switches y redes. Los switches que proporcionan una conexión separada para cada nodo en la red interna de una compañía se denominan switches LAN. Esencialmente, un switch LAN crea una serie de redes instantáneas que contienen sólo los dos dispositivos que se comunican entre sí en ese momento en particular. Nos concentraremos en las redes Ethernet que utilizan switches LAN. Aprenderá qué es un switch LAN y cómo funciona el bridging transparente. También aprenderá acerca de las VLANs, troncales y spanning trees.

Agregado de Switches

En el tipo de red más básico que se encuentra hoy en día, los nodos simplemente se conectan mediante el uso de hubs. A medida que una red crece, surgen algunos problemas potenciales con esta configuración:

- **Escalabilidad**: En una red de hubs, el ancho de banda compartido limitado hace difícil el acomodar un crecimiento significativo sin sacrificar el desempeño. Las aplicaciones de hoy en día necesitan más ancho de banda que nunca antes. Muy a menudo, la totalidad de la red debe rediseñarse periódicamente para dar lugar al crecimiento.
- **Latencia**: La cantidad de tiempo que le lleva a un paquete el llegar a su destino. Puesto que cada nodo de una red basada en hubs tiene que esperar una oportunidad de transmitir para evitar las **colisiones**, la latencia puede incrementarse significativamente a medida que se agregan más nodos. O si alguien está transmitiendo un archivo grande a través de la red, entonces todos los otros nodos están esperando la oportunidad de enviar sus propios paquetes. Probablemente usted ha visto esto antes en el trabajo. Está intentando acceder a un servidor o a la Internet y súbitamente todo pierde velocidad.
- **Fallo en la Red**: En una red típica, un dispositivo en un hub puede ocasionar problemas para otros dispositivos conectados al hub debido a configuraciones de velocidad erróneas (100Mbps en un hub de10Mbps) o broadcasts excesivos. Los switches pueden configurarse para limitar los niveles de broadcast.
- **Colisiones**: Ethernet utiliza un proceso denominado **Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD)** para comunicarse a través de la red. Bajo CSMA/CD, un nodo no enviará un paquete hacia el exterior a menos que la red esté libre de tráfico. Si dos nodos envían paquetes al mismo tiempo, tiene lugar una colisión y los paquetes se pierden. Entonces ambos nodos esperan una cantidad aleatoria de tiempo y retransmiten los paquetes. Cualquier parte de la red donde exista una posibilidad de que los paquetes provenientes de dos o más nodos interfieran entre sí se considera parte del mismo **dominio de colisión**. Una red con una gran cantidad de nodos en el mismo segmento a menudo tendrá muchas colisiones y por lo tanto un gran dominio de colisión.

Mientras que los hubs proporcionan una manera fácil de escalar y acortar la distancia que los paquetes deben recorrer para llegar desde un nodo a otro, no dividen la red real en segmentos discretos. En este punto es donde intervienen los switches.



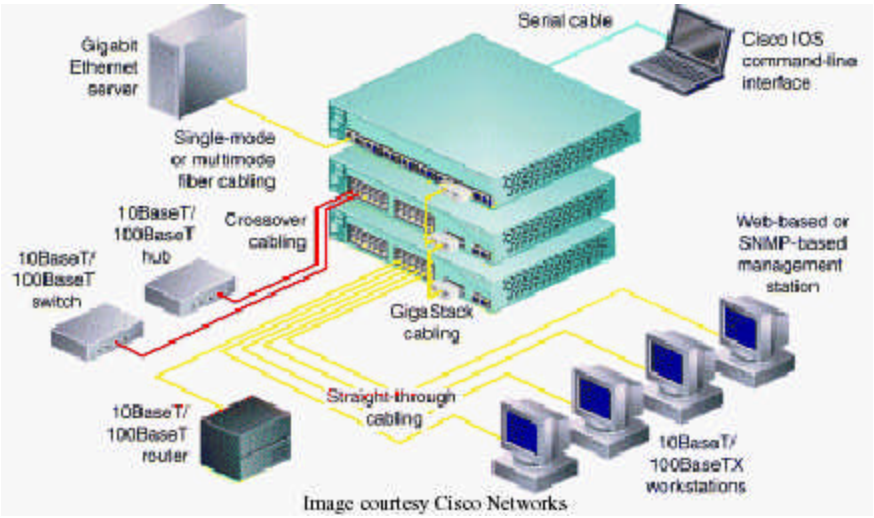
Imagine que cada vehículo es un paquete de datos esperando su oportunidad para continuar su viaje.

Pensemos en un hub como en una intersección de cuatro sentidos donde todo el mundo tiene que detenerse. Si más de un auto llega a la intersección al mismo tiempo, tienen que esperar su turno para proceguir. Pero un switch es como una intersección de tipo cruce de trébol. Cada auto puede dirigirse hacia una rampa de salida para llegar a su destino sin tener que detenerse y esperar a que pase otro tráfico. Ahora imaginemos lo que pasaría si una docena o incluso cien caminos se intersectaran en un único punto. La cantidad de espera y el potencial de que exista una colisión se incrementa significativamente si cada auto tiene que verificar todos los otros caminos antes de continuar. Pero, ¿no sería asombroso si uno pudiera dirigirse hacia una rampa de salida desde cualquiera de esos caminos hacia el camino de su elección? ¡Eso es exactamente lo que hace un switch con el tráfico de red!

Una diferencia vital entre un hub y un switch es que todos los nodos conectados a un hub comparten el ancho de banda entre sí mientras que un dispositivo conectado a un puerto de switch tiene la totalidad del ancho de banda para sí mismo. Por ejemplo, si 10 nodos se están comunicando utilizando un hub en una red de 10 Mbps, entonces cada nodo puede sólo obtener una porción de los 10 Mbps si otros nodos del hub desean comunicarse también. Pero con un switch, cada nodo podría eventualmente comunicarse con los 10 Mbps completos. Pensemos en nuestra analogía del camino. Si todo el tráfico llega a una intersección común, entonces tiene que compartir esa intersección con todo el resto. Pero un cruce de trébol permite que todo el tráfico continúe a toda velocidad desde un camino hasta el siguiente.

En una **red completamente conmutada**, los switches reemplazan a todos los hubs de una red Ethernet con un segmento dedicado para cada nodo. Estos segmentos se conectan a un switch, que soporta múltiples segmentos dedicados (a veces por cientos).

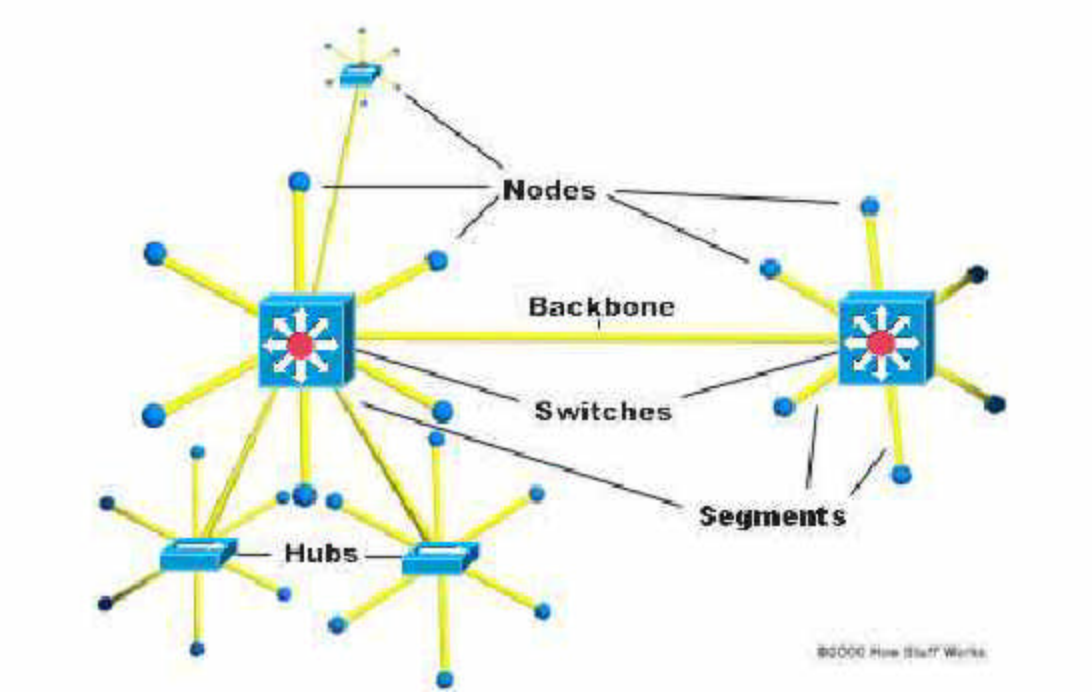
Puesto que los únicos dispositivos de cada segmento son el switch y el nodo, el switch recoge cada transmisión antes de que alcance a otro nodo. El switch luego envía el frame a través del segmento apropiado. Puesto que cualquier segmento contiene sólo un único nodo, el frame sólo llega al receptor al que estaba destinado. Esto permite que tengan lugar muchas conversaciones simultáneamente en una red conmutada.



Ejemplo de red que utiliza un switch.

La conmutación permite a una red mantener Ethernet full-duplex. Antes de la conmutación, Ethernet era half-duplex, lo que significa que sólo un dispositivo de la red podía transmitir en un momento determinado. En una red completamente conmutada, los nodos sólo se comunican con el switch y nunca directamente entre sí. Utilizando nuestra analogía del camino, half-duplex es similar al problema de un carril único, como en el caso en que un camino que está en construcción cierra el uso de un carril de un camino de dos carriles. El tráfico intenta utilizar el mismo carril en ambas direcciones. Esto significa que el tráfico que va en un sentido debe esperar hasta que el tráfico proveniente de la otra dirección se detenga. ¡De otro modo, chocarían de frente!

Las redes completamente conmutadas emplean cableado de par trenzado o de fibra óptica, y ambos utilizan conductores separados para enviar y recibir datos. En este tipo de entorno, los nodos Ethernet pueden desistir del proceso de detección de colisiones y transmitir a discreción, ya que son los únicos dispositivos que potencialmente pueden acceder al medio. En otras palabras, el tráfico que fluye en cada dirección tiene un carril para sí. Esto permite a los nodos transmitir al switch al mismo tiempo que el switch transmite hacia ellos, logrando un entorno libre de colisiones. La transmisión en ambas direcciones también puede duplicar eficazmente la velocidad aparente de la red cuando dos nodos se encuentran intercambiando información. Por ejemplo, si la velocidad de la red es de 10 Mbps entonces cada nodo puede transmitir a 10Mbps al mismo tiempo.



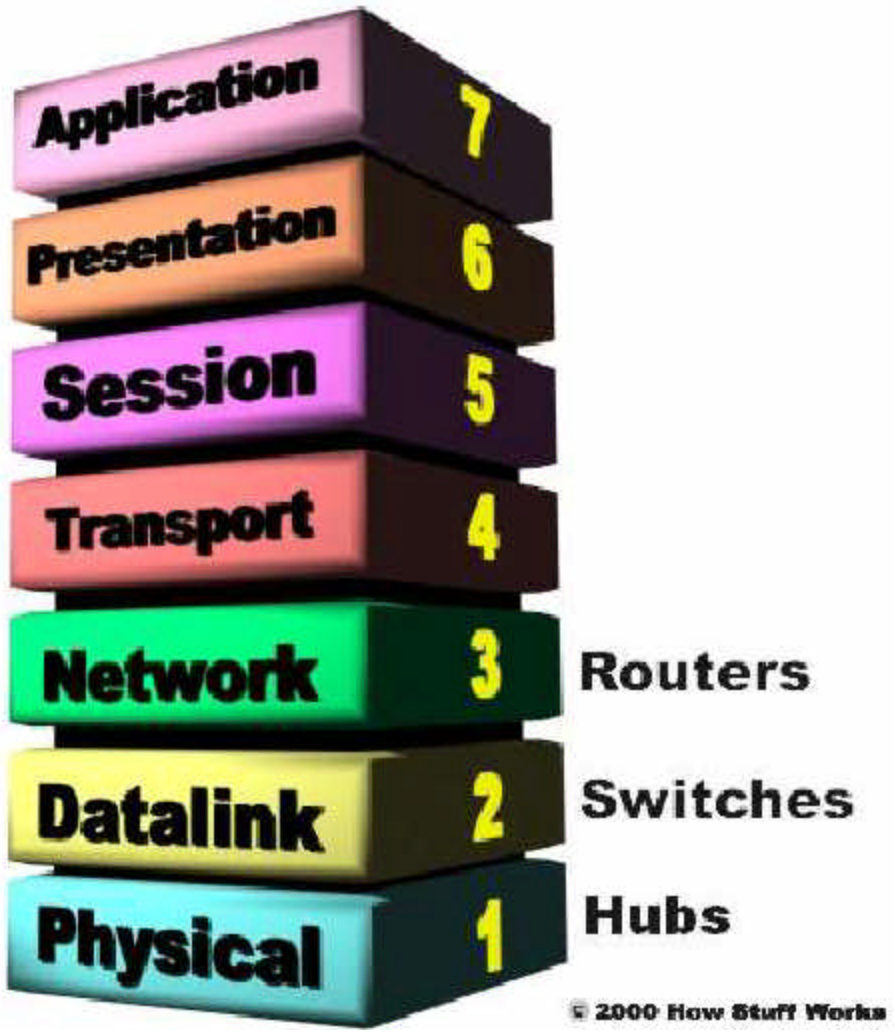
Una red combinada con dos switches y tres hubs.

La mayoría de las redes no son completamente conmutadas a causa de los costos en los cuales se incurre al reemplazar los hubs con switches. En lugar de esto, se utiliza una combinación de switches y hubs para crear una red eficaz aunque eficiente en costo. Por ejemplo, una compañía puede tener hubs que conecten a las computadoras de cada departamento y un switch que conecte todos los hubs a nivel departamental.

Tecnologías de Conmutación

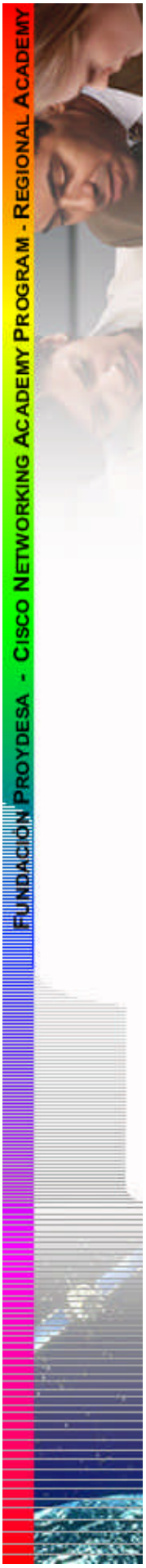
Puede apreciarse que un switch tiene el potencial de cambiar radicalmente la forma en la cual los nodos se comunican entre sí. Pero uno puede preguntarse en qué se diferencia de un router. Los switches usualmente funcionan en la **Capa 2 (de Datos o de Enlace de Datos)** del Modelo de Referencia OSI utilizando direcciones MAC mientras que los routers funcionan en la **Capa 3 (de Red)** con direcciones de Capa 3 (IP, IPX o Appletalk dependiendo de qué protocolos de Capa 3 se estén utilizando). El algoritmo utilizado por los switches para decidir cómo enviar paquetes es diferente a los algoritmos utilizados por los routers para enviar paquetes. Una de estas diferencias en los algoritmos entre switches y routers es cómo se manejan los **broadcasts**. En cualquier red, el concepto de un paquete de broadcast es vital para la operabilidad de la misma. Ya sea que un dispositivo necesite enviar información pero no sepa a quién debería enviarla, envía un broadcast. Por ejemplo, cada vez que una nueva computadora u otro dispositivo entra a la red, envía un paquete de broadcast para anunciar su presencia. Los otros nodos (tal como un servidor de dominio) pueden agregar la computadora a su **lista buscadora** (semejante a una agenda de direcciones) y comunicarse en forma directa con

dicha computadora desde ese punto en adelante. Los broadcasts se utilizan cada vez que un dispositivo necesita hacer un anuncio al resto de la red no está seguro de quién deberá ser el receptor de la información.



El Modelo de Referencia OSI consta de 7 capas que van desde la del cableado (Física) hasta la del software (Aplicación).

Un hub o un switch pasarán cualquier paquete de broadcast que reciban a todos los otros segmentos del dominio de broadcast pero un router no. Pensemos nuevamente en nuestra intersección de cuatro sentidos. En nuestra analogía, todo el tráfico atravesaba la intersección sin importar hacia dónde se dirigía. Ahora imaginemos que esta intersección es una frontera internacional. Para atravesar la intersección, se debe proporcionar al guardián de la frontera la dirección específica hacia la cual uno se dirige. Si no se tiene un destino específico, entonces el guardia no nos dejará pasar. Un router funciona de esta forma. Sin la dirección específica de otro dispositivo, no dejará pasar al paquete de datos. Esto es algo bueno para mantener a las redes separadas la una de la



otra pero no es tan bueno cuando se desea establecer una conversación entre diferentes partes de la misma red. En este punto es cuando intervienen los switches.

Los switches LAN se basan en la **Conmutación de paquetes**. El switch establece una conexión entre dos segmentos lo suficientemente largos como para enviar el paquete actual. Los paquetes entrantes (parte de un **frame** Ethernet) se guardan en un área de memoria temporaria **(buffer)**, la dirección MAC contenida en el encabezado del frame se lee y luego se compara con una lista de direcciones mantenida en la **tabla de búsqueda** del switch. En una LAN basada en Ethernet, un frame Ethernet contiene un paquete normal como payload del frame con un encabezado especial que incluye la información de la dirección MAC relativa al origen y el destino del paquete.

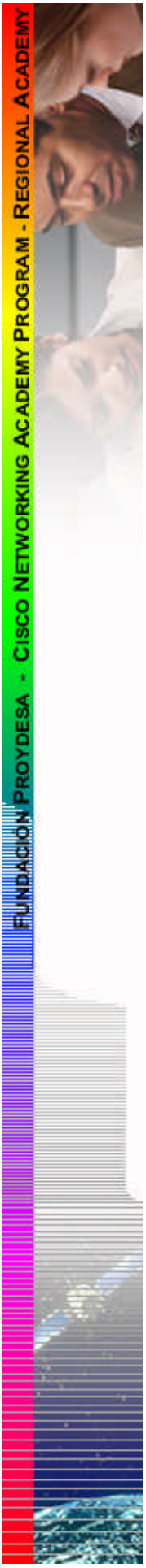
Los switches basados en paquetes utilizan uno de los siguientes tres métodos para enrutar el tráfico:

- 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 un paquete. Después de almacenar los seis bytes que componen la información acerca de la dirección, inmediatamente comienzan a enviar el paquete al nodo de 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, luego se lo descarta. De otro modo, el switch verifica la dirección MAC y envía el paquete hacia el nodo de destino. 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.



Los switches LAN varían en su diseño físico. Actualmente, existen tres configuraciones populares en uso:

- **Memoria compartida** – Almacena todos los paquetes entrantes en un buffer de memoria común compartido por todos los **puertos** del swith (conexiones de entrada y salida), luego los envía al puerto correcto para el nodo de destino.
- **Matrix** – Este tipo de switch tiene una grilla interna con los puertos de entrada y de salida cruzándose entre sí. Cuando se detecta un paquete en un puerto de entrada, la dirección MAC se compara con la tabla de búsqueda para encontrar el puerto de salida apropiado. El switch efectúa entonces una conexión en la grilla en el punto donde se intersectan estos dos puertos.
- **Arquitectura de bus** – En lugar de una grilla, una ruta de transmisión interna **(bus común)** es compartida por todos los puertos que utilicen TDMA. Un switch basado en esta configuración tiene un buffer de memoria dedicado para cada puerto y un ASIC para controlar el acceso interno al bus.

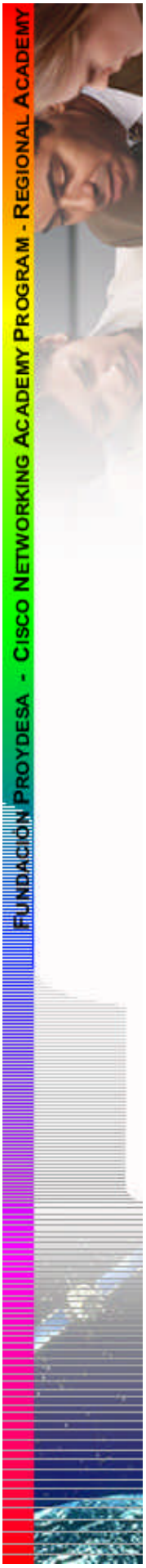
Bridging Transparente

La mayoría de los switches LAN Ethernet utilizan un sistema muy interesante denominado **bridging transparente** para crear sus tablas de búsqueda de direcciones. El bridging transparente es una tecnología que permite a un switch aprender todo lo que necesita acerca de la ubicación de los nodos en la red sin que el administrador de la misma tenga que hacer nada. El bridging transparente tiene cinco partes:

- Aprendizaje
- Flooding
- Filtrado
- Envío
- Envejecimiento

He aquí cómo funciona:

- El switch se agrega a la red y los diversos segmentos se conectan a los puertos del switch.
- Una computadora (Nodo A) del primer segmento (Segmento A) envía datos a una computadora (Nodo B) que se encuentra en otro segmento (Segmento C).
- El switch obtiene el primer paquete de datos del Nodo A. Lee la dirección MAC y la guarda en la tabla de búsqueda para el Segmento A. El switch ahora sabe dónde encontrar el Nodo A cada vez que un paquete está dirigido al mismo. Este proceso se denomina **aprendizaje**.

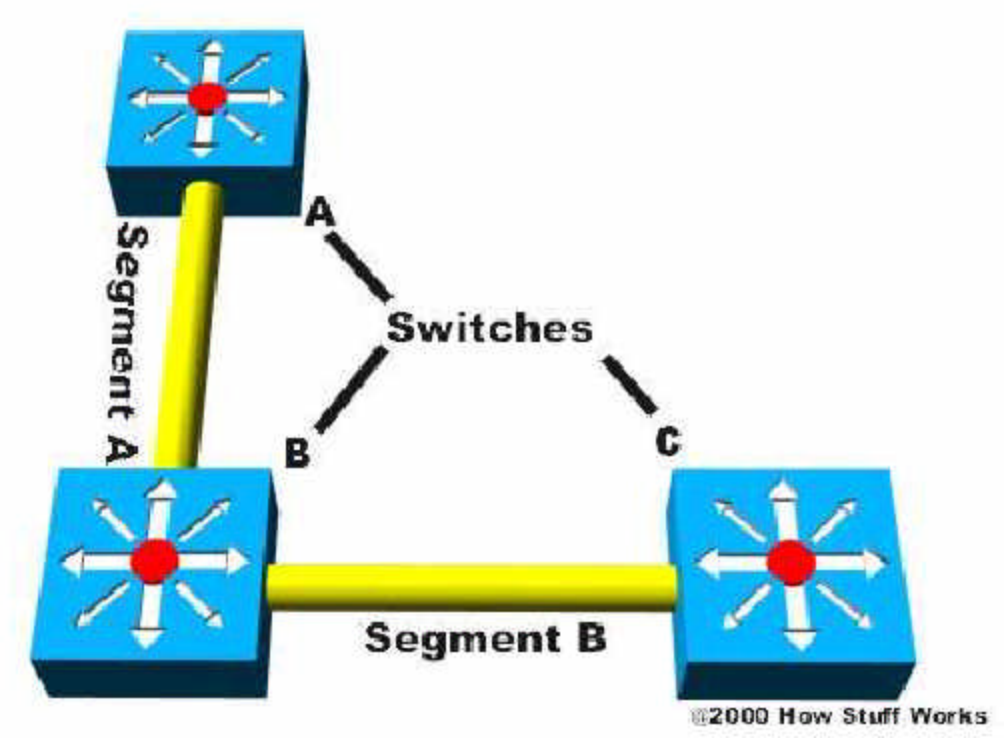


- Puesto que el switch no sabe dónde se encuentra el Nodo B, envía el paquete a todos los segmentos excepto a aquél al que ha llegado (Segmento A). Cuando un switch envía un paquete hacia todos los segmentos para encontrar un nodo específico, esto se denomina **flooding**.
- El Nodo B obtiene el paquete y envía un paquete de regreso al Nodo A como confirmación.
- El paquete proveniente del Nodo B llega al switch. Ahora el switch puede agregar la dirección MAC del Nodo B a la tabla de búsqueda para el Segmento C. Puesto que el switch ya conoce la dirección del Nodo A, envía el paquete directamente hacia el mismo. Puesto que el Nodo A está en un segmento diferente que el Nodo B, el switch debe conectar los dos segmentos para enviar el paquete. Esto se denomina **envío**.
- El siguiente paquete desde el Nodo A hacia el Nodo B llega al switch. El switch ahora tiene la dirección del Nodo B también, de modo tal que envía el paquete directamente al Nodo B.
- El Nodo C envía información al switch para el Nodo A. El switch verifica la dirección MAC del Nodo C y la agrega a la tabla de búsqueda del Segmento A. El switch ya tiene la dirección del Nodo A y determina que ambos nodos se encuentran en el mismo segmento. Por lo tanto, no necesita conectar el Segmento A a otro segmento para que los datos viajen desde el Nodo C hasta el Nodo A. Por lo tanto, el switch ignorará los paquetes entre nodos ubicados en el mismo segmento. Esto es el **filtrado**.
- El aprendizaje y el flooding continúan a medida que el switch agrega nodos a las tablas de búsqueda. La mayoría de los switches tienen la suficiente cantidad de memoria como para mantener tablas de búsqueda, pero borran la información más antigua de modo tal que el switch no pierda tiempo buscando entre direcciones antiguas. Para optimizar el uso de esta memoria, los switches utilizan una técnica denominada **envejecimiento**. Básicamente, cuando una se agrega una entrada relativa a un nodo a la tabla de búsqueda, se le adjudica una etiqueta temporal. Cada vez que un paquete se recibe desde un nodo, la etiqueta temporal se actualiza. El switch tiene un temporizador configurable por el usuario que borra la entrada después de que haya transcurrido una determinada longitud de tiempo sin actividad proveniente de ese nodo. Esto libera valiosos recursos de memoria para otras entradas. Como puede verse, ¡ el bridging transparente es una manera muy buena y esencialmente libre de mantenimiento para agregar toda la información que un switch necesita para hacer su trabajo!

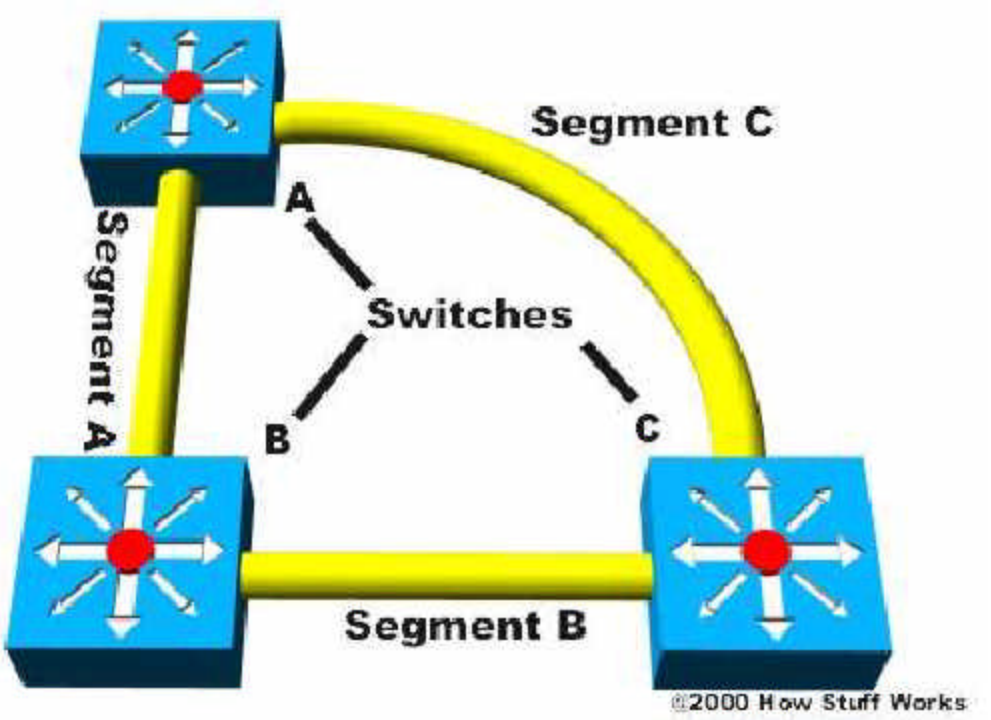
En nuestro ejemplo, dos nodos comparten cada segmento. En una red conmutada LAN ideal, cada nodo tendría su propio segmento. Esto eliminaría la posibilidad de que existan colisiones y también la necesidad del filtrado. Nótese que mientras que un nodo del Segmento A está intercambiando información con un nodo del Segmento B a 10 Mbps, un nodo del Segmento C puede comunicarse con un nodo del Segmento D también a 10 Mbps.

Redundancia y Tormentas de Broadcasts

Cuando anteriormente hablábamos acerca de las redes de bus y de anillo, un problema que surgió era la posibilidad de un único punto de fallo. En una red en estrella o en estrella de bus el punto con mayor potencial para dejar inactiva a toda o parte de la red es un switch o un hub. Observemos el siguiente ejemplo:

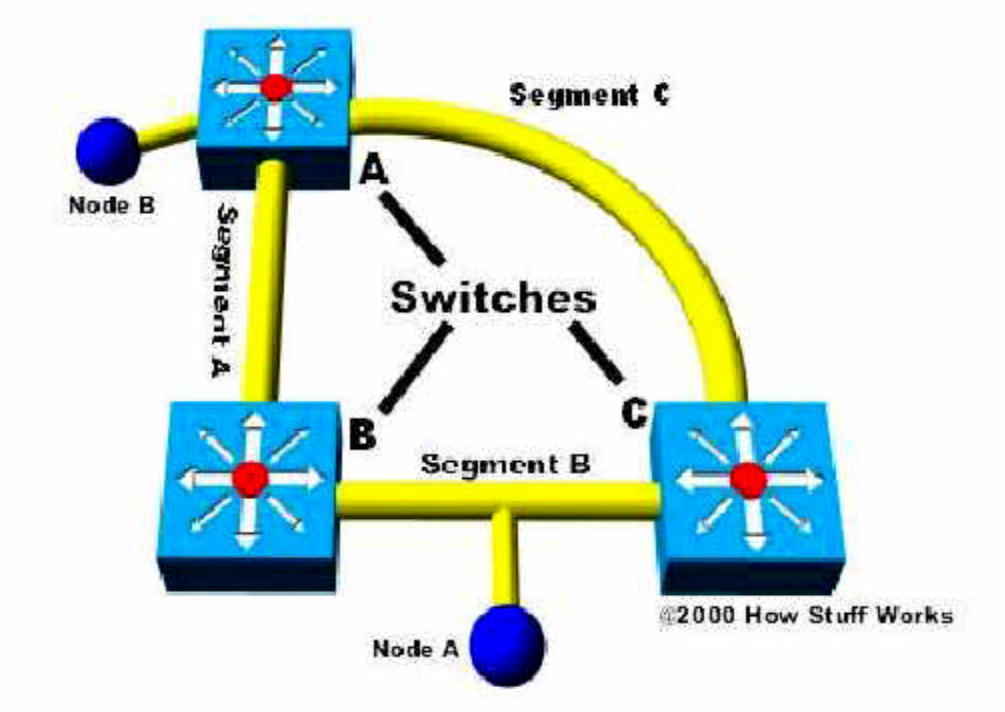


En este ejemplo, si el switch A o el C fallan entonces los nodos conectados a ese switch en particular se ven afectados pero los nodos en los otros dos switches aún pueden comunicarse. No obstante, si el switch B falla entonces toda la red queda inactiva. ¿Qué sucede si agregamos otro segmento a nuestra red que conecte los switches A y C?



Incluso si uno de los switches falla, la red continuará. Esto proporciona **redundancia** y elimina eficazmente el único punto de fallo.

Ahora se nos presenta un nuevo problema. En la sección anterior, descubrimos cómo aprenden los switches dónde están ubicados los nodos. Con todos los switches conectados ahora en un bucle, un paquete proveniente de un nodo podría posiblemente llegar a un switch desde dos segmentos diferentes. Por ejemplo, imagine que el Nodo B está conectado al Switch A y necesita comunicarse con el Nodo A que se encuentra en el Segmento B. El Switch A no sabe quién es el Nodo A, de modo tal que hace flood del paquete.

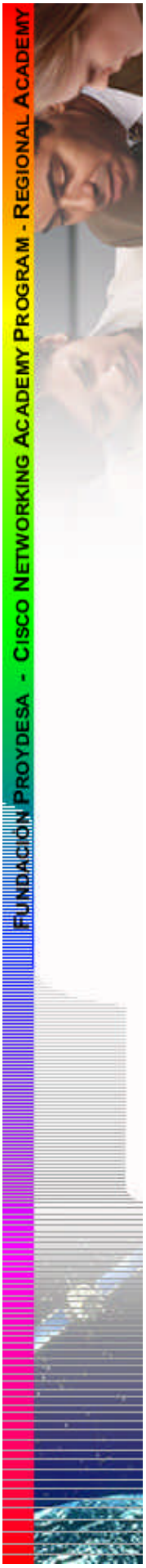


El paquete viaja a través del Segmento A o el Segmento C hacia los otros dos switches (B y C). El Switch B agregará el Nodo B a la tabla de búsqueda que mantiene para el Segmento A mientras que el Switch C lo agregará a la tabla de búsqueda para el Segmento C. Supongamos que ninguno de los switches ha aprendido la dirección para el Nodo A todavía. Harán flood al Segmento B buscando el Nodo A. Cada switch tomará el paquete enviado por el otro switch y hará flood del mismo nuevamente de forma inmediata ya que aún no saben quién es el Nodo A. El Switch A recibirá el paquete proveniente de cada segmento y hará flood del mismo hacia el otro segmento. Esto ocasiona una **tormenta de broadcasts** ya que los paquetes son transmitidos como broadcast, recibidos y retransmitidos como broadcast por cada switch resultando en una congestión de la red potencialmente severa.

Lo cual nos conduce hacia los **spanning trees**…

Spanning Trees

Para evitar las tormentas de broadcast y otros efectos colaterales no deseados del empleo de bucles, **Digital Equipment Corporation** creó el **Protocolo Spanning Tree (STP)** que fue estandarizado como especificación **802.1d** por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE). Esencialmente, un spanning tree utiliza el algoritmo spanning tree (STA) que detecta que el switch tiene más de un camino para comunicarse con un nodo, determina cuál de ellos es el mejor y bloquea la(s) otra(s) ruta(s). Lo bueno es que



mantiene un rastreo de la(s) otra(s) ruta(s) sólo en caso de que la ruta principal no esté disponible.

He aquí cómo funciona STP:

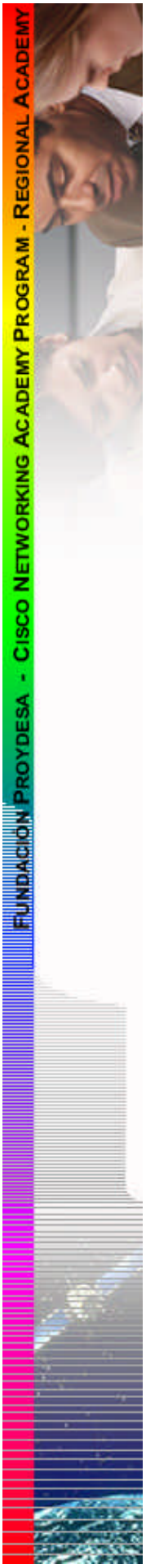
- A cada switch se le asigna un grupo de IDs, una para el switch en sí y otra para cada puerto del switch. El identificador del switch, denominado **ID de Bridge (BID)** tiene 8 bytes de largo y contiene una prioridad de bridge (2 bytes) junto con una de las direcciones MAC del switch (6 bytes). Cada **ID de Puerto** tiene 16 bits de largo y consta de dos partes, una configuración de prioridad de 6 bits y un número de puerto de 10 bits.
- Se le adjudica un valor de **costo de la ruta** a cada puerto. El costo se basa típicamente en una guía establecida como parte de 802.1d. De acuerdo a la especificación original, el costo es de 1000 Mbps (1 gigabit por segundo) dividido por el ancho de banda del segmento conectado al puerto. Por lo tanto, una conexión de 10 Mbps tendría un costo de 100 (1000 dividido 10).

Para compensar por la creciente velocidad de las redes más allá del rango de un gigabit, el costo estándar ha sido levemente modificado. Los nuevos valores de costo son:

Ancho de Banda	Valor del Costo STP
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

También deberá notarse que el Costo de la Ruta puede ser un valor arbitrario asignado por el administrador de la red en lugar de los valores de costo estándar.

- Cada switch comienza un proceso de descubrimiento para escoger qué rutas de la red para cada segmento deberá utilizar. Esta información es compartida entre todos los switches que utilicen frames de red especiales denominados **bridge protocol data units (BPDU)**. Las partes de una BPDU son:
  - BID Raíz – Ésta es la BID del **Bridge Raíz** actual.



■ Costo de la Ruta al Bridge Raíz – Determina cuán lejos se encuentra el Bridge Raíz. Por ejemplo, si los datos tienen que viajar a lo largo de tres segmentos de 100 Mbps para llegar al Bridge Raíz entonces el costo es 38 (19 + 19 + 0). El segmento adjunto al Bridge Raíz normalmente tendrá un Costo de Ruta de cero.

■ BID Emisora – La BID del switch que envía la BPDU.

■ ID de Puerto – El puerto real en el switch desde el cual se envió la BPDU.

Todos los switches están enviando constantemente BPDUs entre sí intentando determinar la mejor ruta entre diversos segmentos. Cuando un switch recibe una BPDU proveniente de otro switch que sea mejor que aquél para el cual está haciendo broadcasting para el mismo segmento, dejará de hacer broadcasting de su BPDU hacia el mismo. En lugar de eso, almacenará la BPDU del otro switch para referencia y para hacer broadcastings a **segmentos inferiores** tales como los segmentos que están localizados más lejos del bridge raíz.

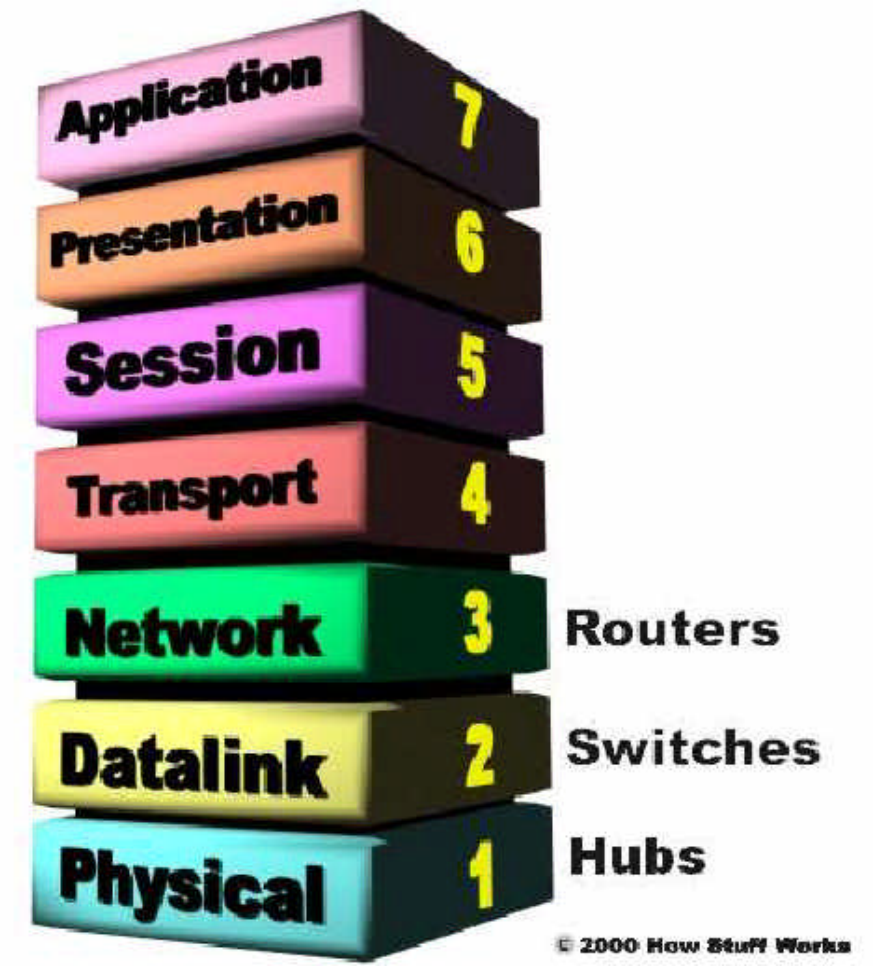
- Un **Bridge Raíz** se elige basándose en los resultados del proceso de la BPDU entre los switches. ¡Inicialmente, cada switch se considera a sí mismo el Bridge Raíz! Cuando un switch se enciende por primera vez en la red, envía una BPDU son su propia BID como BID Raíz. Cuando los otros switches reciben la BPDU, comparan la BID con la que ya tienen almacenada como BID Raíz. Si la nueva BID Raíz tiene un valor inferior, reemplazan a la guardada. Pero si la BID Raíz guardada es inferior, se envía una BPDU al nuevo switch con esta BID como la BID Raíz. Cuando el nuevo switch recibe la BPDU, se da cuenta de que no es el Bridge Raíz y reemplaza la BID Raíz de su tabla con la que acaba de recibir. El resultado es que el switch que tiene la BID más baja es elegido por los otros switches como Bridge Raíz.
- Basándose en la ubicación del Bridge Raíz, los otros switches determinan cuál de sus puertos tiene el costo de ruta más bajo hacia el Bridge Raíz. Estos puertos se denominan **Puertos Raíz** y cada switch (que no sea el Bridge Raíz actual) debe tener uno.
- Los switches determinan quién tendrá **Puertos Designados**. Un Puerto Designado es la conexión que se utiliza para enviar y recibir paquetes en un segmento específico. ¡Con un solo Puerto Designado por segmento, se resuelven todos los problemas de bucles!

  Los Puertos Designados se seleccionan basándose en el costo de ruta más bajo al Bridge Raíz para un segmento. Puesto que el Bridge Raíz tendrá un costo de ruta de "0", todos los puerto que se encuentren en él que estén conectados a segmentos se convertirán en Puertos Designados. Para los otros switches, el costo de la ruta se compara para un segmento dado. Si se determina que un puerto tiene un costo de ruta más bajo, entonces se convierte en el Puerto Designado para ese segmento. Si dos o más puertos tienen el mismo costo de ruta, entonces se elige el switch con la BID más baja.
- Una vez que el Puerto Designado para un segmento de red ha sido escogido, todos los otros puertos que se conectan a ese segmento se convierten en **Puertos no Designados**. Impiden que el tráfico de la red tome esa ruta para que sólo pueda acceder a ese segmento a través del Puerto Designado.

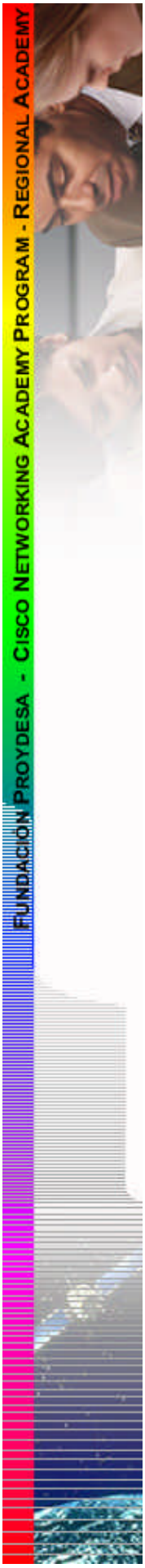
Cada switch tiene una tabla de BPDUs que actualiza continuamente. La red está configurada ahora como un único spanning tree con el Bridge Raíz como troncal y todos los otros switches como ramas. Cada switch se comunica con el Bridge Raíz a través de los Puertos Raíz y con cada segmento a través de los Puertos Designados para mantener una red libre de bucles. En el caso de que el Bridge Raíz comience a fallar o tenga problemas de red, STP permite a los otros switches el reconfigurar inmediatamente la red con otro switch actuando como Bridge Raíz. Este asombroso proceso proporciona a una compañía la capacidad de contar un una red compleja que sea tolerante a los fallos y aún así sea fácil de mantener.

Routers y Conmutación de Capa 3

Mientras que la mayoría de los switches operan en la **Capa de datos (Capa 2)** del Modelo de Referencia OSI, algunos incorporan las características de un router y operan también en la **Capa de red (Capa 3)**. De hecho, un switch de Capa 3 es increíblemente similar a un router.



Al igual que los routers,
los switches de Capa 3 realmente funcionan en la capa de Red.

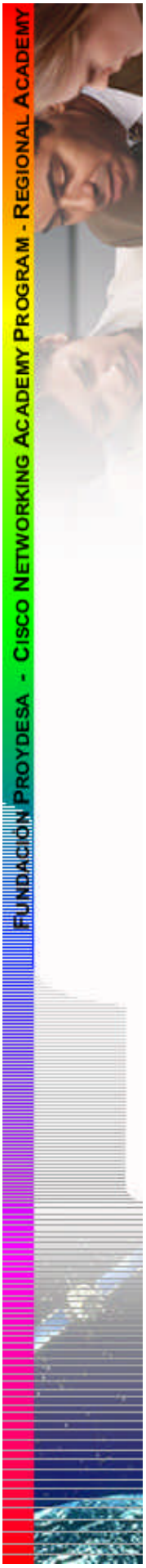


Cuando un router recibe un paquete, observa las direcciones de origen y destino de Capa 3 (la Capa de Red) para determinar la ruta que el paquete deberá tomar. Esto se considera actividad de networking de Capa 3 (de Red). Un switch estándar se basa en las direcciones MAC para determinar el origen y el destino de un paquete, lo cual es networking de Capa 2 (de Datos). La diferencia fundamental entre un router y un switch de Capa 3 es que los switches de Capa 3 tienen un hardware optimizado para hacer pasar los datos tan rápido como los switches de Capa 2, y aún así toman decisiones acerca de cómo transmitir el tráfico en la Capa 3, al igual que lo haría un router. Dentro del entorno LAN, un switch de Capa 3 usualmente es más rápido que un router porque está construido sobre hardware de conmutación. De hecho, muchos de los switches de Capa 3 de Cisco son realmente routers que operan más rápido porque están construidos en base a hardaware de "conmutación" con chips personalizados dentro de la caja.

La coincidencia de patrones y la aplicación de la caché en los switches de Capa 3 son similares a la coincidencia de patrones y a la aplicación de la caché en un router. Ambos utilizan un protocolo de enrutamiento y una tabla de enrutamiento para determinar la mejor ruta. No obstante, un switch de Capa 3 tiene la capacidad para reprogramar el hardware dinámicamente con la información de enrutamiento de Capa 3 actual. Es esto lo que permite un procesamiento de paquetes más rápido. En los switches de Capa 3 actuales como el Cisco Catalyst 6000, la información recibida de los protocolos de enrutamiento se utiliza para actualizar las tablas de caché del hardware. El 6000 es una muy buena manera de conectarse a la Internet porque tiene tarjetas WAN, pero los routers simples de diversos tamaños usualmente son buenos para conectarse a la Internet basándose en el flujo de tráfico y en el presupuesto. Un punto importante para ser notado, es que los routers son necesarios al establecer una comunicación entre dos VLANs...

VLANs

Al crecer las redes en tamaño y complejidad, muchas compañías han acudido a las **Redes de Área Local Virtuales (VLANs)** para proporcionar alguna manera de estructurar su crecimiento en forma lógica. Básicamente, una VLAN es un conjunto de nodos que se agrupan en un único **dominio de broadcast** que se basa en algo más que la ubicación física. Ya aprendimos antes acerca de los broadcasts y cómo un router no los pasa. Un dominio de broadcast es una red (o porción de una red) que recibirá un paquete de broadcast proveniente de cualquier nodo ubicado dentro de esa red. En una red típica, todo lo que se encuentra en el mismo lado del router es parte del mismo dominio de broadcast. Un switch en el que se han implementado VLANs tiene ahora múltiples dominios de broadcast de manera similar a un router. Pero aún necesita un router para enrutar de una VLAN a otra, porque el switch no puede hacerlo por sí mismo.



He aquí algunas razones comunes por las cuales una compañía podría tener VLANs:

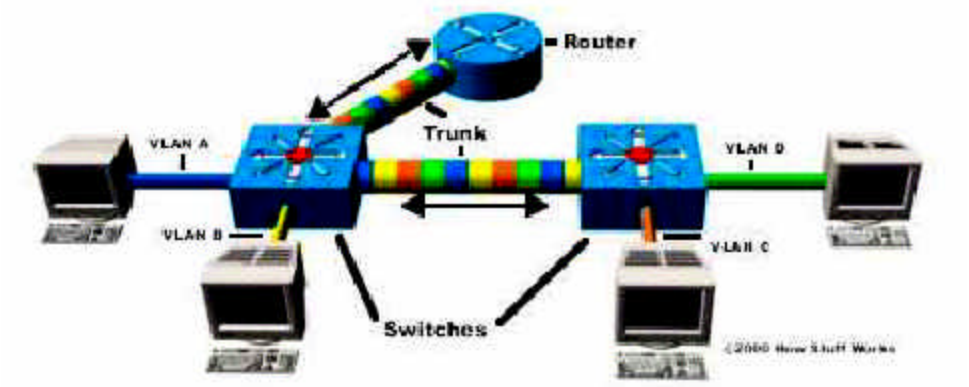
- Seguridad – La separación de sistemas con datos sensibles del resto de la red disminuye la oportunidad de que alguien obtenga acceso a información que no están autorizados para ver.
- Proyectos/Aplicaciones especiales – La gestión de un proyecto o el trabajo con una aplicación especializada pueden simplificarse por medio del uso de una VLAN que reúna a todos los nodos requeridos.
- Desempeño/Ancho de banda – Un monitoreo cuidadoso del uso de la red permite al administrador de la red crear VLANs que reduzcan la cantidad de saltos del router e incrementen el ancho de banda aparente para los usuarios de la red.
- Broadcasts/Flujo del tráfico – Puesto que un principio de una VLAN es el hecho de que no pasa tráfico de broadcast a nodos que no sean parte de la VLAN, automáticamente reduce los broadcasts. Las **listas de acceso** proporcionan al administrador de red una manera de controlar quién ve qué tráfico de red. Una lista de acceso es una tabla que crea el administrador de red que coloca en una lista qué direcciones tienen acceso a dicha red.
- Departamentos/Tipos de trabajos específicos – Las compañías pueden desear que las VLANs configuren departamentos que sean usuarios de la red con alta densidad (tales como Multimedia o Ingeniería) o una VLAN que atraviese departamentos que estén dedicados a tipos específicos de empleados (tales como los gerentes o la gente de ventas).

Se puede crear una VLAN utilizando la mayoría de los switches simplemente haciendo log in al switch a través de Telnet e introduciendo los parámetros para la VLAN (asignaciones de nombre, dominio y puerto). Después de haber creado la VLAN, luego todos los segmentos de red conectados a los puertos asignados se convertirán en parte de dicha VLAN.

Aunque se pueden tener más de una VLAN en un switch, éstas no pueden comunicarse directamente entre sí. Si lo hicieran acabarían con el propósito de tener una VLAN, que es aislar parte de una red. Comunicarse entre VLANs requiere el uso de un router.

Las VLANs pueden abarcar múltiples switches y puede tener más de una VLAN en cada switch. Para que múltiples VLANs en múltiples switches puedan comunicarse a través de un único enlace entre los switches, se debe utilizar un proceso denominado **trunking**; trunking es la tecnología que permite a la información proveniente de múltiples VLANs el ser transportada a través de un solo enlace entre switches.

El **Protocolo de Trunking de VLAN (VTP)** es el protocolo que utilizan los switches para comunicarse entre sí acerca de la configuración de la VLAN.



En la imagen superior, cada switch tiene dos VLANs. En el primer switch, la VLAN A y la VLAN B se envían a través de un único puerto (troncal) tanto al router como a través de otro puerto al segundo switch. La VLAN C y la VLAN D son troncales desde el segundo switch al primer switch y a través del router. Este troncal puede transportar tráfico proveniente de las cuatro VLANs. El enlace troncal desde el primer switch al router también puede transportar a la totalidad de las 4 VLANs. De hecho, esta conexión al router realmente permite al router aparecer en la totalidad de las 4 VLANs, como si tuvieran 4 puertos físicos diferentes conectados al switch.

Las VLANs pueden comunicarse entre sí a través de la conexión troncal entre los dos switches que utilizan el router. Por ejemplo, los datos de una computadora en la VLAN A que necesitan llegar a la computadora en la VLAN B (o la VLAN C o la VLAN D) deben viajar desde el switch al router y nuevamente al switch. A causa del algoritmo de bridging transparente y del troncal, ¡ambas PCs y el router piensan que están en el mismo segmento físico!

Como se puede observar, los switches LAN son una tecnología asombrosa que realmente puede lograr una diferencia en la velocidad y la calidad de su red. Para más información, por favor asegúrese de verificar los excelentes enlaces que figuran más abajo.

El presente es traducción directa del original en inglés: “How LAN Switches Work”
disponible en www.cisco.com
Todos los gráficos contenidos en la misma,
Están tomados del mencionado original en inglés.