Universidad Juárez Autónoma de Tabasco

"Estudio en la duda, acción en la fe"

11111000011

Teleproceso

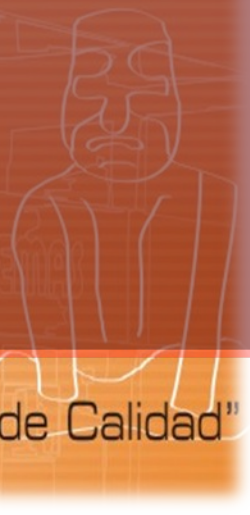
División Académica de Informática y Sistemas

Nombre del Maestro:

LSC. Rafael Mena de la Rosa

Expositores:

- Ofelia Romero Díaz
- David Robles Martínez
- Sergio Mayo Valencia
- Luis Enrique Morales Alonzo



"Por la Universidad de Calidad"

Configuración y Conceptos Básicos del Switch

Elementos Clave de las Redes 802.3/Ethernet

Introducción a las LAN 802.3/Ethernet

En este capítulo aprenderá a:

- Resumir el funcionamiento de Ethernet como se definió para las LAN de 100/1 000 Mbps en el estándar IEEE 802.3.
- Explicar las funciones que permiten que un switch envíe tramas de Ethernet en una LAN.
- Configurar un switch para que funcione en una red diseñada para admitir transmisiones de voz, video y datos.
- Configurar la seguridad básica de un switch que funciona en una red diseñada para admitir transmisiones de voz, video y datos.

Elementos clave de las redes 802.3/Ethernet

- **CSMA/CD**

Las señales de Ethernet se transmiten a todos los hosts que están conectados a la LAN mediante un conjunto de normas especiales que determinan cuál es la estación que puede tener acceso a la red.

- **Detección de portadora**

Método de acceso, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

- **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.

- **Detección de colisiones**

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

- **Señal de congestión y postergación aleatoria**

La señal de congestionamiento avisa a los demás dispositivos acerca de la colisión para que éstos invoquen un algoritmo de postergación.

Un período de postergación aleatorio garantiza que los dispositivos involucrados en la colisión no intenten enviar tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso.

Elementos clave de las redes 802.3/Ethernet

Comunicaciones Ethernet

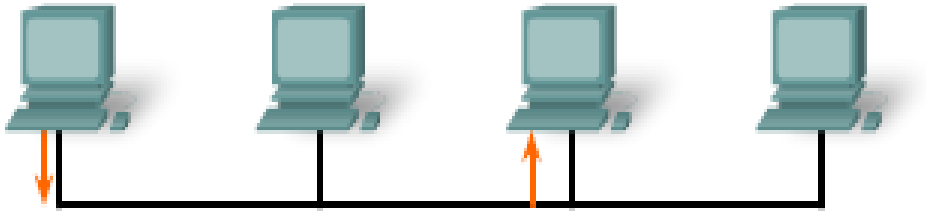
Unicast: Comunicación en la que un host envía una trama a un destino específico.

Broadcast: Comunicación en la que se envía una trama desde una dirección hacia todas las demás direcciones.

Multicast: Comunicación en la que se envía una trama a un grupo específico de dispositivos o clientes.

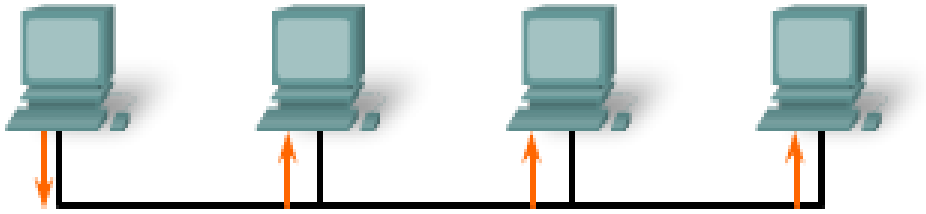
Unicast:

Un emisor y un receptor



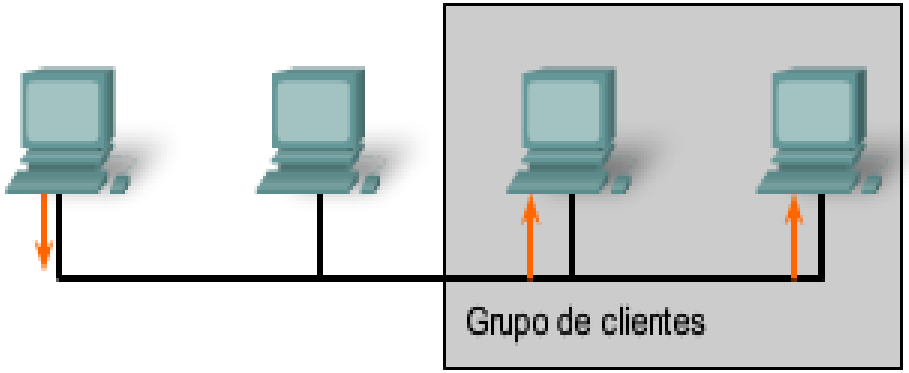
Broadcast:

Un emisor a todas las otras direcciones



Multicast:

Un emisor a un grupo de direcciones



Trama de Ethernet

Se utilizan para la sincronización entre los dispositivos emisores y receptores.

Es el identificador del receptor deseado.

Define la longitud exacta del campo Datos de la trama.

contienen la información encapsulada de una capa superior, que es una PDU de Capa 3 genérica, o, más comúnmente, un paquete de IPv4.

Identifica la NIC o interfaz que origina la trama. Los switches utilizan esta dirección para agregar dicha interfaz a sus tablas de búsqueda.

Detecta errores en una trama. Utiliza una comprobación de redundancia cíclica (CRC).

Elementos clave de las redes 802.3/Ethernet

Dirección MAC

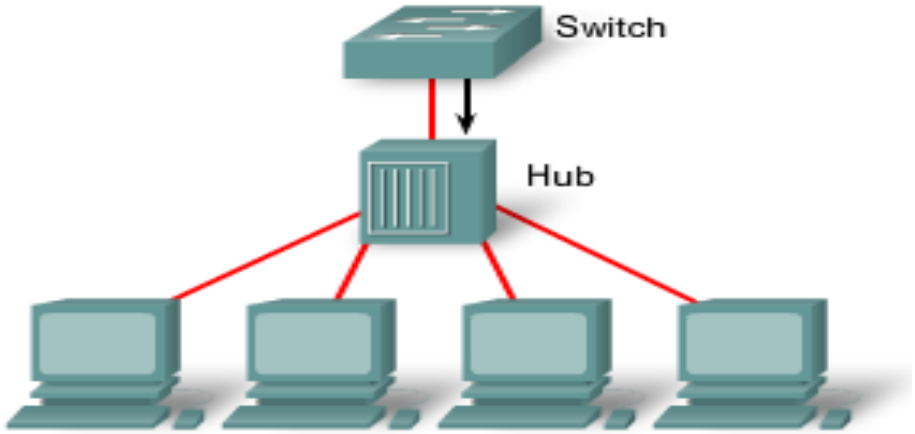
- Los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC.
- La Utiliza para determinar si deben pasarse los mensajes a las capas superiores para su procesamiento.
- Está codificada de manera permanente dentro de un chip ROM en una NIC.
- La dirección MAC se compone:
  - Del identificador exclusivo de organización (OUI)
    - Bit multicast o broadcast.
    - Bit de direcciones administrado de manera local.
  - Del número de asignación del fabricante.

Elementos clave de las redes 802.3/Ethernet

Configuración de Duplex

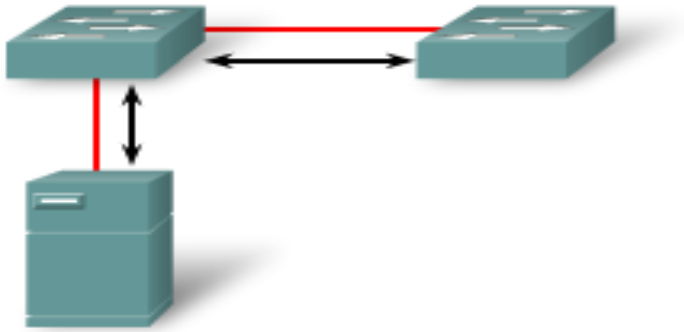
Half Duplex (CSMA/CD)

- 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

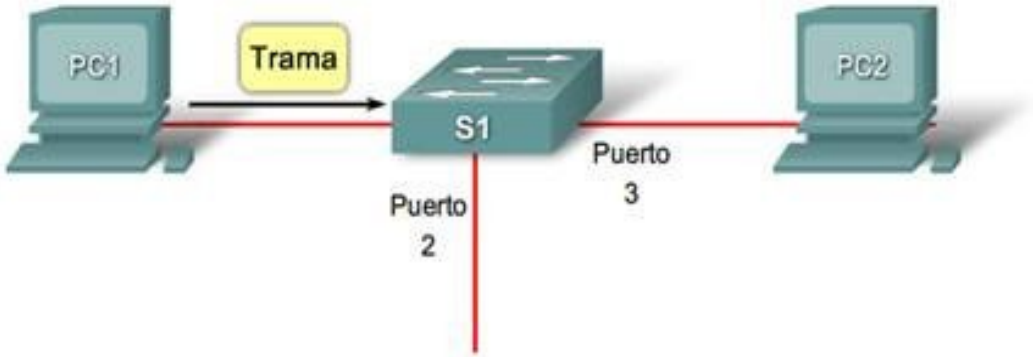
Configuración del puerto de switch

El puerto de un switch debe configurarse con parámetros duplex que coincidan con el tipo de medio.

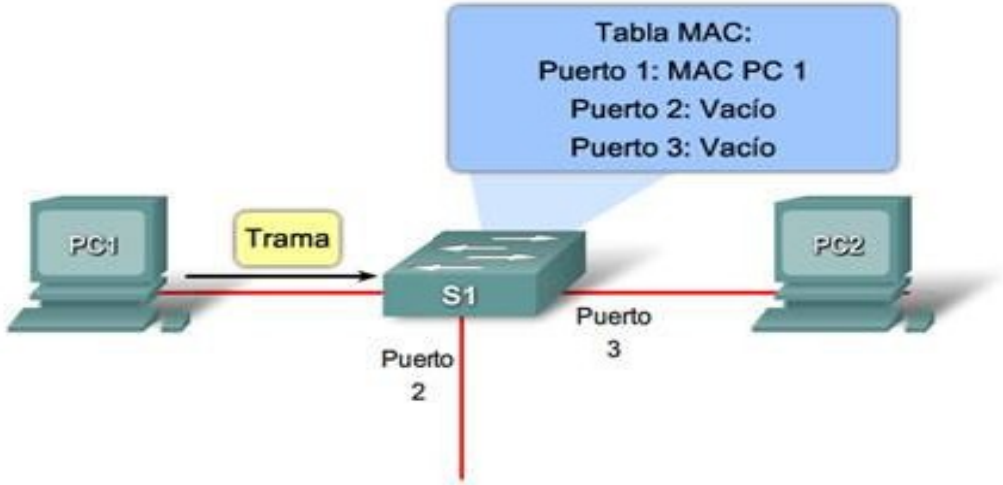
- La opción auto establece el modo autonegociación de duplex. Cuando este modo se encuentra habilitado, los dos puertos se comunican para decidir el mejor modo de funcionamiento.
- La opción full establece el modo full-duplex.
- La opción half establece el modo half-duplex.

Elementos clave de las redes 802.3/Ethernet

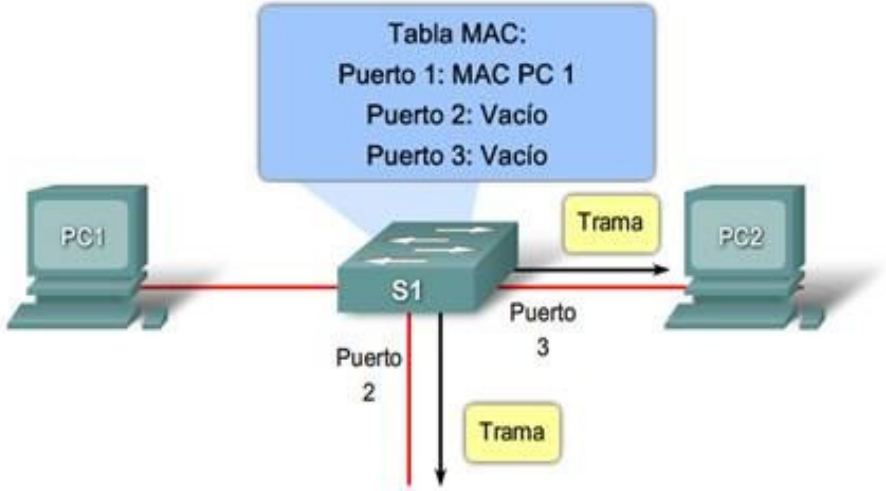
La estructura del switch son los circuitos integrados y la programación de máquina adjunta que permite controlar las rutas de datos a través del switch. El switch debe primero saber qué nodos existen en cada uno de sus puertos para poder definir cuál será el puerto que utilizará para transmitir una trama unicast.



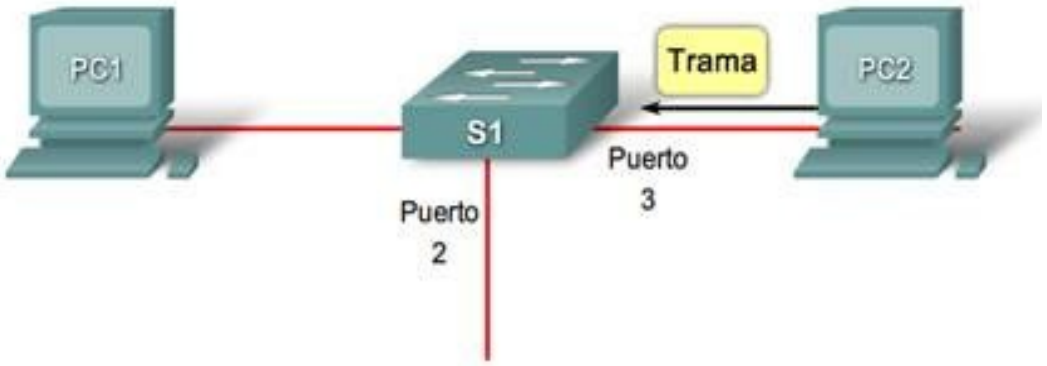
Paso 1: El switch recibe una trama con destino a la PC2 en el puerto 1 de la PC1.



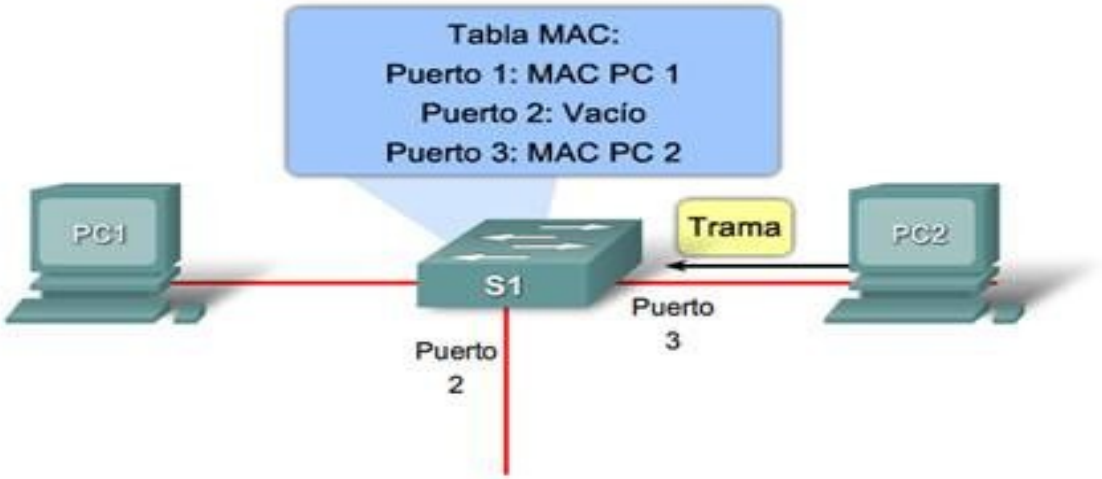
Paso 2: El switch ingresa la dirección MAC de origen y el puerto de switch que recibió la trama en la tabla MAC.



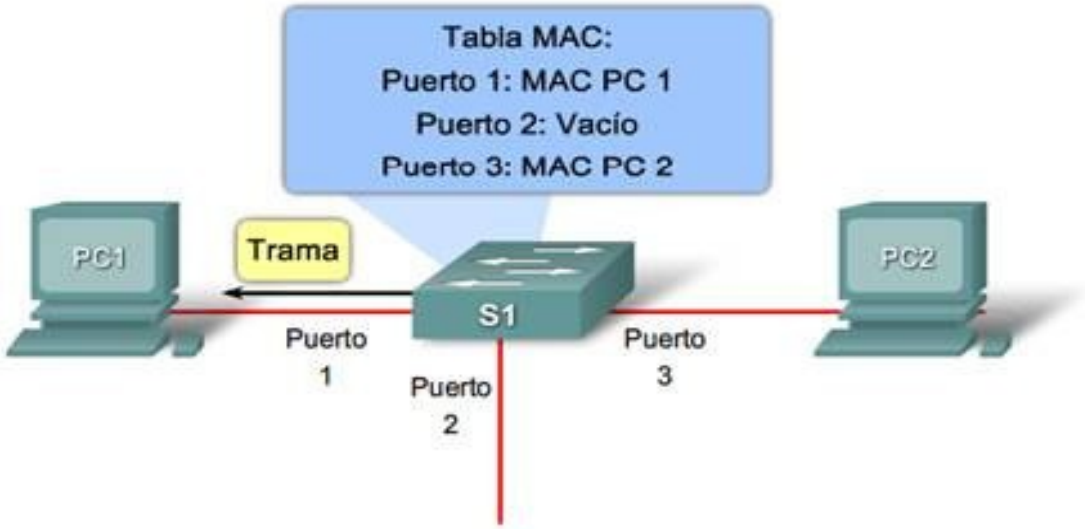
Paso 3: Debido a que la dirección de destino es un broadcast, el switch envía la trama a todos los puertos, excepto al puerto en el cual se recibió la trama.



Paso 4: El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.



Paso 5: El switch ingresa la dirección MAC de origen de la PC 2 y el número de puerto del puerto de switch que recibió la trama en la tabla MAC. En la tabla MAC pueden encontrarse la dirección de destino de la trama y su puerto asociado.



Paso 6: Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin flooding, ya que cuenta con entradas en la tabla MAC que identifican a los puertos asociados.

Elementos clave de las redes 802.3/Ethernet

- **Ancho de banda y rendimiento**

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.

Por ello, es importante comprender que al establecer el ancho de banda de la red Ethernet en 10 Mb/s, el ancho de banda completo para la transmisión estará disponible sólo una vez que se hayan resuelto las colisiones.

- **Dominios de colisión**

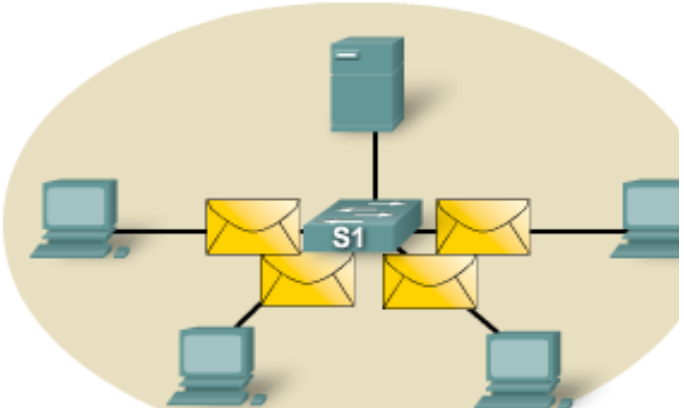
El área de red donde se originan las tramas y se producen las colisiones se denomina dominio de colisiones.

Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red.

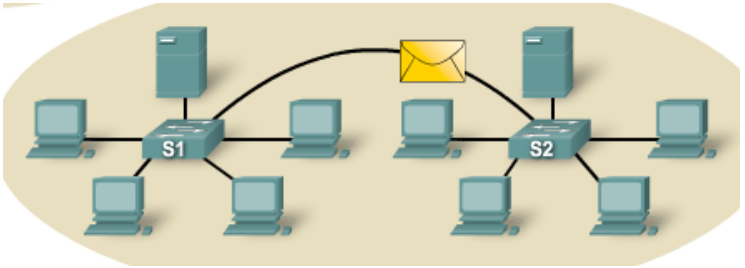
Elementos clave de las redes 802.3/Ethernet

✓ Dominios de broadcast:

- Una serie de switches interconectados forma un dominio de broadcast simple.



El dominio de broadcast de la Capa 2 se conoce como dominio de broadcast MAC. El dominio de broadcast MAC incluye todos los dispositivos de la LAN que reciben broadcasts de tramas a través de un host a todas las demás máquinas en la LAN.



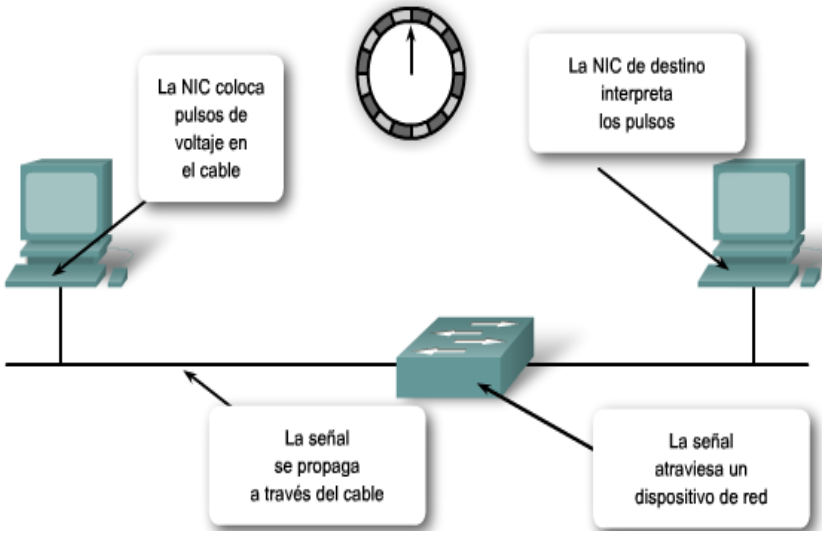
Elementos clave de las redes 802.3/Ethernet

✓ Latencia de red.

- La latencia es el tiempo que una trama o paquete tarda en hacer el recorrido desde la estación origen hasta su destino final.

- Los switches también admiten alta velocidad de transmisión de voz, video y redes de datos mediante circuitos integrados de aplicaciones específicas.

- Otras características de los switches: el búfer de memoria basado en puerto, calidad de servicio (QoS) de nivel de puertos y administración de congestión, también ayudan a reducir la latencia en la red.

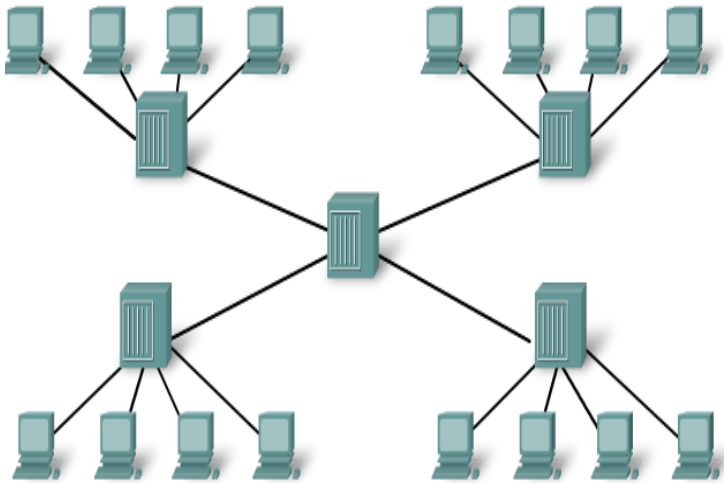


Elementos clave de las redes 802.3/Ethernet

✓ Congestión de red

causas más comunes de congestión de red:

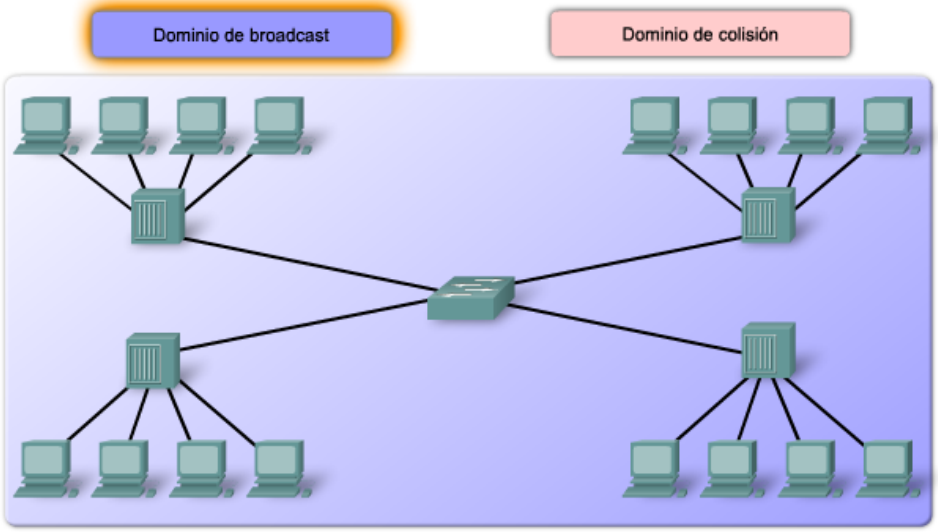
- Tecnología de redes y computadoras cada vez más potentes. una mayor velocidad.
- Volumen de tráfico de la red cada vez mayor.
- Aplicaciones con alta demanda de ancho de banda. Las aplicaciones de software son cada vez más ricas en cuanto a funcionalidad y requieren un ancho de banda superior.

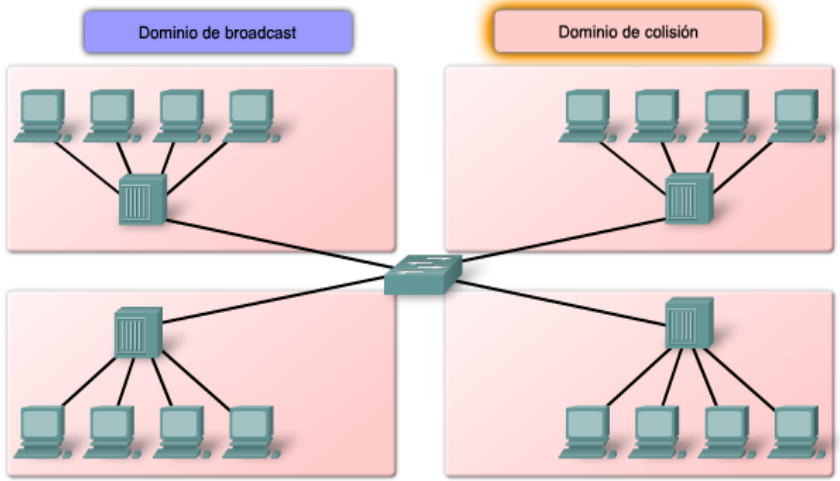


Elementos clave de las redes 802.3/Ethernet

✓ Segmentación LAN

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

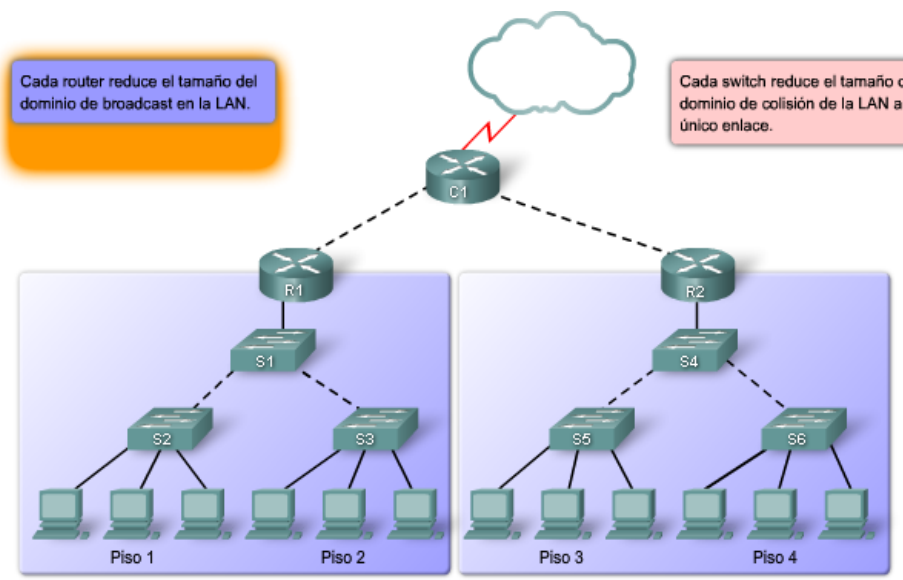


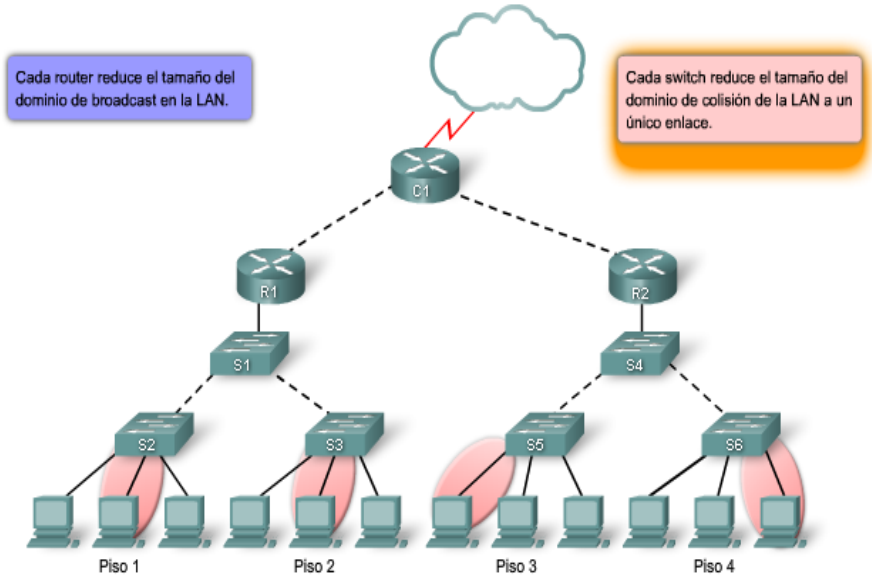


Elementos clave de las redes 802.3/Ethernet

✓Routers

Aunque el switch LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch pertenecen al mismo dominio de broadcast. Los routers pueden utilizarse para crear dominios de broadcast, ya que no reenvían tráfico de broadcast predeterminado.





Elementos clave de las redes 802.3/Ethernet

✓ Control de la latencia de la red

Al diseñar una red para reducir la latencia, se necesita tener en cuenta la latencia originada por cada dispositivo de la red. Los switches pueden provocar latencia cuando se saturan en una red ocupada.

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.

Elementos clave de las redes 802.3/Ethernet

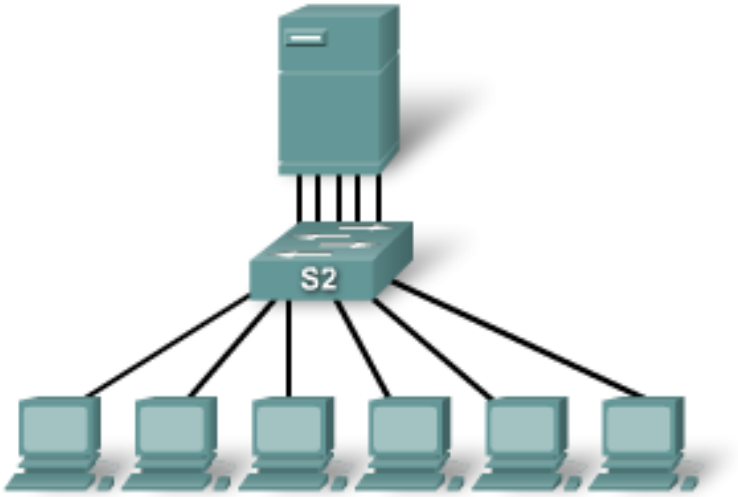
❖ Eliminación de los cuellos de botellas

- Los cuellos de botella son lugares donde la alta congestión de la red provoca un bajo rendimiento

Servidor con una NIC de 1000 Mb/s

Ancho de banda de NIC de 167 Mb/s por computadora

Servidor con cinco NIC de 1000 Mb/s

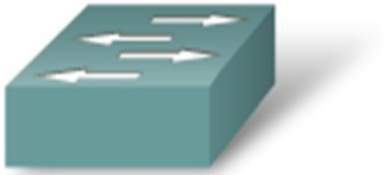


Ancho de banda de NIC de 833 Mb/s por computadora

Reenvió de Tramas Mediante un Switch

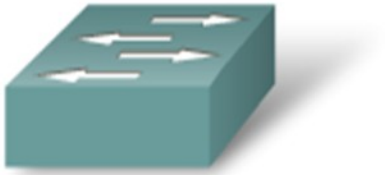
2.2.1-Métodos de Reenvío de Paquetes del Switch

Almacenamiento y envío



Un switch de almacenamiento y envío recibe toda la trama, calcula la CRC y verifica la longitud de la trama. Si la CRC y la longitud de la trama son válidas, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Método de corte



El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.

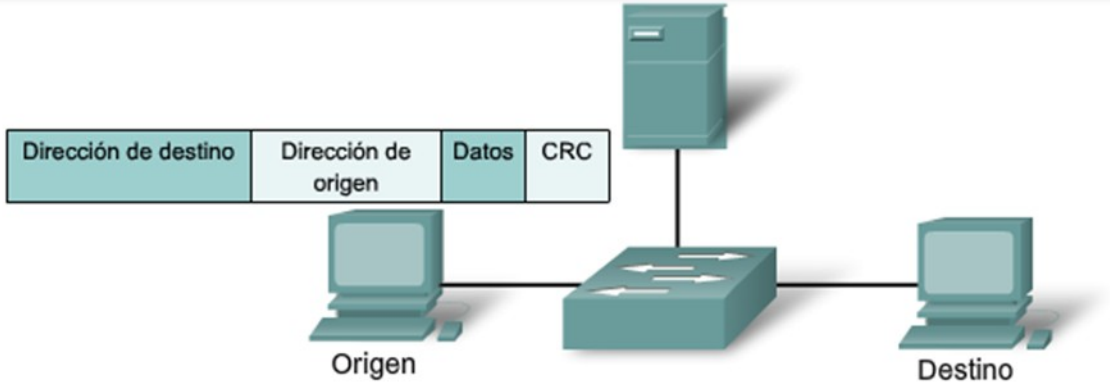
Conmutación de Almacenamiento y Envío

El switch lleva a cabo una verificación de errores utilizando la porción del tráiler de comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check) de la trama de Ethernet.

La CRC utiliza una fórmula matemática, basada en la cantidad de bits de la trama, para determinar si ésta tiene algún error. Después de confirmar la integridad de la trama, ésta se envía desde el puerto correspondiente hasta su destino. Cuando se detecta un error en la trama, el switch la descarta.

La conmutación por almacenamiento y envío se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, en donde se necesita una clasificación de la trama para decidir el orden de prioridad del tráfico. Por ejemplo: los flujos de datos de voz sobre IP deben tener prioridad sobre el tráfico de exploración Web.

Conmutación de Almacenamiento y Envío



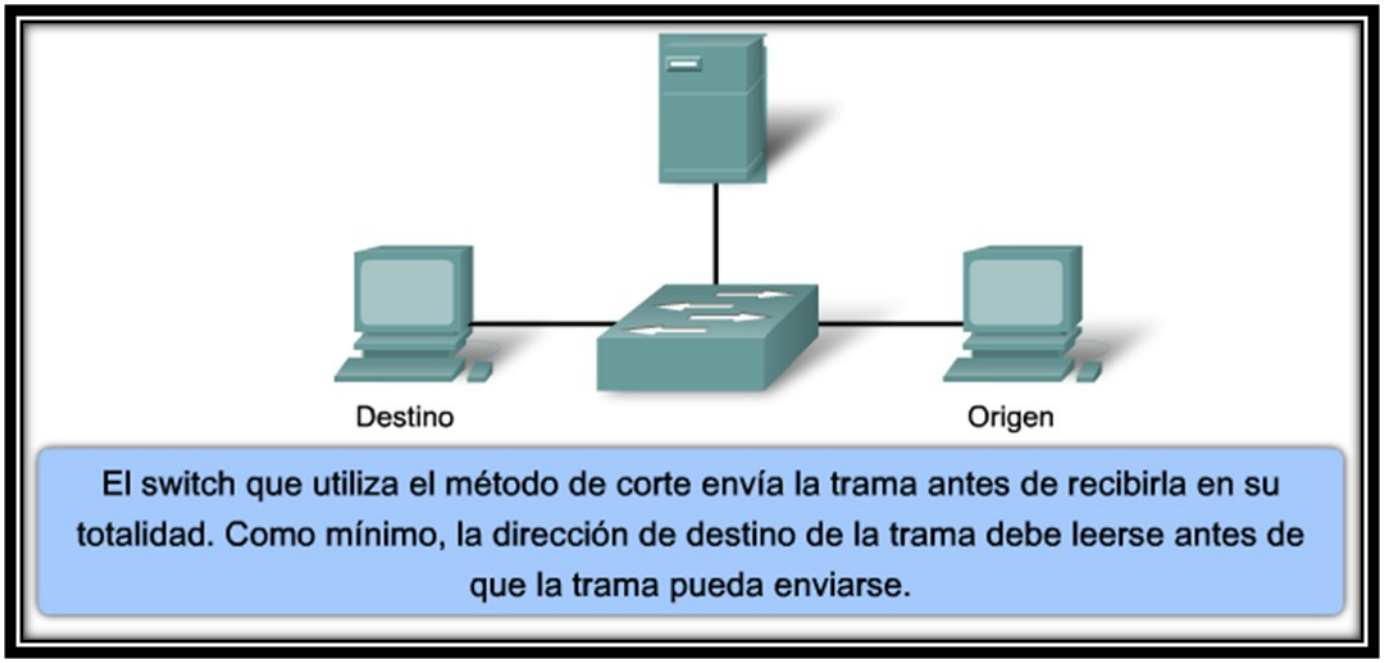
Un switch de almacenamiento y envío recibe toda la trama, calcula la CRC y verifica la longitud de la trama. Si la CRC y la longitud de la trama son válidas, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por Método de Corte

El switch no lleva a cabo ninguna verificación de errores en la trama. Dado que el switch no tiene que esperar que la trama se almacene de manera completa en el búfer y que no realiza ninguna verificación de errores, la conmutación por método de corte es más rápida que la de almacenamiento y envío.

No obstante, al no llevar a cabo ninguna verificación de errores, el switch reenvía tramas dañadas a través de la red. Las tramas dañadas consumen ancho de banda mientras se reenvían. Al final, la NIC de destino descarta las tramas dañadas.

Conmutación por Método de Corte



Conmutación por Método de Corte

El switch no lleva a cabo ninguna verificación de errores en la trama. Dado que el switch no tiene que esperar que la trama se almacene de manera completa en el búfer y que no realiza ninguna verificación de errores, la conmutación por método de corte es más rápida que la de almacenamiento y envío.

No obstante, al no llevar a cabo ninguna verificación de errores, el switch reenvía tramas dañadas a través de la red. Las tramas dañadas consumen ancho de banda mientras se reenvían. Al final, la NIC de destino descarta las tramas dañadas.

Conmutación por Método de Corte

Dos variantes de la conmutación por método de corte:

Conmutación por envío rápido: La conmutación por envío rápido ofrece el más bajo nivel de latencia. La conmutación por envío rápido reenvía el paquete inmediatamente después de leer la dirección de destino. Como la conmutación por envío rápido comienza a reenviar el paquete antes de haberlo recibido en forma completa, es probable que a veces los paquetes se entreguen con errores.

Conmutación Libre de fragmentos: En la conmutación libre de fragmentos, el switch almacena los primeros 64 bytes de la trama antes de reenviarla, ya que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. También puede ser vista como un acuerdo entre la conmutación por almacenamiento y envío, y la conmutación por método de corte.

2.2.2-Conmutación Simétrica y Asimétrica

Asimétrica

Un switch LAN asimétrica proporciona conexiones conmutadas entre puertos con distinto ancho de banda; por ejemplo, una combinación de puertos de 10 Mb/s, 100 Mb/s y 1000 Mb/s.

La conmutación asimétrica permite un mayor ancho de banda dedicado al puerto de conmutación del servidor para evitar que se produzca un cuello de botella. Esto brinda una mejor calidad en el flujo de tráfico, donde varios clientes se comunican con un servidor al mismo tiempo.

Se requieren buffers de memoria en un switch asimétrico. Para que el switch coincida con las distintas velocidades de datos en los distintos puertos, se almacenan tramas enteras en los buffers de memoria y se envían al puerto una después de la otra según se requiera.

Conmutación Simétrica y Asimétrica

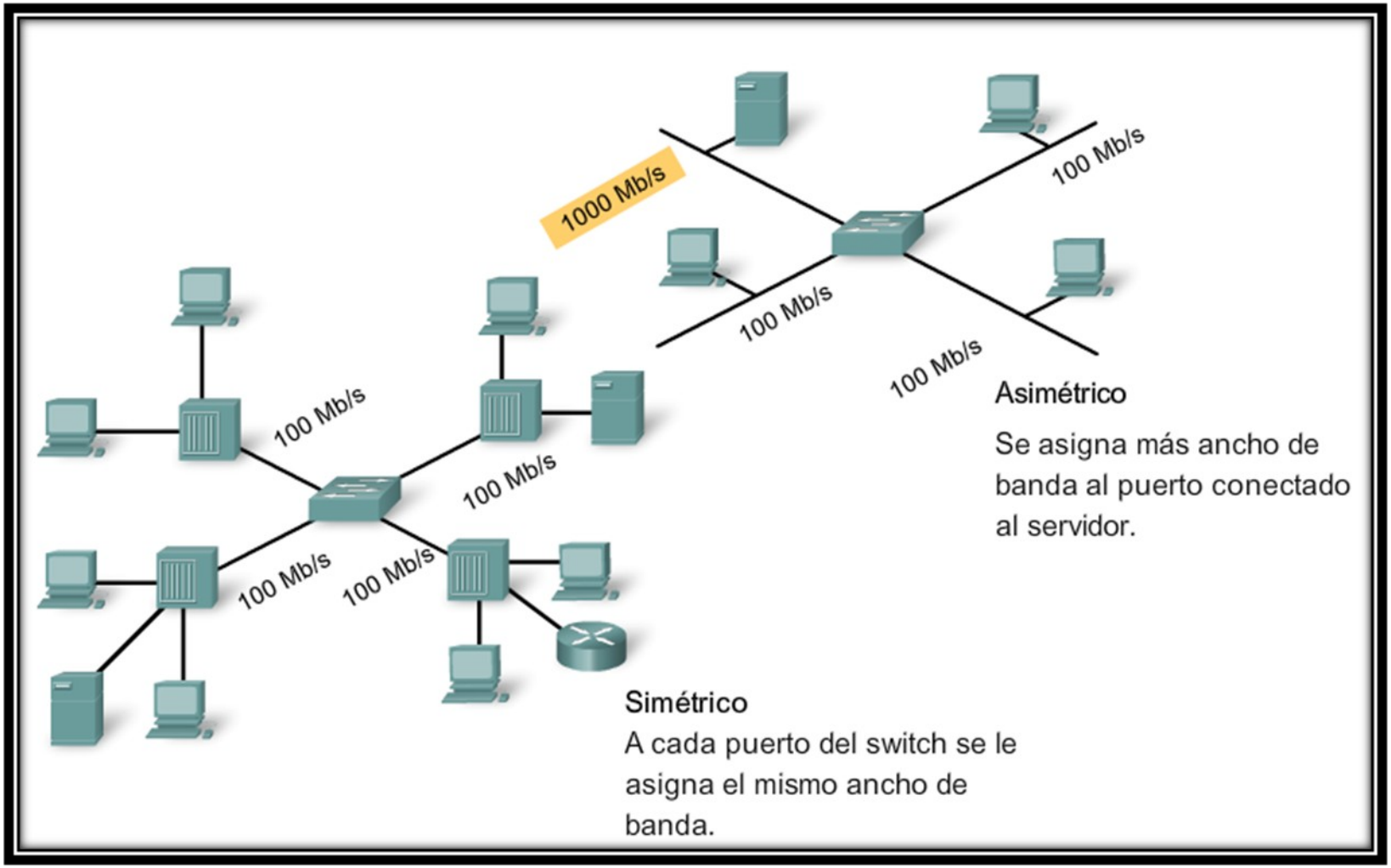
Simétrico

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.

En un switch simétrico, todos los puertos cuentan con el mismo ancho de banda. La conmutación simétrica se ve optimizada por una carga de tráfico distribuida de manera uniforme, como en un entorno de escritorio entre pares.

El administrador de la red debe evaluar la cantidad de ancho de banda que se necesita para las conexiones entre dispositivos a fin de que pueda adaptarse al flujo de datos de las aplicaciones basadas en redes. La mayoría de los switches actuales son asimétricos, ya que son los que ofrecen mayor flexibilidad.

Conmutación Simétrica y Asimétrica



2.2.3-Buffer de Memoria

El empleo de memoria para almacenar datos se denomina almacenamiento en buffers de memoria. El búfer de memoria está integrado al hardware del switch y, además de aumentar la cantidad de memoria disponible, no puede configurarse.

Existen dos tipos de almacenamiento en buffers de memoria:

- Memoria compartida
- Memoria basada en puerto.

Buffer de Memoria

Búfer de Memoria Basada en Puerto

En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada específicos. Una trama se transmite al puerto de salida una vez que todas las tramas que están delante de ella en la cola se hayan transmitido con éxito.

Es posible que una sola trama retarde la transmisión de todas las tramas almacenadas en la memoria debido al tráfico del puerto de destino. Este retardo se produce aunque las demás tramas se puedan transmitir a puertos destino abiertos.

Buffer de Memoria

Búfer de Memoria Compartida

El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch.

El switch conserva un mapa de enlaces de trama a puerto que indica por dónde un paquete debe transmitirse, esta se elimina una vez que la trama se ha transmitido con éxito. La cantidad de tramas almacenadas en el búfer se encuentra limitada por el tamaño del búfer de memoria en su totalidad y no se limita a un solo búfer de puerto. Esto permite la transmisión de tramas más amplias y que se descarte una menor cantidad de ellas. Esto es importante para la conmutación asimétrica, donde las tramas se intercambian entre puertos de distintas velocidades.

Memoria basada en puerto	En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada específicos.
Memoria compartida	El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch.

Pregunta antes de entrar al siguiente tema

2.2.3-Conmutación de Capa 2 y Capa 3

CONMUTACIÓN DE CAPA 2

Un switch LAN de Capa 2 lleva a cabo los procesos de conmutación y filtrado basándose solamente en la dirección MAC de la Capa de enlace de datos (Capa 2) del modelo OSI.

Conmutación de Capa 2

El switch de Capa 2 es completamente transparente para los protocolos de la red y las aplicaciones del usuario. Recuerde que un switch de Capa 2 crea una tabla de direcciones MAC que utiliza para determinar los envíos.

Conmutación de Capa 2 y Capa 3

CONMUTACIÓN DE CAPA 3

Un switch de Capa 3, como el Catalyst 3560, funciona de modo similar a un switch de Capa 2, como el Catalyst 2960, pero en lugar de utilizar sólo la información de las direcciones MAC para determinar los envíos, el switch de Capa 3 puede también emplear la información de la dirección IP.

En lugar de aprender qué direcciones MAC están vinculadas con cada uno de sus puertos, el switch de Capa 3 puede también conocer qué direcciones IP están relacionadas con sus interfaces. Esto permite que el switch de Capa 3 pueda dirigir el tráfico a través de la red en base a la información de las direcciones IP.

Conmutación de Capa 2 y Capa 3

CONMUTACIÓN DE CAPA 3

Los switches de Capa 3 son también capaces de llevar a cabo funciones de enrutamiento de Capa 3, con lo cual se reduce la necesidad de colocar routers dedicados en una LAN.

Dado que los switches de Capa 3 cuentan con un hardware de conmutación especializado, normalmente, pueden enviar datos con la misma rapidez con la que pueden conmutar.

Conmutación de Capa 3

Configuración de la Administración de Switches

Navegacion por los modos de interfaz de lineas de comando

EXEC usuario: Permite que una persona tenga acceso solamente a una cantidad limitada de comandos básicos de monitoreo.

EXEC privilegiado: Permite que una persona tenga acceso a todos los comandos del dispositivo, como aquellos que se utilizan para la configuración y administración

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>`

Alternativas a la CLI basadas en la GUI

Existe una cantidad de alternativas de administración gráfica para administrar un switch de Cisco. El uso de una GUI ofrece facilidad de administración y configuración de switches, y no requiere tener amplio conocimiento sobre la CLI de Cisco.

Asistente de red Cisco

El asistente de red Cisco es una aplicación de la GUI basada en PC para la administración de redes y optimizada para las LAN pequeñas y medianas. Puede configurar y administrar grupos de switches o switches independientes.

Aplicación CiscoView

La aplicación de administración de dispositivos CiscoView proporciona una vista física del switch que se puede utilizar para establecer parámetros de configuración y para ver la información de funcionamiento y el estado del switch.

Administrador de dispositivos Cisco

El administrador de dispositivos Cisco es un software basado en Web que se encuentra almacenado en la memoria del switch. Puede utilizar el Administrador de dispositivos y administrar los switches.

Administración de red SNMP

Se pueden administrar switches desde una estación de administración compatible con SNMP, como HP OpenView. El switch es capaz de proporcionar amplia información de administración y ofrece cuatro grupos de Monitoreo remoto (RMON)

Como utilizar el servicio de ayuda

Ayuda sensible al contexto

Sintaxis del comando de switch de Cisco	

Ejemplo de indicador de comando. En este ejemplo, la función de ayuda proporciona una lista de comandos disponibles en el modo actual que comienzan con cl.	`switch#cl?`
	
	`clear  clock`

Ejemplo de comando incompleto.	`switch#clock`
	
	`% Incomplete command.`

Ejemplo de traducción simbólica.	`switch#colck`
	
	`% Unknown command or computer name, or unable to find computer address`

Ejemplo de indicador de comando. ¿Observa el espacio? En este ejemplo, la función de ayuda proporciona una lista de comandos asociados con el comando clock.	`switch#clock ?`
	
	`set  Establece la hora y fecha`

En este ejemplo, la función de ayuda proporciona una lista de argumentos de comandos para el comando clock set.	`switch#clock set ?`
	
	`hh:mm:ss  Hora actual`

Conmutación de Capa 2 y Capa 3

Mensajes de error de consola

Los mensajes de error de la consola ayudan a identificar problemas cuando se ha ingresado un comando incorrecto. La figura proporciona ejemplos de mensajes de error, qué significan y cómo obtener ayuda cuando éstos se muestran.

Ejemplo de mensaje de error	Significado	Cómo obtener ayuda
`switch#cl` `% Ambiguous command: "cl"`	No ingresó la cantidad suficiente de caracteres para que el dispositivo reconozca al comando.	Vuelva a ingresar el comando seguido de un signo de interrogación (?), sin espacio entre el comando y dicho signo. Se muestran las posibles palabras clave que puede ingresar con el comando.
`switch#clock` `% Incomplete command.`	No ingresó todas las palabras clave o valores requeridos por este comando.	Vuelva a ingresar el comando seguido de un signo de interrogación (?), con un espacio entre el comando y dicho signo.

`switch#clock set aa:12:23`
`^`
`% Invalid input detected at '^' marker.`
	Ingresó el comando de manera incorrecta. El símbolo del acento circunflejo (^) marca el lugar del error.	Ingrese un signo de interrogación (?) para mostrar todos los comandos o parámetros disponibles.

Acceso al historial de comandos

Búfer de historial de comandos

Al configurar varias interfaces en un switch, se puede ahorrar tiempo y evitar escribir los comandos nuevamente mediante el búfer del historial de comandos del IOS de Cisco

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.

Búfer del historial de comandos

```
switch#show history
  enable
  show history
  enable
  config
  t
  confi
  t
  show history
switch#
```

Utilice el comando **show history** para ver los comandos EXEC ingresados recientemente.

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**

Secuencia de arranque y de switch

El switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa que se encuentra almacenado en la NVRAM y que se ejecuta cuando el switch se enciende por primera vez.

El cargador de arranque:

Lleva a cabo la inicialización de bajo nivel de la CPU. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.

Realiza el auto diagnóstico al encender (POST) para el subsistema de la CPU. Comprueba la DRAM de la CPU y la parte del dispositivo flash que integra el sistema de archivos flash.

Inicializa el sistema de archivos flash en la tarjeta del sistema.

Carga una imagen predeterminada del software del sistema operativo en la memoria y hace arrancar al switch.

Prepacion para la consola de switch

El inicio de un switch Catalyst requiere la ejecución de los siguientes pasos:

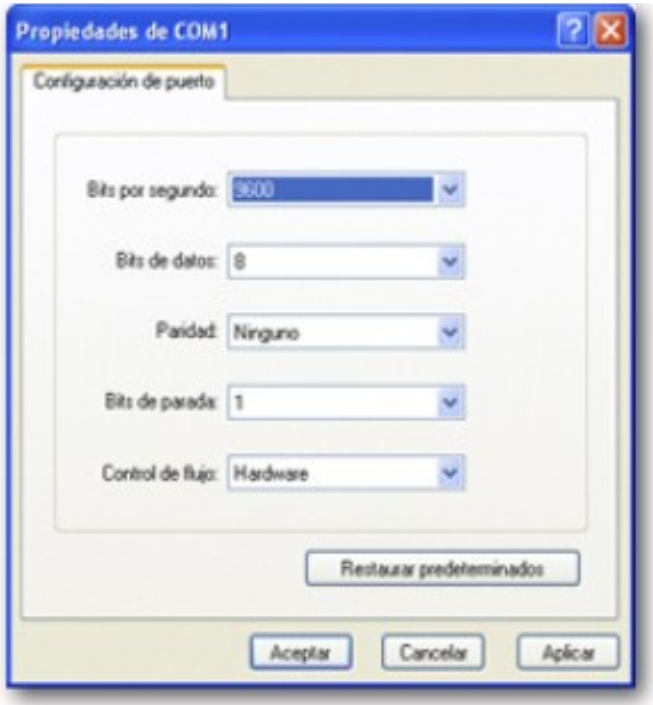
Paso 1. Antes de poner en funcionamiento el switch, verifique que:

Todos los cables de red estén correctamente conectados.

La PC o el terminal estén conectados al puerto de consola.

La aplicación del emulador de terminal, como HyperTerminal, esté funcionando y esté correctamente configurada.

La figura muestra una PC conectada a un switch mediante el puerto de consola.



Configurar Hyperterminal

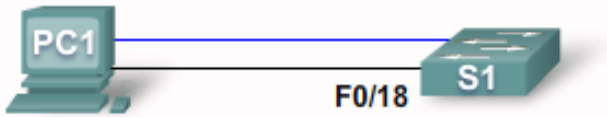
Consideracion basica del Switch

Consideraciones de la interfaz de administración

Un switch de capa de acceso se parece mucho a una PC en que se necesita configurar una dirección IP, una máscara de subred y una Gateway predeterminada. Para manejar un switch en forma remota mediante TCP/IP, se necesita asignar al switch una dirección IP.

La configuración predeterminada del switch es que su administración sea controlada a través de la VLAN 1. Sin embargo, la configuración básica recomendada para el switch es que la administración esté controlada por una VLAN que no sea la VLAN 1

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

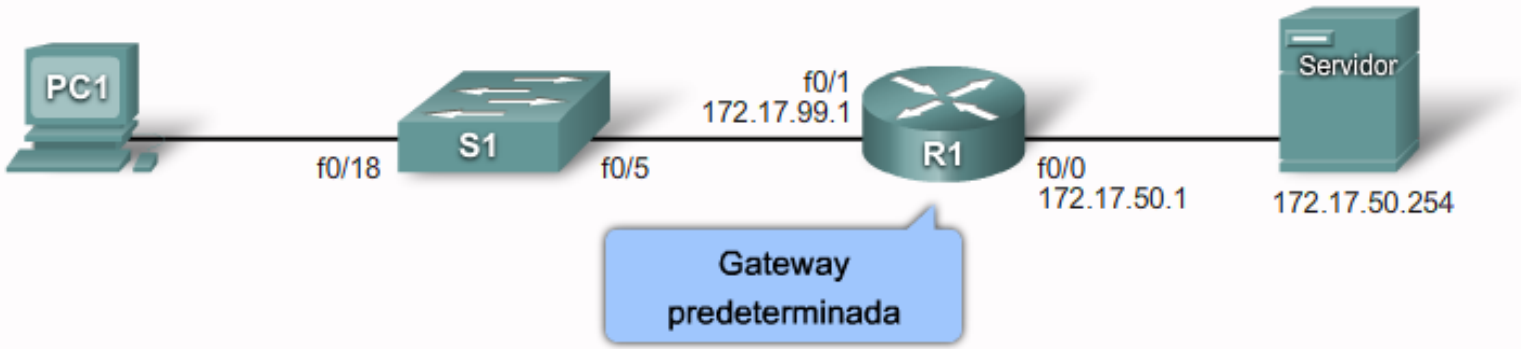
Consideraciones de interfaz de administración

Configurar la conectividad IP

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**

Configurar interfaz de administración

Configurar la conectividad IP



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`

Configurar Gateway predeterminada

Configurar la conectividad IP

```
S1#show running-config
…
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
…
!
```

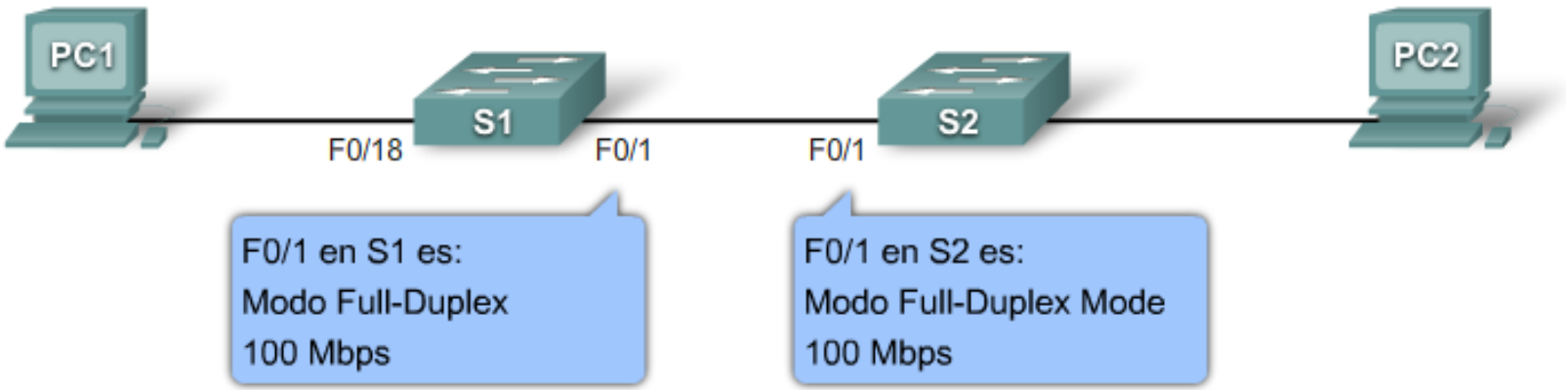
VLAN 99 configurada en el puerto F0/18

```
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
```

Estado de VLAN 99 y del puerto F0/18

Verificar configuración

Configurar Duplex y Velocidad



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`

Configurar una interfaz de web

Los switches modernos de Cisco cuentan con una serie de herramientas de configuración basadas en Web que requieren que el switch se configure como servidor HTTP.

Para controlar las personas que obtienen acceso a los servicios HTTP del switch, puede configurarse de manera opcional la autenticación. Los métodos de autenticación pueden ser complejos. Es probable que sean tantas las personas que utilizan los servicios HTTP que se requeriría un servidor independiente utilizado específicamente para administrar la autenticación de los usuarios.

Los switches utilizan tablas de direcciones MAC para determinar cómo enviar tráfico de puerto a puerto.

Las direcciones dinámicas son las direcciones MAC de origen que el switch registra y que luego expiran cuando no están en uso. Es posible cambiar el valor del tiempo de expiración de las direcciones MAC.

El switch proporciona direccionamiento dinámico al registrar la dirección MAC de origen de cada trama que recibe en cada puerto y al agregar luego la dirección MAC de origen y el número de puerto relacionado con ella a la tabla de direcciones MAC. A

Verificacion de la configuracion del 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 [interface-id]`
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`

Comandos show

show running-config

show interfaces

Administracion basica del Switch

Respaldar y restaurar el 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. Presionar la tecla Enter para aceptar y usar 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. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy running-config startup-config** Destination filename [startup-config]?
Hacer una copia de respaldo de startup-config en un archivo almacenado en NVRAM flash. Confirmar el nombre de archivo de destino. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy startup-config flash:config.bak1** Destination filename [config.bak1]?

Respaldar configuraciones

Respaldar y restaurar el 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. Presionar la tecla Enter para aceptar y usar 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 presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**reload** Se ha modificado la configuracin del sistema. Save? [yes/no]: n Proceed with reload? [confirm]?

Restaurar configuraciones

Configuración de la Seguridad del Switch

Configuracion de opciones de las contraseñas

La seguridad de los switches comienza con la protección de ellos contra el acceso no autorizado. Se pueden realizar todas las opciones de configuración desde la consola. Para acceder a la consola, se necesita tener acceso físico local al dispositivo. Si no se asegura la consola de forma adecuada, usuarios malintencionados podrían comprometer la configuración del 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`

Eliminación de la contraseña de consola

Si necesita eliminar la contraseña y la solicitud de ingreso de contraseña al iniciar sesión, siga los pasos a continuación:

Paso 1.Cambie de modo EXEC privilegiado a modo de configuración global. Ingrese el comando configure terminal.

Paso 2. Cambie del modo de configuración global al modo de configuración de línea para la consola 0. La indicación del comando (config-line)# señala que se encuentra en el modo de configuración de línea. Ingrese el comando line console 0.

Paso 3. Elimine la contraseña de la línea de la consola mediante el comando no password.

Precaución: Si no se ha establecido ninguna contraseña y el inicio de sesión aún se encuentra habilitado, no se podrá tener acceso a la consola.

Paso 4. Elimine la solicitud de ingreso de contraseña al iniciar sesión en la consola mediante el comando no login.

Paso 5. Salga del modo de configuración de línea y regrese al modo EXEC privilegiado mediante el comando end.

Configurar contraseñas del modo EXEC

El modo EXEC privilegiado permite que cualquier usuario habilite este modo en un switch Cisco para configurar cualquier opción disponible en el switch. También puede ver todos los parámetros de la configuración en curso del switch e incluso algunas de las contraseñas encriptadas. Por este motivo, es importante resguardar el acceso al modo EXEC privilegiado.

El comando de configuración global enable password permite especificar una contraseña para restringir el acceso al modo EXEC privilegiado.

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 **contraseña de habilitación** para ingresar al modo EXEC privilegiado.	S1(config)#**enable password** *password*
Configura la **contraseña de habilitación** secreta para ingresar al modo EXEC privilegiado.	S1(config)#**enable secret** *password*
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	S1(config)#**end**

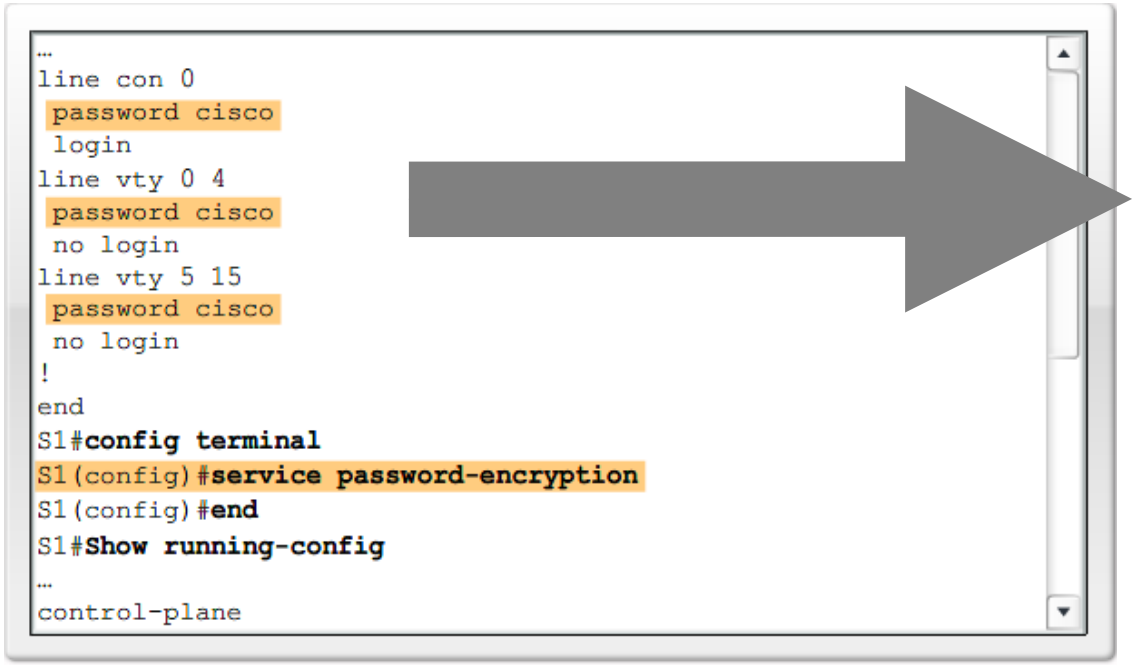
Eliminación de la contraseña del modo EXEC

Si desea eliminar la solicitud de contraseña para obtener acceso al modo EXEC privilegiado, puede utilizar los comandos no enable password y no enable secret desde el modo de configuración global.

Configuración de contraseñas encriptadas

El comando del IOS de Cisco service password-encryption habilita la encriptación de la contraseña de servicio.

Si desea eliminar el requisito de almacenar todas las contraseñas del sistema en formato encriptado, ingrese el comando no service password-encryption desde el modo de configuración global.



Las contraseñas en texto sin cifrar están resaltadas en color naranja

Para recuperar la contraseña de un switch Cisco 2960, lleve a cabo los siguientes pasos:

Paso 1. Conecte un terminal o PC, con el software de emulación de terminal, al puerto de consola del switch.
Paso 2. Establezca la velocidad de línea del software de emulación en 9600 baudios.
Paso 3. Apague el switch. Vuelva a conectar el cable de alimentación al switch y, en no más de 15 segundos, presione el botón Mode mientras la luz verde del LED del sistema esté parpadeando. Siga presionando el botón Mode hasta que el LED del sistema cambie al color ámbar durante unos segundos y luego verde en forma permanente. Suelte el botón Mode.
Paso 4. Inicialice el sistema de archivos Flash a través del comando flash_init.
Paso 5. Cargue archivos helper mediante el comando load_helper.
Paso 6. Visualice el contenido de la memoria Flash a través del comando dir flash:

Para recuperar la contraseña de un switch Cisco 2960, lleve a cabo los siguientes pasos:

Se mostrará el sistema de archivos del switch:
Directory of flash:/
13 drwx 192 Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX
11-rwx 5825 Mar 01 1993 22:31:59 config.text
18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat
16128000 bytes total (10003456 bytes free)

Paso 7. Cambie el nombre del archivo de configuración por config.text.old, que contiene la definición de la contraseña, mediante el comando rename flash:config.text flash:config.text.old.

Paso 8. Reinicie el sistema con el comando boot.

Paso 9. Se solicitará que ejecute el programa de configuración inicial. Ingrese N ante la solicitud y, luego, cuando el sistema pregunte si desea continuar con el diálogo de configuración, ingrese N.

Paso 10. Ante la indicación de switch, ingrese al modo EXEC privilegiado por medio del comando enable.

Paso 11. Cambie el nombre del archivo de configuración y vuelva a colocarle el nombre original mediante el comando rename flash:config.text.old flash:config.text.
Paso 12. Copie el archivo de configuración en la memoria a través del comando copy flash:config.text system:running-config. Después de ingresar este comando, se mostrará el siguiente texto en la consola:
Source filename [config.text]?
Destination filename [running-config]?
Presione Return en respuesta a las solicitudes de confirmación. El archivo de configuración se ha cargado nuevamente y, ahora, se puede cambiar la contraseña.
Paso 13. Ingrese al modo de configuración global mediante el comando configure terminal.
Paso 14. Cambie la contraseña mediante el comando enable secret password.
Paso 15. Regrese al modo EXEC privilegiado mediante el comando exit.
Paso 16. Escriba la configuración en ejecución en el archivo de configuración de inicio mediante el comando copy running-config startup-config.
Paso 17. Vuelva a cargar el switch mediante el comando reload.

Mensaje de inicio de sesion

El conjunto del comando IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes se llaman mensajes de inicio de sesión y mensajes del día (MOTD).

Configuración de un mensaje de inicio de sesión

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configurar un mensaje de inicio de sesión.	`S1(config)#banner login "¡Personal autorizado únicamente!"`

Configuración de un mensaje MOTD

El mensaje MOTD se muestra en todos los terminales conectados en el inicio de sesión y es útil para enviar mensajes que afectan a todos los usuarios de la red (como desconexiones inminentes del sistema). Si se configura, el mensaje MOTD se muestra antes que el mensaje de inicio de sesión.

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configurar un mensaje de MOTD de inicio de sesión.	`S1(config)#banner motd "¡El mantenimiento del dispositivo se realizará el viernes!"`

Configuracion Telnet y SSH

Telnet es el protocolo predeterminado que admite vty en un switch de Cisco. Cuando se asigna una dirección IP de administración al switch de Cisco, puede conectarlo utilizando el cliente Telnet. Inicialmente, las líneas vty son inseguras al permitir el acceso a cualquier usuario que intenta conectarse a ellas.

SSH es una característica criptográfica de seguridad que está sujeta a exportar restricciones. Para utilizar esta característica se debe instalar una imagen criptográfica en su switch.

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

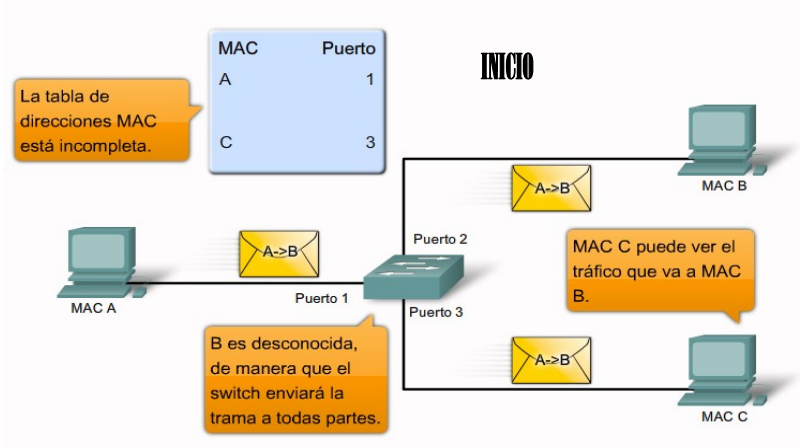
Configuración de TELNET

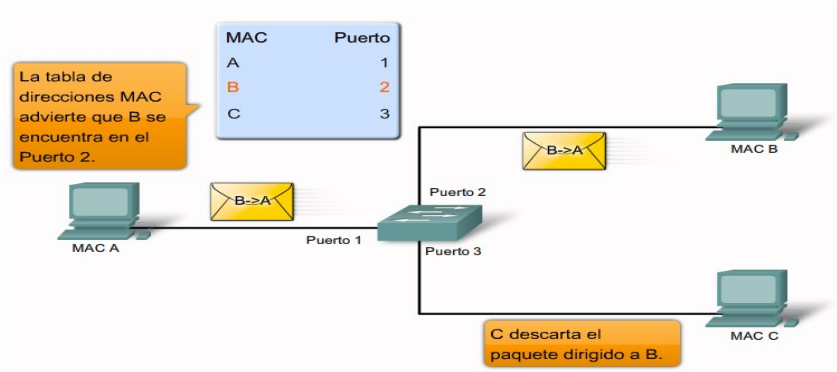
```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

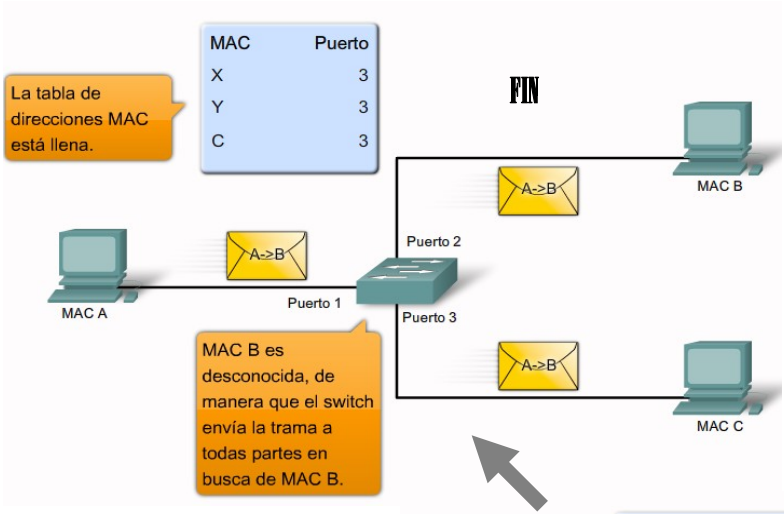
Configuración de SSH

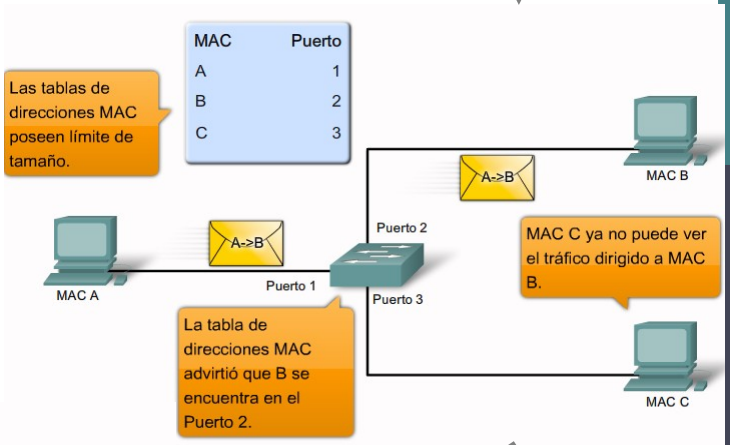
```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

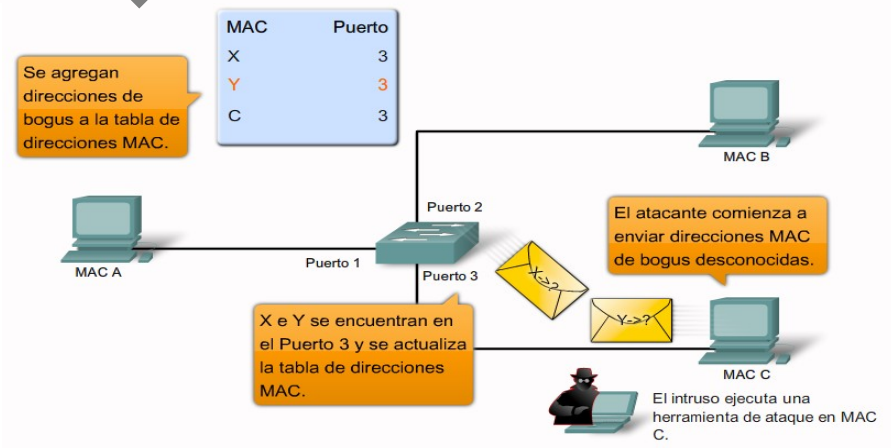
Ataques de seguridad comunes
Saturación de la dirección MAC





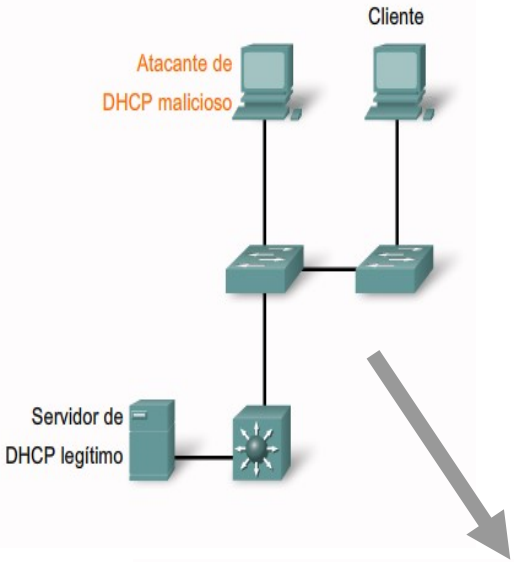




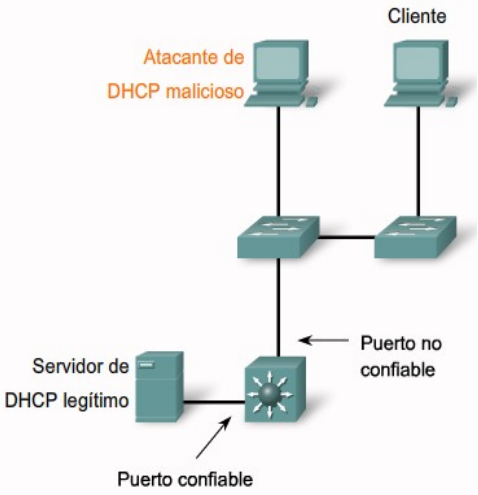


Ataques de suplantación de identidad

1) Un atacante activa un servidor de DHCP en un segmento de red.
2) El cliente envía un broadcast de solicitud de información de configuración de DHCP.
3) El servidor de DHCP malicioso responde antes de que lo haga el servidor de DHCP legítimo y asigna información de configuración de IP definida por el atacante.
4) Los paquetes de host son redirigidos a la dirección del atacante, ya que el mismo emula un gateway predeterminado para la dirección de DHCP errónea provista al cliente.



- El snooping de DHCP permite saber si la configuración de los puertos es confiable o no.
  - Los puertos confiables pueden enviar solicitudes de DHCP y acuses de recibo.
  - Los puertos no confiables sólo pueden enviar solicitudes de DHCP.
- El snooping de DHCP permite que el switch construya una tabla enlazada que asigna una dirección MAC de cliente, dirección IP, VLAN e ID de puerto.
- Utilice el comando **`ip dhcp snooping`** .



Estos pasos ilustran la forma en que se configura el snooping de DHCP en un switch de Cisco:

Paso 1. Habilitar el snooping de DHCP mediante el comando de configuración global ip dhcp snooping.

Paso 2. Habilitar el snooping de DHCP para VLAN específicas mediante el comando ip dhcp snooping vlan number [número].

Paso 3. Definir los puertos como confiables o no confiables a nivel de interfaz identificando los puertos confiables mediante el comando ip dhcp snooping trust.

Paso 4. (Opcional) Limitar la tasa a la que un atacante puede enviar solicitudes de DHCP bogus de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando ip dhcp snooping limit rate rate.

Ataques en CDP

El Protocolo de descubrimiento de Cisco (CDP) es un protocolo de propiedad de Cisco que puede configurarse en todos los dispositivos de Cisco. CDP descubre otros dispositivos de Cisco conectados directamente, lo que permite que configuren sus conexiones en forma automática, simplificando la configuración y la conectividad. Los mensajes de CDP no están encriptados.

CDP contiene información sobre el dispositivo, como la dirección IP, la versión del software, la plataforma, las capacidades y la VLAN nativa. Cuando esta información está disponible para el atacante, puede utilizarla para encontrar vulnerabilidades para atacar la red, en general en la forma de ataque de Denegación de servicio (DoS).

Ataques de Telnet

Tipos de ataques de Telnet:
-Ataques de contraseña de fuerza bruta
-Ataques DoS

Protección contra un ataque de contraseña de fuerza bruta:
-cambie su contraseña con frecuencia
-utilice contraseñas fuertes
-limite la cantidad de usuarios que pueden comunicarse con las líneas vty

Protección contra un ataque DoS:
-Actualice a la versión más reciente del software IOS de Cisco

Herramientas de Seguridad

Las Herramientas de seguridad de red realizan las siguientes funciones:

-Las auditorías de seguridad de red ayudan a
- Revelar qué tipo de información puede recopilar un atacante mediante un simple monitoreo del tráfico de la red.
- Determinar la cantidad ideal de direcciones MAC falsas que deben eliminarse.
- Determinar el período de expiración de la tabla de direcciones MAC.

-Las pruebas de penetración de red ayudan a
- Identificar debilidades dentro de la configuración de los dispositivos de red.
- Iniciar varios ataques para probar la red.
- Precaución: Planifique pruebas de penetración para evitar el impacto en el rendimiento de la red.

Entre las características comunes de una herramienta de seguridad moderna se incluyen:

-Identificación de servicio
-Soporte de servicios SSL
-Pruebas destructivas y no destructivas
-Base de datos de vulnerabilidades

Se pueden utilizar las herramientas de seguridad de red para:

-Capturar mensajes de chat
-Capturar archivos de tráfico NFS
-Capturar solicitudes de HTTP en Formato de registro común
-Capturar mensajes de correo en formato Berkeley mbox
-Capturar contraseñas
-Mostrar URL capturadas en Netscape en tiempo real
-Saturar una LAN conmutada con direcciones MAC aleatorias
-Falsificar las respuestas a direcciones DNS y consultas puntuales
-Interceptar paquetes en una LAN conmutada

Seguridad del puerto

Se implementa seguridad en todos los puertos de switch para:

- Especificar un grupo de direcciones MAC válidas permitidas en el puerto
- Permitir que sólo una dirección MAC acceda al puerto
- Especificar que el puerto se desactiva de manera automática si se detectan direcciones MAC no autorizadas.

Tipos de direcciones MAC seguras

Los siguientes son los tipos de direcciones MAC seguras:

- Direcciones MAC seguras estáticas
- Direcciones MAC seguras dinámicas
- Direcciones MAC seguras sin modificación

Las direcciones MAC seguras sin modificación poseen las siguientes características:

- Se aprenden de manera dinámica y se convierten a direcciones MAC sin modificación almacenadas en la configuración de ejecución.
- Si se deshabilitan las direcciones MAC sin modificación, las mismas se eliminan de la tabla MAC, pero no de la configuración en ejecución.
- Las direcciones MAC seguras sin modificación se pierden cuando el switch se reinicia.
- Si se guardan las direcciones MAC seguras sin modificación en el archivo de configuración de inicio se pueden preservar para el momento de arranque del switch.
- Si se deshabilita el aprendizaje sin modificación, las direcciones MAC sin modificación se convierten en direcciones seguras dinámicas y se eliminan de la configuración en ejecución.

Modos de violación de seguridad

Las violaciones a la seguridad se producen en estas situaciones:

- Una estación cuya dirección MAC no se encuentra en la tabla de direcciones intenta acceder a la interfaz cuando la tabla está llena.
- Se está utilizando una dirección en dos interfaces seguras de la misma LAN.

Entre los modos de violación de seguridad se incluyen: protección, restricción y desactivación.

Modo de violación	Envía tráfico	Envía un mensaje de Syslog	Muestra un mensaje de error	Aumenta el contador de violaciones	Cierra el puerto
Restricción	No	No	No	No	No
Protección	No	Sí	No	Sí	No
Desactivación	No	Sí	No	Sí	Sí

Opciones predeterminadas de seguridad de puerto

Característica	Configuración predeterminada
Seguridad de puerto	Desactivada en un puerto.
Número máximo de direcciones MAC seguras	1
Modo de violación	Shutdown. El puerto se desactiva cuando se supera el número máximo de direcciones MAC seguras y se envía una notificación SNMP trap.
Aprendizaje de direcciones sin modificación	Desactivado.

Configuración de la seguridad del puerto dinámica

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar al modo de configuración global. Use este comando del IOS de Cisco:	S1#**configure terminal**
Especificar el tipo y número de interfaz física a configurar, por ejemplo fastEthernet F0/18, e ingresar al modo de configuración de interfaz. Use este comando del IOS de Cisco:	S1(config)#**interface fastEthernet 0/18**
Establecer el modo de interfaz como acceso. Una interfaz en el modo predeterminado deseado dinámico no se puede configurar como un puerto seguro. Use este comando del IOS de Cisco:	S1(config-if)#**switchport mode access**
Establecer la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security**
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	S1(config-if)#**end**

Configuracion de la seguridad del puerto sin modificacion

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global. Use este comando del IOS de Cisco:	S1#**configure terminal**
Especificar el tipo y número de interfaz física a configurar. Use este comando del IOS de Cisco:	S1(config)#**interface fastEthernet 0/18**
Establecer el modo de interfaz como acceso. Use este comando del IOS de Cisco:	S1(config-if)#**switchport mode access**
Activar la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security**
Establecer el número máximo de direcciones seguras en 50. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security maximum 50**
Activar el aprendizaje sin modificaciones. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security mac-address sticky**
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	S1**(config-if)#end**

Configuracion de la seguridad del puerto

Verificar la configuración de seguridad de puerto

Para mostrar la configuración de seguridad de puerto para el switch o para la interfaz especificada, utilice el comando show port-security [interfaceinterface-id].

```
switch#show port-security interface fastEthernet 0/18
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Verificar las direcciones MAC seguras

Para mostrar todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz especificada, con la información de expiración para cada una, utilice el comando show port-security [interfaceinterface-id].

```
switch#show port-security address
        Secure Mac Address Table
------------------------------------------------------------------------
Vlan   Mac Address       Type                Ports     Remaining Age (mins)
99     0050.BAA6.06CE    SecureConfigured    Fa0/18    -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Seguridad de los puertos no utilizados

Deshabilitar puertos en desuso

Un método simple utilizado por muchos administradores para proteger la red del acceso no autorizado es deshabilitar todos los puertos no utilizados de un switch de la red.

Es simple deshabilitar varios puertos en un switch. Explore todos los puertos no utilizados y emita el comando IOS de Cisco shutdown. Una forma alternativa de desactivar varios puertos es mediante el comando interface range. Si un puerto debe ser activado, se puede ingresar el comando no shutdown en forma manual para esa interfaz.

El proceso de habilitar y deshabilitar puertos puede convertirse en una tarea tediosa, pero el valor obtenido en términos de aumento de la seguridad de la red hace que el esfuerzo no sea en vano.

```
…
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
…
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
…
```

BIBLIOGRAFÍA

- **CISCO NETWORKING ACADEMY**
  CCNA Exploration 4.0