CONFIGURACION DE UN SWITCH

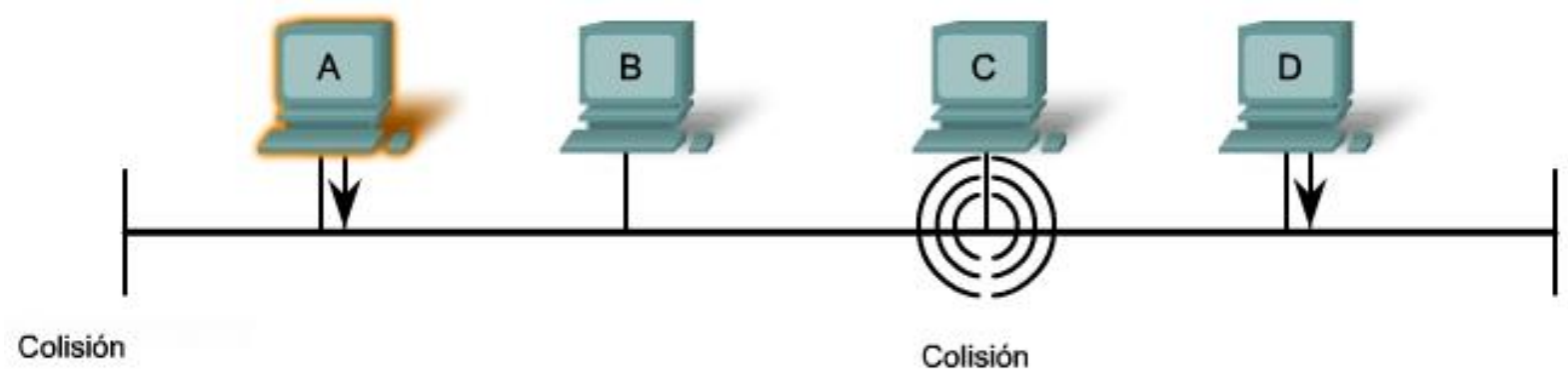
Elementos clave de las redes 802.3/Ethernet

Detección de portadora

- En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

- Si un dispositivo detecta una señal de otro dispositivo, espera un período determinado antes de intentar transmitirla.

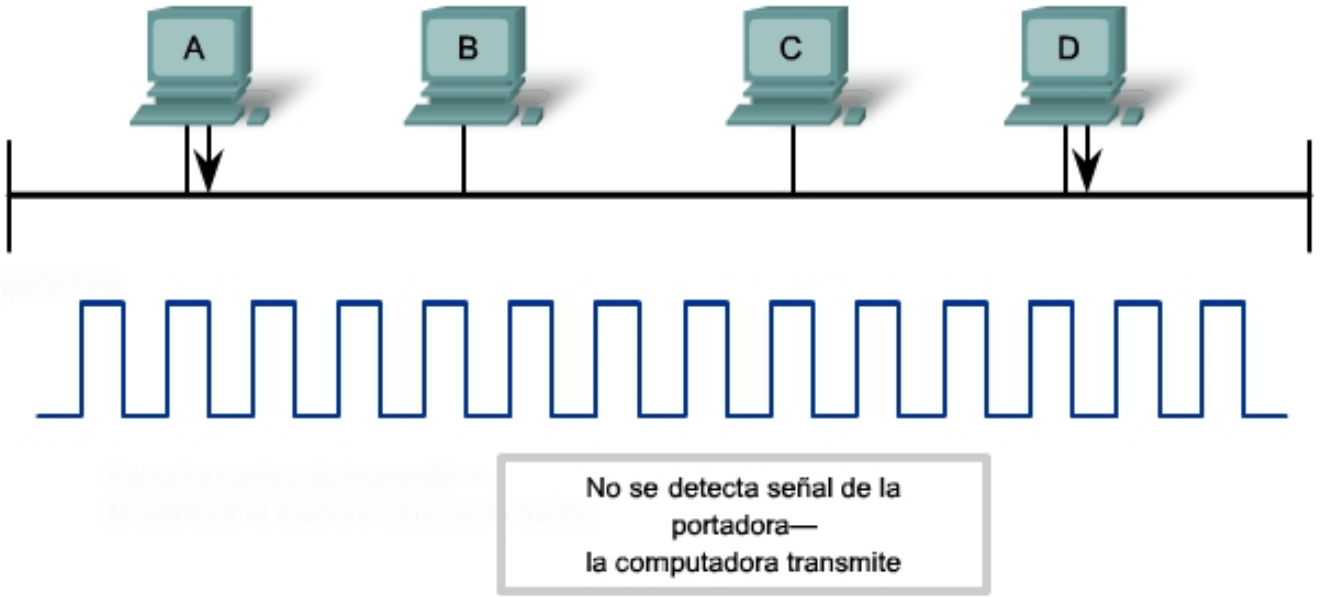
- Cuando no se detecta tráfico alguno, el dispositivo transmite su mensaje. Mientras se produce dicha transmisión, el dispositivo continúa atento al tráfico o a posibles colisiones en la LAN. Una vez enviado el mensaje, el dispositivo vuelve al modo de escucha predeterminado.



Elementos clave de las redes 802.3/Ethernet

Acceso múltiple

- Si la distancia entre los dispositivos es tal que la latencia de las señales de un dispositivo supone la no detección de éstas por parte de un segundo dispositivo, éste también podría comenzar a transmitirlas. De este modo, el medio contaría con dos dispositivos transmitiendo señales al mismo tiempo. Los mensajes se propagan en todo el medio hasta que se encuentran. En ese momento, las señales se mezclan y los mensajes se destruyen: se produce una colisión. Aunque los mensajes se dañan, la mezcla de señales continúa propagándose en todo el medio.

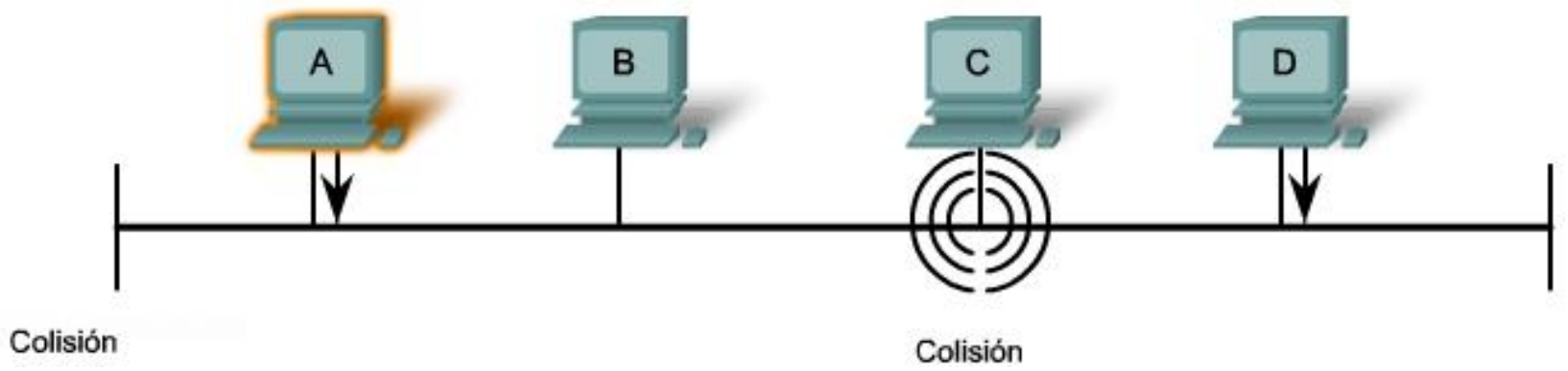


Elementos clave de las redes 802.3/Ethernet

Detección de colisiones

- Cuando un dispositivo está en el modo de escucha, puede detector cuando se produce una colisión en el medio compartido, ya que todos los dispositivos pueden detectar un aumento en la amplitud de la señal que esté por encima del nivel normal.

- Cuando se produce una colisión, los demás dispositivos que están en el modo de escucha, así como todos los dispositivos de transmisión, detectan el aumento de amplitud de la señal.

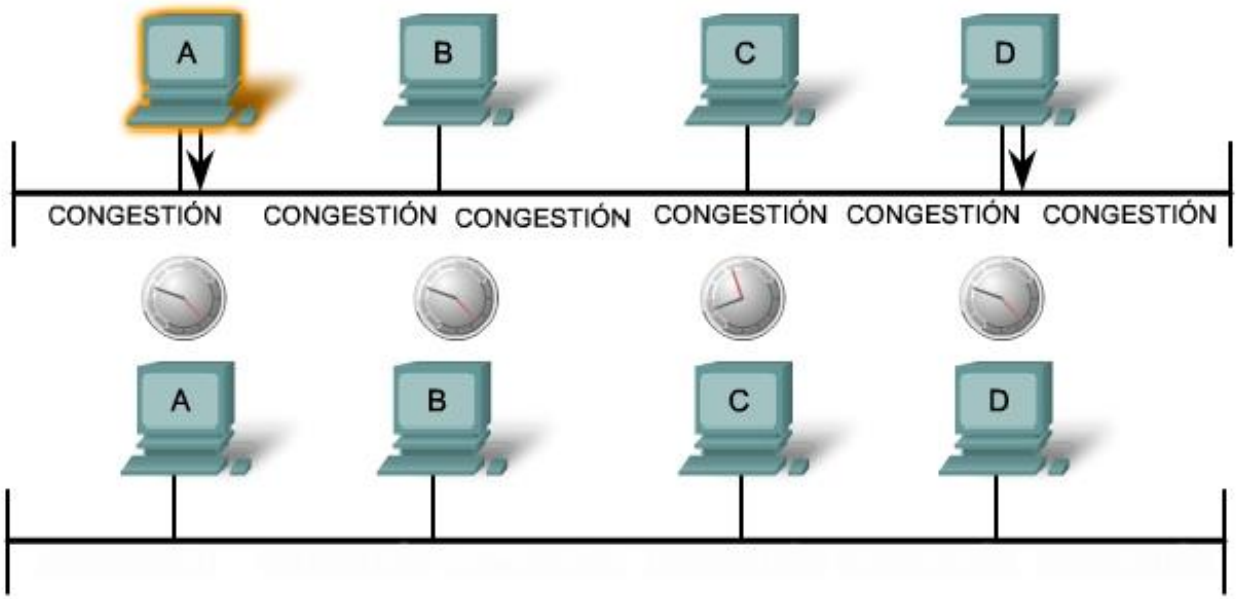


Elementos clave de las redes 802.3/Ethernet

Señal de congestión y postergación aleatoria

- Cuando se detecta una colisión, los dispositivos de transmisión envían una señal de congestionamiento. La señal de congestionamiento avisa a los demás dispositivos acerca de la colisión para que éstos invoquen un algoritmo de postergación. La función de éste es hacer que todos los dispositivos detengan su transmisión durante un período aleatorio, con lo cual se reducen las señales de colisión.

- Una vez que finaliza el retardo asignado a un dispositivo, dicho dispositivo regresa al modo "escuchar antes de transmitir".

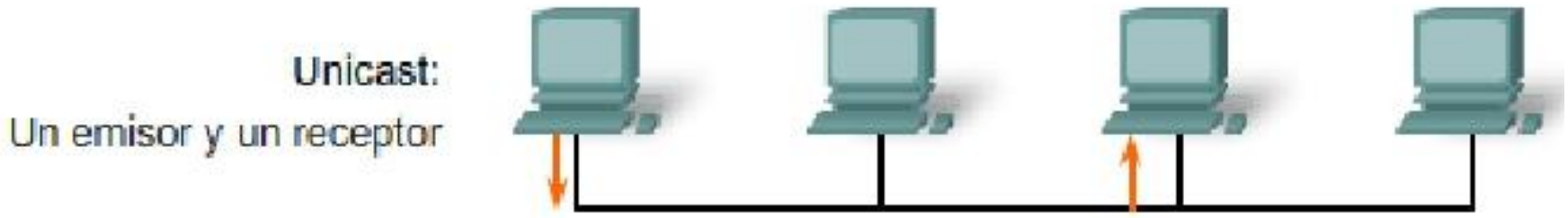


Elementos clave de las redes 802.3/Ethernet

Comunicaciones Ethernet

- Las comunicaciones en una red LAN conmutada se producen de tres maneras: unicast, broadcast y multicast:

- **Unicast:** Comunicación en la que un host envía una trama a un destino específico. En la transmisión unicast sólo existen un emisor y un receptor. La transmisión unicast es el modo de transmisión predominante en las LAN y en Internet. Algunos ejemplos de protocolos que usan transmisiones unicast son: HTTP, SMTP, FTP y Telnet.

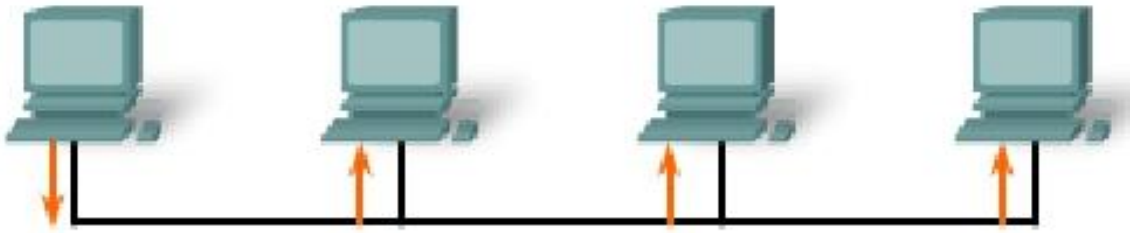


Elementos clave de las redes 802.3/Ethernet

Comunicaciones Ethernet

- **Broadcast:** Comunicación en la que se envía una trama desde una dirección hacia todas las demás direcciones. En este caso, existe sólo un emisor pero se envía la información a todos los receptores conectados. La transmisión broadcast es fundamental cuando se envía el mismo mensaje a todos los dispositivos de la LAN. Un ejemplo de transmisión broadcast es la consulta de resolución de direcciones que envía el protocolo de resolución de direcciones (ARP, Address Resolution Protocol) a todas las computadoras en una LAN.

Broadcast:
Un emisor a todas las otras direcciones

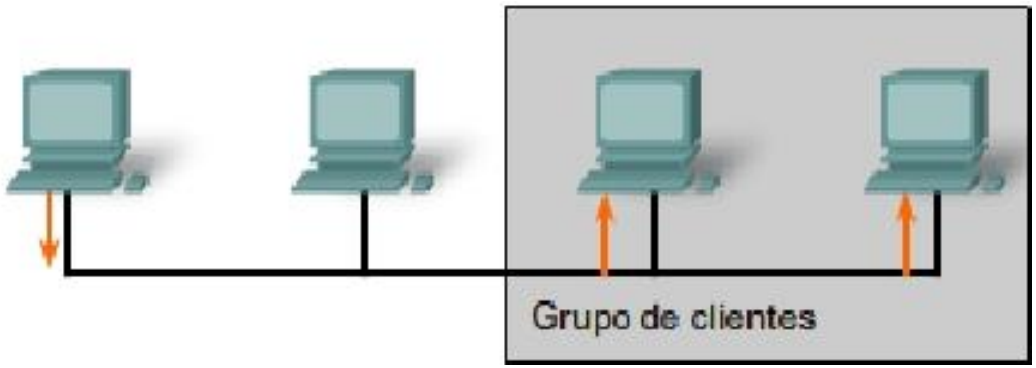


Elementos clave de las redes 802.3/Ethernet

Comunicaciones Ethernet

- **Multicast:** Comunicación en la que se envía una trama a un grupo específico de dispositivos o clientes. Los clientes de la transmisión multicast deben ser miembros de un grupo multicast lógico para poder recibir la información. Un ejemplo de transmisión multicast son las transmisiones de voz y video relacionadas con las reuniones de negocios en conferencia basadas en la red.

Multicast:
Un emisor a un grupo de direcciones



Elementos clave de las redes 802.3/Ethernet

Trama de Ethernet

- ✓ Campos Preámbulo y Delimitador de inicio de trama
- Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte) se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos primeros 8 bytes de la trama se emplean para captar la atención de los nodos receptores. Básicamente, los primeros bytes sirven para que los receptores se preparen para recibir una nueva trama.

IEEE 802.3						
7	1	6	6	2	46 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud/ Tipo	Encabezado y datos 802.2	Secuencia de verificación de trama

Elementos clave de las redes 802.3/Ethernet

Trama de Ethernet

✓ Campo Dirección MAC destino

- El campo Dirección MAC destino (6 bytes) es el identificador del receptor deseado. La Capa 2 utiliza esta dirección para ayudar a que un dispositivo determine si la trama está dirigida a él. Se compara la dirección de la trama con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

✓ Campo Dirección MAC origen

- El campo Dirección MAC origen (6 bytes) identifica la NIC o interfaz de origen de la trama. Los switches utilizan esta dirección para agregar dicha interfaz a sus tablas de búsqueda.

Elementos clave de las redes 802.3/Ethernet

Trama de Ethernet

✓ Campo Longitud/Tipo

- El campo Longitud/Tipo (2 bytes) define la longitud exacta del campo Datos de la trama. Este campo se utiliza más adelante como parte de la Secuencia de verificación de trama (FCS, Frame Check Sequence) con el objeto de asegurar que se haya recibido el mensaje de manera adecuada.

✓ Campos Datos y Relleno

- Los campos Datos y Relleno (de 46 a 1500 bytes) contienen la información encapsulada de una capa superior, que es una PDU de Capa 3 genérica o, más comúnmente, un paquete de IPv4. Todas las tramas deben tener una longitud mínima de 64 bytes (longitud mínima que colabora en la detección de colisiones). Si se encapsula un paquete menor, el campo Relleno se utiliza para incrementar el tamaño de la trama hasta alcanzar el tamaño mínimo.

Elementos clave de las redes 802.3/Ethernet

Trama de Ethernet

- ✓ Campo Secuencia de verificación de trama
- El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación de redundancia cíclica (CRC, cyclic redundancy check). El dispositivo emisor incluye los resultados de la CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, no se ha producido ningún error. Si los cálculos no coinciden, la trama se descarta.

Elementos clave de las redes 802.3/Ethernet

Trama de Ethernet

✓ Dirección MAC

- Una dirección Ethernet MAC es un valor binario de 48 bits que se compone de dos partes y se expresa como 12 dígitos hexadecimales. Los formatos de las direcciones podrían ser similares a 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, ó 0005.9A3C.7800.

- Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. La NIC utiliza la dirección MAC para determinar si deben pasarse los mensajes a las capas superiores para su procesamiento.

- La dirección MAC se compone del identificador exclusivo de organización (OUI, Organizational Unique Identifier) y del número de asignación del fabricante.

Elementos clave de las redes 802.3/Ethernet

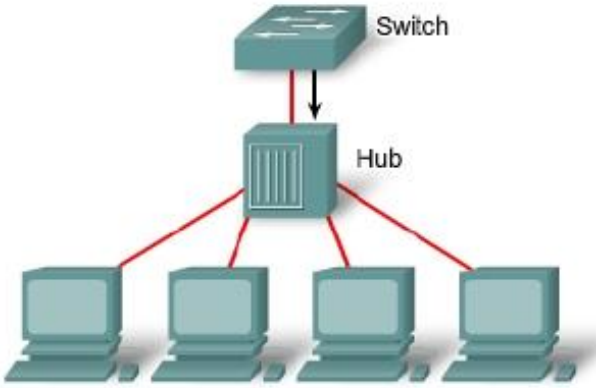
Configuración de Dúplex

- Se utilizan dos tipos de parámetros dúplex para las comunicaciones en una red Ethernet: **half duplex** y **full duplex**.

Configuración de Dúplex

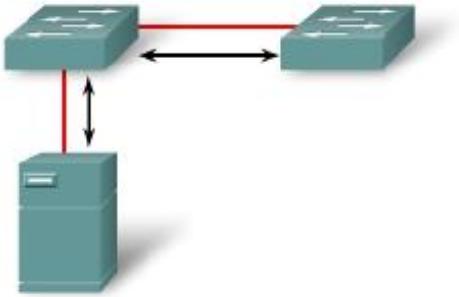
Half Duplex (CSMA/CD)

- Flujo de datos unidireccional
- Alto potencial para las colisiones
- Conectividad de hub



Full duplex

- Sólo punto a punto
- Conectado a puerto de switch dedicado
- Requiere soporte para full-duplex en ambos extremos
- Sin colisiones
- Circuito de detección de colisiones deshabilitado



Elementos clave de las redes 802.3/Ethernet

Configuración de Dúplex

✓ Configuración del puerto de switch

- El puerto de un switch debe configurarse con parámetros dúplex que coincidan con el tipo de medio. Los switches Cisco Catalyst cuentan con tres parámetros:

- La opción auto establece el modo autonegociación de dúplex. Cuando este modo se encuentra habilitado, los dos puertos se comunican para decidir el mejor modo de funcionamiento.

- La opción full establece el modo full-duplex.

- La opción half establece el modo half-duplex.

Elementos clave de las redes 802.3/Ethernet

auto-MDIX

- Las conexiones entre dispositivos específicos, como de switch a switch o de switch a router, solían requerir el uso de ciertos tipos de cables (de conexión cruzada o de conexión directa). Ahora, en cambio, se puede utilizar el comando de mdix auto de la CLI para habilitar la función automática de conexión cruzada de interfaz dependiente del medio (auto-MDIX).

- Al habilitar la función auto-MDIX, el switch detecta el tipo de cable que se requiere para las conexiones Ethernet de cobre y, conforme a ello, configura las interfaces. Por lo tanto, se puede utilizar un cable de conexión directa o cruzada para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que se encuentre en el otro extremo de la conexión.

Elementos clave de las redes 802.3/Ethernet

Direccionamiento MAC y Tablas de direcciones MAC de los switches

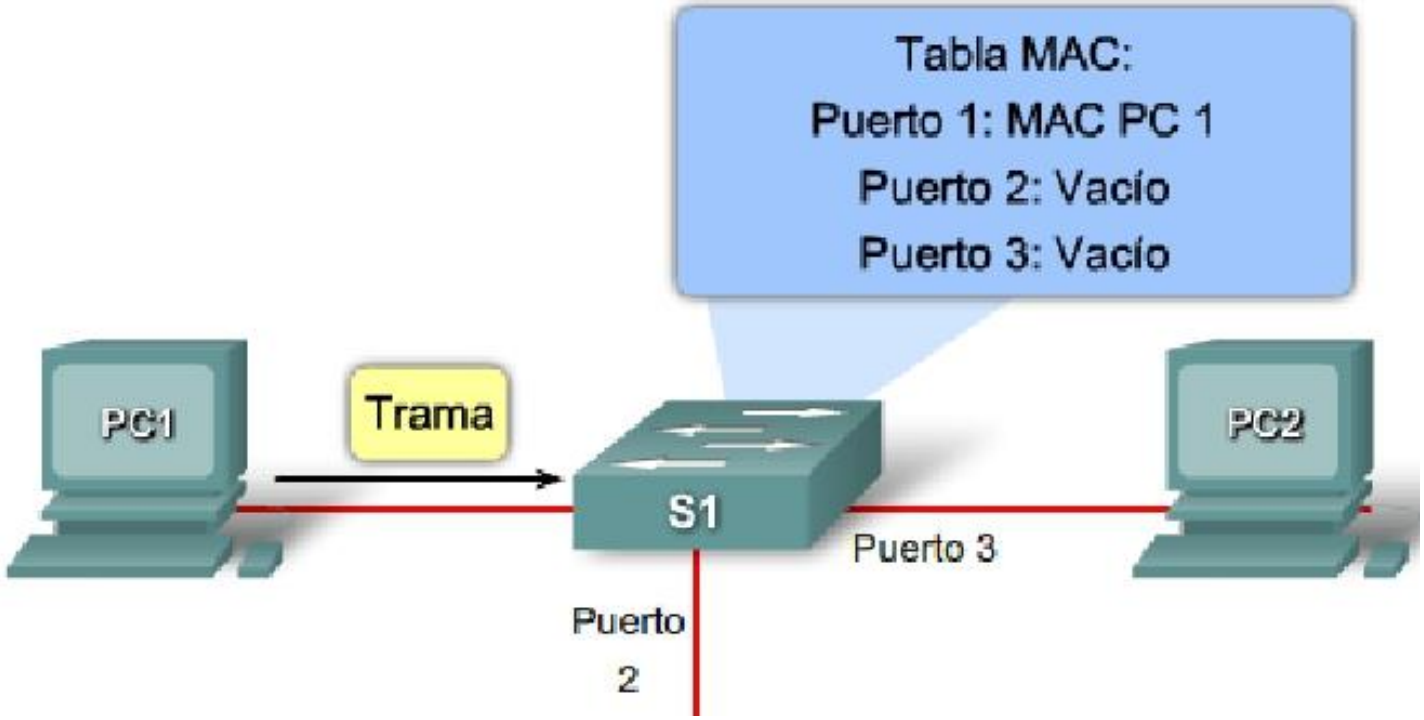
- Los switches emplean direcciones MAC para dirigir las comunicaciones de red a través de su estructura al puerto correspondiente hasta el nodo de destino. El switch debe primero saber qué nodos existen en cada uno de sus puertos para poder definir cuál será el puerto que utilizará para transmitir una trama unicast.

- El switch determina cómo manejar las tramas de datos entrantes mediante una tabla de direcciones MAC. El switch genera su tabla de direcciones MAC grabando las direcciones MAC de los nodos que se encuentran conectados en cada uno de sus puertos. Una vez que la dirección MAC de un nodo específico en un puerto determinado queda registrada en la tabla de direcciones, el switch ya sabe enviar el tráfico destinado a ese nodo específico desde el puerto asignado a dicho nodo para posteriores transmisiones.

Elementos clave de las redes 802.3/Ethernet

Direccionamiento MAC y Tablas de direcciones MAC de los switches

- Cuando un switch recibe una trama de datos entrantes y la dirección MAC de destino no figura en la tabla, éste reenvía la trama a todos los puertos excepto al que la recibió en primer lugar. Cuando el nodo de destino responde, el switch registra la dirección MAC de éste en la tabla de direcciones del campo dirección de origen de la trama.



Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

Ancho de banda y rendimiento

- Una importante desventaja de las redes Ethernet 802.3 son las colisiones. Las colisiones se producen cuando dos hosts transmiten tramas de forma simultánea. Cuando se produce una colisión, las tramas transmitidas se dañan o se destruyen. Los hosts transmisores detienen la transmisión por un período aleatorio, conforme a las reglas de Ethernet 802.3 de CSMA/CD.

- El rendimiento neto del puerto (la cantidad promedio de datos eficazmente transmitidos) disminuirá de manera significativa según la cantidad de nodos adicionales que se utilicen en la red. Los hubs no ofrecen mecanismo alguno que sirva para eliminar o reducir estas colisiones y el ancho de banda disponible que cualquier nodo tenga que transmitir se verá reducido en consecuencia.

Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

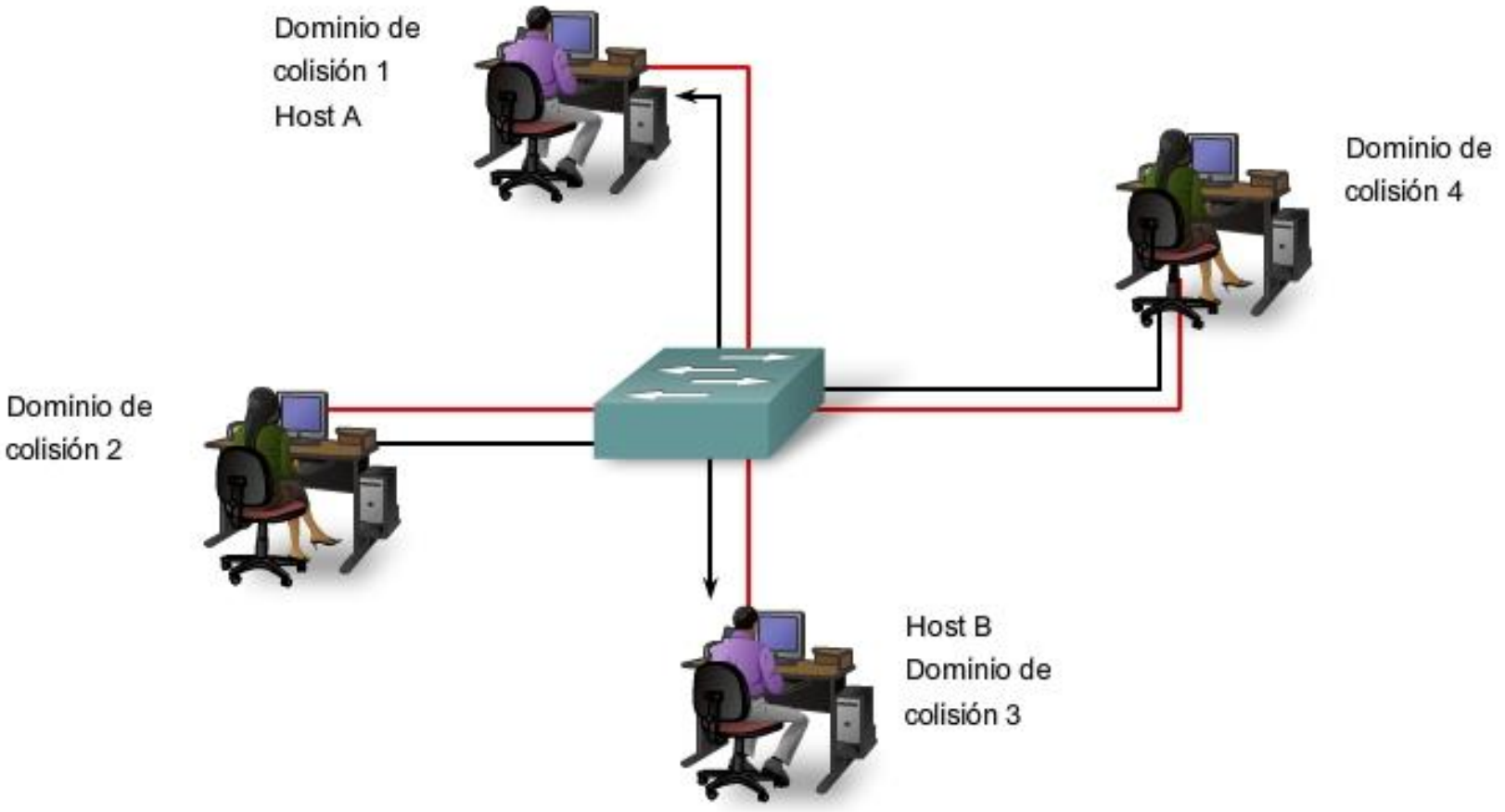
Dominios de colisiones

- Al expandir una LAN Ethernet para alojar más usuarios con mayores requisitos de ancho de banda, aumenta la posibilidad de que se produzcan colisiones. Para reducir el número de nodos en un determinado segmento de red, se pueden crear segmentos físicos de red individuales llamados dominios de colisiones.

- El área de la red donde se originan las tramas y se producen las colisiones se denomina dominio de colisiones. Todos los entornos del medio compartido, como aquéllos creados mediante el uso de hubs, son dominios de colisión. Cuando un host se conecta a un puerto de switch, el switch crea una conexión dedicada. Esta conexión se considera como un dominio de colisiones individual, dado que el tráfico se mantiene separado de cualquier otro y, por consiguiente, se eliminan las posibilidades de colisión.

Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

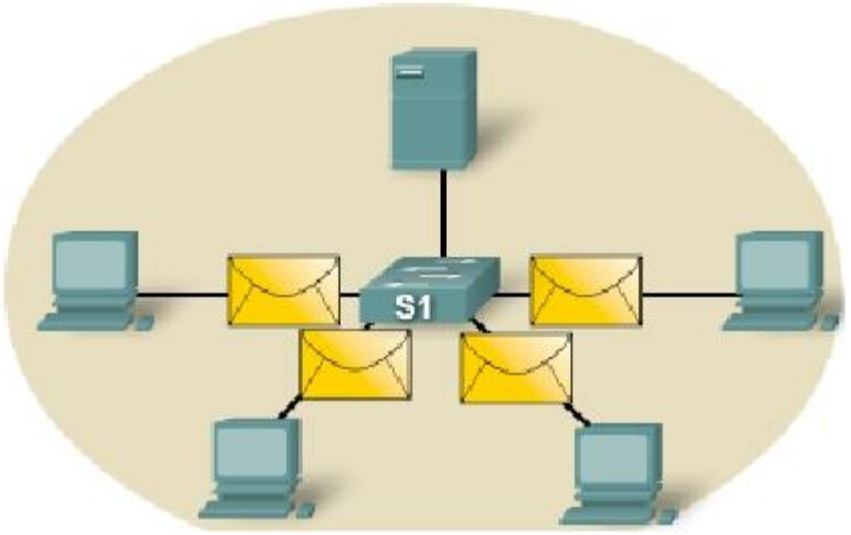
Dominios de colisiones



Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

Dominios de broadcast

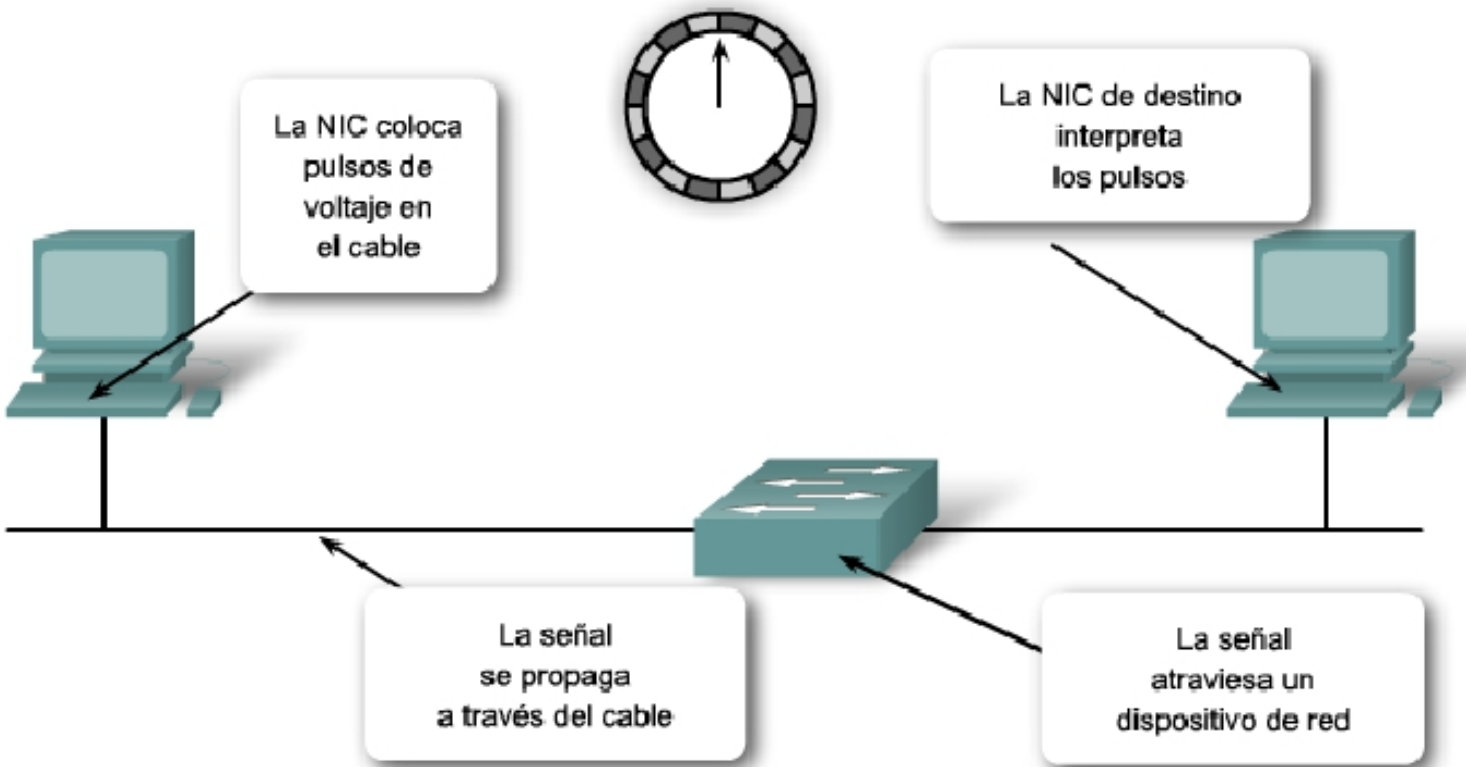
- Si bien los switches hacen pasar por un filtro a la mayoría de las tramas según las direcciones MAC, no hacen lo mismo con las tramas de broadcast. Una serie de switches interconectados forma un dominio de broadcast simple. Sólo una entidad de Capa 3, como un router o una LAN virtual (VLAN), puede detener un dominio de broadcast de Capa 3. Los routers y las VLAN se utilizan para segmentar los dominios de colisión y de broadcast.



Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

Latencia de red

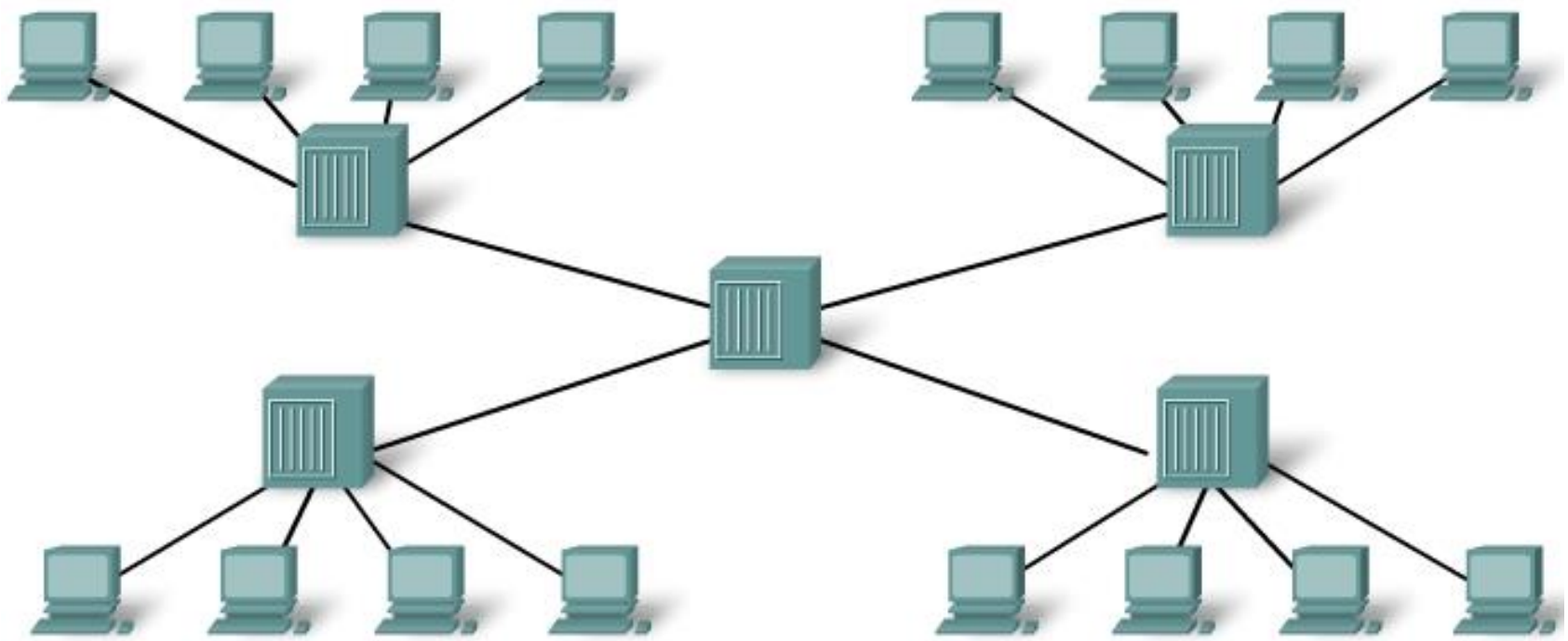
- La latencia es el tiempo que le toma a una trama o a un paquete hacer el recorrido desde la estación origen hasta su destino final.



Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

Congestión de la red

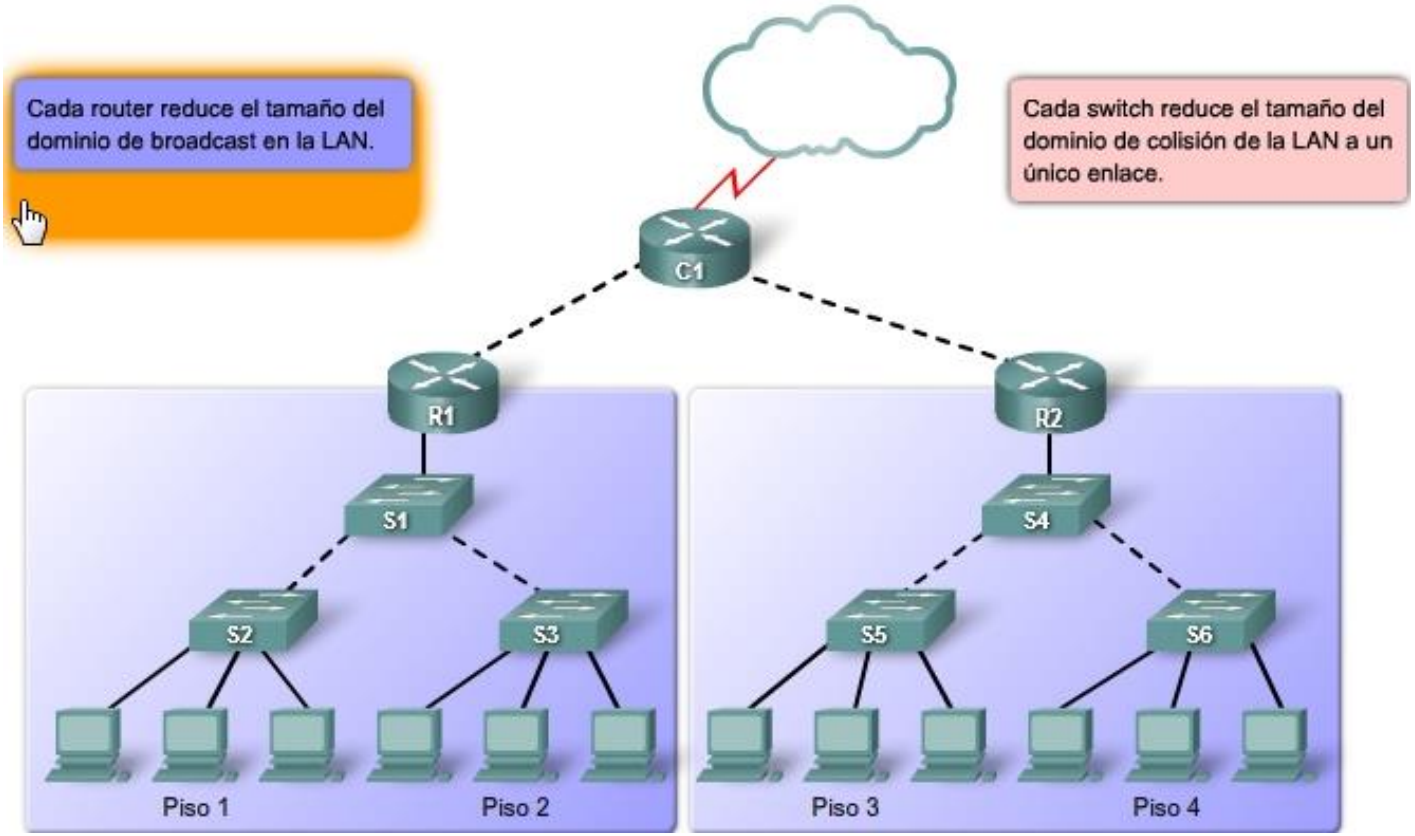
- El primer motivo para segmentar una LAN en partes más pequeñas es el de aislar el tráfico y lograr una mejor utilización del ancho de banda por usuario. Al no segmentarla, la LAN se obstruye rápidamente debido al tráfico y a las colisiones.



Aspectos que se deben tener en cuenta para las redes 802.3/Ethernet

Segmentación de las LAN

- Las LAN se segmentan en varios dominios de broadcast y de colisiones más pequeños mediante el uso de routers y switches.



Consideraciones del diseño LAN

Control de la latencia de la red

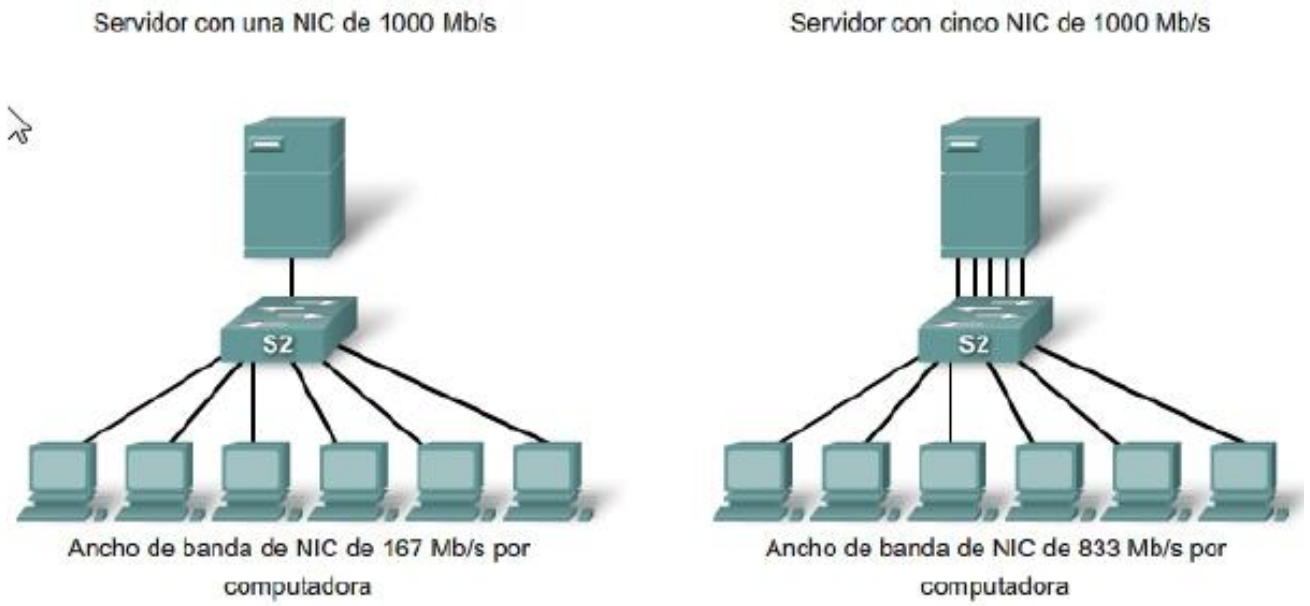
- Considere la latencia producida por cada dispositivo de la red.
  - Un switch de nivel de núcleo que mantiene 48 puertos, ejecutándose a 1000 Mb/s full duplex, requiere un rendimiento interno de 96 Gb/s para mantener la velocidad de cable total en todos los puertos al mismo tiempo.

- Los dispositivos de las capas OSI más altas también pueden aumentar la latencia de la red.
  - El router debe quitar los campos de la Capa 2 de la trama para poder interpretar la información de direccionamiento de la Capa 3. El tiempo de procesamiento adicional provoca latencia.
  - Se balancea el uso de dispositivos de capas superiores para deducir la latencia de la red con la necesidad de evitar la contención del tráfico de broadcast o las altas tasas de colisiones.

Consideraciones del diseño LAN

Eliminación de los cuellos de botella

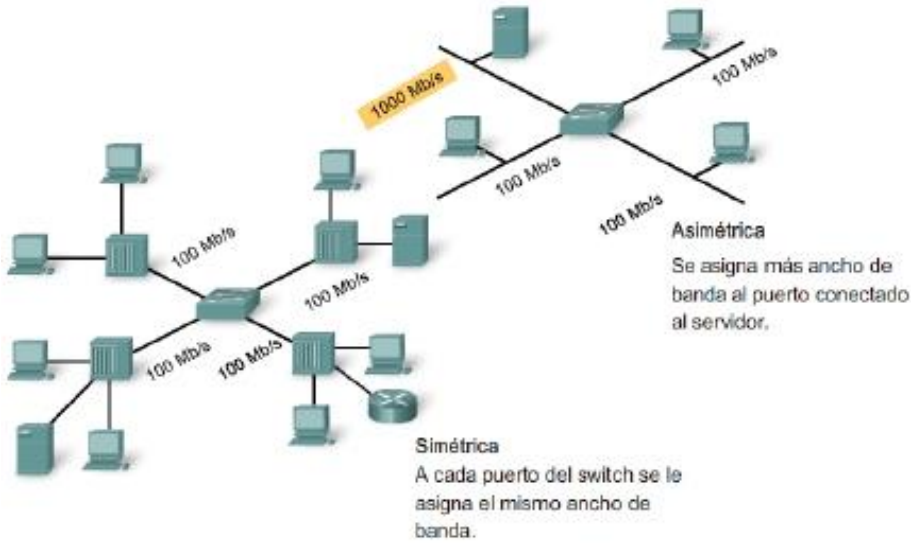
- Los cuellos de botella son lugares donde la alta congestión de la red provoca un bajo rendimiento.
- Si se utilizan enlaces de mayor capacidad (por ejemplo, actualizar una conexión de 100 Mb/s hasta 1000 Mb/s) y se emplean varios enlaces promoviendo una tecnología de unificación de enlaces (por ejemplo, combinar dos enlaces como si fueran uno para duplicar la capacidad de la conexión) pueden reducirse los cuellos de botella creados por los enlaces de switches interconectados y de routers.



Reenvío de tramas mediante un switch

Conmutación simétrica y asimétrica

- La conmutación LAN se puede clasificar como simétrica o asimétrica según la forma en que el ancho de banda se asigna a los puertos de conmutación.
- La conmutación simétrica proporciona conexiones conmutadas entre puertos con el mismo ancho de banda; por ejemplo, todos los puertos de 100 Mb/s o todos los puertos de 1000 Mb/s. Un switch LAN asimétrico proporciona conexiones conmutadas entre puertos con distinto ancho de banda; por ejemplo, una combinación de puertos de 10 Mb/s y puertos de 1000 Mb/s. La figura muestra las diferencias entre la conmutación simétrica y la asimétrica.



Configuración de la administración de Switch

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC usuario a modo EXEC privilegiado.	`switch>`**`enable`**
Si una contraseña ha sido configurada para modo EXEC privilegiado, se le solicitará que la ingrese ahora.	`password:`**`Contraseña`**
La petición de entrada # significa modo EXEC privilegiado.	`switch#`
Cambia de modo EXEC privilegiado a modo EXEC usuario.	`switch#`**`disable`**
La petición de entrada > significa modo EXEC usuario.	`switch>`

Configuración de la administración de Switch

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC privilegiado a modo de configuración global.	`switch#configure terminal`
La petición de entrada (config)# significa que el switch está en modo de configuración global.	`switch(config)#`
Cambia de modo de configuración global a modo de configuración de interfaz para la interfaz 0/1 fast ethernet.	`switch(config)#interface fastethernet 0/1`
La petición de entrada (config)# significa que el switch está en modo de configuración de interfaz.	`switch(config-if)#`
Cambia de modo de configuración de interfaz a modo de configuración global.	`switch(config-if)#exit`
La petición de entrada (config)# significa que el switch está en modo de configuración global.	`switch(config)#`
Cambia de modo de configuración global a modo EXEC privilegiado.	`switch(config)#exit`
La petición de entrada # significa que el switch está en modo EXEC privilegiado.	`switch#`

Configuración de la administración de Switch

El historial de comandos permite llevar a cabo las siguientes tareas:

- Mostrar los contenidos del búfer de comandos.
- Establecer el tamaño del búfer del historial de comandos.
- Recordar comandos previamente ingresados y almacenados en el búfer del historial. Cada modo de configuración cuenta con un búfer exclusivo.

Sintaxis de comando de la CLI del IOS de Cisco	
Habilite el historial del terminal. Este comando se puede ejecutar desde el modo EXEC privilegiado o usuario.	`switch#terminal history`
Configura el tamaño del historial del terminal. El historial del terminal puede mantener de 0 a 256 líneas de comando.	`switch#terminal history size 50`
Restablece el tamaño del historial del terminal al valor predeterminado de 10 líneas de comando.	`switch#terminal no history size`
Inhabilita el historial del terminal.	`switch#terminal no history`

Configuración de la administración de Switch

Descripción de la secuencia de arranque

Secuencia de arranque de un switch de Cisco:

-El switch carga el software cargador de arranque de NVRAM.

-El cargador de arranque:

- Realiza la inicialización de la CPU a bajo nivel.
- Realiza el POST para el subsistema de la CPU.
- Inicializa el sistema de archivos flash en la placa del sistema.
- Carga una imagen predeterminada de software de sistema operativo en la memoria y arranca el switch.

-El sistema operativo se ejecuta utilizando el archivo config.text, guardado en el almacenamiento flash del switch.

El cargador de arranque puede ser de utilidad en la recuperación en caso de un colapso del sistema operativo:

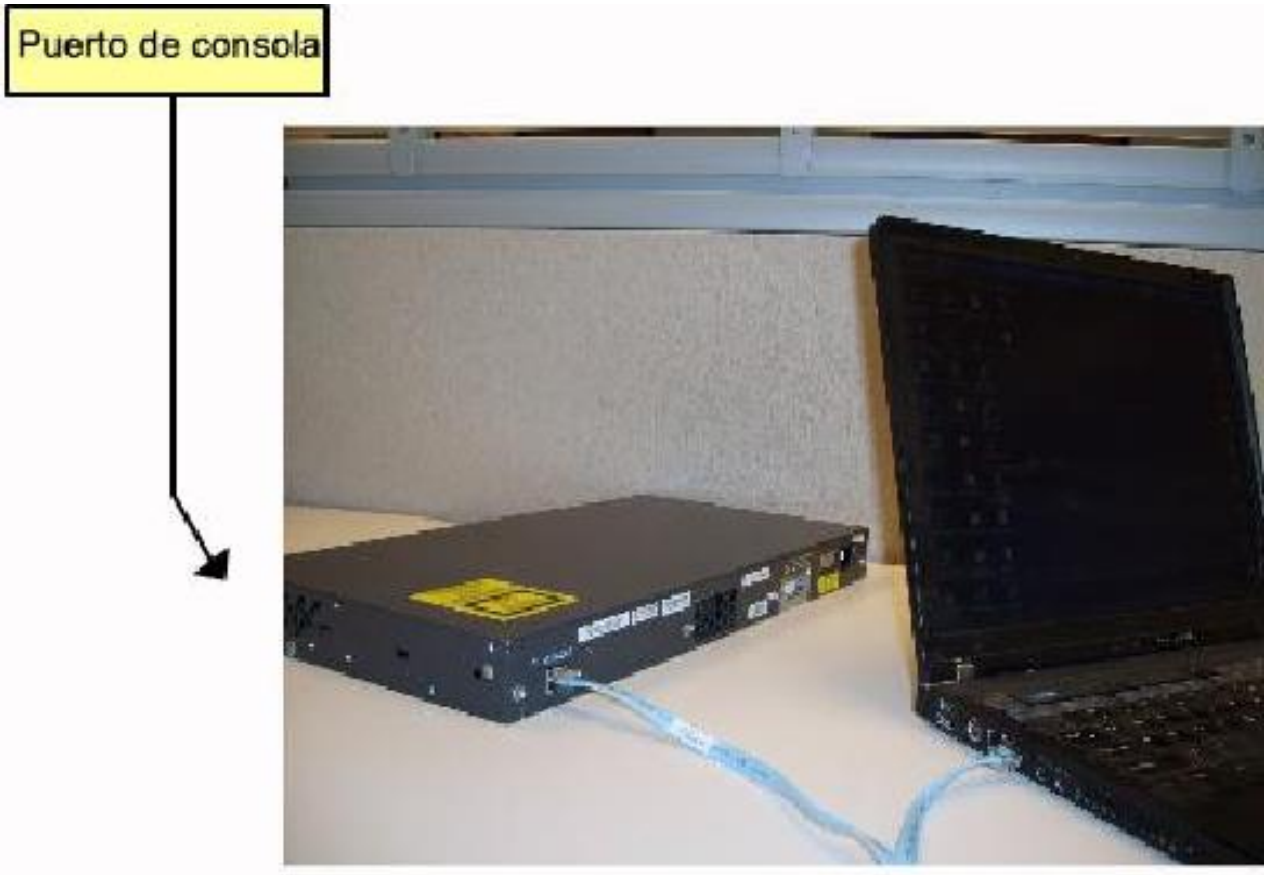
-Proporciona acceso al switch si el sistema operativo tiene problemas lo suficientemente graves como para quedar inutilizable.

-Proporciona acceso a los archivos almacenados en flash antes de que se cargue el sistema operativo.

-Utilice la línea de comandos del cargador de arranque para las operaciones de recuperación.

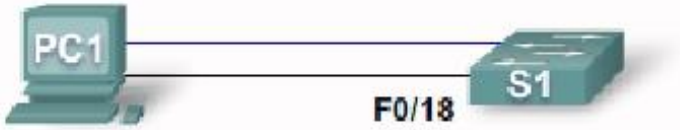
Configuración de la administración de Switch

- Conexión al switch, a través de su puerto de consola y la interfaz COM del PC.



Configuración de la administración de Switch

Configurar la conectividad IP



PC1:
- Dirección IP: 172.17.99.12
- Conectada a puerto de consola
- Conectada a puerto F0/18 de S1

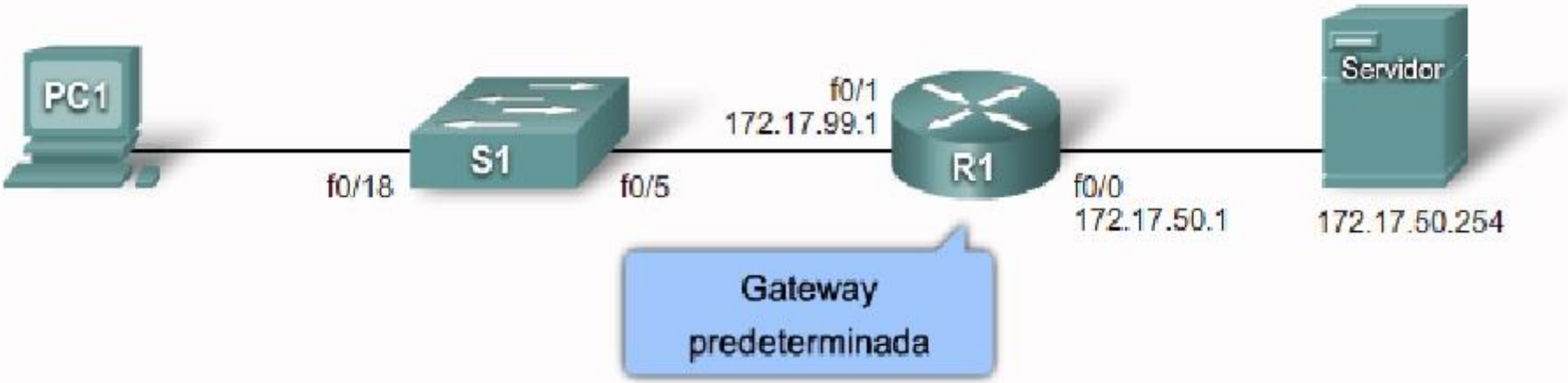
S1:
- VLAN 99
- VLAN de administración
- Dirección IP: 172.17.99.11
- Puerto F0/18 asignado a VLAN 99

- Para la administración de TCP/IP debe asignarse una dirección de la Capa 3 al switch.
- VLAN 1 es la interfaz de administración predeterminada para todos los switches
- Existen riesgos de seguridad asociados con el uso de VLAN 1
- Cree otra VLAN, por ejemplo VLAN 99 o VLAN 150.
- Asigne dicha VLAN a un puerto adecuado, por ejemplo F0/18

Configuración de la administración de Switch

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Ingrese al modo de configuración de interfaz para la interfaz de VLAN 99.	`S1(config)#interface vlan 99`
Configurar la dirección IP de la interfaz.	`S1(config-if)#dirección IP 172.17.99.11 255.255.255.0`
Habilitar la interfaz.	`S1(config-if)#no shutdown`
Regrese al modo EXEC privilegiado.	`S1(config-if)#end`
Ingrese al modo de configuración global.	`S1#configure terminal`
Ingrese la interfaz para asignar la VLAN.	`S1(config)#interface fastethernet 0/18`
Defina el modo de membresía de la VLAN para el puerto.	`S1(config-if)#switchport mode access`
Asigne el puerto a una VLAN.	`S1(config-if)#switchport acces vlan 99`
Regrese al modo EXEC privilegiado.	`S1(config-if)#end`
Guardar la configuración en ejecución en la configuración de inicio del switch.	`S1#copy running-config startup-config`

Configuración de la administración de Switch



Sintaxis del comando de CLI IOS de Cisco	
Configura la gateway predeterminada en el switch.	`S1(config)#ip default-gateway 172.17.99.1`
Regrese al modo EXEC privilegiado.	`S1(config)#end`
Guardar la configuración en ejecución en la configuración de inicio del switch.	`S1#copy running-config startup-config`

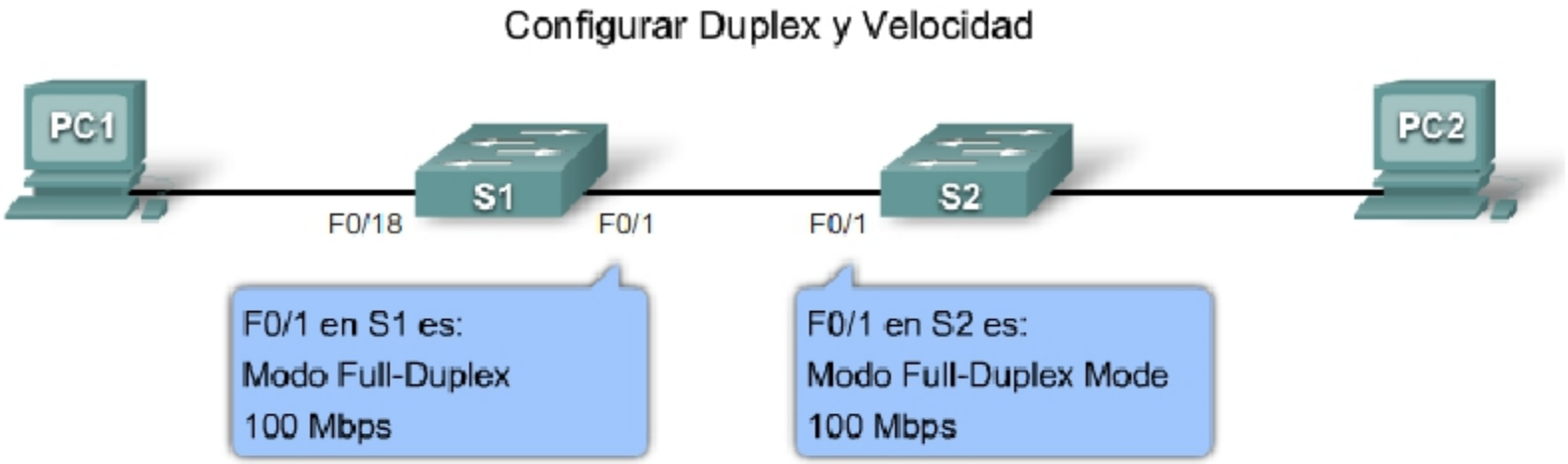
Configuración de la administración de Switch

```
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
…
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no ip route-cache
!
```

VLAN 99 configurada en el puerto F0/18

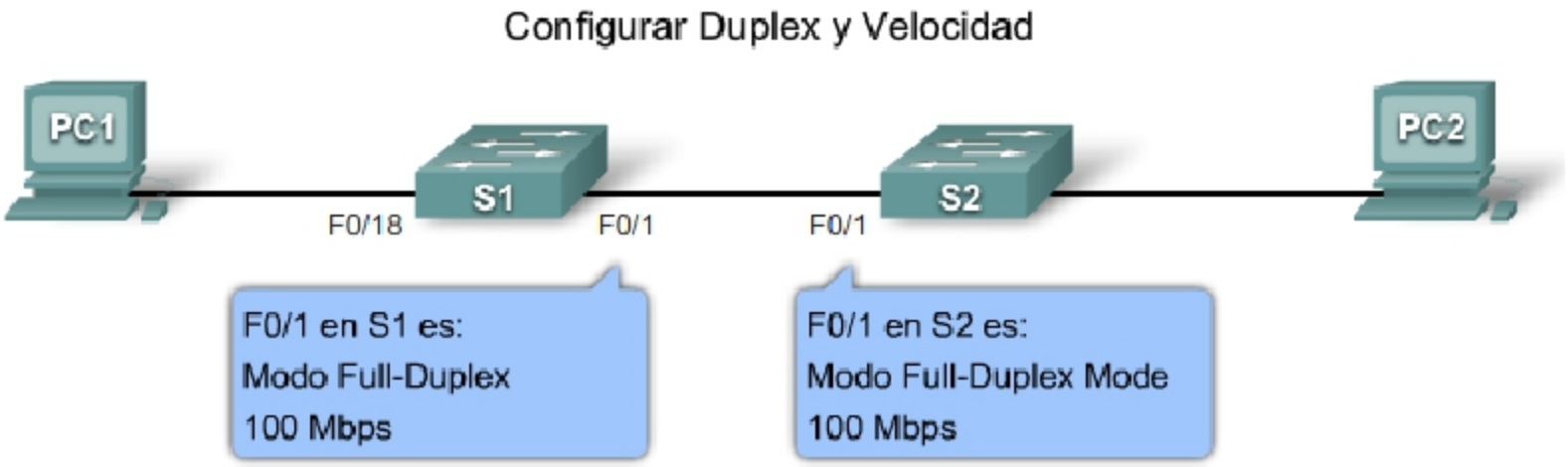
```
S1#show ip interface brief
Interface              IP-Address      OK?   Method    Status
Protocol
…
Vlan99                 172.17.99.11    YES   manual    up          up
…
FastEthernet0/18       unassigned      YES   unset     up          up
FastEthernet0/19       unassigned      YES   unset     down        down
```

Configuración de la administración de Switch



Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Ingresar al modo de configuración de interfaz.	`S1(config)#Interface fastethernet 0/1`
Configurar el modo duplex de interfaz para activar la configuración duplex automática.	`S1(config-if)#duplex auto`
Configurar duplex y velocidad de la interfaz y activar la configuración de velocidad automática.	`S1(config-if)#speed auto`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`
Guardar la configuración en ejecución en la configuración inicial del switch.	`S1#copy running-config startup-config`

Configuración de la administración de Switch



Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Ingresar al modo de configuración de interfaz.	`S1(config)#Interface fastethernet 0/1`
Configurar el modo duplex de interfaz para activar la configuración duplex automática.	`S1(config-if)#duplex auto`
Configurar duplex y velocidad de la interfaz y activar la configuración de velocidad automática.	`S1(config-if)#speed auto`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`
Guardar la configuración en ejecución en la configuración inicial del switch.	`S1#copy running-config startup-config`

Configuración de la administración de Switch

Administración de la tabla de direcciones MAC

- Los switches utilizan tablas de direcciones MAC para determinar cómo enviar tráfico de puerto a puerto. Estas tablas de direcciones MAC incluyen direcciones estáticas y dinámicas. El comando **show mac-address-table** muestra la tabla de direcciones MAC que incluye estas direcciones.

- Para crear una asignación estática en la tabla de direcciones MAC, ingrese el comando **mac-address-table static <dirección MAC> vlan {1-4096, ALL} interface id** de la interfaz.

Configuración de la administración de Switch

Uso de los comandos show

Sintaxis del comando de CLI IOS de Cisco	
Muestra el estado de la interfaz y la configuración para una o todas las interfaces disponibles del switch.	`show interfaces [id de la interfaz]`
Muestra el contenido de la configuración de inicio.	`show startup-config`
Muestra la configuración de funcionamiento actual.	`show running-config`
Muestra información acerca de flash: sistema de archivos.	`show flash:`
Muestra el estado del hardware y el software del sistema.	`show version`
Muestra el historial de comandos de sesión.	`show history`
Muestra información de IP. La opción interface muestra el estado de la interfaz de IP y la configuración. La opción http muestra información de HTTP acerca del administrador de dispositivos que se ejecuta en el switch. La opción arp muestra la tabla ARP de IP.	`show ip {interface | http | arp}`
Muestra la tabla MAC de envío.	`show mac-address-table`

Configuración de la administración de Switch

```
S1#show running-config
Building configuration...

Current configuration : 1664 bytes
!
version 12.2
...
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
.....
!
interface Vlan99
 ip address 172.17.99.11 255.255.0.0
 no ip route-cache
!
ip default-gateway 172.17.50.1
ip http server
```

Configuración de la administración de Switch

```
S1#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0019.aa9e.b001 (bia 0019.aa9e.b001)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicast)
```

Configuración de la administración de Switch

Configuraciones de respaldo y restauración del switch

Sintaxis del comando de CLI IOS de Cisco	
Versión formal del comando copy de IOS de Cisco. Confirmar el nombre de archivo de destino. Presione la tecla Enter para aceptar y utilice la combinación de teclas Crtl+C para cancelar.	S1#**copy system:running-config flash:startup-config** Destination filename [startup-config]?
Versión informal del comando copy. Se supone que running-config se está ejecutando en el sistema y que el archivo startup-config se almacenará en NVRAM flash. Presione la tecla Enter para aceptar y utilice la combinación de teclas Crtl+C para cancelar.	S1#**copy running-config startup-config** Destination filename [startup-config]?
Hace una copia de respaldo de startup-config en un archivo almacenado en NVRAM flash. Confirmar el nombre de archivo de destino. Presione la tecla Enter para aceptar y utilice la combinación de teclas Crtl+C para cancelar.	S1#**copy startup-config flash:config.bak1** Destination filename [config.bak1]?

Configuración de la administración de Switch

Configuraciones de respaldo y restauración del switch

Sintaxis del comando de CLI IOS de Cisco	
Copia el archivo config.bak1 almacenado en flash a la configuración de inicio supuestamente almacenada en flash. Presione la tecla Enter para aceptar y utilice la combinación de teclas Crtl+C para cancelar.	S1#**copy flash:config.bak1 startup-config** Destination filename [startup-config]?
Permite que IOS de Cisco ejecute el reinicio del switch. Si se ha modificado el archivo de configuración en ejecución se le solicitará que lo guarde. Confirme con 'y' o con 'n'. Para confirmar la recarga presione la tecla Enter para aceptar y utilice la combinación de teclas Crtl+C para cancelar.	S1#**reload** System configuration has been modified. Save? [yes/no]: n Proceed with reload? [confirm]?

Configuración de la administración de Switch

- Respaldo a un servidor TFTP.

```
S1#copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
Writing tokyo-confg!!! [OK]
```

Configuración de la administración de Switch

- Borrado del archivo de configuración.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [con
firm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

Configurar seguridad básica en un switch

Configuración del acceso a la consola

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Cambio del modo de configuración global a modo de configuración de línea para la consola 0.	`S1(config)#line con 0`
Establece cisco como contraseña para la línea de la consola 0 del switch.	`S1(config-line)#password cisco`
Establece la línea de consola para que solicite el ingreso de la contraseña antes de conceder el acceso.	`S1(config-line)#login`
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config-line)#end`

Configurar seguridad básica en un switch

Configurar el acceso de la terminal virtual

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Cambio del modo de configuración global a modo de configuración de línea para las líneas vty de 0 a 4.	`S1(config)#line vty 0 4`
Establezca cisco como contraseña para las líneas vty del switch.	`S1(config-line)#password cisco`
Establezca las líneas vty para que soliciten el ingreso de la contraseña antes de conceder el acceso.	`S1(config-line)#login`
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config-line)#end`

Configurar seguridad básica en un switch

Configuración de las contraseñas para el modo EXEC

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configura la **enable password** para ingresar al modo EXEC privilegiado.	`S1(config)#enable password` *contraseña*
Configura la **enable secret** para ingresar al modo EXEC privilegiado.	`S1(config)#enable secret` *contraseña*
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config)#end`

Configurar seguridad básica en un switch

Configuración de contraseñas encriptadas

```
…
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 no login
line vty 5 15
 password cisco
 no login
!
end
S1#config terminal
S1(config)#service password-encryption
S1(config)#end
S1#Show running-config
…
control-plane
```

Configurar seguridad básica en un switch

Configurar un título de MOTD

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configurar un título de MOTD de inicio de sesión.	`S1(config)#banner motd "Device maintenance will be occurring on Friday!"`

Configurar seguridad básica en un switch

Telnet y SSH

Telnet

-Método de acceso más común

-Envía corrientes de mensaje de texto claras

-No es seguro

SSH

-Debería ser el método de acceso común

-Envía corrientes de mensajes encriptados

-Es seguro

Configurar seguridad básica en un switch

Configuración de Telnet

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

Configurar seguridad básica en un switch

Configuración de SSH

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```