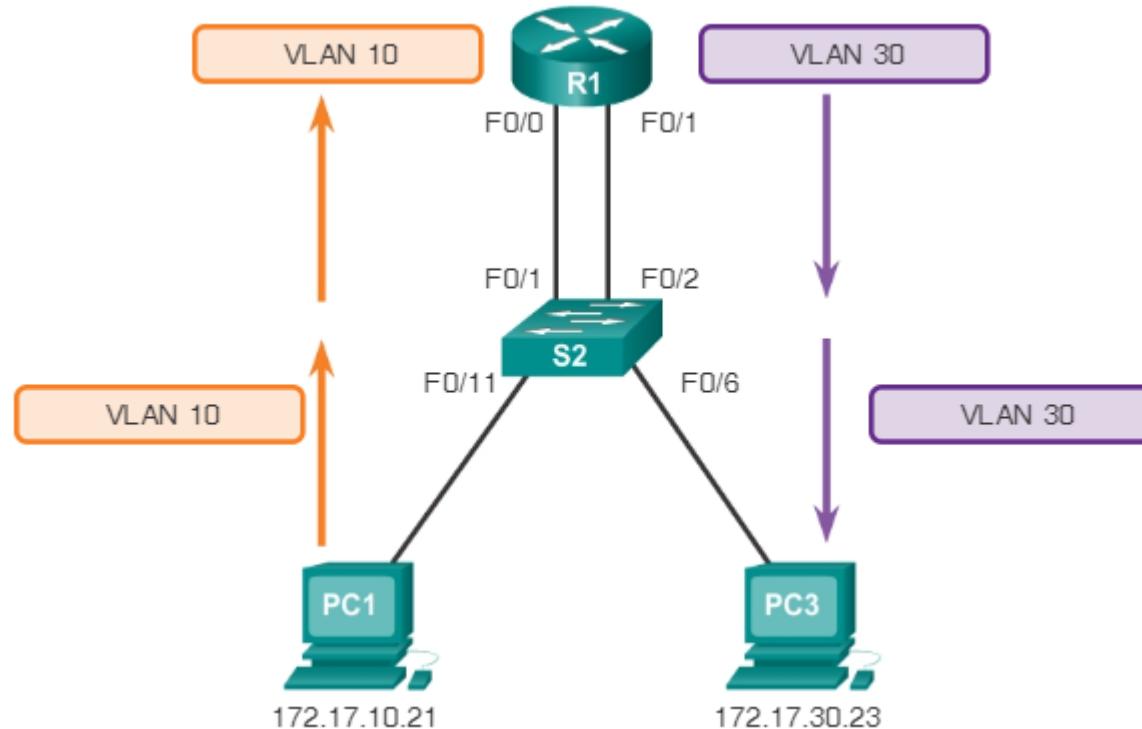
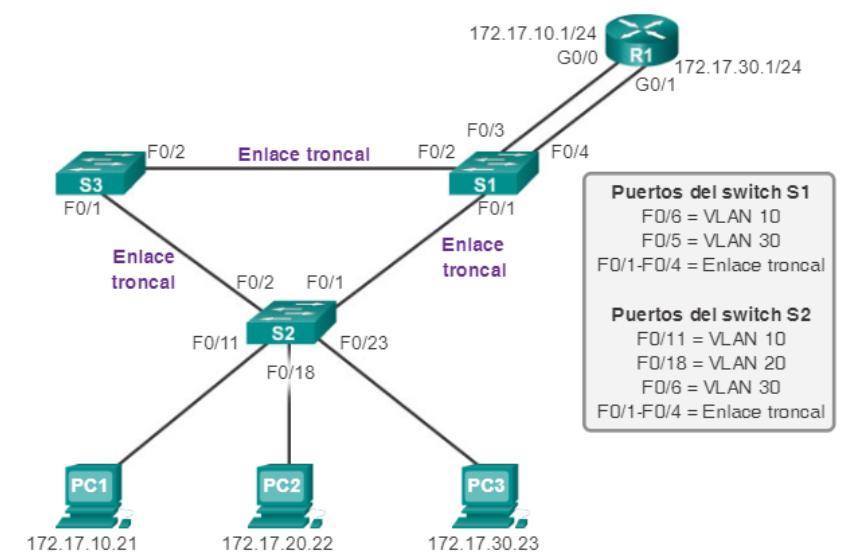


Enrutamiento entre VLANs



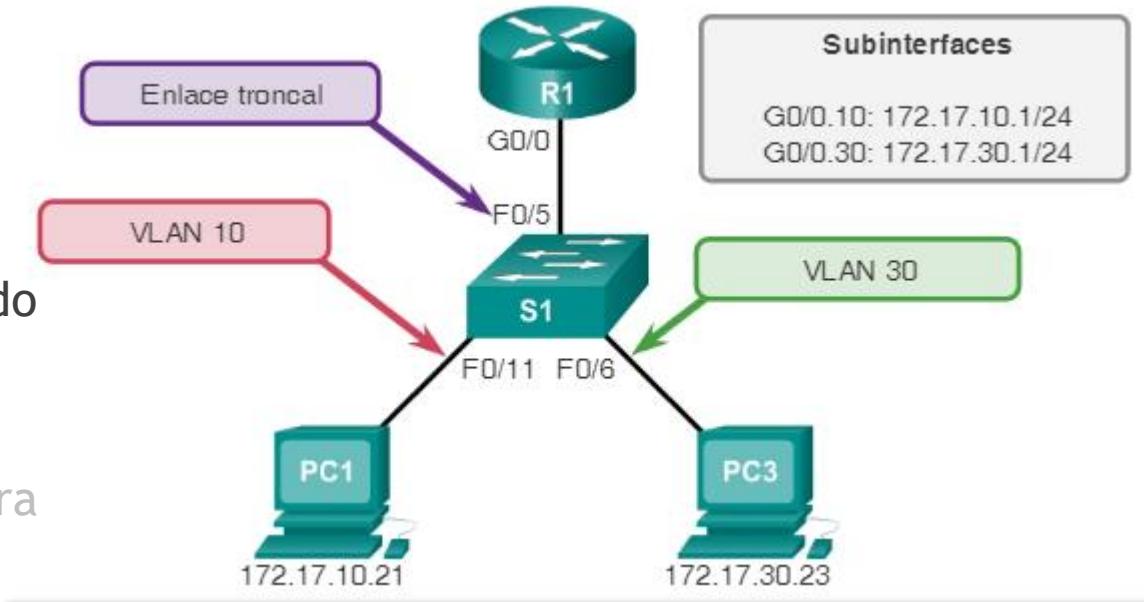
Enrutamiento entre VLANs

- ▶ Para establecer comunicación entre varios host de VLAN distintas, sería necesario establecer una comunicación desde el Switch hacia un router, y en el router tener una interface asignada para cada VLAN que tenga una puerta de enlace predeterminada correspondiente a cada una de las VLAN, similar a la ilustración.
- ▶ Dada la cantidad de puertos que normalmente un Router posee se dificultaría esta acción cuando el Switch trabajara con múltiples VLANs.
- ▶ Entonces se realiza el proceso denominado “Router-on-a-Stick”, el cual utiliza subinterfaces lógicas o virtuales para utilizar un único enlace físico entre el Switch y el Router, pero lógicamente el Router se encarga de administrar la interface como si fueran varias interfaces, de ahí el término subinterfaces.



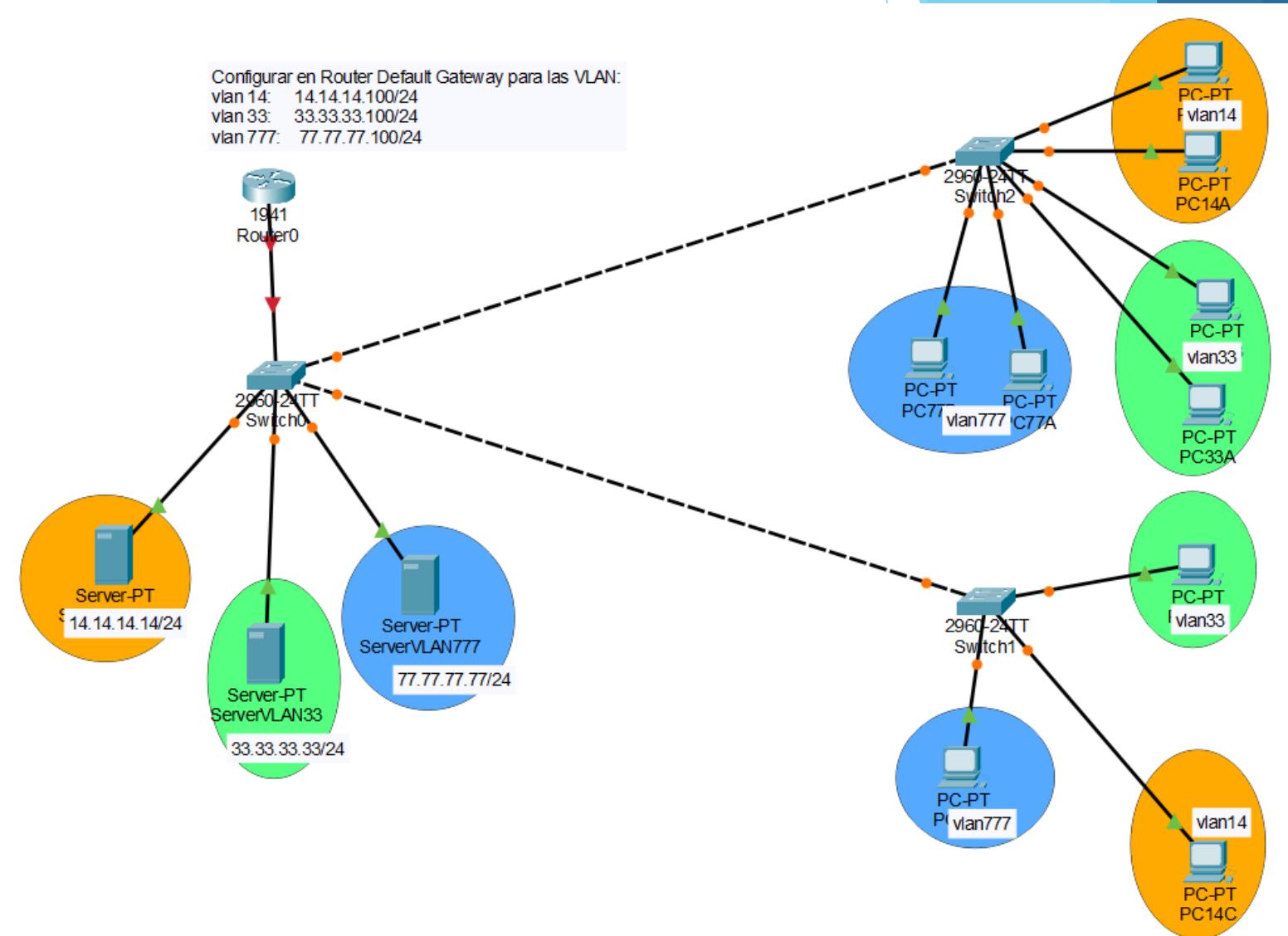
Configuración del routing entre VLAN

- ▶ **EN EL SWITCH:** Primero debemos contar con la conexión entre el Switch y el Router en modo troncal.
- ▶ **EN EL ROUTER:** Creamos las subinterfaces agregando un punto seguido de un identificado de las subinterfaces con el comando `interface gi0/0.10`
(Esto significa que se creará la subinterface .10 para la interface física gi0/0)
- ▶ A la subinterface hay que aplicarle el método de encapsulación .1q, a través del comando:
`encapsulation dot1q 10` (10 es el número de VLAN)
- ▶ Luego de esto ya se configura la ip address y se habilita la interface como si se tratara de cualquier interface física.



Crearemos la siguiente topología en Packet Tracer:

- ▶ Lo realizaremos en clase para practicar configuración de VLANs, Enlaces Troncales y la comunicación entre VLANs.





Configuración de un switch



**Comunicación y conexión inalámbrica de LAN.
Capítulo 2**



Objetivos

- Resumir la función de Ethernet establecida para las LAN de 100/1000 Mbps según el estándar IEEE 802.3
- Explicar las funciones que le permiten a un switch enviar tramas Ethernet en una LAN
- Configurar un switch para que funcione en una red diseñada para admitir transmisiones de voz, video y datos
- Configurar seguridad básica en un switch que funcionará en una red diseñada para admitir transmisiones de voz, video y datos

Redes 802.3/Ethernet

CSMA/CD

El conjunto de normas que utiliza Ethernet se basa en la tecnología de acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD, carrier sense multiple access/collision detect)

Detección de portadora

Acceso múltiple

Detección de colisiones

Señal de congestión y postergación aleatoria

Comunicaciones Ethernet

- Unicast: Comunicación en la que un host envía una trama a un destino específico. Ej. HTTP, SMTP, FTP y Telnet.
- Broadcast: Comunicación en la que se envía una trama desde una dirección hacia todas las demás direcciones. Ej. ARP
- Multicast: Comunicación en la que se envía una trama a un grupo específico de dispositivos o clientes.

Trama de Ethernet

- Campos Preámbulo y Delimitador de inicio de trama: (7 bytes) SFD (1 byte) se utilizan para la sincronización entre los dispositivos emisores y receptores.
- Campo Dirección MAC destino: (6 bytes) es el identificador del receptor deseado.
- Campo Dirección MAC origen: (6 bytes) identifica la NIC o interfaz de origen de la trama.
- Campo Longitud/Tipo: (2 bytes) define la longitud exacta del campo
- 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.
- 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).

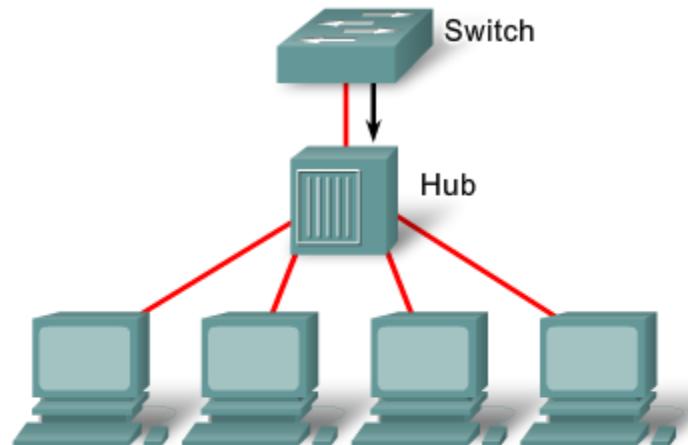
IEEE 802.3						
7	1	6	6	2	46 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud/ Tipo	Encabezado y datos 802.2	Secuencia de verificación de trama

Configuración Duplex

Configuración de Dúplex

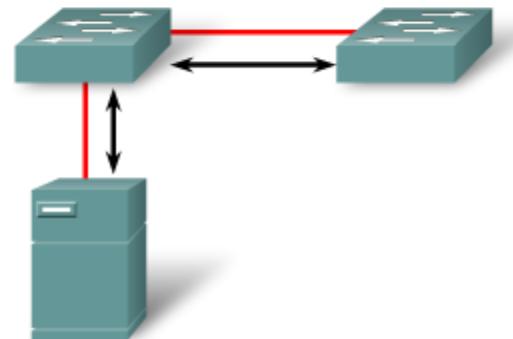
Half Duplex (CSMA/CD)

- 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



Configuración del puerto de switch

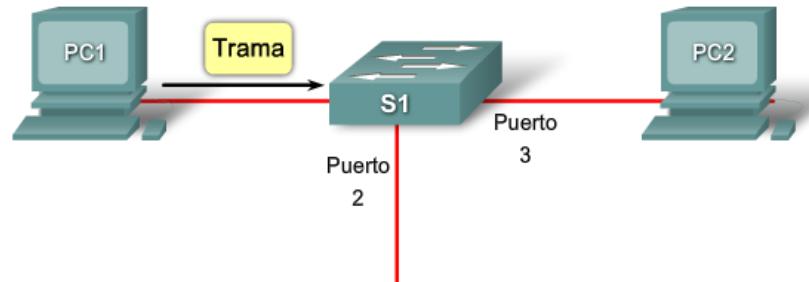
Los puertos de switch de la serie Cisco Catalyst 2960 pueden configurarse de tres maneras:

- **auto**: permite que los dos puertos se comuniquen para decidir el modo.
- **full**: establece el modo full-duplex.
- **half**: establece el modo half-duplex.

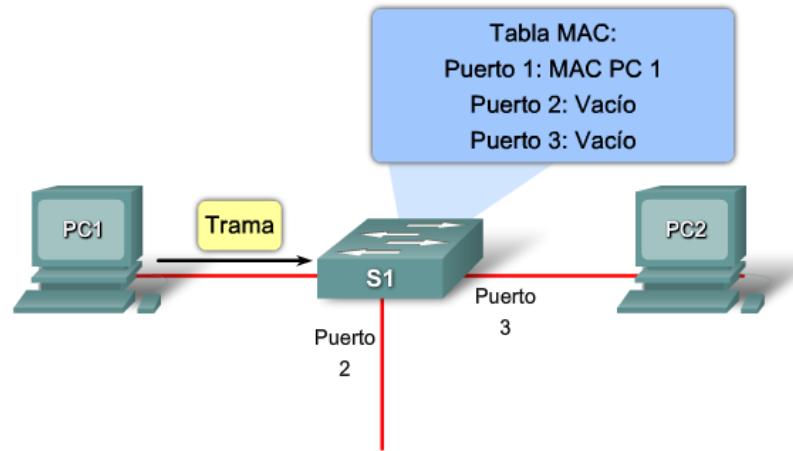
auto-MDIX

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).

Direccionamiento MAC y Tablas de direcciones MAC de los switches

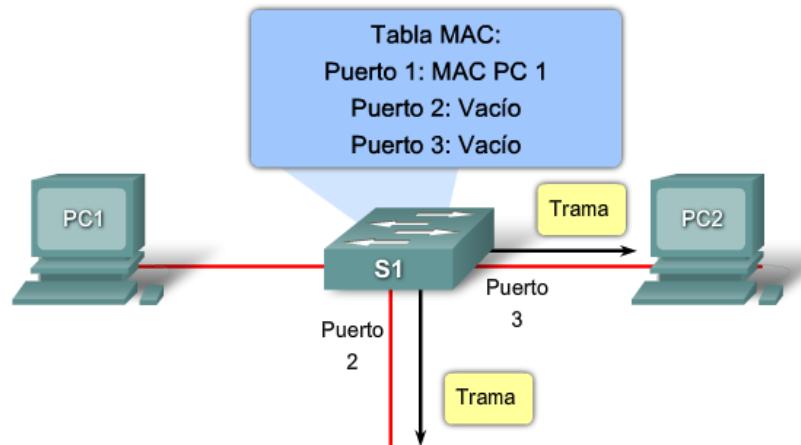


Paso 1: El switch recibe una trama de broadcast de la PC 1 en el Puerto 1.

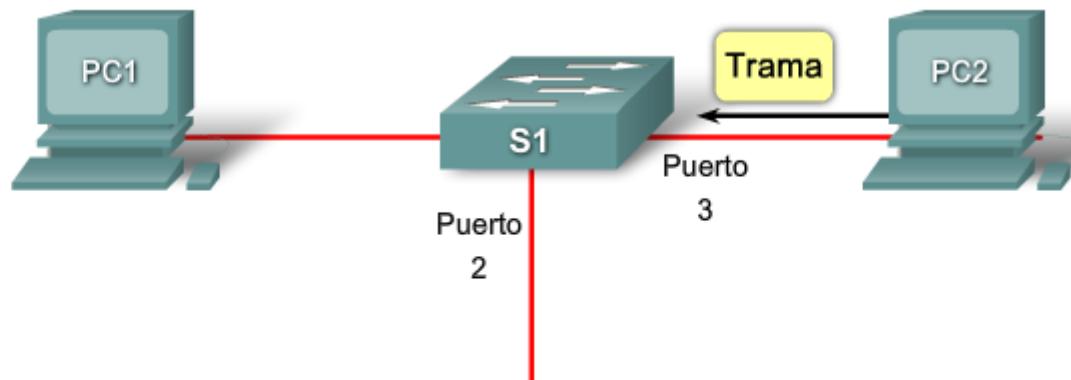


Paso 2: El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.

Direccionamiento MAC y Tablas de direcciones MAC de los switches

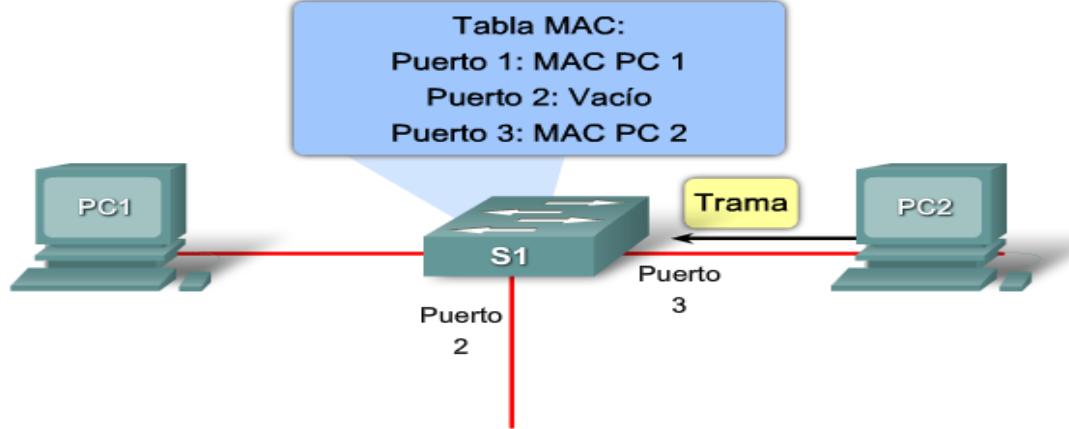


Paso 3: Dado que la dirección de destino es broadcast, el switch genera flooding en todos los puertos enviando la trama, excepto el puerto que la recibió.

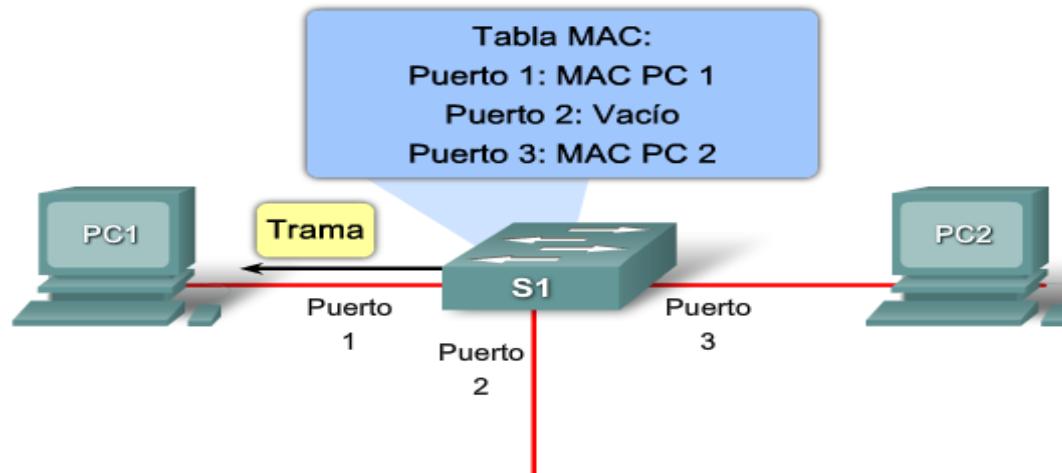


Paso 4: El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.

Direccionamiento MAC y Tablas de direcciones MAC de los switches

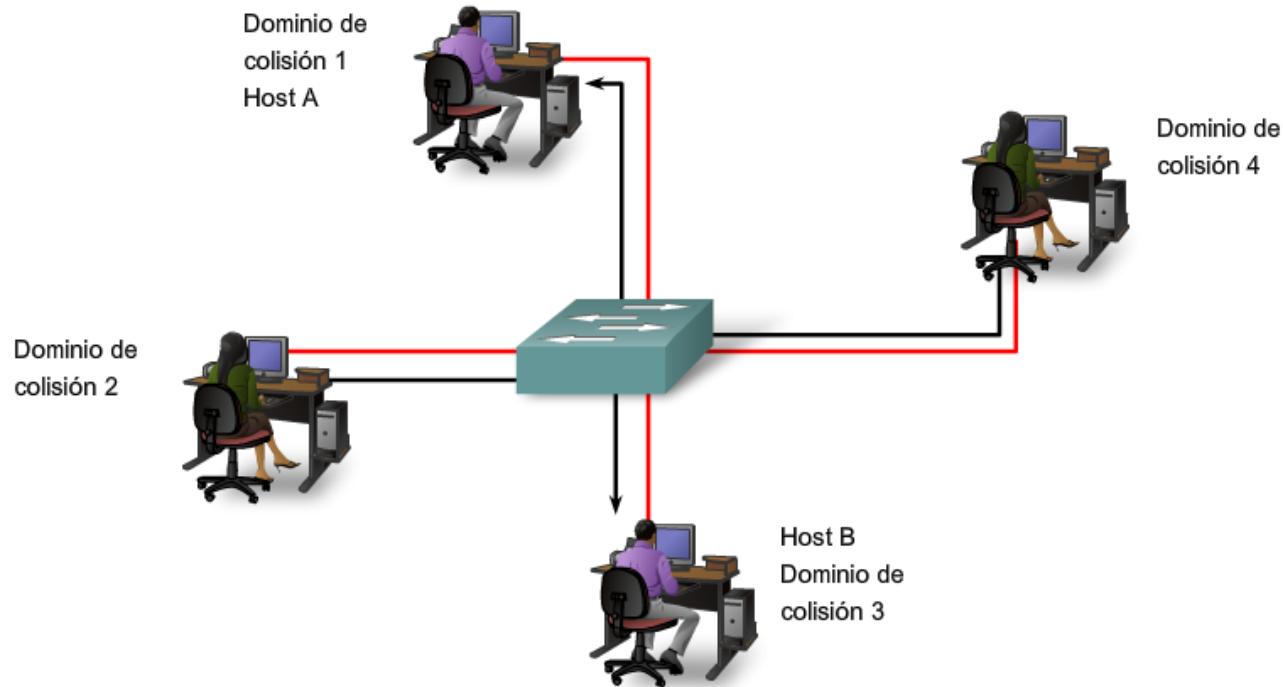


Paso 5: El switch ingresa la dirección MAC de origen de la PC2 y el número de puerto del switch que recibió la trama en la tabla de direcciones. La dirección de destino de la trama y el puerto relacionado a ella se encuentran en la tabla de direcciones MAC.



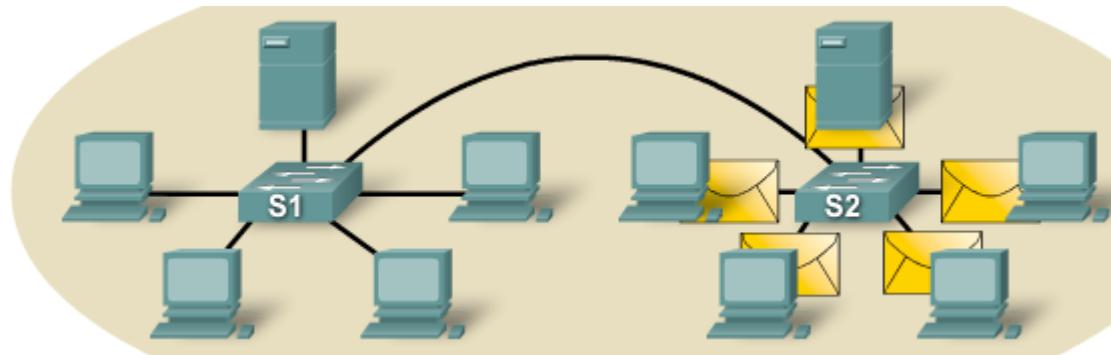
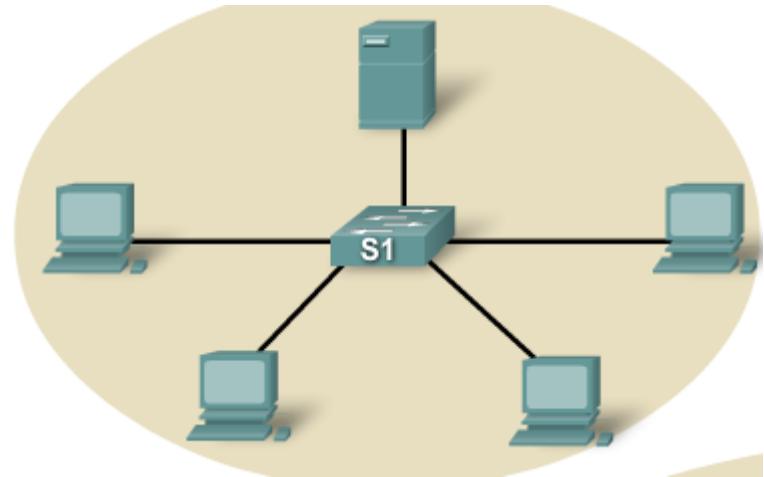
Paso 6: Ahora el switch puede enviar tramas entre los dispositivos de origen y de destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.

- Ancho de banda y rendimiento
- Dominios de colisiones



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. Para que otros switches de la LAN obtengan tramas de broadcast, éstas deben ser reenviadas por switches. 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.



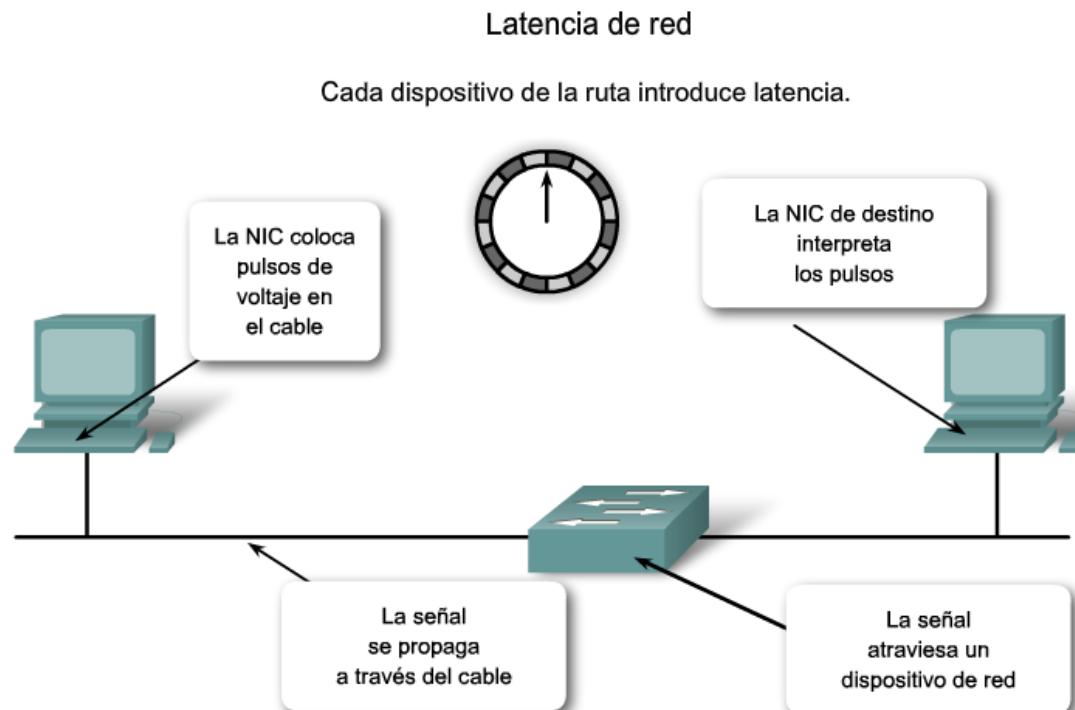
Latencia de red

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. Los usuarios de las aplicaciones basadas en redes experimentan la latencia cuando tienen que esperar varios minutos para obtener acceso a la información almacenada en un centro de datos o cuando un sitio Web tarda varios minutos en cargar el explorador. La latencia depende de al menos tres factores.

El tiempo que le toma a la NIC de origen aplicar pulsos de voltaje en el cable y el tiempo que le toma a la NIC de destino interpretar estos pulsos.

el retardo de propagación real, ya que la señal tarda en recorrer el cable. Normalmente, éste es de unos 0.556 microsegundos por 100 m para Cat 5 UTP.

La latencia aumenta según los dispositivos de red que se encuentren en la ruta entre dos dispositivos



Congestión de la red

A continuación se mencionan las causas más comunes de congestión:

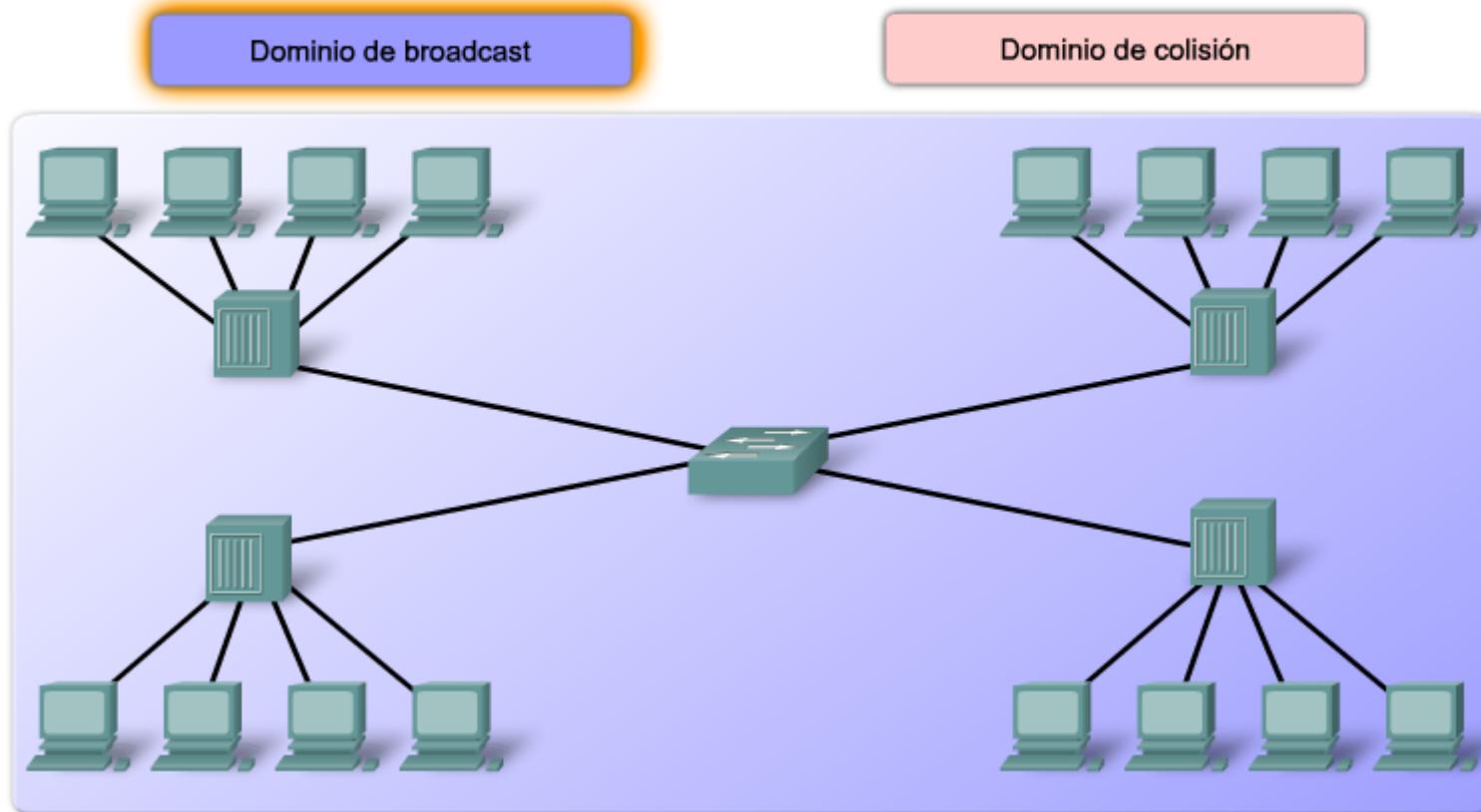
Tecnología de redes y computadoras cada vez más potentes.

Volumen de tráfico de la red cada vez mayor.

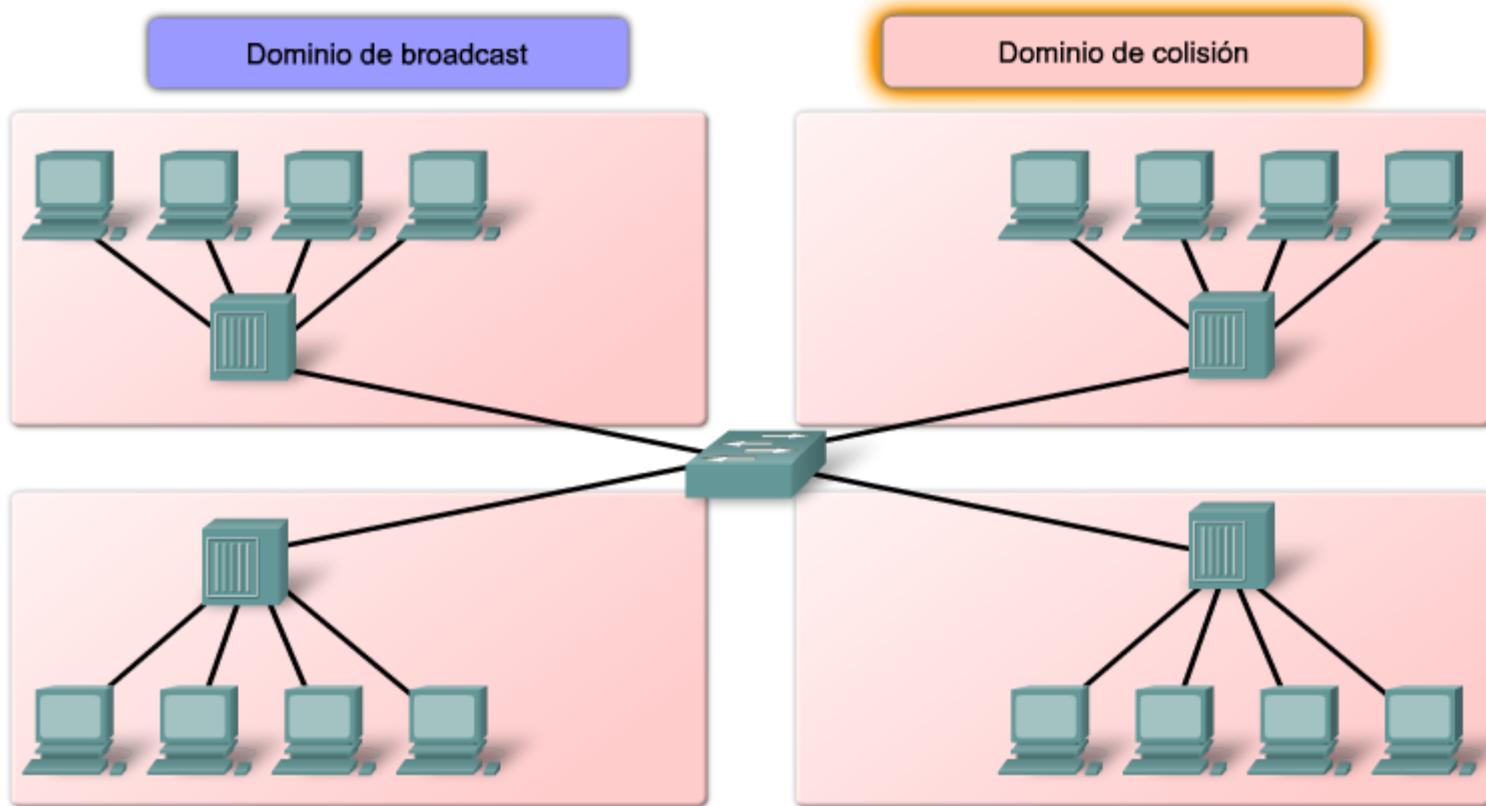
Aplicaciones con alta demanda de ancho de banda.

Segmentación de las LAN Dominio de Broadcast

Dominios de colisión y de broadcast



Dominio de Colisión



Consideración de diseño de red

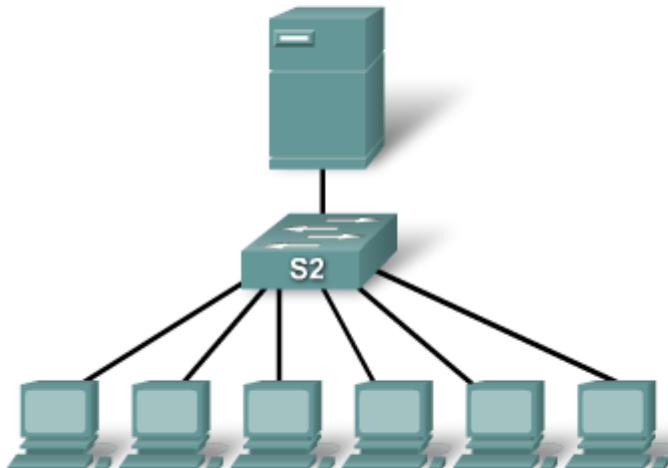
■ Control de la latencia de la red

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.

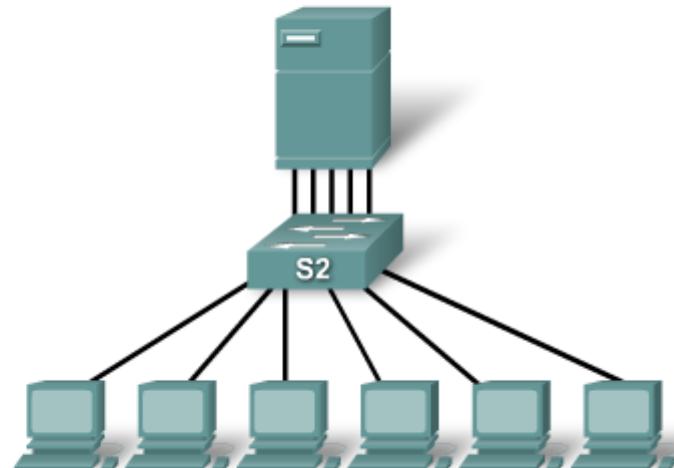
Eliminación de los cuellos de botella

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

Métodos de reenvío de 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.

Conmutacion simetrica y asimetrica

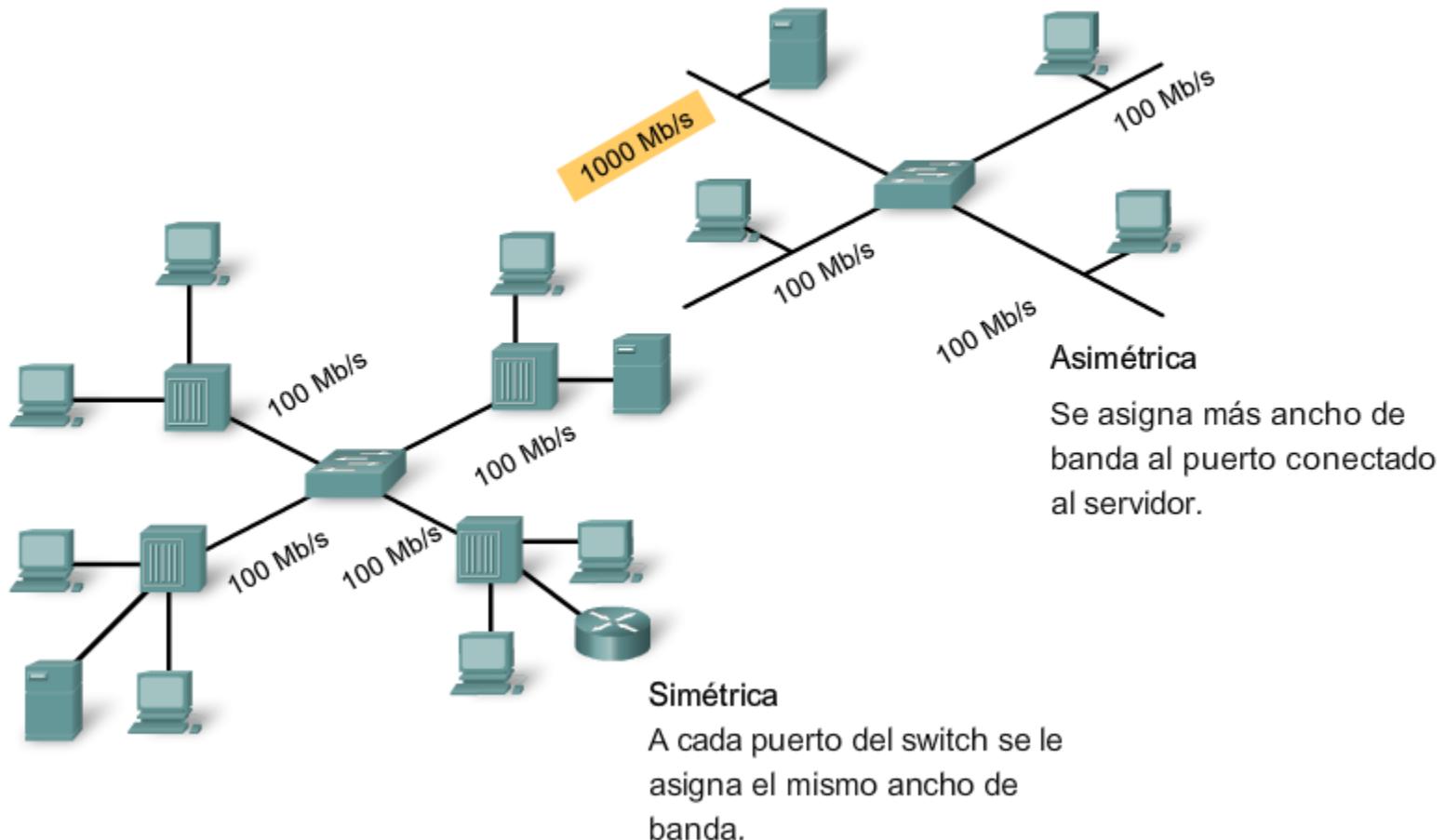
- Asimétrica

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.

- Simétrica

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

Comutación simétrica y asimétrica



Búfer de memoria basado en puerto y búfer de memoria compartida

- Como se describió en el tema anterior, el switch analiza parte del paquete o su totalidad antes de reenviarlo al host de destino mediante el método de reenvío. El switch almacena el paquete en un búfer de memoria durante un breve período. En este tema se estudiará cómo se utilizan dos tipos de búferes de memoria durante el reenvío.
- Un switch Ethernet puede usar una técnica de búferes para almacenar tramas antes de enviarlas. El almacenamiento en buffers también puede utilizarse cuando el puerto de destino está ocupado debido a una congestión.

Búfer de memoria basado en puerto y búfer de memoria compartida

Memoria basada en puerto	En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada y de salida 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.

Comunicación de Capa 2 y Capa 3

- 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. El switch de Capa 2 es completamente transparente para los protocolos de la red y las aplicaciones del usuario.
- 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 de la Capa 2 para determinar los envíos, el switch de Capa 3 puede también emplear la información de la dirección IP.

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, pueden normalmente enviar datos con la misma rapidez con la que pueden conmutar.



Comunicación de Capa 2



Comunicación de Capa 3



Comparación entre el switch de Capa 3 y el router

Característica	Switch de Capa 3	Router
Enrutamiento de Capa 3	Con soporte	Con soporte
Administración del tráfico	Con soporte	Con soporte
Soporte de WIC		Con soporte
Protocolos de enrutamiento avanzados		Con soporte
Enrutamiento por velocidad de cable	Con soporte	

Navegacion por los modos de interfaz de las lineas de comandos

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>

Modos de configuracion

Los modos Interfaz de la línea de comando

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-if)# 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#

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 Set the time and date
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 Current Time

Mensajes de error de la consola

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.

```
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.

Configuración del búfer de historial de comandos

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.	<code>switch#terminal history</code>
Configura el tamaño del historial del terminal. El historial del terminal puede mantener de 0 a 256 líneas de comando.	<code>switch#terminal history size 50</code>
Restablece el tamaño del historial del terminal al valor predeterminado de 10 líneas de comando.	<code>switch#terminal no history size</code>
Inhabilita el historial del terminal.	<code>switch#terminal no history</code>

Descripción de la secuencia de arranque del Switch

Descripción de la secuencia de arranque

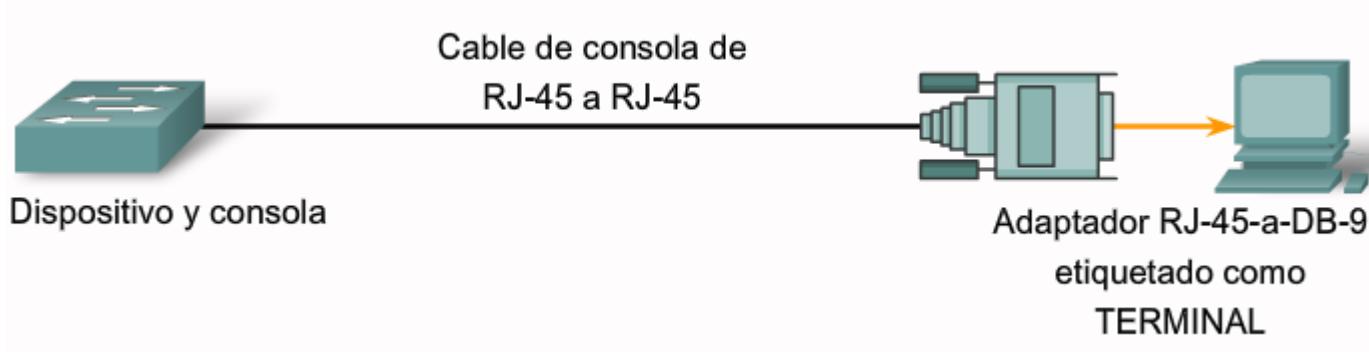
Secuencia de arranque de un switch de Cisco:

- 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.

Preparación para la configuración del switch



Configuración básica 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

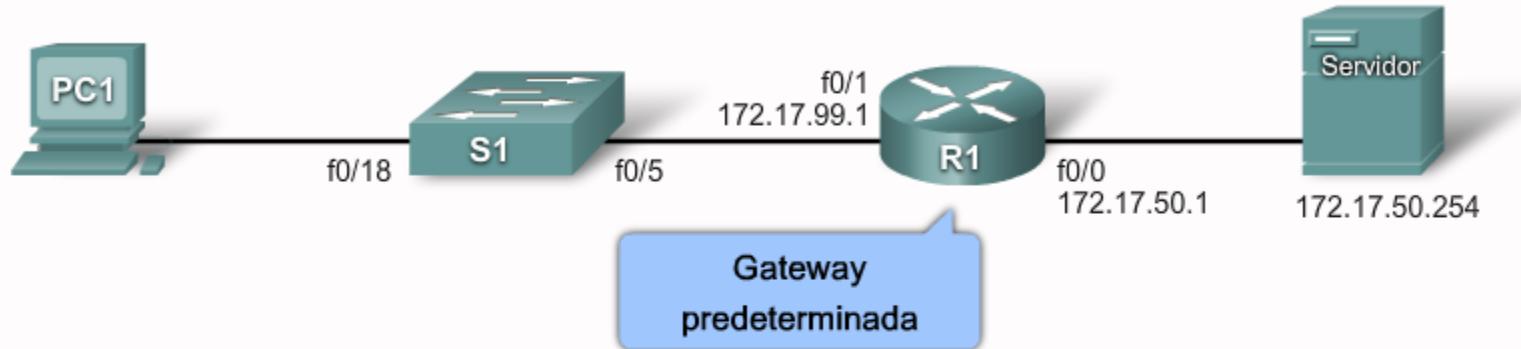
Configuración básica de switch

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

Configuración básica de switch

Configurar la conectividad IP



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

Consideraciones de interfaz de administración

Configurar interfaz de administración

Configurar gateway predeterminado

Verificar configuración

Configuración básica de switch

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

Configurar Dúplex y Velocidad

Configurar Duplex y Velocidad



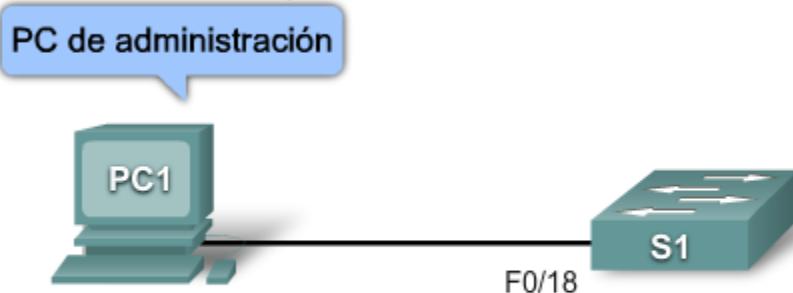
F0/1 en S1 es:
Modo Full-Duplex
100 Mbps

F0/1 en S2 es:
Modo Full-Duplex Mode
100 Mbps

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 una interfaz Web

Configuración de una interfaz Web



Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	S1# configure terminal
Configurar la interfaz del servidor HTTP para el tipo de autenticación activado. Las otras opciones son. enable: se usa la contraseña enable, que es el método predeterminado de autenticación de usuario de servidor HTTP. local: se usa la base de datos local del usuario, según se define en el router Cisco o servidor de acceso tacacs: se usa el servidor TACACS.	S1(config)#ip http authentication enable
Activar el servidor HTTP.	S1(config)# ip http server
Volver al modo EXEC privilegiado.	S1(config)# end
Guardar la configuración en ejecución en la configuración inicial del switch.	S1# copy running-config startup-config

Administración de la tabla de direcciones MAC

- show mac-address-table, que incluye direcciones MAC estáticas y dinámicas.
- 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.

Comandos show

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.	<code>show interfaces [id de la interfaz]</code>
Muestra el contenido de la configuración de inicio.	<code>show startup-config</code>
Muestra la configuración de funcionamiento actual.	<code>show running-config</code>
Muestra información acerca de flash: sistema de archivos.	<code>show flash:</code>
Muestra el estado del hardware y el software del sistema.	<code>show version</code>
Muestra el historial de comandos de sesión.	<code>show history</code>
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.	<code>show ip {interface http arp}</code>
Muestra la tabla MAC de envío.	<code>show mac-address-table</code>

Configuraciones de respaldo y restauración del 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 Ctrl+C para cancelar.	<pre>S1#copy system:running-config flash:startup-config Destination filename [startup-config] ?</pre>
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 Ctrl+C para cancelar.	<pre>S1#copy running-config startup-config Destination filename [startup-config] ?</pre>
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 Ctrl+C para cancelar.	<pre>S1#copy startup-config flash:config.bak1 Destination filename [config.bak1] ?</pre>

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 Ctrl+C para cancelar.	<pre>S1#copy flash:config.bak1 startup-config Destination filename [startup-config] ?</pre>
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 Ctrl+C para cancelar.	<pre>S1#reload System configuration has been modified. Save? [yes/no] : n Proceed with reload? [confirm] ?</pre>

Copia de respaldo de los archivos de configuración en un servidor TFTP

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

■ Eliminación de los archivos de configuración

```
S1#erase nvram:
Erasing the nvram filesystem will remove all configuration
files!
Continue? [confirm]
[OK]
Erase of nvram: complete
S1#
```

■ Eliminación de un archivo de configuración almacenado

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 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

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

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
```

Recuperación de la contraseña de enable

- 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 a 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`:

Recuperación de la contraseña de enable

- **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]?

Oprima Regresar en respuesta al indicador de confirmación. El archivo de configuración está cargado nuevamente y usted puede modificar la contraseña.

Recuperación de la contraseña de enable

- Paso 13. Ingrese al modo de configuración global mediante el comando `configure terminal`.
- Paso 14. Cambie la contraseña mediante el comando `enable secret contraseña`.
- 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`.

Configurar un título 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 título de inicio de sesión.	S1(config)# banner login "Authorized Personnel Only!"

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!"

Telnet y SSH

Telnet y SSH

Shell seguro (SSH).

SSH proporciona el mismo tipo de acceso que Telnet, con el beneficio agregado de seguridad.

La comunicación entre el cliente SSH y el servidor SSH está encriptada. Se recomienda que implemente SSHv2 cuando sea posible, debido a que utiliza un algoritmo de encriptación de seguridad mejor que SSHv1.

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

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

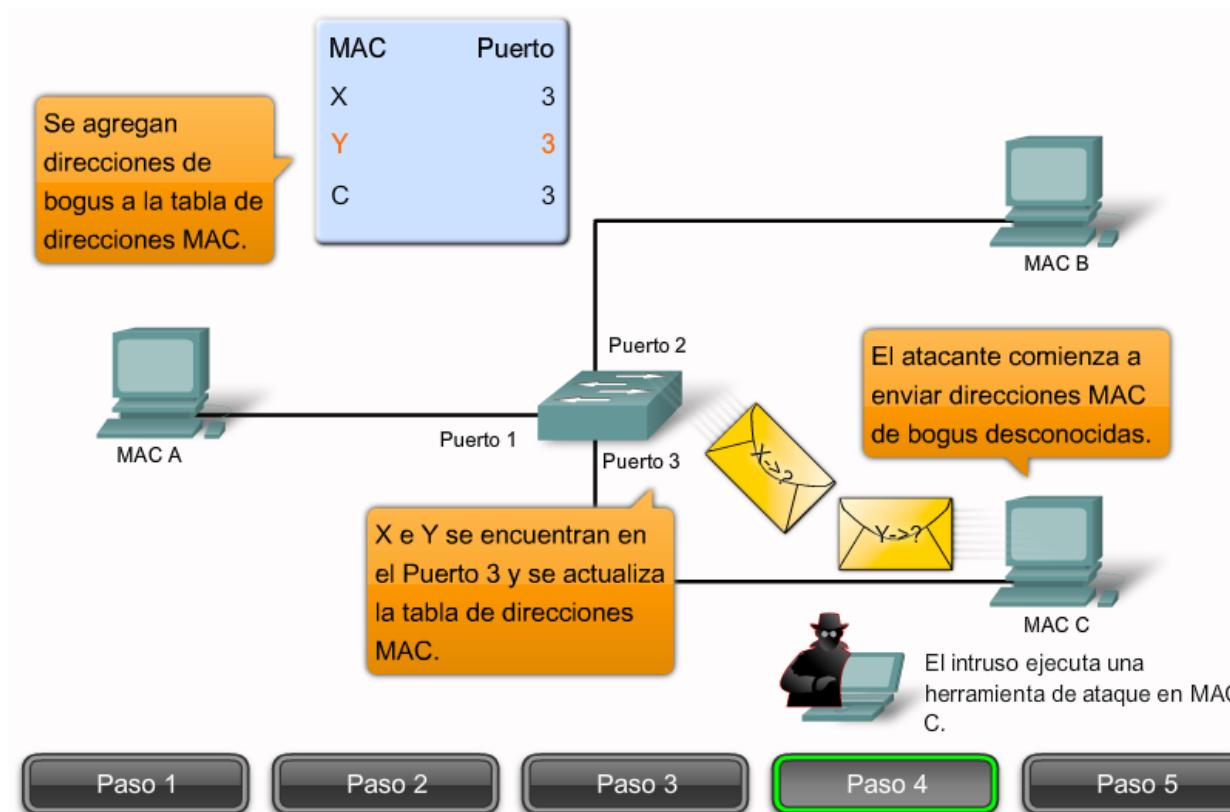
Configuracion SSH

- Paso 1. Ingrese al modo de configuración global mediante el comando `configure terminal`.
- Paso 2. Configure un nombre de host para su switch utilizando el comando `hostname nombre del host`.
- Paso 3. Configure un dominio de host para su switch utilizando el comando `ip domain-name nombre del dominio`.
- Paso 4. Habilite el servidor SSH para la autenticación remota y local en el switch y genere un par de claves RSA utilizando el comando `crypto key generate rsa`.
Cuando genera claves RSA se le indica que ingrese una longitud de módulo. Cisco recomienda utilizar un tamaño de módulo de 1024 bits. Una longitud de módulo más larga puede ser más segura, pero demora más en generar y utilizar.
- Paso 5. Regrese al modo EXEC privilegiado utilizando el comando `end`.
- Paso 6. Muestre el estado del servidor SSH en el switch utilizando el comando `show ip ssh` o `show ssh`.
- Para eliminar el par de claves RSA, utilice el comando `crypto key zeroize rsa` de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

```
(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
```

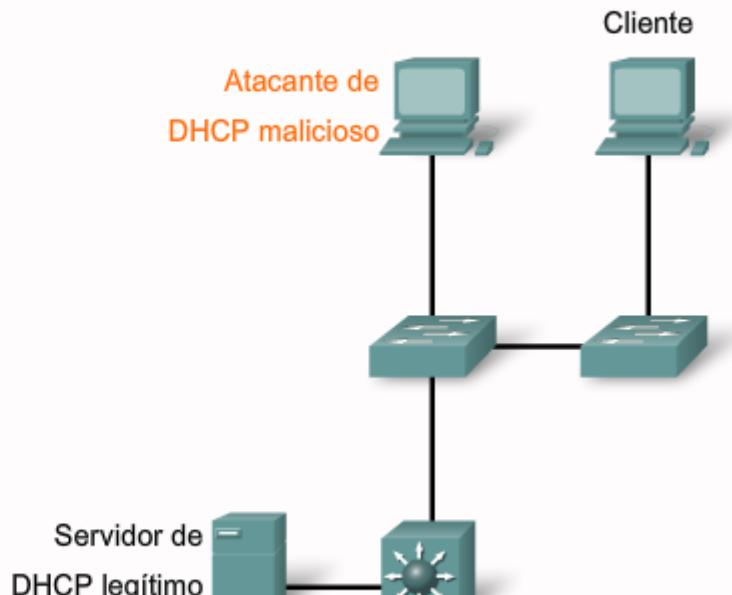
Ataques de seguridad comunes

■ Saturación de direcciones MAC



Ataques de suplantación de identidad

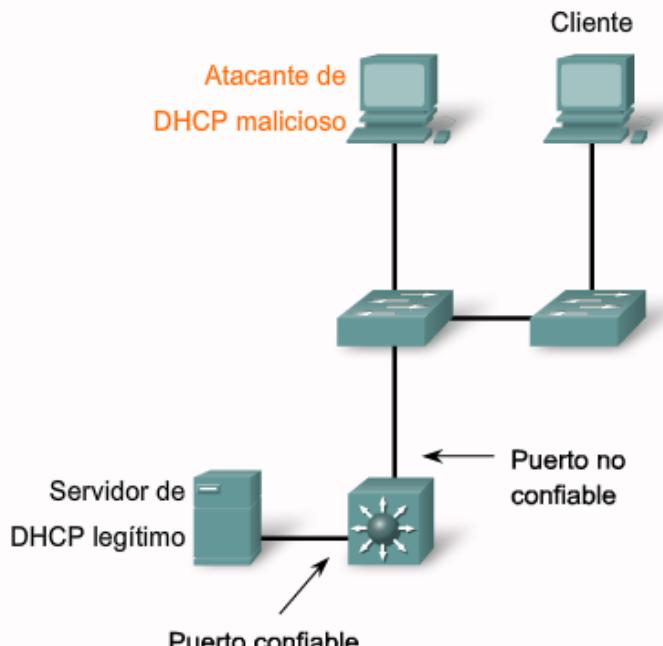
- 1) Un atacante activa un servidor de DHCP en un segmento de red.
- 2) El cliente envía un broadcast de solicitud de información de configuración de DHCP.
- 3) El servidor de DHCP malicioso responde antes de que lo haga el servidor de DHCP legítimo y asigna información de configuración de IP definida 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.



Snooping DHCP y funciones de seguridad de puerto de los switches Catalyst de Cisco

- 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 velocidad.

- 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**.



Ataques en CDP

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
- límite 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.

Características de las herramientas de seguridad de 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

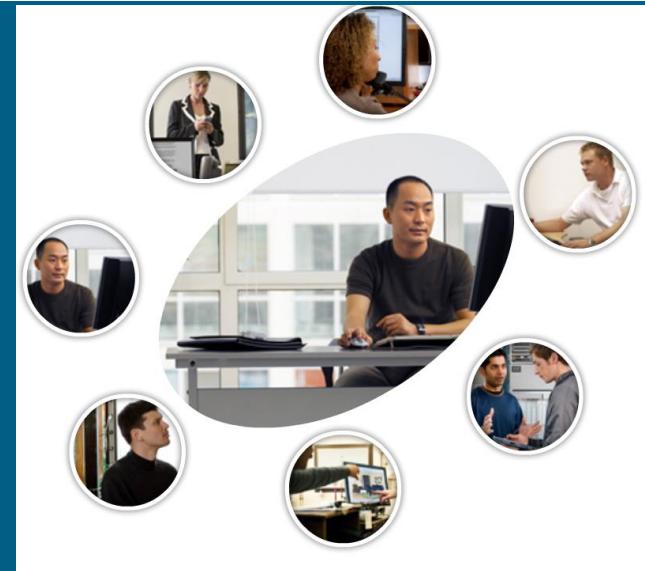
Configuracion de seguridad de puertos

- Direcciones MAC seguras estáticas: Las direcciones MAC se configuran manualmente mediante el comando de configuración de interfaz switchport port-security mac-address dirección MAC.
- Cuando se habilita el aprendizaje sin modificación en una interfaz mediante el comando de configuración de interfaz switchport port-security mac-address sticky,





VLAN



Conmutación y conexión inalámbrica de LAN. Capítulo 3

Objetivos

- Explicar la función de las VLAN en una red convergente
- Explicar la función de las VLAN con enlace troncal en una red convergente
- Configurar VLAN en switches de una topología de red convergente
- Resolver los errores comunes de configuración de software o hardware relacionados con VLAN en switches de una topología de red convergente

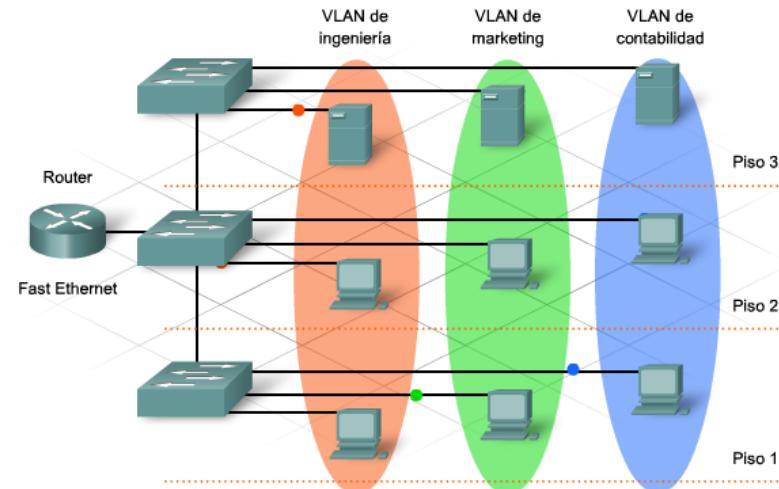
Introducción

En este capítulo aprenderá a:

- Explicar el rol de las VLAN en una red.
- Explicar el rol del enlace troncal de las VLAN en una red.
- Configurar las VLAN en los switches en una topología de la red.
- Realizar el diagnóstico de fallas comunes de la configuración de software o hardware asociadas con las VLAN en los switches en una topología de la red.

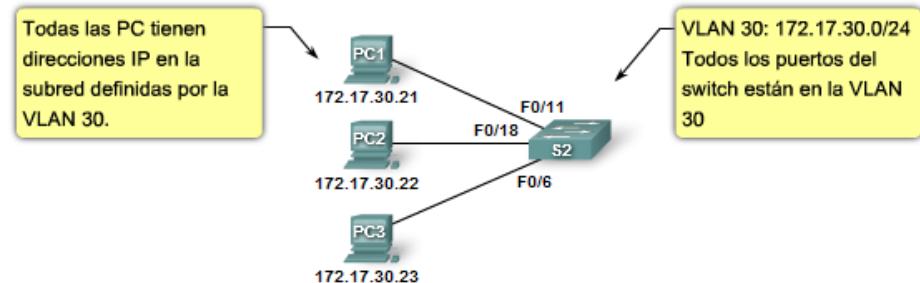
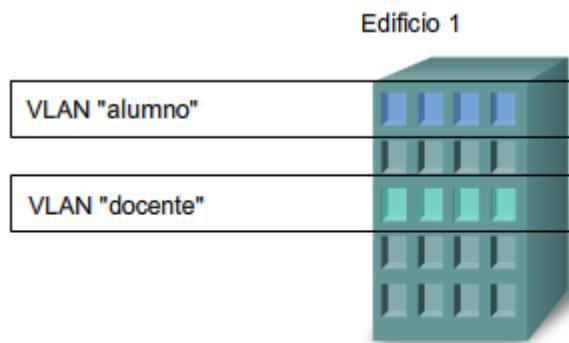
VLAN

- La diferencia entre una red física y una red virtual o lógica puede ilustrarse mediante el siguiente ejemplo:
- Los estudiantes de una escuela se dividen en dos grupos. Los estudiantes del primer grupo se identifican con tarjetas rojas. Los del segundo grupo se identifican con tarjetas azules. El director anuncia que los estudiantes con tarjetas rojas sólo pueden hablar con los compañeros que también tengan tarjetas rojas, y que los estudiantes con tarjetas azules sólo pueden hablar con sus compañeros poseedores de tarjetas azules. Ahora los estudiantes están separados lógicamente en dos grupos virtuales, o VLAN.



Definición

Las VLAN permiten a los profesionales de red agrupar lógicamente dispositivos de red, de modo que los usuarios de estos dispositivos puedan actuar como si estuvieran en su propia LAN

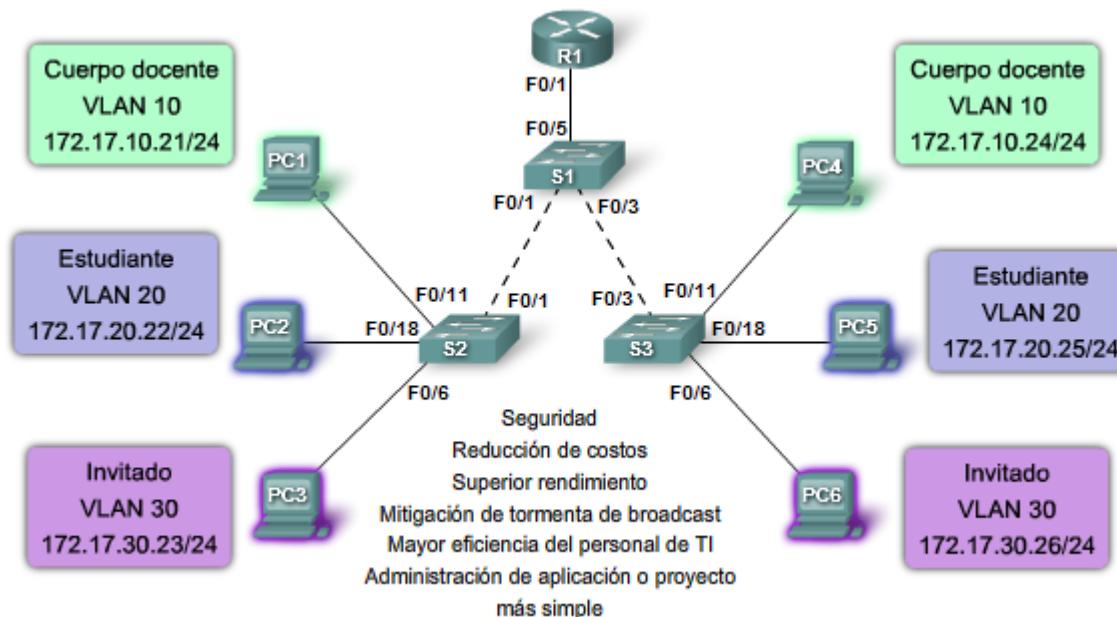


- Una VLAN es una red LAN independiente.
- Una VLAN permite que las PC del alumno y del docente estén separadas, aunque comparten la misma infraestructura.
- Se le puede otorgar un nombre a la VLAN para facilitar su identificación

- Una VLAN = Subred (en las LAN comutadas modernas)
- En el switch
 - Configurar la VLAN
 - Asignar el puerto a la VLAN
- En la PC asignar una dirección IP en la subred de VLAN

Ventajas

- Seguridad
- Reducción de costos
- Mayor rendimiento
- Mitigación de la tormenta de broadcast
- Mejor nivel de eficiencia del personal de tecnologías de la información (TI)
- Administración más simple de la aplicación o el proyecto

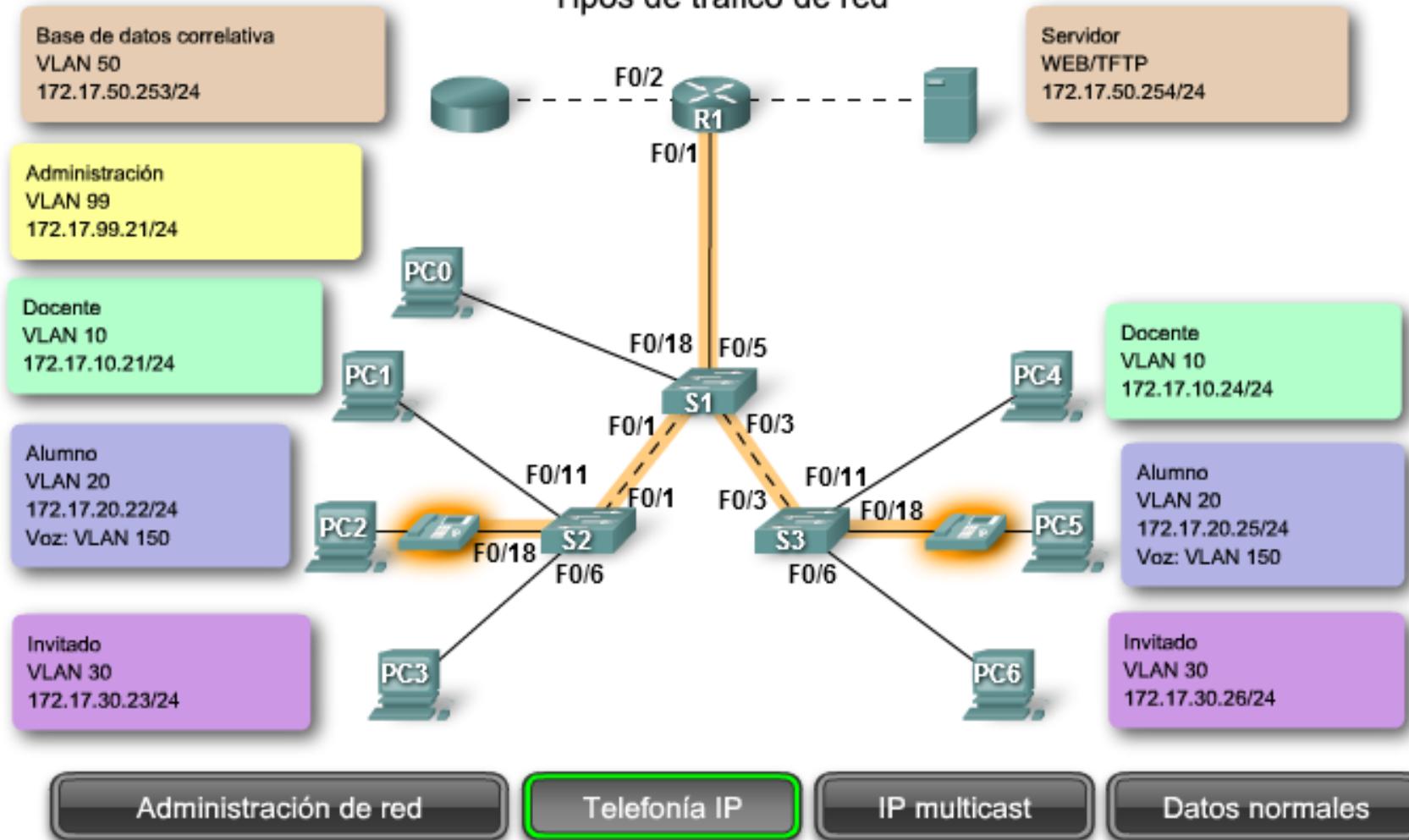


Tipos de VLAN

- 1. Una VLAN de datos es aquella que el administrador ha decidido que sólo transportará tráfico de usuario.
- 2. Una VLAN predeterminada es aquella VLAN de la que todos los puertos de un switch son miembros en el arranque inicial. No se la puede volver a nombrar ni eliminar. Si no se configura ninguna VLAN en un switch, éste es el modo en el cual funcionará.
- 3. Una VLAN nativa es un tipo de VLAN que se puede asignar a un puerto troncal 802.1Q. Los puertos troncales se tratarán en detalle más adelante, pero por ahora deberían saber que los puertos troncales transportan tráfico de todas las VLAN entre switches y entre un switch y un router.

- 4. La VLAN de administración es una VLAN configurada para acceder a las funciones de administración de un switch. La VLAN de administración predeterminada es la VLAN1. Sin embargo, es mejor cambiar la VLAN de administración a un número que no sea 1.
- 5. Las VLAN de voz son necesarias para admitir la calidad de servicio (QoS) que requiere VoIP. Una red VoIP requiere un ancho de banda garantizado para asegurar calidad de voz, prioridad de transmisión sobre otros tipos de tráfico de la red, capacidad para ser enrutada en áreas congestionadas de la red y un retardo de menos de 150 ms en toda la red. Para cumplir con estos requisitos, toda la red tiene que actualizarse para admitir VoIP.

Tipos de tráfico de red



Tipos de VLAN



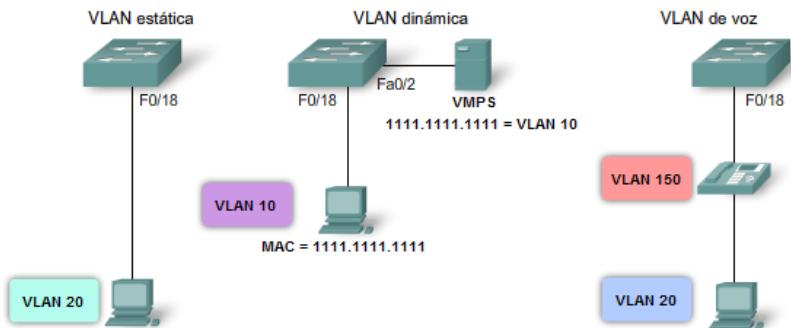
Identificadores

Características de VLAN

- ID de VLAN
 - ID de campo normal
 - 1 – 1005
 - 1002 -1005 se reservan para Token Ring y las VLAN FDDI
 - 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar
 - Se guarda en el archivo `vlan.dat` en la memoria flash
 - ID de campo ampliado
 - 1006 – 4094
 - Se diseñan para los proveedores de servicios
 - Poseen menos opciones que las VLAN de campo normal
 - Se guardan en el archivo de configuración en ejecución
- Un switch Cisco Catalyst 2960 admite 255 VLAN de campo normal y ampliado

Modos de puerto

Modos de membresía del puerto de la VLAN



Modos de membresía del puerto de la VLAN

Configuración del modo de puerto estático

```
S3#configure terminal  
Enter configuration commands, one per line. End with CNTL/z.  
S3(config)#interface fastEthernet0/18  
S3(config-if)#switchport mode access  
S3(config-if)#switchport access vlan 20  
S3(config-if)#end
```

VLAN estática

- Una VLAN estática requiere que el administrador asigne de forma manual cada puerto a una VLAN específica. Por ejemplo, el puerto fa0/3 puede asignarse a la VLAN 20. Cualquier dispositivo que se conecte al puerto fa0/3 es miembro de la VLAN 20 de forma automática.
- Una VLAN estática es el más fácil de configurar y también es el más difundido; sin embargo, requiere un mayor grado de apoyo administrativo en caso de adiciones, traslados y cambios.

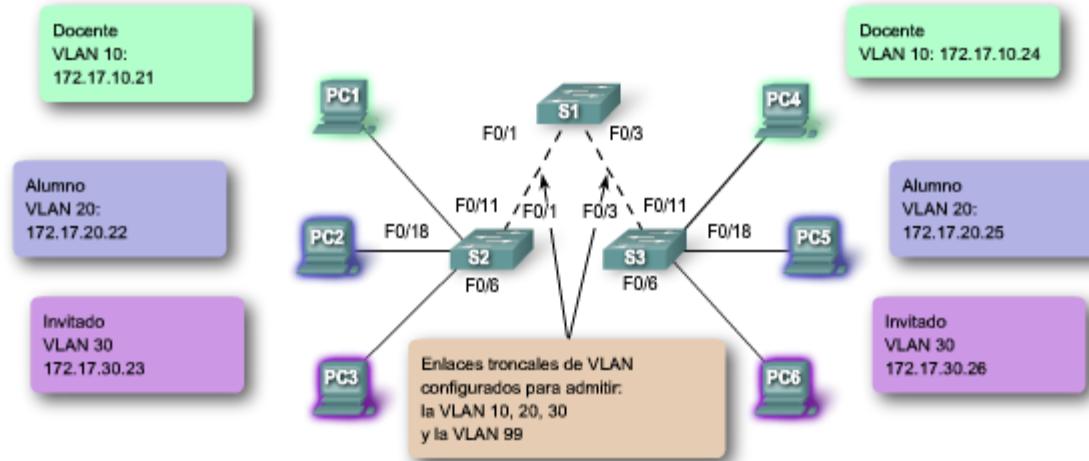
VLAN Dinámica

- VLAN dinámica requiere un servidor de política de administración de VLAN (VMPS). El VMPS contiene una base de datos que asigna direcciones MAC a la VLAN. Cuando se conecta un dispositivo a un puerto del switch, el VMPS busca en la base de datos una coincidencia con la dirección MAC, y asigna ese puerto de forma temporal a la VLAN correspondiente.
- VLAN Dinámica requiere más organización y configuración, pero crea una estructura con mucha más flexibilidad que la membresía estática a una VLAN. En una VLAN dinámica, los traslados, las adiciones y los cambios están automatizados, y no requieren intervenciones por parte del administrador.
- Nota: no todos los switches de Catalyst son compatibles con el uso de VMPS.

Enlaces troncales

VLAN 10 Docentes/personal: 172.17.10.0/24
VLAN 20 Alumnos: 172.17.20.0/24
VLAN 30 Invitados: 172.17.30.0/24
VLAN 99 Administración y nativa: 172.17.99.0/24

Puertos
F0/1 a 5 son interfaces de enlaces troncales 802.1Q con VLAN 99 nativa
F0/11 a17 están en la VLAN 10
F0/18 a 24 están en la VLAN 20
F0/6 a10 están en la VLAN 30



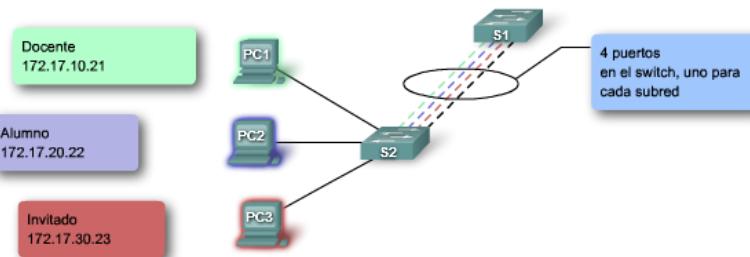
Enlace Troncal

- un enlace troncal es un canal de transmisión único entre dos puntos que, por lo general, son puertos de un switch. El enlace troncal es una conexión física que transporta o habilita enlaces lógicos. Los enlaces troncales Ethernet llevan el tráfico de múltiples VLAN por un único enlace. Un enlace troncal VLAN extiende las VLAN por toda una red. Cisco admite IEEE 802.1Q
- Un enlace troncal no pertenece a una VLAN específica. En cambio, es un conducto para las VLAN entre los switches y los routers. Un enlace troncal resuelve el problema de la necesidad de un enlace físico independiente para cada VLAN al permitir que múltiples VLAN pasen por un enlace físico.

Enlaces troncales

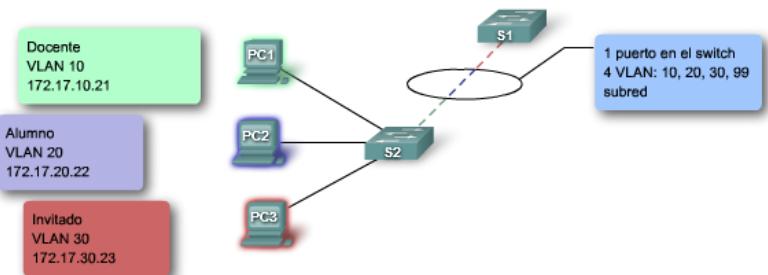
Docente: 172.17.10.0/24
Alumnos: 172.17.20.0/24
Invitado: 172.17.30.0/24
Administración y nativa: 172.17.99.0/24

Sin enlaces troncales de VLAN



VLAN 10: Docente = 172.17.10.0/24
VLAN 20: Alumnos = 172.17.20.0/24
VLAN 30: Invitado = 172.17.30.0/24
VLAN 99: Administración y nativa = 172.17.99.0/24

Con enlaces troncales de VLAN



Etiquetado

VLAN Nativas y Enlace troncal 802.1Q

Tramas con etiquetas en la VLAN nativa

- Descartadas por el switch
- Los dispositivos no deben etiquetar el tráfico de control destinado a la VLAN nativa

VLAN nativa

Tramas sin etiquetas en la VLAN nativa

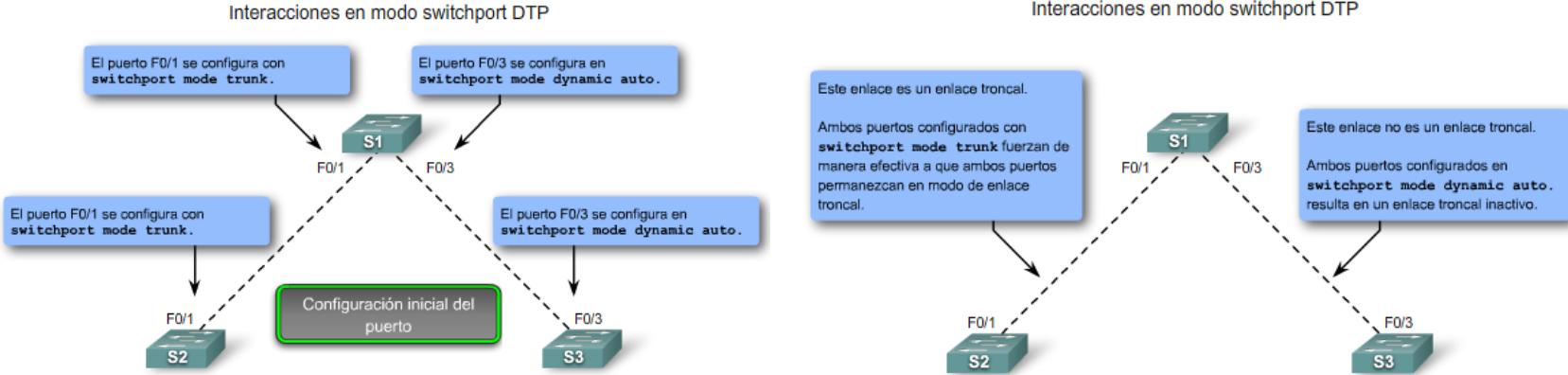
- Tienen su PVID modificado al valor de la VLAN nativa configurada
- Permanece sin etiquetar
- Son reenviadas en la VLAN nativa configurada

VLAN Nativas y Enlace troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco

Ingresar el modo de configuración global en el switch S1.	<code>S1#configure terminal</code>
Ingresar el modo de configuración de interfaz.	<code>S1(config)#interface F0/1</code>
Definir la interfaz F0/1 como un enlace troncal IEEE 802.1Q.	<code>S1(config-if)#switchport mode trunk</code>
Configurar la VLAN 99 para que sea la VLAN nativa.	<code>S1(config-if)#switchport trunk native vlan 99</code>
Volver al modo EXEC privilegiado.	<code>S1(config-if)#end</code>

Modos de enlace troncal

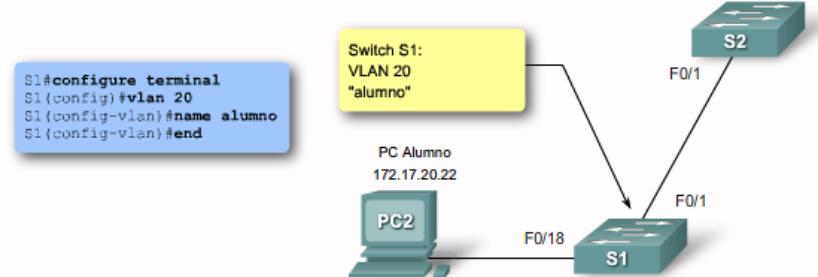


Los switches Cisco ejecutan el Dynamic Trunking Protocol (DTP)

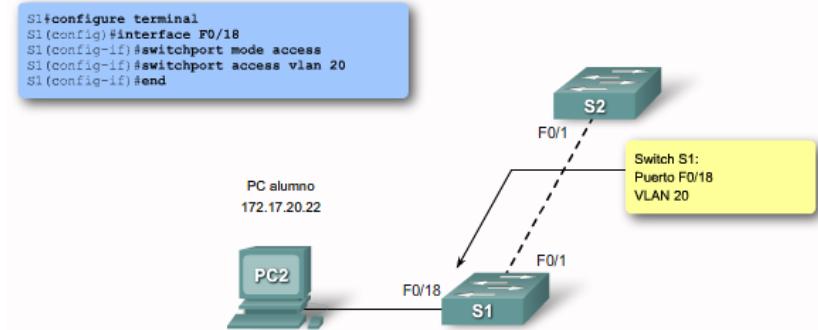
El protocolo DTP permite configurar los puertos del switch de modo que dinámicamente reconozcan el otro extremo del enlace y determinen si deben operar en modo troncal o como puertos de acceso. DTP está activo por defecto en los puertos de los switches Catalyst. Para definir dinámicamente el modo de los puertos Cisco IOS permite configurar los puertos como `dynamic auto` o `dynamic desirable`. La primera es la opción por defecto e implica que el puerto aguardará pasivamente la indicación del otro extremo del enlace para pasar a modo troncal. Sólo pasa a modo troncal si el otro extremo está en modo troncal o en modo deseable. En modo deseable en cambio, el puerto activamente intenta convertir el enlace en un enlace troncal. De este modo, si en el otro extremo encuentra un puerto en modo troncal, o en modo `dynamic auto` o en modo `dynamic desirable` (en todos los casos), pasará a operar en modo troncal.

Configuración VLAN

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	<code>S1#configure terminal</code>
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	<code>S1(config)#vlan vlan id</code>
(Opcional) Especificar un único nombre de VLAN para identificar la misma.	<code>S1(config-vlan)#name Nombre de VLAN</code>
Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo <code>vlan.dat</code> y para que la configuración entre en vigencia.	<code>S1(config-vlan)#end</code>



Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	<code>S1#configure terminal</code>
Ingresar la interfaz para asignar la VLAN.	<code>S1(config)#interface interface id</code>
Definir el modo de asociación de VLAN para el puerto.	<code>S1(config-if)#switchport mode access</code>
Asignar el puerto a una VLAN.	<code>S1(config-if)#switchport access vlan vlan id</code>
Volver al modo EXEC privilegiado.	<code>S1(config-if)#end</code>



Como configurar una VLAN

```
Switch#configure terminal
Switch(config)#vlan 27
Switch(config-vlan)#name accounting
Switch(config-vlan)#exit
Switch(config)#interface fa0/13
Switch(config-if)#switchport access vlan 27
Switch(config-if)#exit
Switch(config)#vlan 28
Switch(config-vlan)#name engineering
Switch(config-vlan)#exit
Switch(config)#interface fa0/6-12
Switch(config-if)#switchport access vlan 28
Switch(config-if)#end
Switch#show vlan
VLAN      Name           Status      Ports
-----  -----
1        default        active      Fa0/1, Fa0/4, Fa0/5
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                         Fa0/22, Fa0/23, Fa0/24
27       accounting     active      Fa0/13
28       engineering   active      Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Fa0/11, Fa0/12
1002     fddi-default   active
1003     token-ring-default active
1004     fddinet-default active
1005     trnet-default   active
```



Verificar la VLAN

- **show vlan:**

Muestra una lista detallada de todos los números y nombres de la VLAN que están activos actualmente en el switch, así como los puertos asociados con cada uno.

Muestra las estadísticas de STP si está configurado en cada VLAN.

- **show vlan brief:**

Muestra una lista abreviada solamente de las VLAN activas y los puertos asociados con cada una.

- **show vlan id id_number:**

Muestra información sobre una VLAN específica, según el número de ID.

- **show vlan name vlan_name:**

Muestra información sobre una VLAN específica, según el nombre.

```

Switch#show vlan

VLAN      Name           Status    Ports
-----  -----
1        default         active    Fa0/1, Fa0/4, Fa0/5
                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                           Fa0/22, Fa0/23, Fa0/24
27       accounting     active    Fa0/13
28       engineering    active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                           Fa0/10, Fa0/11, Fa0/12
1002     fddi-default   active
1003     token-ring-default active
1004     fddinet-default active
1005     trnet-default   active

VLAN Type    SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----

```

```

Switch#show vlan brief

VLAN      Name           Status    Ports
-----  -----
1        default         active    Fa0/1, Fa0/4, Fa0/5,
                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                           Fa0/22, Fa0/23, Fa0/24
27       accounting     active    Fa0/13
28       engineering    active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                           Fa0/10, Fa0/11, Fa0/12
1002     fddi-default   active
1003     token-ring-default active
1004     fddinet-default active
1005     trnet-default   active

```

Para eliminar una VLAN:

- Para desvincular un puerto de una VLAN específica:
Switch(config)#interface fa0/port_number
- Switch(config-if)#no switchport access vlan vlan_number

```
Switch(config)#interface fa0/8
Switch(config-if)#no switchport access vlan 28
Switch(config-if)#exit
Switch(config)#no vlan 27
Switch(config)#end
Switch#show vlan

VLAN      Name           Status      Ports
-----  -----
1        default        active     Fa0/1, Fa0/4, Fa0/5, Fa0/8
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                         Fa0/22, Fa0/23, Fa0/24
```

Estoy eliminando la VLAN 27. También estoy desasociando el puerto 8 de la VLAN 28.



- Switch(config)#no vlan vlan_number

```
Switch#show vlan id 28
```

VLAN	Name	Status	Ports
28	engineering	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Tran1	Trans2
28	enet	100028	1500	-	-	-	-	-	0	0

RemoteSPAN VLANS

Disabled

```
Switch#show vlan name engineering
```

VLAN	Name	Status	Ports
28	engineering	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9

VLAN	Type	SAID	MTU	Parent	Ring	NoBridgeNo	Stp	BrdgMode	Tran1
28	enet	100028	1500	-	-	-	-	-	0

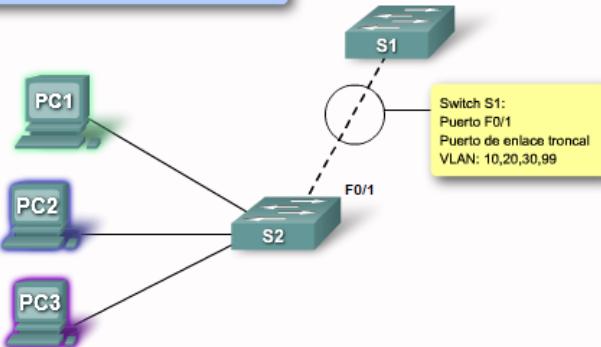
Remote SPAN VLANS

Disabled

Configuración enlace troncal

Configurar un enlace troncal 802.1Q

VLAN 10: Docente/personal = 172.17.10.0/24
VLAN 20: Alumnos = 172.17.20.0/24
VLAN 30: Invitado (predeterminado) = 172.17.30.0/24
VLAN 99: Administración y nativa = 172.17.99.0/24



Configurar un enlace troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global.	S1#configure terminal
Ingresar el modo de configuración de interfaz para la interfaz definida.	S1(config)#interface interface id
Hacer que el enlace que conecta los switches sea un enlace troncal.	S1(config-if)#switchport mode trunk
Especificar otra VLAN como la VLAN nativa para los enlaces troncales IEEE 802.1Q sin etiquetar.	S1(config-if)#switchport trunk native vlan vlan id
Volver al modo EXEC privilegiado.	S1(config-if)#end

```
S1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end
```

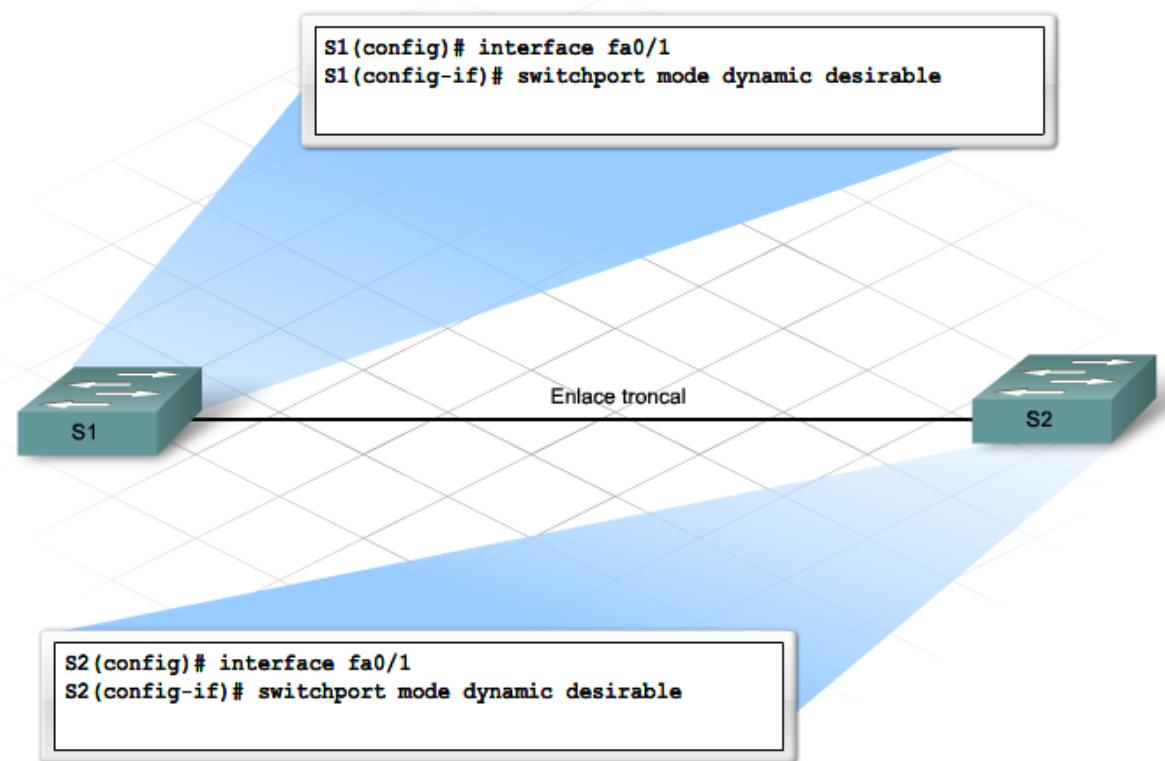
```
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```



Enlace Troncal

- Los switches más modernos tienen la capacidad de detectar el tipo de enlace configurado en el otro extremo. Según el servicio conectado, el enlace se configura como puerto de enlace troncal o como puerto de acceso.
- `Switch(config-if)#switchport mode dynamic {desirable | auto}`
- En el modo deseable, el puerto se convierte en puerto de enlace troncal si el otro extremo se establece como enlace troncal o deseable.
- En el modo automático, el puerto se convierte en puerto de enlace troncal si el otro extremo se establece como enlace troncal o deseable.

- Para volver a establecer un puerto de enlace troncal después de establecerlo como puerto de acceso, utilice cualquiera de los siguientes comandos:
 - Switch(config)#interface fa0/port_number
 - Switch(config-if)#no switchport mode trunk
 - o
 - Switch(config-if)#switchport mode access



Problemas comunes con troncales

Problema	Resultado	Ejemplo
Falta de concordancia en la VLAN nativa	Presenta un riesgo a la seguridad y crea resultados no deseados.	Por ejemplo, un puerto la ha definido como VLAN 99, el otro como VLAN 100.
Falta de concordancia en el modo de enlace troncal	Causa pérdida de la conectividad de la red.	Por ejemplo, en un puerto está configurado como "off" y en otro como modo de enlace troncal "on".
VLAN y Subredes IP	Causa pérdida de la conectividad de la red.	Por ejemplo, las computadoras de los usuarios pueden haber sido configuradas con las direcciones IP incorrectas.
VLAN permitidas en enlaces troncales	Provoca tráfico no deseado o no se envía el tráfico a través del enlace troncal.	La lista de las VLAN permitidas no admite los requisitos de enlace troncal de VLAN actuales.

Resumen capítulo

En este capítulo, aprendió a:

- Las VLAN separan los dominios de broadcast en los switches.
- Las VLAN mejoran el funcionamiento, la gestión y la seguridad de la red.
- La VLAN se puede usar para el tráfico de datos, voz, protocolo de red y administración de red.
- Existen tres modos de pertenencia diferentes: Modo VLAN estático, dinámico y de voz.
- Se necesitan routers o switches de Capa 3 para la comunicación entre VLAN.
- Los enlaces troncales permiten que muchas VLAN atraviesen un único enlace a fin de simplificar la comunicación intra VLAN, a través de múltiples switches.
- El IEEE 802.1Q es el protocolo de enlace troncal estándar
- El 802.1Q usa un proceso de etiquetado de tramas para mantener el tráfico de VLAN separado mientras atraviesa el enlace troncal.
- El 802.1Q no etiqueta el tráfico de la VLAN nativa, lo que puede resultar en problemas cuando el enlace troncal está mal configurado.





CCNA 3

*Comunicación y
conexión inalámbrica
de LAN*



Cisco | Networking Academy®
Mind Wide Open™



Objetivos

- Centrarnos en los protocolos de conmutación de capa 2
- Los conceptos usados para mejorar la redundancia, propagar la información de VLAN y proteger la parte de la red en la que se accede a los servicios



Capítulo 1

DISEÑO LAN

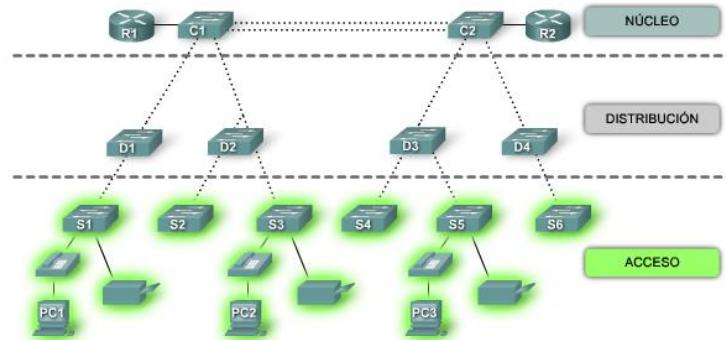
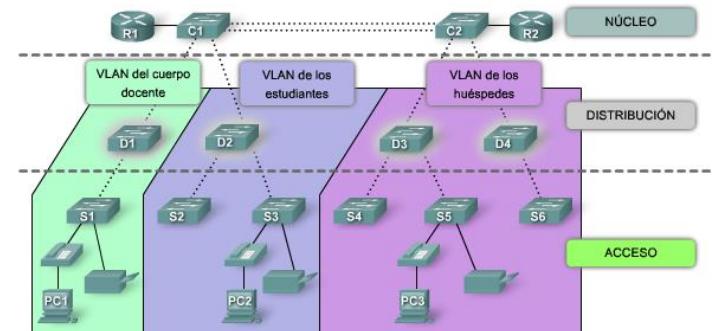
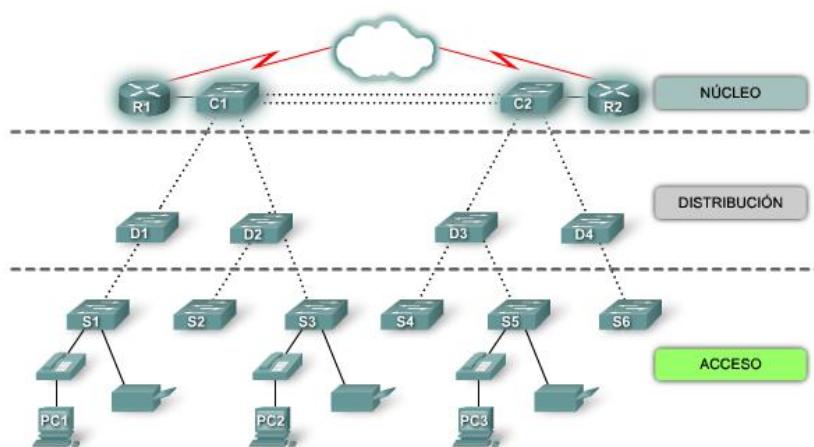


Introducción

En este capítulo aprenderá a:

- Describir cómo una red jerárquica admite las necesidades de voz, video y datos de una pequeña o mediana empresa.
- Describir las funciones de cada uno de los tres niveles del modelo de diseño de una red jerárquica, los principios de diseño de una red jerárquica (conectividad agregada, diámetro de la red y redundancia) y el concepto de una red convergente.
- Aportar ejemplos de cómo la voz y el video sobre IP afectan al diseño de la red.
- Seleccionar los dispositivos apropiados para operar en cada nivel de la jerarquía, incluyendo componentes de voz y video.
- Hacer coincidir el switch de Cisco adecuado con cada capa en el modelo de diseño de red jerárquica.

Modelo de redes jerárquicas





Beneficios de una red jerárquica

Escalabilidad

- Las redes jerárquicas pueden expandirse con facilidad

Redundancia

- La redundancia a nivel del núcleo y de la distribución asegura la disponibilidad de la ruta

Rendimiento

- El agregado del enlace entre los niveles y núcleo de alto rendimiento y switches de nivel de distribución permite casi la velocidad del cable en toda la red

Seguridad

- La seguridad del puerto en el nivel de acceso y las políticas en el nivel de la distribución hacen que la red sea más segura

Facilidad de administración

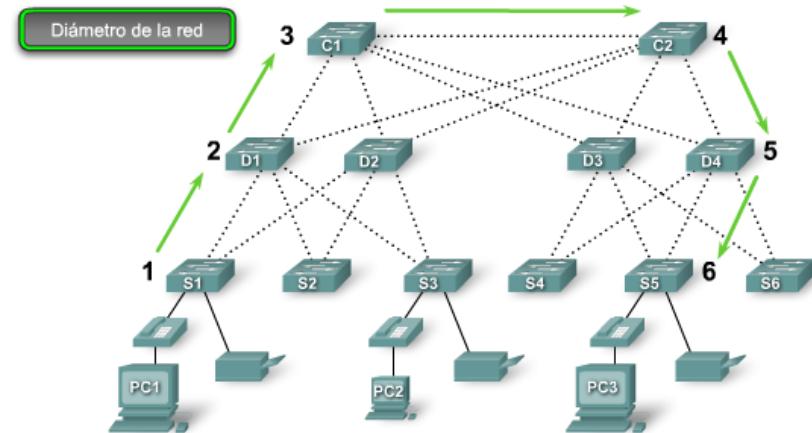
- La consistencia entre los switches en cada nivel hace que la administración sea más simple

Facilidad de mantenimiento

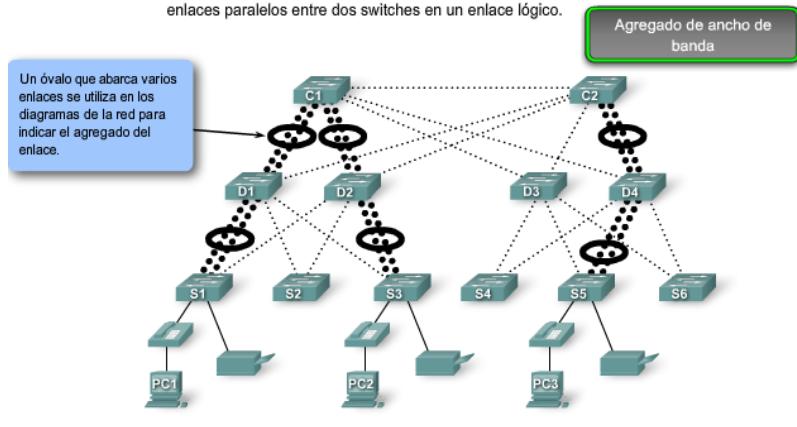
- La modularidad del diseño jerárquico permite que la red escale sin volverse demasiado complicada

Diseño de redes

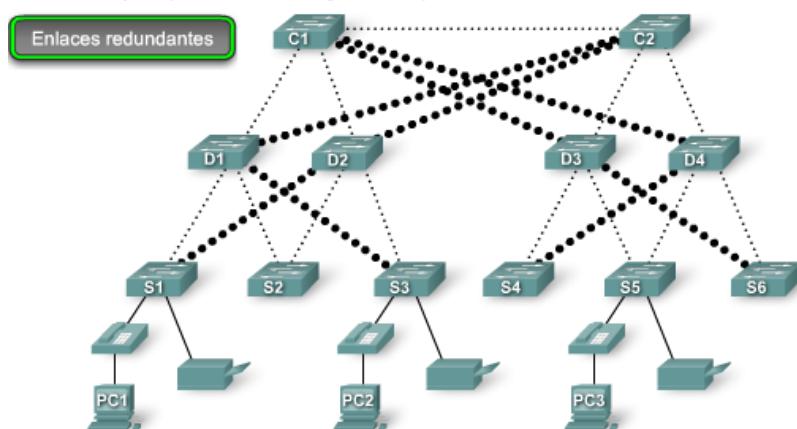
El diámetro de la red es el número de switches en la ruta del tráfico entre dos puntos finales.



El agregado de ancho de banda se implementa normalmente al combinar varios enlaces paralelos entre dos switches en un enlace lógico.



Las redes modernas utilizan enlaces redundantes entre las capas de redes jerárquicas a fin de asegurar la disponibilidad de la red.



Redes convergentes

Redes de voz, video y datos



Características de los switches

Factores de forma del switch

Switches de configuración fija



Las características y las opciones se limitan a aquellas que originalmente vienen con el switch.

Switches de configuración modular



El chasis acepta tarjetas de línea que contienen los puertos.

Switches de configuración apilable



Los switches apilables, conectados por un cable especial, operan con eficacia como un gran switch.

La densidad del puerto en el número de puertos disponibles en un solo switch.

switch de 24 puertos



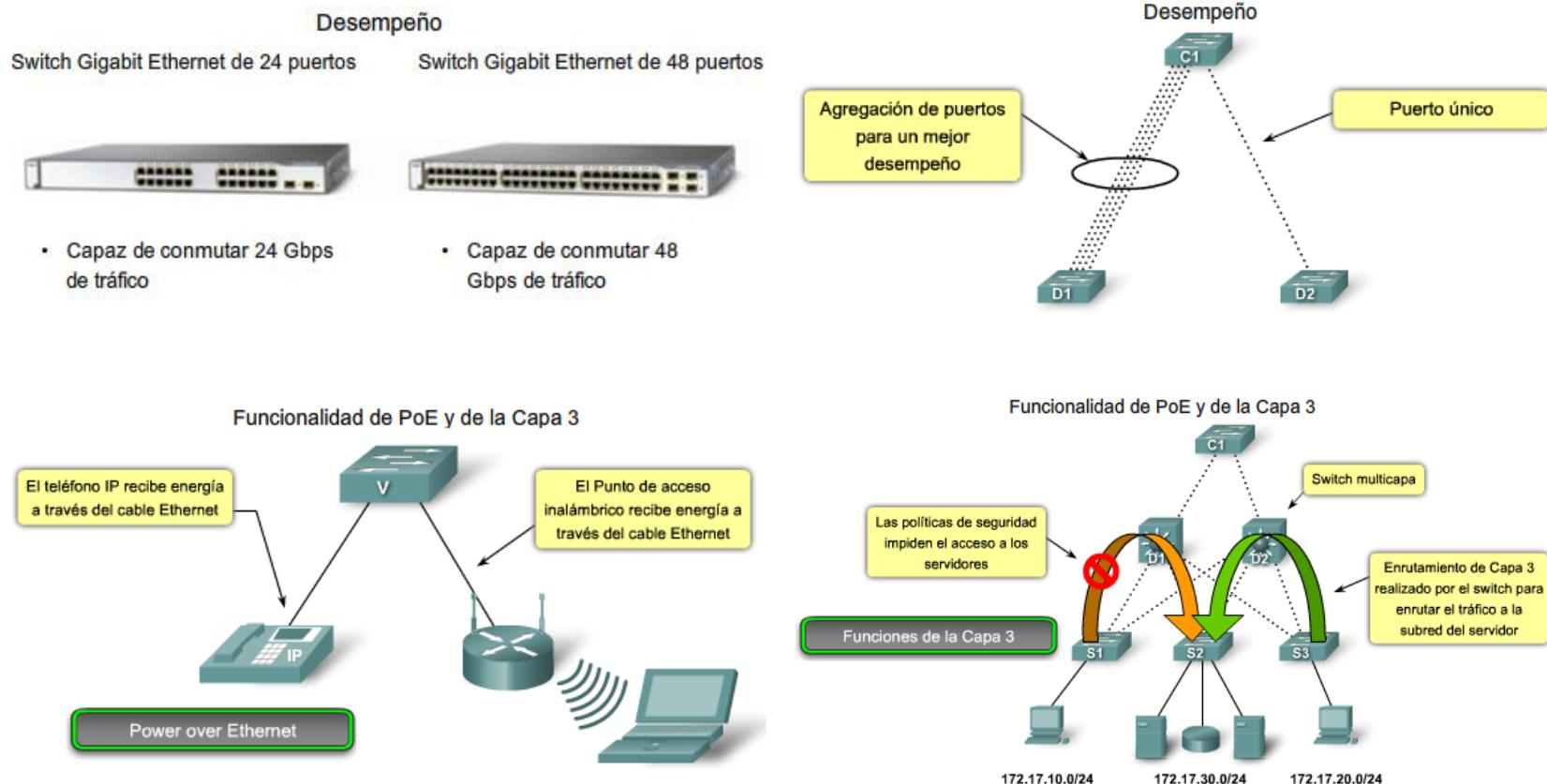
switch de 48 puertos



Switch modular con hasta más de 1000 puertos



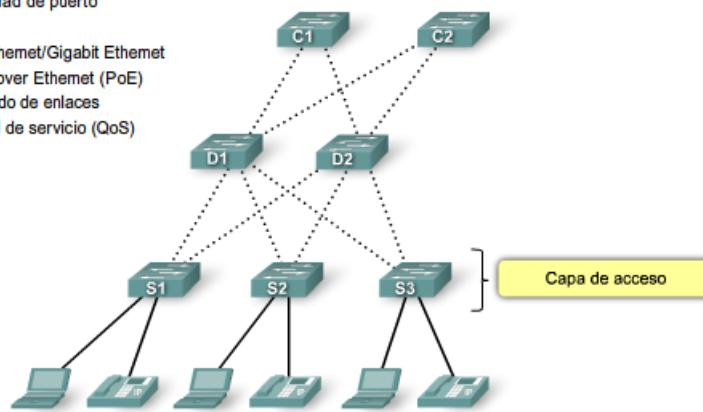
Características de los switches



Características del switch en una red jerárquica

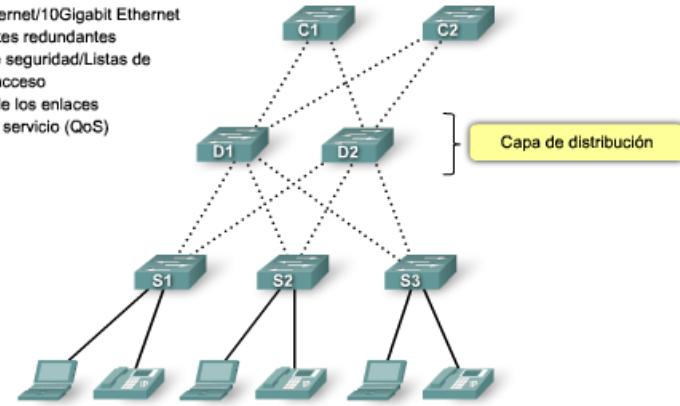
Características del switch de la capa de acceso

- Seguridad de puerto
- VLAN
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Agregado de enlaces
- Calidad de servicio (QoS)



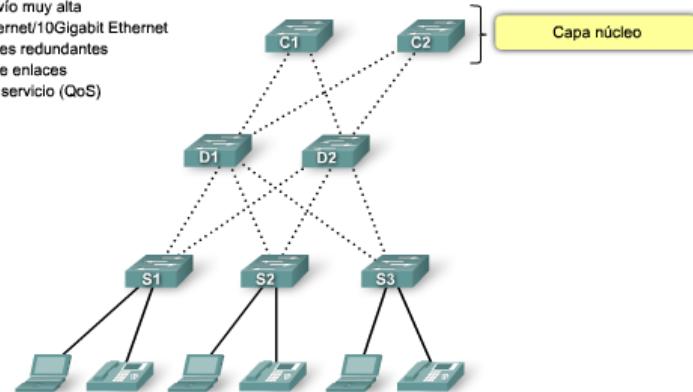
Características del switch de capa de distribución

- Soporte de la Capa 3
- Tasa de envío alta
- Gigabit Ethernet/10Gigabit Ethernet
- Componentes redundantes
- Políticas de seguridad/Listas de control de acceso
- Agregado de los enlaces
- Calidad del servicio (QoS)



Características del switch de capa núcleo

- Soporte de Capa 3
- Tasa de envío muy alta
- Gigabit Ethernet/10Gigabit Ethernet
- Componentes redundantes
- Agregado de enlaces
- Calidad del servicio (QoS)





Resumen capítulo

En este capítulo aprendió que:

- El modelo de diseño jerárquico mejora en cuanto a la limitación de la malla parcial y plana, y a los modelos del diseño de malla al mejorar el rendimiento, la escalabilidad, la disponibilidad, la facilidad de administración y el mantenimiento de la red.
- Las topologías de las redes jerárquicas facilitan la convergencia de la red al proporcionar el rendimiento necesario para que se combinen los datos de voz y video en la red de datos existente.
- Se pueden realizar los análisis de flujo del tráfico, de las comunidades de usuarios, de los medios de almacenamiento de datos y la ubicación del servidor y del diagrama de la topología para ayudar a identificar los cuellos de botella de la red.
- Luego, se pueden direccionar los cuellos de botella para mejorar el rendimiento de la red y determinar con exactitud los requerimientos apropiados del hardware para satisfacer el rendimiento deseado de la red.
- Los switches Cisco combinan los factores de forma específicos, el rendimiento, la PoE y el soporte de la Capa 3 que admite los niveles del diseño de la red jerárquica.

Introducción a los protocolos de enrutamiento dinámico



Conceptos y protocolos de enrutamiento. Capítulo 3



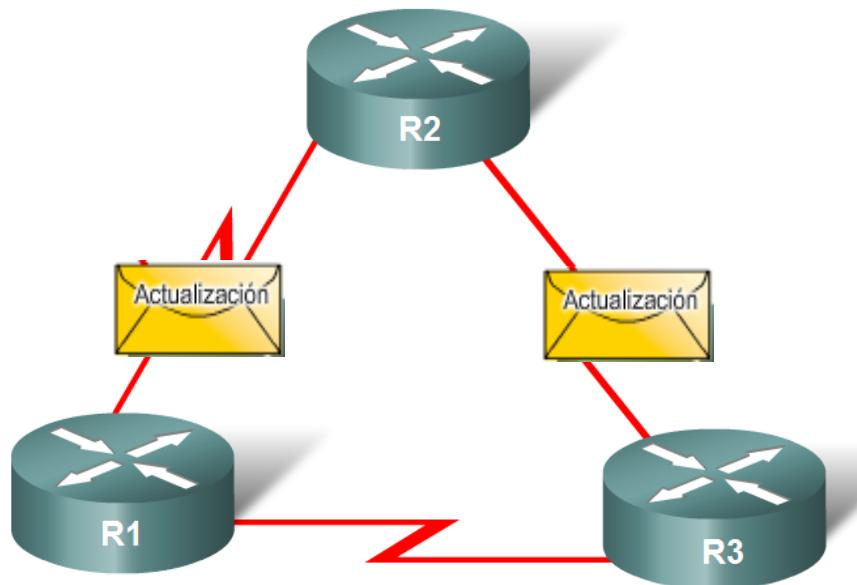
Objetivos

- Describir la función de los protocolos de enrutamiento dinámico y ubicar estos protocolos en el contexto del diseño de redes actual.
- Identificar varias formas de clasificar los protocolos de enrutamiento.
- Describir cómo los protocolos de enrutamiento usan las métricas e identificar los tipos de métricas que usan los protocolos de enrutamiento dinámico.
- Determinar la distancia administrativa de una ruta y describir su importancia para el proceso de enrutamiento.
- Identificar los distintos elementos de la tabla de enrutamiento.

Protocolos de enrutamiento dinámico

- Funciones de los protocolos de enrutamiento dinámico:
 - Compartir información de forma dinámica entre routers.
 - Actualizar las tablas de enrutamiento de forma automática cuando cambia la topología.
 - Determinar cuál es la mejor ruta a un destino.

Los routers envían las actualizaciones de manera dinámica



Protocolos de enrutamiento dinámico

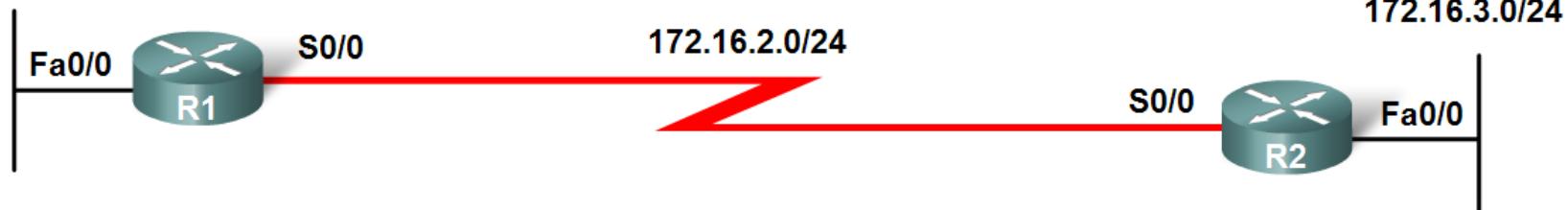
- El **objetivo de los protocolos de enrutamiento dinámico** es:

- Descubrir redes remotas
- Mantener la información de enrutamiento actualizada
- Seleccionar la mejor ruta a las redes de destino
- Brindar la funcionalidad necesaria para encontrar una nueva mejor ruta si la actual deja de estar disponible

Funcionamiento del protocolo de enrutamiento

Los protocolos de enrutamiento se utilizan para intercambiar información de enrutamiento entre los routers.

172.16.1.0/24



Protocolos de enrutamiento dinámico

- **Componentes de los protocolos de enrutamiento dinámico**

Algoritmo

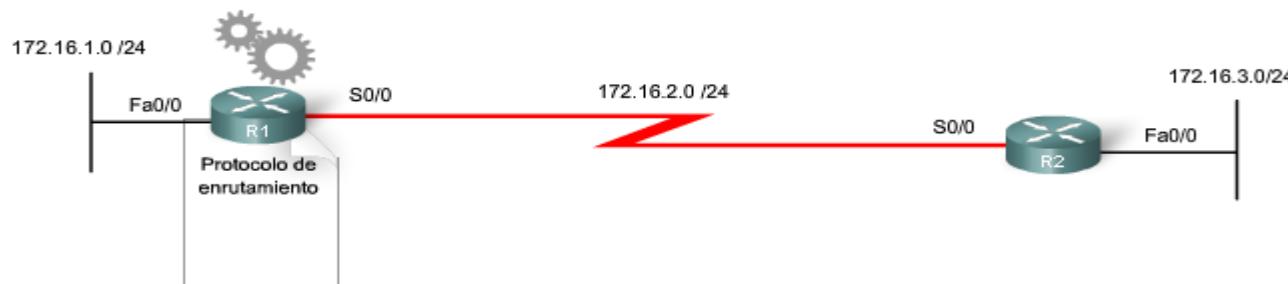
En el contexto de los protocolos de enrutamiento, los algoritmos se usan para facilitar información de enrutamiento y determinar la mejor ruta.

Mensajes de los protocolos de enrutamiento

Estos mensajes se utilizan para descubrir routers vecinos e intercambiar información de enrutamiento.

Funcionamiento del protocolo de enrutamiento

Los protocolos de enrutamiento se utilizan para intercambiar información de enrutamiento entre los routers.





Protocolos de enrutamiento dinámico

■ Ventajas del **enrutamiento estático**:

- Puede realizar copias de seguridad de varias interfaces o redes en un router
- Es fácil de configurar
- No se necesitan recursos adicionales
- Es más seguro

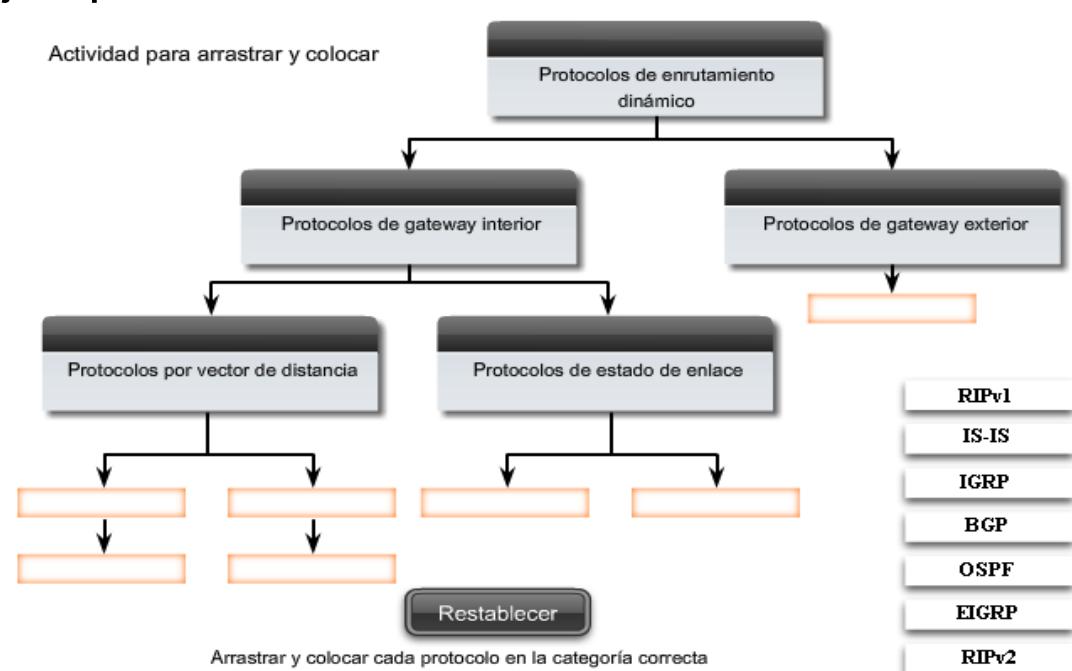
■ Desventajas del **enrutamiento estático**:

- Los cambios de la red requieren reconfiguraciones manuales.
- No permite una escalabilidad eficaz en topologías grandes

Clasificación de protocolos de enrutamiento

- Los protocolos de enrutamiento dinámico se agrupan según sus características. Por ejemplo:

- RIP
- IGRP
- EIGRP
- OSPF
- IS-IS
- BGP

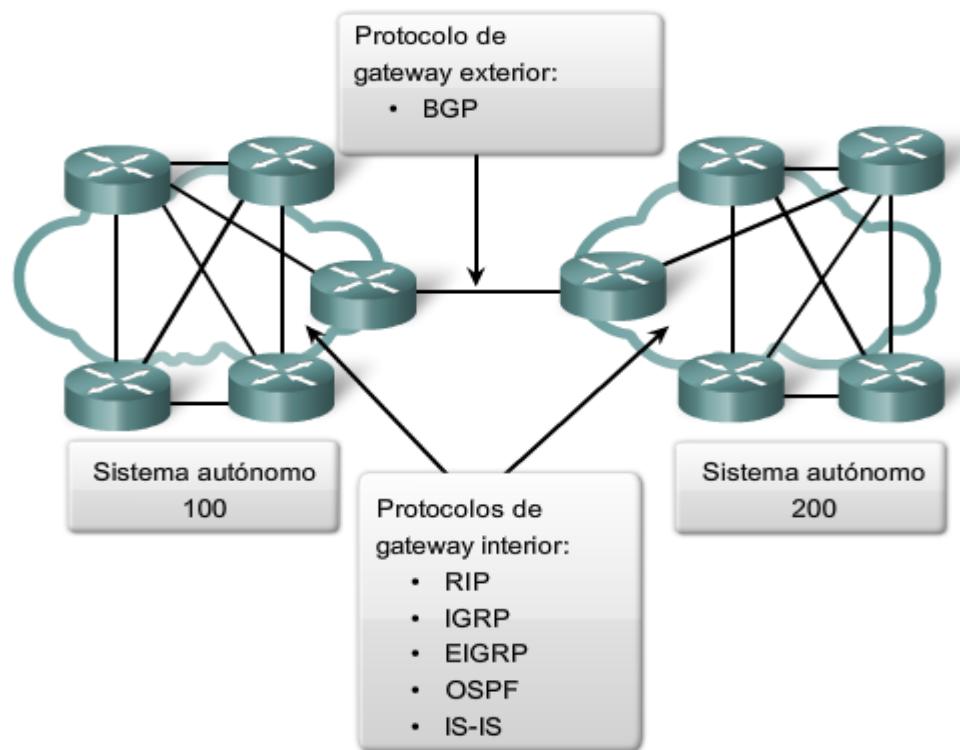


- Un sistema autónomo es un grupo de routers controlados por una autoridad única.

Clasificación de protocolos de enrutamiento

- Tipos de protocolos de enrutamiento:
 - Protocolos de gateway interiores (IGP)
 - Protocolos de gateway exterior (EGP)

Comparación entre protocolos de enrutamiento IGP y EGP





Clasificación de protocolos de enrutamiento

- **Protocolos de enrutamiento de gateway interior (IGP)**
 - Se usan para el enrutamiento dentro de un sistema autónomo y dentro de redes individuales
 - Por ejemplo: RIP, EIGRP, OSPF
- **Protocolos de enrutamiento exterior (EGP)**
 - Se usan para el enrutamiento entre sistemas autónomos
 - Por ejemplo: BGPv4

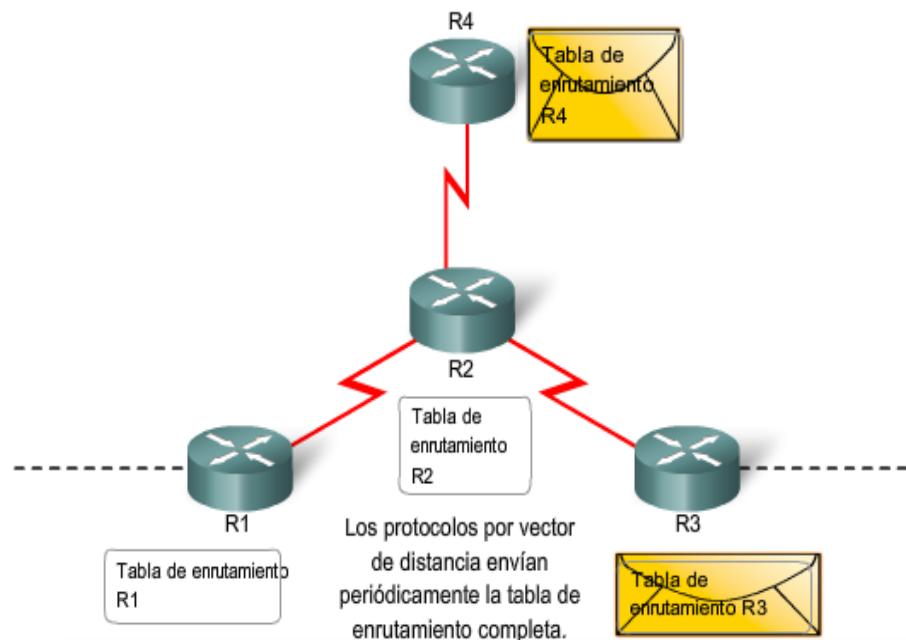
Clasificación de protocolos de enrutamiento

- IGP: **comparación de los** protocolos de enrutamiento **de vector de distancia** con los **de estado de enlace**

Vector de distancia

- Las rutas se anuncian como vectores de distancia y dirección
- Brinda una vista incompleta de la topología de la red
- Por lo general, se realizan actualizaciones periódicas

Funcionamiento del protocolo por vector de distancia

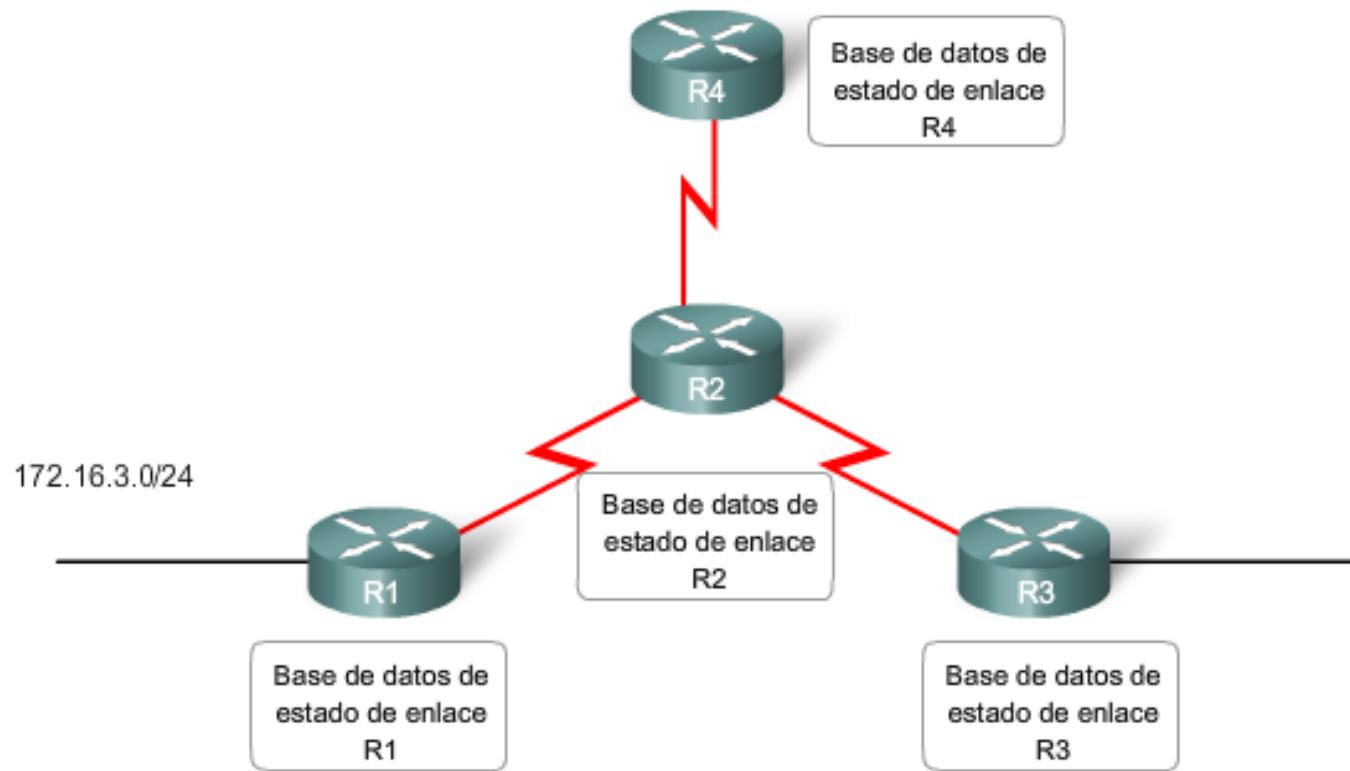


Estado de enlace

- Se crea una vista completa de la topología de la red
- Las actualizaciones no son periódicas

Clasificación de protocolos de enrutamiento

Funcionamiento del protocolo de estado de enlace



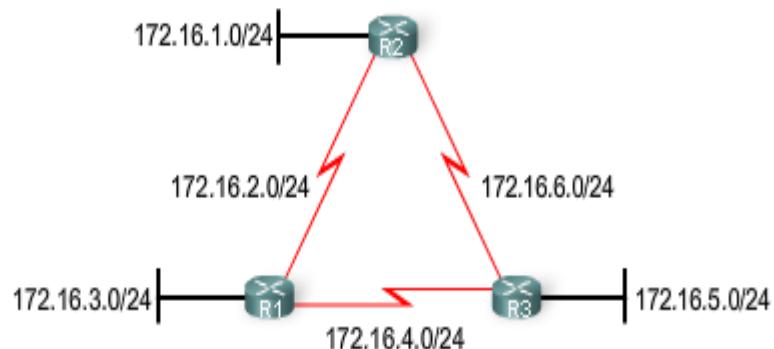
Los protocolos de estado de enlace envían actualizaciones cuando cambia el estado de un enlace.

Clasificación de protocolos de enrutamiento

Comparación entre enrutamiento con clase y sin clase

■ Protocolos de enrutamiento classful

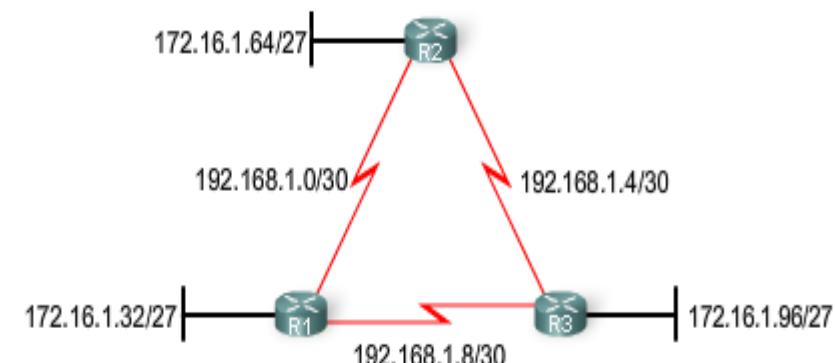
NO envían la máscara de subred durante las actualizaciones de enrutamiento



■ Protocolos de enrutamiento classless

Envían la máscara de subred durante las actualizaciones de enrutamiento

Con clase: La máscara de subred es la misma en toda la topología

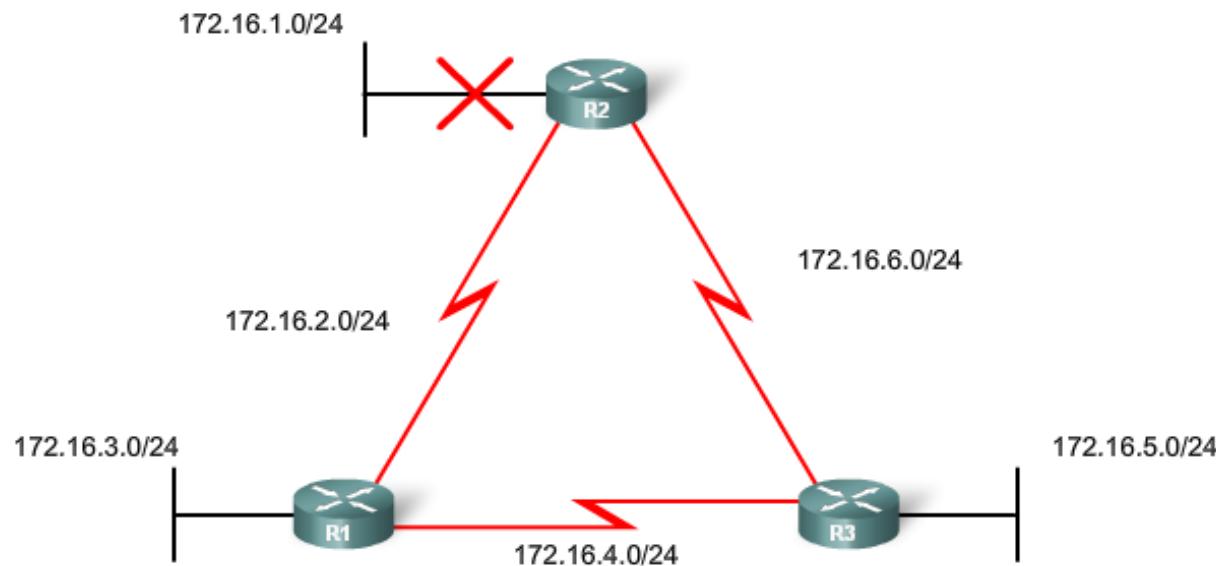


Sin clase: La máscara de subred puede variar en la topología

Clasificación de protocolos de enrutamiento

- **La convergencia** se define como el estado en el que las tablas de enrutamiento de todos los routers son uniformes

Comparación de convergencia



Convergencia más lenta: RIP y IGRP

Convergencia más rápida: EIGRP y OSPF

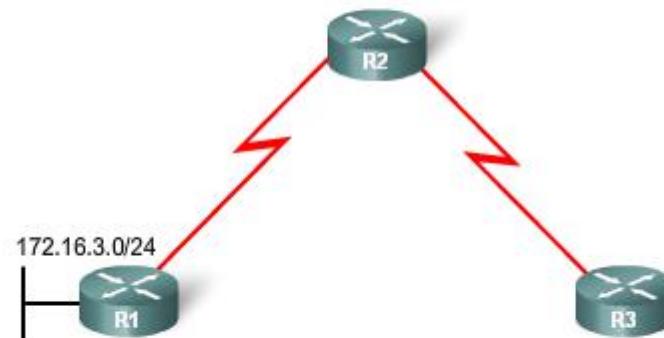
Métricas de los protocolos de enrutamiento

■ Métrica

Es un valor que usan los protocolos de enrutamiento para determinar qué rutas son mejores que otras.

Métrica

Red	Saltos
172.16.3.0	1



Red	Saltos
172.16.3.0	0

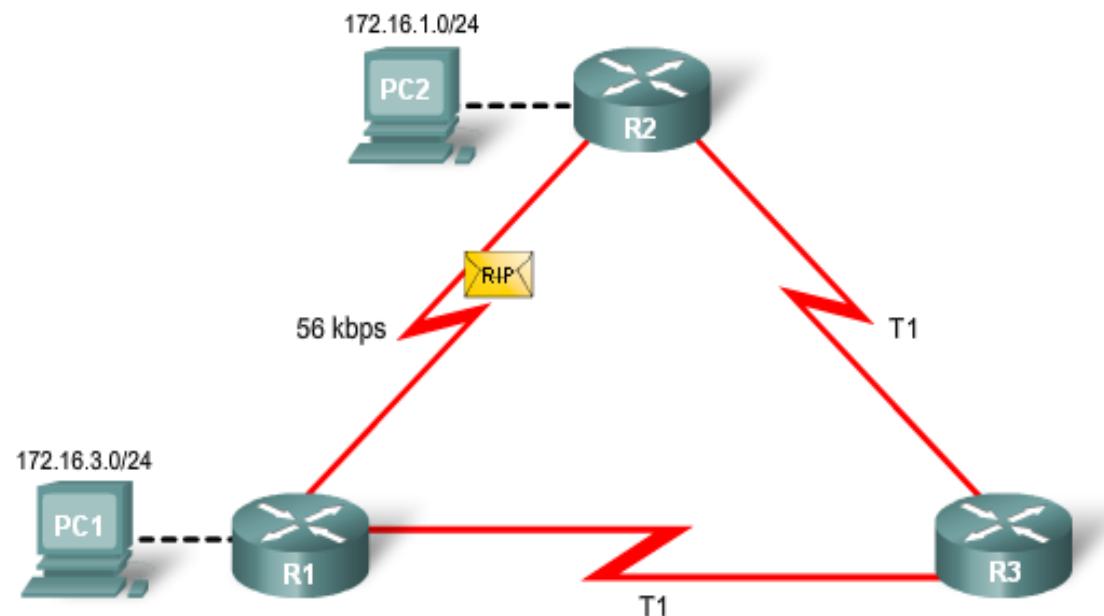
Red	Saltos
172.16.3.0	2

Métricas de los protocolos de enrutamiento

■ Métricas usadas en los protocolos de enrutamiento IP:

- Ancho de banda
- Costo
- Retraso
- Conteo de saltos
- Carga
- Confiabilidad

Comparación entre el conteo de saltos y el ancho de banda

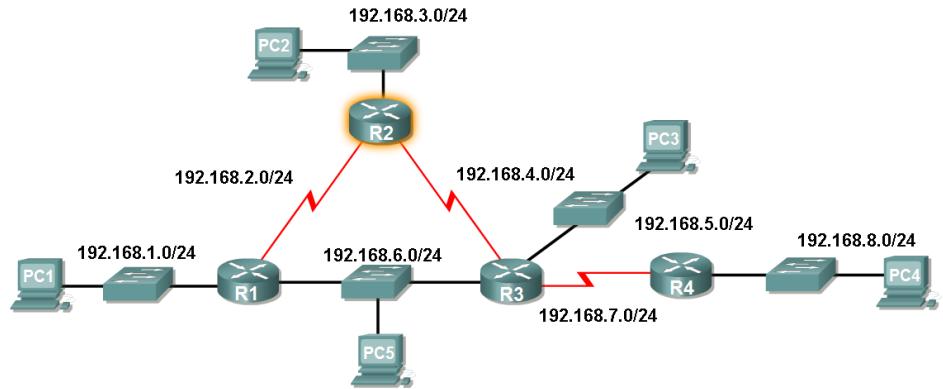


RIP dice la ruta más corta de acuerdo con el conteo de saltos.

OSPF dice la ruta más corta de acuerdo con el ancho de banda.

Métricas de los protocolos de enrutamiento

- El campo de métrica de la tabla de enrutamiento
- **Métrica** que se usa para cada **protocolo** de enrutamiento:
 - RIP: conteo de saltos
 - IGRP y EIGRP: ancho de banda (usado por defecto), retraso (usado por defecto), carga, confiabilidad
 - IS-IS y OSPF: costo, ancho de banda (implementación de Cisco)



```
R2#show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```
R  192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
C  192.168.2.0/24 is directly connected, Serial0/0
C  192.168.3.0/24 is directly connected, FastEthernet0/0
C  192.168.4.0/24 is directly connected, Serial0/1
R  192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R  192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
                                         [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R  192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R  192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/1
```

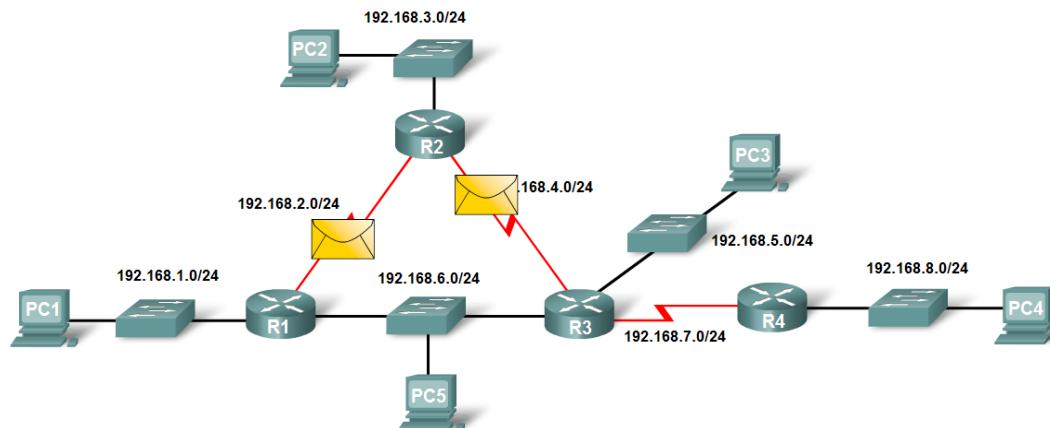
Son 2 saltos desde R2 a 192.168.8.0/24

Métricas de los protocolos de enrutamiento

■ Balanceo de carga

Ésta es la capacidad de un router de distribuir paquetes entre varias rutas de igual costo.

Balanceo de carga a través de rutas del mismo costo



```
R2#show ip route
<output omitted>
R    192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
                [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
```

Distancia administrativa de una ruta

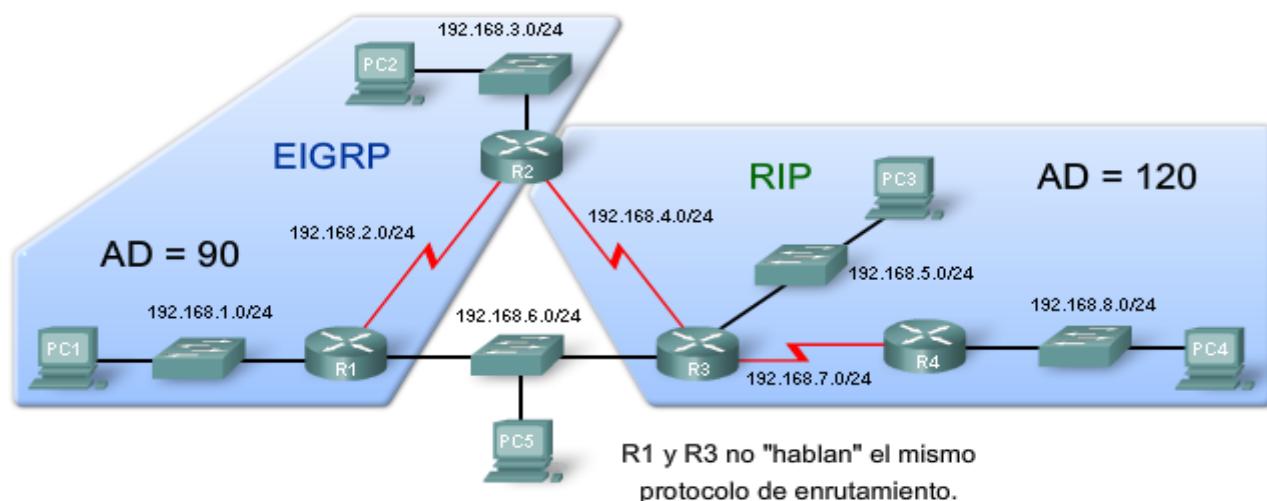
- **Objetivo de una métrica**

Es un valor calculado **que se usa para determinar la mejor ruta a un destino.**

- **Objetivo de la Distancia Administrativa**

Es un valor numérico que **especifica la preferencia por una ruta determinada.**

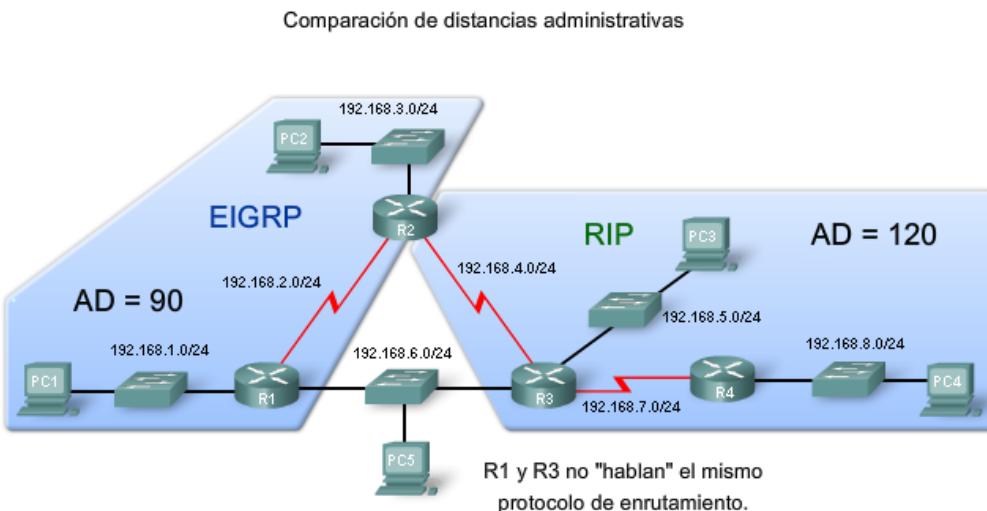
Comparación de distancias administrativas



Distancia administrativa de una ruta

- Identificación de la **Distancia Administrativa** (AD) en una tabla de enrutamiento

Es el **primer número del valor entre paréntesis** de la tabla de enrutamiento.



```
R2#show ip route
<output omitted>

Gateway of last resort is not set

D  192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C  192.168.2.0/24 is directly connected, Serial0/0/0
C  192.168.3.0/24 is directly connected, FastEthernet0/0
C  192.168.4.0/24 is directly connected, Serial0/0/1
R  192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D  192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R  192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R  192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

```
R2#show ip rip database
192.168.3.0/24    directly connected, FastEthernet0/0
192.168.4.0/24    directly connected, Serial0/0/1
192.168.5.0/24
[1] via 192.168.4.1, Serial0/0/1
192.168.6.0/24
[1] via 192.168.4.1, Serial0/0/1
192.168.7.0/24
[1] via 192.168.4.1, Serial0/0/1
192.168.8.0/24
[2] via 192.168.4.1, Serial0/0/1
```

Distancia administrativa de una ruta

- Protocolos de enrutamiento dinámico

Distancias administrativas predeterminadas

Origen de la ruta	Distancia administrativa
Conectado	0
Estática	1
Ruta sumarizada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Distancia administrativa de una ruta

- **Rutas conectadas directamente**

- Tienen una **AD por defecto de 0**

- **Rutas estáticas**

- La distancia administrativa de una ruta estática tiene un **valor por defecto de 1**

```
R2#show ip route 172.16.3.0
Routing entry for 172.16.3.0/24
Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
    * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1
```

Distancia administrativa de una ruta

■ Rutas conectadas directamente

- Aparecen de forma inmediata en la tabla de enrutamiento
apenas se configura la interfaz

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
C        172.16.1.0 is directly connected, FastEthernet0/0
C        172.16.2.0 is directly connected, Serial0/0/0
S        172.16.3.0 is directly connected, Serial0/0/0
C        192.168.1.0/24 is directly connected, Serial0/0/1
S        192.168.2.0/24 [1/0] via 192.168.1.1
```

Resumen

- **Los protocolos de enrutamiento dinámico tienen las siguientes funciones:**
 - Comparten información de forma dinámica entre routers.
 - Actualizan las tablas de enrutamiento de forma automática cuando cambia la topología.
 - Determinan cuál es la mejor ruta a un destino.
- **Los protocolos de enrutamiento se agrupan en:**
 - Protocolos de gateway interiores (IGP) o
 - Protocolos de gateway exterior (EGP)
- **Los tipos de IGP incluyen:**
 - Protocolos de enrutamiento classless: incluyen la máscara de subred durante las actualizaciones de enrutamiento.
 - Protocolos de enrutamiento classful: no incluyen la máscara de subred durante las actualizaciones de enrutamiento.



Resumen

- Los protocolos de enrutamiento dinámico usan **las métricas** para determinar la mejor ruta a un destino.
- **La distancia administrativa** es un valor entero que se usa para indicar la confiabilidad de un router.
- Entre los **componentes de una tabla de enrutamiento**, se encuentran:
 - Origen de la ruta
 - Distancia administrativa
 - Métrica



Protocolos de enrutamiento por vector de distancia



Conceptos y protocolos de enrutamiento. Capítulo 4



Objetivos

- Identificar las características de los protocolos de enrutamiento de vector de distancia.
- Describir el proceso de detección de redes de los protocolos de enrutamiento de vector de distancia por medio del uso del protocolo de información de enrutamiento (RIP).
- Describir los procesos que usan los protocolos de enrutamiento de vector de distancia para mantener tablas de enrutamiento precisas.
- Identificar las situaciones que ocasionan un bucle de enrutamiento y explicar las consecuencias para el rendimiento del router.
- Reconocer los protocolos de enrutamiento de vector de distancia usados en la actualidad.



Protocolos de enrutamiento de vector de distancia

- **Ejemplos de protocolos de enrutamiento de vector de distancia:**
 - Protocolo de información de enrutamiento (RIP)
 - Protocolo de enrutamiento de gateway interior (IGRP)
 - Protocolo de enrutamiento de gateway interior mejorado (EIGRP)



Protocolos de enrutamiento de vector de distancia

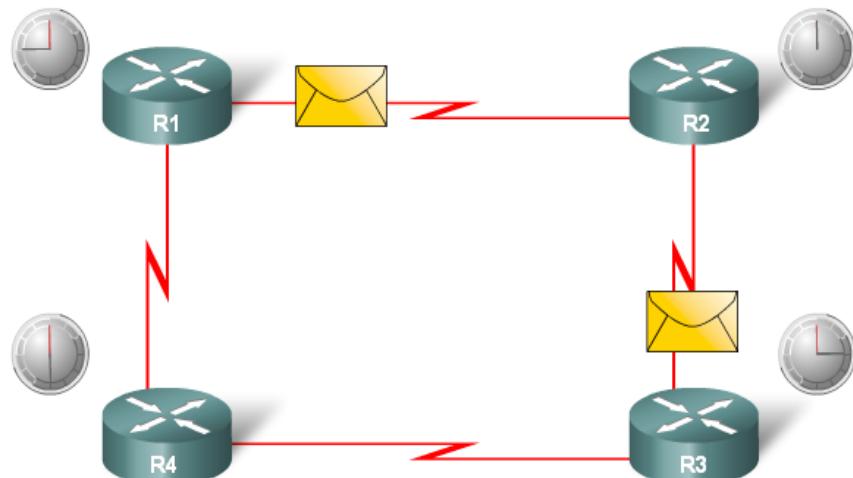
- Tecnología de vector de distancia
 - **Significado del vector de distancia:**
 - Un router que usa protocolos de enrutamiento de vector de distancia tiene información sobre 2 elementos:
 - La distancia al destino final
 - El vector, o la dirección, hacia donde deb dirigirse el tráfico

Protocolos de enrutamiento de vector de distancia

Características de los protocolos de enrutamiento de vector de distancia:

- Actualizaciones periódicas
- Vecinos
- Actualizaciones de broadcast
- Toda la tabla de enrutamiento se incluye en la actualización de enrutamiento

Actualizaciones periódicas del vector de distancia



Protocolos de enrutamiento de vector de distancia

- Algoritmos de los protocolos de enrutamiento:
 - Se define como un procedimiento para realizar cierta tarea



Red	Interfaz	Salto
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	S0/0/0	1

Red	Interfaz	Salto
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	Fa0/0	0
172.16.1.0/24	S0/0/0	1



Protocolos de enrutamiento de vector de distancia

Características de los protocolos de enrutamiento

- Los criterios que se usan para comparar protocolos de enrutamiento incluyen:
 - Tiempo de convergencia
 - Escalabilidad
 - Uso de recursos
 - Implementación y mantenimiento



Protocolos de enrutamiento de vector de distancia

Ventajas y desventajas de los protocolos de enrutamiento por vector de distancia

Ventajas:	Desventajas:
<p>Implementación y mantenimiento simples. No se requiere de mucho conocimiento para implementar y posteriormente mantener una red con protocolo por vector de distancia.</p>	<p>Convergencia lenta. La utilización de actualizaciones periódicas puede hacer que la convergencia sea más lenta. Incluso si se utilizan técnicas avanzadas, como por ejemplo, los updates disparados (que se analizarán más adelante), la convergencia general aún sigue siendo más lenta en comparación con los protocolos de enrutamiento de estado de enlace.</p>
<p>Pocos requisitos de recursos. Los protocolos por vector de distancia generalmente no requieren una gran cantidad de memoria para almacenar información. Tampoco requieren de una CPU muy potente. Dependiendo del tamaño de la red y del direccionamiento IP implementado, generalmente tampoco requieren de un alto nivel de ancho de banda de enlace para enviar actualizaciones de enrutamiento. Sin embargo, esto puede representar un problema si se implementa un protocolo por vector de distancia en una gran red.</p>	<p>Escalabilidad limitada. La convergencia lenta puede limitar el tamaño de la red porque las redes más grandes requieren más tiempo para propagar la información de enrutamiento.</p>
	<p>Routing loops. Los routing loops pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios.</p>

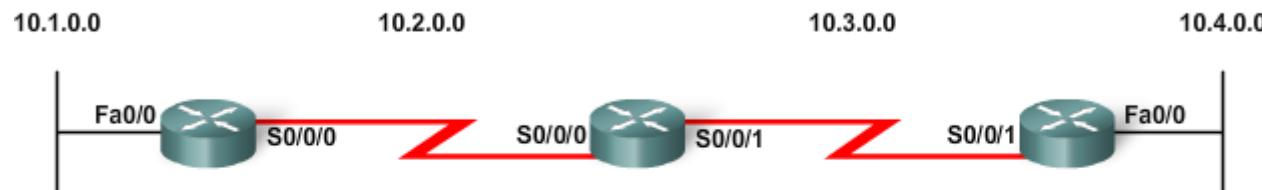
Detección de redes

- Inicio del router (arranque en frío)

- Detección inicial de redes

- Inicialmente, las redes conectadas directamente se agregan a la tabla de enrutamiento

Descubrimiento de red: arranque en frío



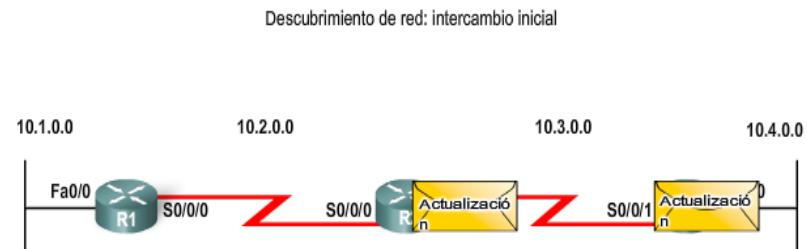
Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Detección de redes

- Intercambio inicial de información de enrutamiento
 - Si hay un protocolo de enrutamiento configurado:
 - Los routers intercambian información de enrutamiento
- Actualizaciones de enrutamiento recibidas de otros routers:
 - El router comprueba si hay actualizaciones de información nueva
 - Si hay información nueva:
 - Se actualiza la métrica
 - Se almacena la información nueva en la tabla de enrutamiento



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

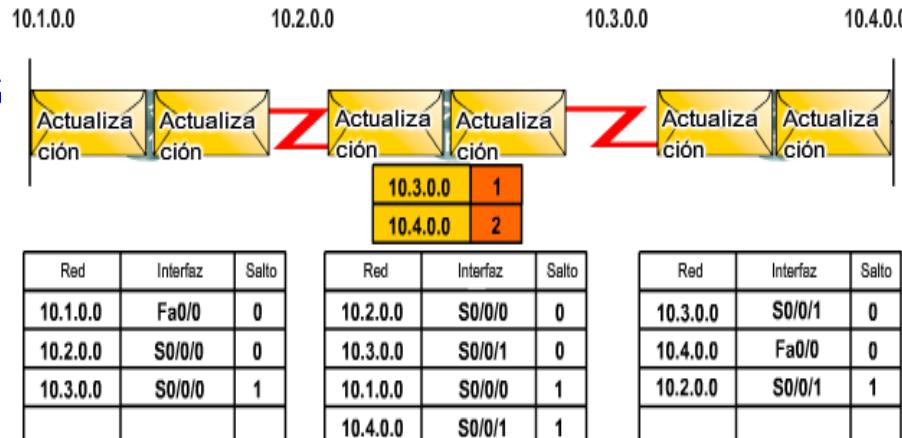
Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/0	0
10.4.0.0	Fa0/0	0

Detección de redes

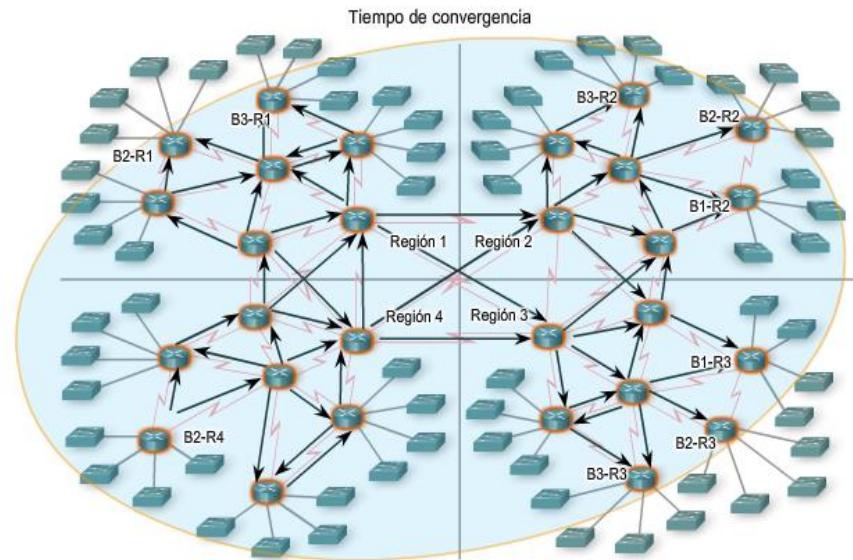
- Intercambio de información de enrutamiento
 - La convergencia de routers se logra cuando:
 - Todas las tablas de enrutamiento de la red contienen la misma información de la red
 - Los routers siguen intercambiando información de enrutamiento
 - Si no hay información nueva, significa que los routers son convergentes

Descubrimiento de red: siguiente actualización



Detección de redes

- **Para que se considere que la red funciona correctamente**, debe lograrse la convergencia
- La velocidad con la que se logra la convergencia está formada por 2 categorías independientes:
 - La velocidad con la que se hace broadcast de la información de enrutamiento
 - La velocidad con la que se calculan las rutas

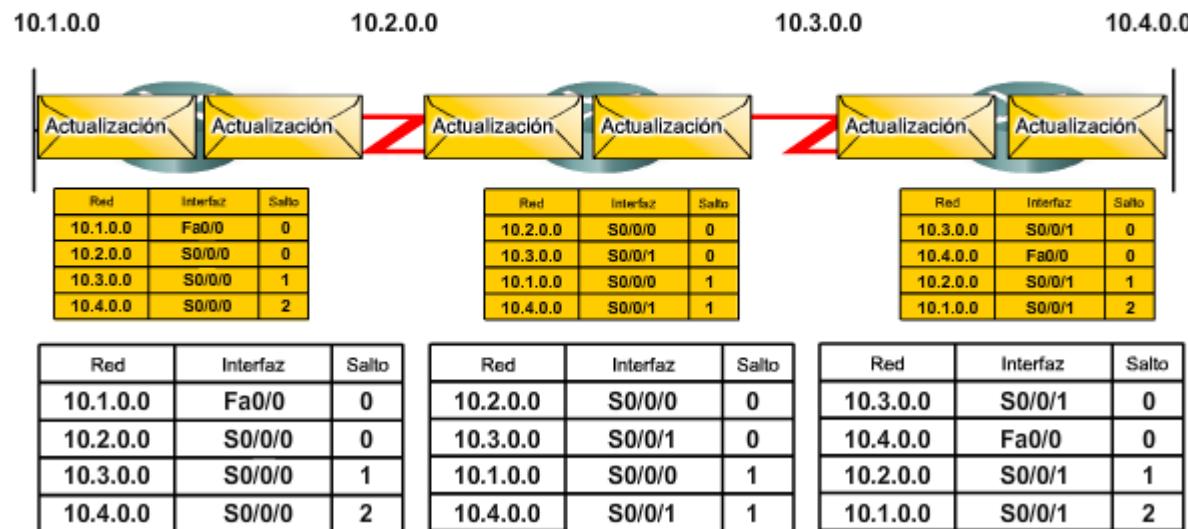


Mantenimiento de las tablas de enrutamiento

- **Actualizaciones periódicas:** RIPv1 y RIPv2

Son los **intervalos de tiempo** con los que un router envía la tabla de enrutamiento completa

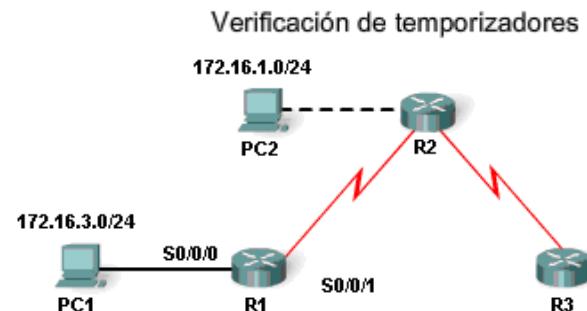
Actualizaciones periódicas



Mantenimiento de las tablas de enrutamiento

- RIP usa 4 temporizadores:

- Temporizador de actualizaciones
- Temporizador no válido
- Temporizador de espera
- Temporizador de purga



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

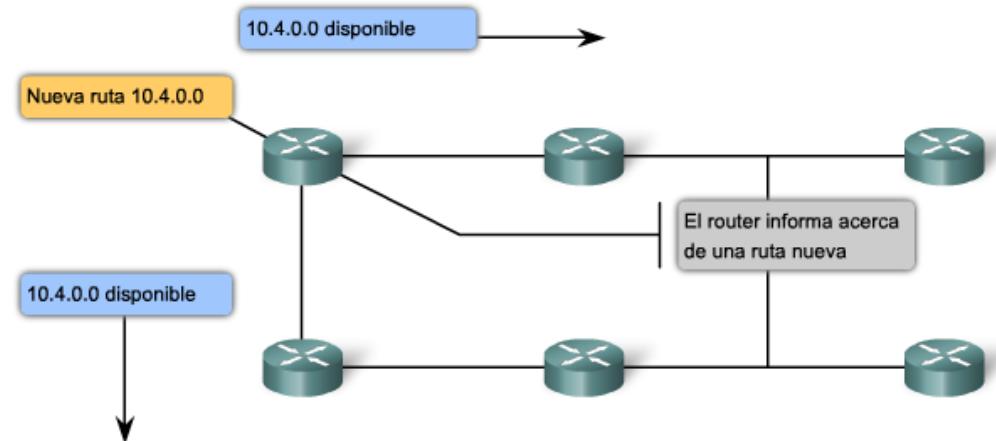
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
R        172.16.1.0 [120/1] via 172.16.2.2, 00:00:18, Serial0/0/0
C        172.16.2.0 is directly connected, Serial0/0/0
C        172.16.3.0 is directly connected, FastEthernet0/0
R        192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:27, Serial0/0/1
                                         [120/1] via 172.16.2.2, 00:00:18, Serial0/0/0
C        192.168.3.0/24 is directly connected, Serial0/0/1
R1#
```

Mantenimiento de las tablas de enrutamiento

- **Actualizaciones limitadas: EIGRP**
- Actualizaciones de enrutamiento EIRPG:
 - Son actualizaciones parciales
 - Se generan cuando se producen cambios en la topología
 - Son limitadas
 - No son periódicas

Actualizaciones limitadas: EIGRP



Mantenimiento de las tablas de enrutamiento

■ Updates disparados

- A continuación, se incluyen las situaciones en que se envían las actualizaciones generadas por eventos:
 - Cambio de estado de la interfaz
 - La ruta pasa a ser inalcanzable
 - Se agrega la ruta a la tabla de enrutamiento



Mantenimiento de las tablas de enrutamiento

■ Fluctuación aleatoria de fase

Actualizaciones sincronizadas

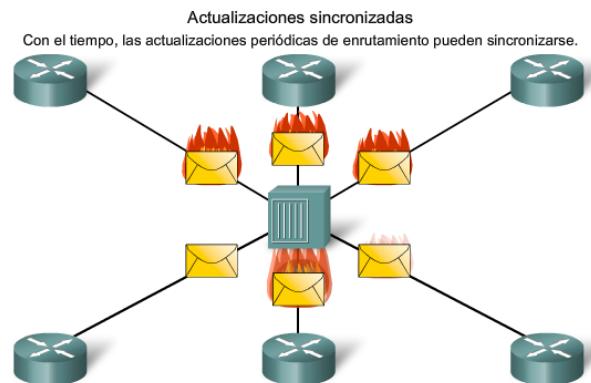
Ésta es una situación en la cual varios routers en segmentos LAN de acceso múltiple transmiten actualizaciones de enrutamiento al mismo tiempo.

■ Problemas de las actualizaciones sincronizadas:

- Utilización del ancho de banda
- Colisiones de paquetes

■ Resolución de problemas de las actualizaciones sincronizadas:

- Uso de variable aleatoria llamada RIP_JITTER (fluctuación aleatoria de fase)

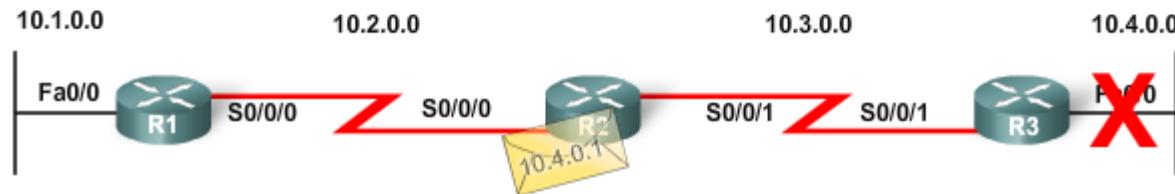


Bucles de enrutamiento

- Los bucles de enrutamiento constituyen una situación en la cual se transmite de forma continua un paquete dentro de una serie de routers, pero nunca llega al destino.

Bucles de enrutamiento

La red ahora tiene un loop.



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	2
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2



Bucles de enrutamiento

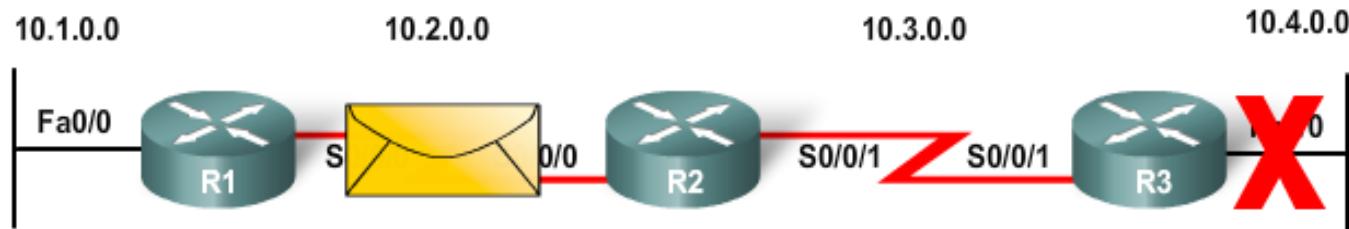
- Las causas de **los bucles de enrutamiento** pueden ser:
 - La configuración incorrecta de las rutas estáticas
 - La configuración incorrecta de la redistribución de rutas
 - La convergencia lenta
 - La configuración incorrecta de las rutas de descarte
- Los **bucles de enrutamiento** pueden ocasionar los siguientes problemas:
 - Uso excesivo del ancho de banda
 - Mayor exigencia de los recursos de la CPU
 - Convergencia de la red degradada
 - Es posible que se pierdan las actualizaciones de enrutamiento o que no se procesen oportunamente

Bucles de enrutamiento

■ Conteo al infinito

Éste es un bucle de enrutamiento que hace que los paquetes reboten continuamente en una red.

R2 envía una actualización a R1 con un conteo de saltos de 8 hacia la red 10.4.0.0.



10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	6

10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	7

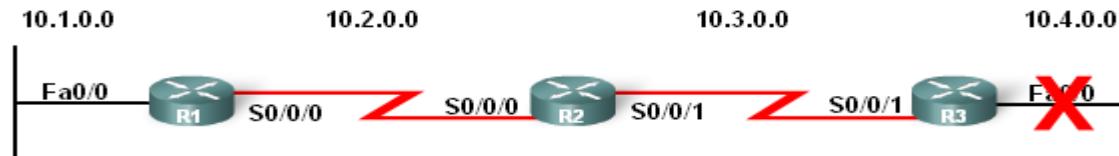
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	6
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Bucles de enrutamiento

- Establecimiento de un máximo
- **Los protocolos de enrutamiento de vector de distancia establecen un valor de métrica especificado para indicar el infinito**

Una vez que un router “cuenta al infinito”, marca la ruta como inalcanzable

10.4.0.0 es inalcanzable. El conteo de saltos es de 16.



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	16

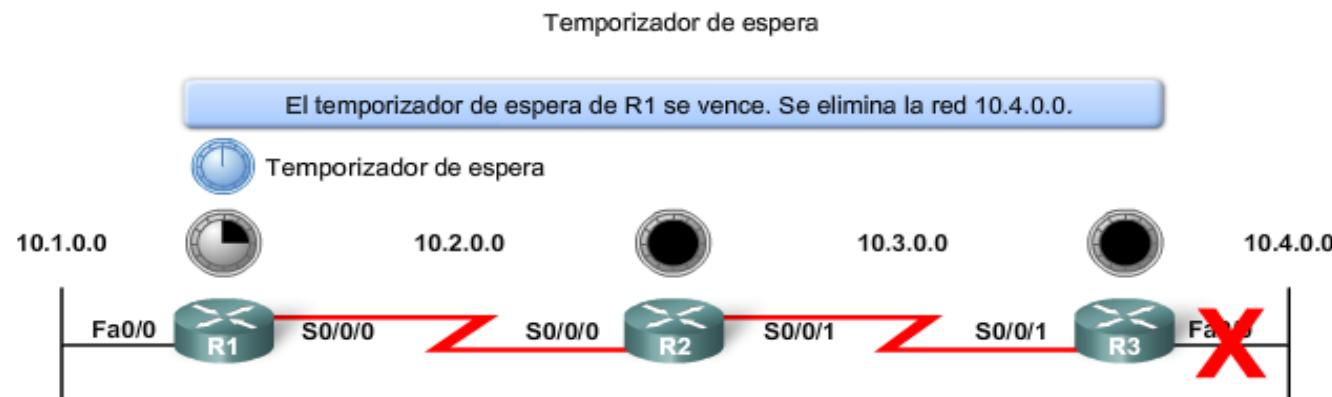
Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Bucles de enrutamiento

■ Prevención de bucles con temporizadores de espera

- Los temporizadores de espera permiten que un router rechace los cambios realizados a una ruta durante un período de tiempo especificado.
- Los temporizadores de espera se usan porque...
 - Permiten que las actualizaciones de enrutamiento se propaguen a través de la red con la información más actualizada.



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Bucles de enrutamiento

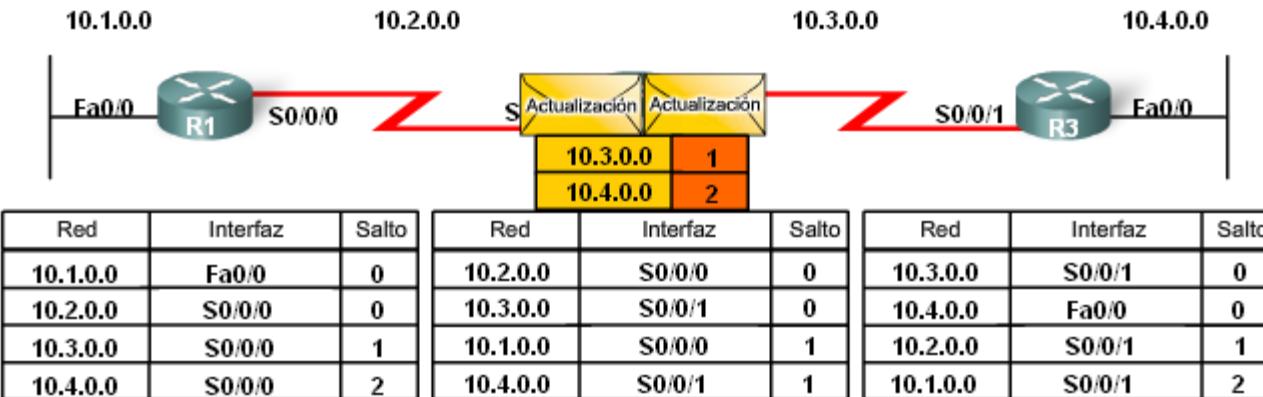
- La **regla de horizonte dividido** se usa para evitar que se produzcan bucles de enrutamiento.
- **Regla de horizonte dividido:**

Un router no debe anunciar una red a través de la interfaz por la cual ingresó la actualización.

Regla de horizonte dividido para la red 10.4.0.0

R2 sólo publica la red 10.3.0.0 y 10.4.0.0 a R1.

R2 sólo publica la red 10.2.0.0 y 10.1.0.0 a R3.



Bucles de enrutamiento

- **Horizonte dividido con envenenamiento en reversa**

Esta regla establece que, una vez que un router detecta una ruta inalcanzable a través de una interfaz, debe anunciar que es inalcanzable a través de la misma interfaz.

Envenenamiento de ruta

R3 "envenena" la ruta con una métrica "infinita".



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Red	Interfaz	Salto
10.1.0.0	S0/0/0	0
10.2.0.0	S0/0/1	0
10.3.0.0	S0/0/1	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.1.0.0	S0/0/1	0
10.2.0.0	Fa0/0	16
10.3.0.0	S0/0/1	1
10.4.0.0	Fa0/0	16

R2 "envenena" la ruta con una métrica "infinita".



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Red	Interfaz	Salto
10.1.0.0	S0/0/0	0
10.2.0.0	S0/0/1	0
10.3.0.0	S0/0/1	1
10.4.0.0	S0/0/1	16

Red	Interfaz	Salto
10.1.0.0	S0/0/1	0
10.2.0.0	Fa0/0	16
10.3.0.0	S0/0/1	1
10.4.0.0	Fa0/0	16



Bucles de enrutamiento

- IP y TTL
 - Función del campo TTL

El campo TTL se encuentra en los encabezados IP y se usa para evitar que los paquetes se transmitan a través de una red de forma indefinida.

- Funcionamiento del campo TTL
 - El campo TTL contiene un valor numérico

Cada router de la ruta hacia el destino disminuye este valor en un punto.

Si el valor numérico llega a 0, el paquete se descarta.

Protocolos de enrutamiento en la actualidad

- Los factores que se usan para determinar si se usa RIP o EIGRP incluyen:

- El tamaño de la red
- La compatibilidad entre modelos de routers
- Los conocimientos administrativos

Comparación de los protocolos de enrutamiento por vector de distancia

	Ripv1	Ripv2	IGRP	EIGRP
Velocidad de convergencia	Lento	Lento	Lento	Rápido
Escalabilidad: tamaño de la red	Pequeño	Pequeño	Pequeño	Grande
Uso de VLSM	No	Sí	No	Sí
Uso de recursos	Bajo	Bajo	Bajo	Medio
Implementación y mantenimiento	Simple	Simple	Simple	Complejo



Protocolos de enrutamiento en la actualidad

- **RIP**
 - **Características de RIP:**
 - Brinda soporte para las reglas de horizonte dividido y horizonte dividido con envenenamiento en reversa
 - Proporciona funcionalidades de balanceo de carga
 - Es fácil de configurar
 - Funciona en un entorno de routers de varios proveedores



Protocolos de enrutamiento en la actualidad

- **EIGRP**

- **Características de EIGRP:**

- Brinda actualizaciones generadas por eventos
 - Se utiliza el protocolo de saludo de EIGRP para establecer adyacencias con los vecinos
 - Brinda soporte para VLSM y summarización de rutas
 - Usa la tabla de topología para el mantenimiento de todas las rutas
 - Protocolo de enrutamiento de vector de distancia classless
 - Protocolo propietario de Cisco



Resumen

- **Características de los protocolos de enrutamiento de vector de distancia:**
 - Actualizaciones periódicas
 - Las actualizaciones de enrutamiento RIP incluyen toda la tabla de enrutamiento
 - Los routers vecinos son los que comparten un enlace y están configurados para que usen el mismo protocolo
- **Proceso de detección de redes para el protocolo de enrutamiento de vector de distancia**
 - Las rutas conectadas directamente se agregan primero a la tabla de enrutamiento
 - Si hay un protocolo de enrutamiento configurado...
 - Los routers intercambian información de enrutamiento
 - La convergencia ocurre cuando todos los routers de una red tienen la misma información de la red



Resumen

- **Los protocolos de enrutamiento de vector de distancia realizan el mantenimiento de las tablas de enrutamiento de la siguiente forma:**
 - RIP envía actualizaciones periódicas.
 - RIP usa 4 temporizadores diferentes para asegurar que la información sea precisa y que se logre la convergencia oportunamente.
 - EIGRP envía actualizaciones generadas por eventos.
- **Es posible que los protocolos de enrutamiento de vector de distancia sean propensos a generar bucles de enrutamiento:**
 - Los bucles de enrutamiento constituyen una situación en la cual los paquetes se transmiten de forma continua a través de la red.
 - Los mecanismos que se usan para minimizar los bucles de enrutamiento incluyen la definición del conteo de saltos máximo, los temporizadores de espera, la regla de horizonte dividido, el envenenamiento de ruta y las actualizaciones generadas por eventos.



Resumen

- **Las situaciones que pueden generar bucles de enrutamiento incluyen:**
 - Configuración incorrecta de las rutas estáticas
 - Configuración incorrecta de la redistribución de rutas
 - Convergencia lenta
 - Configuración incorrecta de las rutas de descarte
- **Los bucles de enrutamiento pueden afectar el rendimiento de la red de la siguiente forma:**
 - Uso excesivo del ancho de banda
 - Mayor exigencia de los recursos de la CPU
 - Convergencia de la red degradada
 - Es posible que se pierdan las actualizaciones de enrutamiento o que no se procesen



Resumen

- **Protocolo de información de enrutamiento (RIP)**

Es un protocolo de vector de distancia que tiene 2 versiones

RIPv1: protocolo de enrutamiento classful

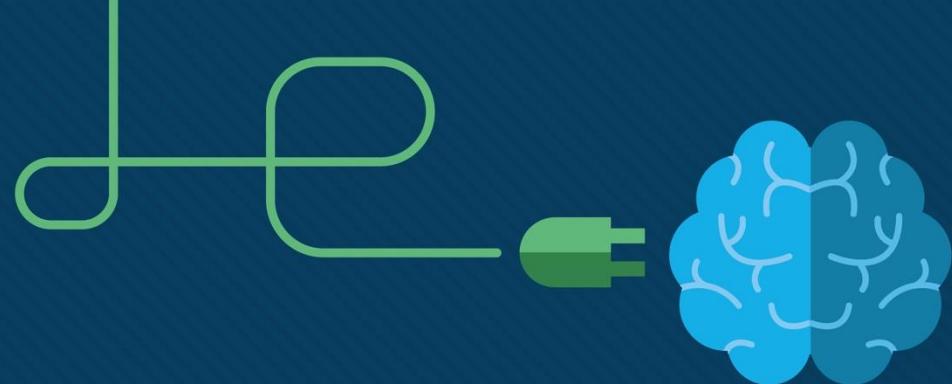
RIPv2: protocolo de enrutamiento classless

- **Protocolo de enrutamiento de gateway interna mejorada (EIGRP)**

- Es un protocolo de enrutamiento de vector de distancia que tiene ciertas características de los protocolos de enrutamiento de estado de enlace

- Es un protocolo propietario de Cisco





Módulo 12: Conceptos de WLAN

Switching, Routing y Wireless Essentials v7.0
(SRWE)



Objetivos del Módulo

Título del módulo: Conceptos de WLAN

Objetivo del módulo: Explivar cómo las WLAN habilitan la conectividad de red.

Título del Tema	Objetivo del Tema
Introducción a la Tecnología Inalámbrica	Describir la tecnología y los estándares WLAN.
Componentes de las WLAN	Describir los componentes de una infraestructura WLAN.
Funcionamiento de WLAN	Explicar cómo la tecnología inalámbrica permite el funcionamiento de WLAN.
Funcionamiento de CAPWAP	Explicar cómo un WLC utiliza CAPWAP para administrar múltiples AP.
Administración de Canales	Describir la administración de canales en una WLAN.
Amenazas a la WLAN	Describir las amenazas a las WLAN.
WLAN Seguras	Describir los mecanismos de seguridad de WLAN.

12.1 - Introducción a la Tecnología Inalámbrica

Beneficios de la Tecnología Inalámbrica

- Una LAN Inalámbrica (WLAN) es un tipo de red inalámbrica que se usa comúnmente en hogares, oficinas y entornos de campus.
- Las WLAN hacen posible la movilidad dentro de los entornos domésticos y comerciales.
- Las infraestructuras inalámbricas se adaptan a las necesidades y tecnologías que cambian rápidamente.



Introducción a la Tecnología Inalámbrica

Tipos de Redes Inalámbricas

- **Red Inalámbrica de Área Personal (WPAN)** – Baja potencia y corto alcance (20-30 pies o 6-9 metros). Basado en el estándar IEEE 802.15 y una frecuencia de 2.4 GHz. Bluetooth y Zigbee son ejemplos de WPAN.
- **LAN Inalámbrica (WLAN)** – Redes de tamaño mediano de hasta aproximadamente 300 pies. Basado en el estándar IEEE 802.11 y una frecuencia de 2.4 GHz o 5.0 GHz.
- **Wireless MAN (WMAN)** – Gran área geográfica, como ciudad o distrito. Utiliza frecuencias específicas con licencia.
- **WAN inalámbrica (WWAN)** – Área geográfica extensa para la comunicación nacional o global. Utiliza frecuencias específicas con licencia.

Introducción a la Tecnología Inalámbrica

Tecnologías Inalámbricas

Bluetooth – Estándar IEEE WPAN utilizado para emparejar dispositivos a una distancia de hasta 300 pies (100 m).

- Bluetooth de Baja Energía (BLE) - Admite topología de malla para dispositivos de red a gran escala.
- Bluetooth velocidad básica/mejorada (BR / EDR) - Admite topologías punto a punto y está optimizada para la transmisión de audio.

WiMAX (Interoperabilidad mundial para acceso por microondas) – Conexiones alternativas a Internet de banda ancha por cable. IEEE 802.16 WLAN estándar para hasta 30 millas (50 km).



Introducción a la Tecnología Inalámbrica

Tecnologías Inalámbricas (Cont.)

Banda Ancha celular – Transporte de voz y datos. Usado por teléfonos, automóviles, tabletas y computadoras portátiles.

- Global System of Mobile (GSM) – Reconocido internacionalmente
- Code Division Multiple Access (CDMA) – Principalmente utilizado en los Estados Unidos.

Banda ancha satelital – Utiliza una antena parabólica direccional alineada con el satélite en órbita geoestacionaria. Necesita una línea clara del sitio. Normalmente se usa en ubicaciones rurales donde el cable y el DSL no están disponibles.



Introducción a la Tecnología Inalámbrica

Estándares 802.11

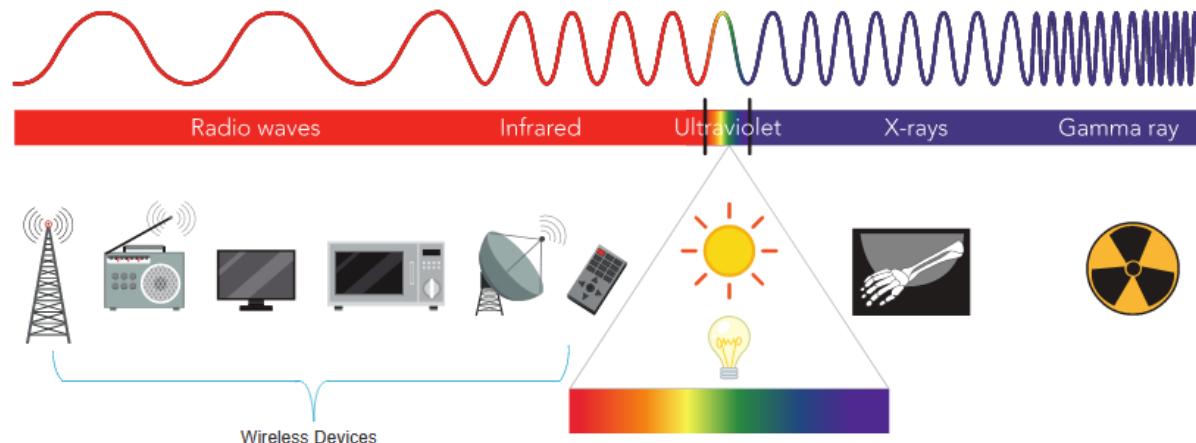
Los estándares 802.11 WLAN definen cómo se usan las frecuencias de radio para los

Estándar IEEE	Frecuencias de radio	Descripción
802.11	2,4 GHz	Velocidades de datos de hasta 2 Mb/s
802.11a	5 GHz	Velocidades de datos de hasta 54 Mb / s No interoperable con 802.11b o 802.11g
802.11b	2,4 GHz	Velocidades de datos de hasta 11 Mb / s Mayor alcance que 802.11a y mejor penetración en las estructuras de los edificios.
802.11g	2,4 GHz	Velocidades de datos de hasta 54 Mb / s Compatible con versiones anteriores de 802.11b
802.11n	2,4 Hz y 5 GHz	Velocidades de datos 150 - 600 Mb/s Requiere múltiples antenas con tecnología MIMO
802.11ac	5 GHz	Velocidades de datos 450 Mb/s – 1.3 Gb/s Admite hasta ocho antenas
802.11ax	2,4 GHz y 5 GHz	High-Efficiency Wireless (HEW) Capaz de usar frecuencias de 1 GHz y 7 GHz

Radio Frecuencias

Todos los dispositivos inalámbricos funcionan en el rango del espectro electromagnético. Las redes WLAN funcionan en bandas de frecuencia de 2,4 y 5 GHz.

- 2.4 GHz (UHF) - 802.11b/g/n/ax
- 5 GHz (SHF) – 802.11a/n/ac/ax



Organizaciones de Estándares Inalámbricos

Los estándares aseguran la interoperabilidad entre dispositivos fabricados por diferentes fabricantes. A nivel internacional, las tres organizaciones que influyen en los estándares WLAN:

- **International Telecommunication Union (UIT)**: – Regula la asignación del espectro radioeléctrico y las órbitas satelitales.
- **Institute of Electrical and Electronics Engineers (IEEE)** – Especifica cómo se modula una frecuencia de radio para transportar información. Mantiene los estándares para redes de área local y metropolitana (MAN) con la familia de estándares IEEE 802 LAN / MAN.
- **Alianza Wi-Fi** – Promueve el crecimiento y la aceptación de las WLAN. Es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de los productos que se basan en el estándar 802.1

12.2 - Componentes de la WLAN

Video – Componentes de WLAN

Este video cubrirá lo siguiente:

- Antenas
- Router inalámbrico
- Puerto de Internet
- Punto de acceso inalámbrico
- Puntos de acceso autónomos y basados en controlador

Componentes WLAN NICs inalámbrica

Para comunicarse de forma inalámbrica, las computadoras portátiles, tabletas, teléfonos inteligentes e incluso los últimos automóviles incluyen NIC inalámbricas integradas que incorporan un transmisor / receptor de radio.

Si un dispositivo no tiene una NIC inalámbrica integrada, se puede utilizar un adaptador inalámbrico USB.



Router de Hogar Inalámbrico

Un usuario doméstico generalmente interconecta dispositivos inalámbricos utilizando un pequeño router inalámbrico.

Los routers inalámbricos sirven de la siguiente manera:

- **Punto de acceso** – Para proporcionar acceso por cables
- **Switch** – Para interconectar dispositivos cableados
- **Router** - Para proporcionar una puerta de enlace predeterminada a otras redes e Internet



Punto de acceso inalámbrico

Los clientes inalámbricos usan su NIC inalámbrica para descubrir puntos de acceso cercanos (APs).

Los clientes luego intentan asociarse y autenticarse con un AP.

Después de la autenticación, los usuarios inalámbricos tienen acceso a los recursos de la red.



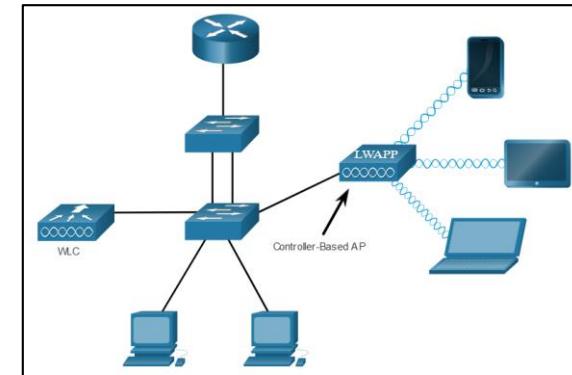
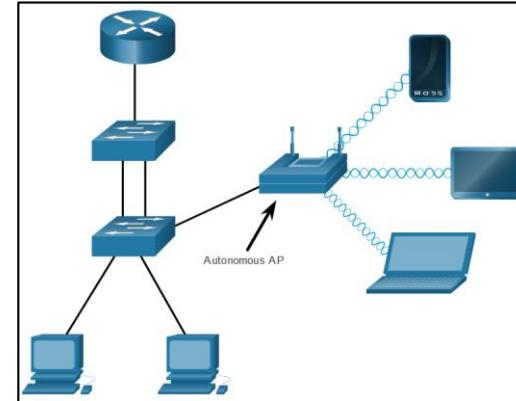
Puntos de acceso Cisco
Meraki Go

Componentes WLAN

Categorías AP

Los AP se pueden categorizar como AP autónomos o AP basados en controladores.

- **AP autónomos** – Dispositivos independientes configurados a través de una interfaz de línea de comandos o GUI. Cada AP autónomo actúa independientemente de los demás y es configurado y administrado manualmente por un administrador.
- **APs basados en controlador** – También conocidos como AP ligeros (LAPs). Utilice el Protocolo de punto de acceso ligero (LWAPP) para comunicarse con un controlador LWAN (WLC). Cada LAP es configurado y administrado automáticamente por el WLC.



Componentes WLAN

Antenas Inalámbricas

Tipos de antenas externas:

- **Omnidireccional**– Proporcionan cobertura de 360 grados. Ideal en áreas de viviendas y oficinas.
- **Direccional**– Enfoca la señal de radio en una dirección específica. Ejemplos son el Yagi y el plato parabólico.
- **Multiple Input Multiple Output (MIMO)** – Utiliza múltiples antenas (hasta ocho) para aumentar el ancho de banda.



12.3 – Funcionamiento de la WLAN

Video – Funcionamiento de la WLAN

Este video cubrirá lo siguiente:

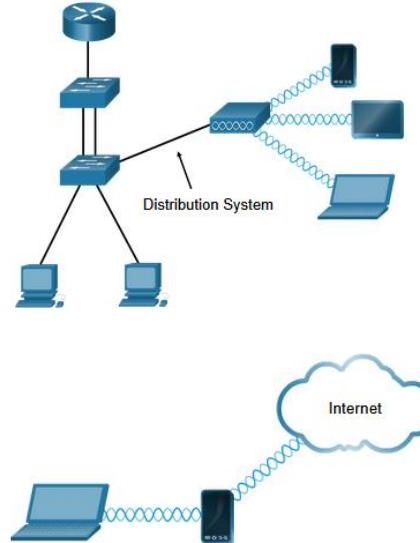
- Modo infraestructura
- Modo ad hoc
- Anclaje a red
- Conjunto de servicios básicos (BSS)
- Conjunto de servicios extendidos (ESS)
- 802.11 Estructura del Frame
- Acceso múltiple por detección de portadora con prevención de colisiones (Carrier Sense Multiple Access Collision Avoidance, CSMA/CA)
- Asociación del cliente AP inalámbrico
- Modo de Entrega Pasiva y Activa

802.11 Modos de topología inalámbrica

Modo ad hoc - Se utiliza para conectar clientes de igual a igual sin un AP.



Modo de infraestructura - Se usa para conectar clientes a la red utilizando un AP.



Tethering - La variación de la topología ad hoc es cuando un teléfono inteligente o tableta con acceso a datos móviles está habilitado para crear un punto de acceso personal.

Operación de WLAN BSS y ESS

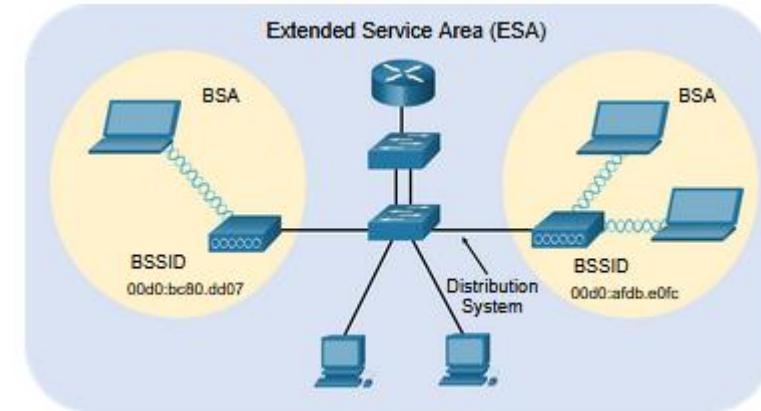
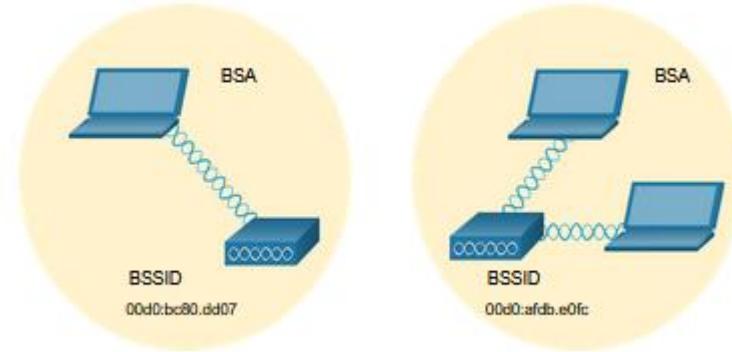
El modo de infraestructura define dos bloques de topología:

Conjunto de Servicios Básicos (BSS)

- Utiliza un AP único para interconectar todos los clientes inalámbricos asociados.
- Los clientes en diferentes BSS no pueden comunicarse.

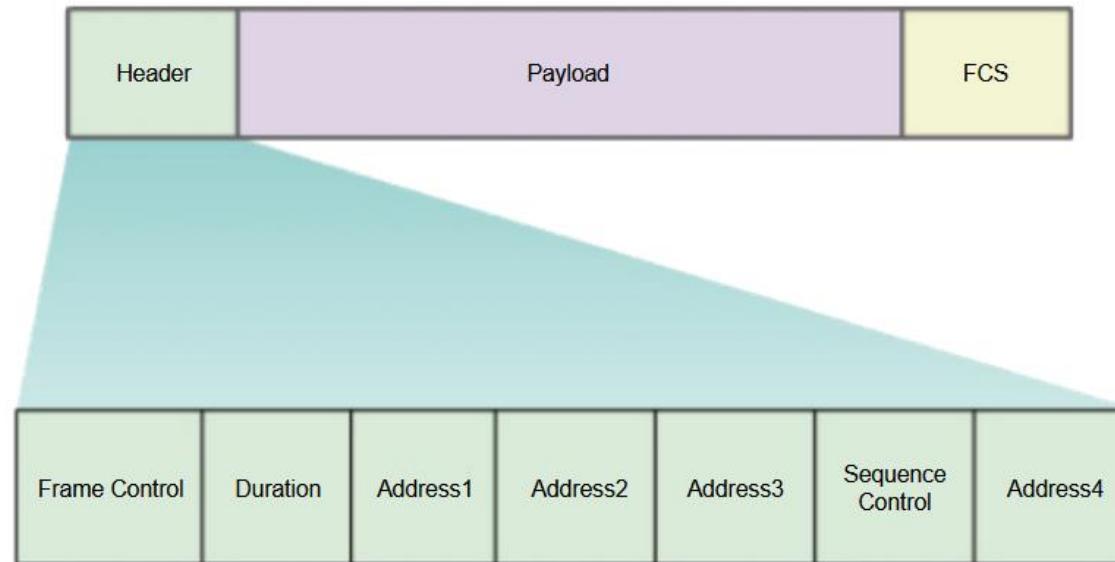
Conjunto de Servicios Extendidos (ESS)

- Una unión de dos o más BSS interconectados por un sistema de distribución por cable.
- Los clientes en cada BSS pueden comunicarse a través del ESS.



802.11 Estructura de trama

El formato de trama 802.11 es similar al formato de trama de Ethernet, excepto que contiene más campos.



Operación de WLAN CSMA/CA

Las WLAN son semidúplex y un cliente no puede "escuchar" mientras envía, por lo que es imposible detectar una colisión.

Las WLAN utilizan el acceso múltiple con detección de operador con evitación de colisiones (CSMA / CA) para determinar cómo y cuándo enviar datos. Un cliente inalámbrico hace lo siguiente:

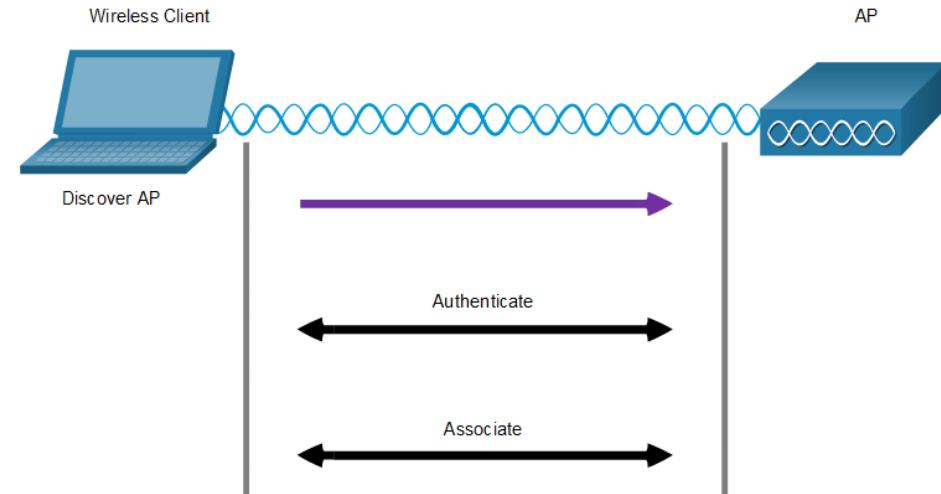
1. Escucha el canal para ver si está inactivo, es decir, no hay otro tráfico actualmente en el canal.
2. Envía un mensaje Ready to Send (RTS) al AP para solicitar acceso dedicado a la red.
3. Recibe un mensaje Clear to Send (CTS) del AP que otorga acceso para enviar.
4. Espera una cantidad de tiempo aleatoria antes de reiniciar el proceso si no se recibe un mensaje CTS.
5. Transmite los datos.
6. Reconoce todas las transmisiones. Si un cliente inalámbrico no recibe el reconocimiento, supone que ocurrió una colisión y reinicia el proceso.

Cliente Inalámbrico y Asociación AP

Para que los dispositivos inalámbricos se comuniquen a través de una red, primero se deben asociar a un AP o un router inalámbrico.

Los dispositivos inalámbricos completan las tres etapas del siguiente proceso:

- Descubre un AP inalámbrico
- Autenticar el AP
- Asociarse con el AP



Cliente Inalámbrico y Asociación AP(Cont.)

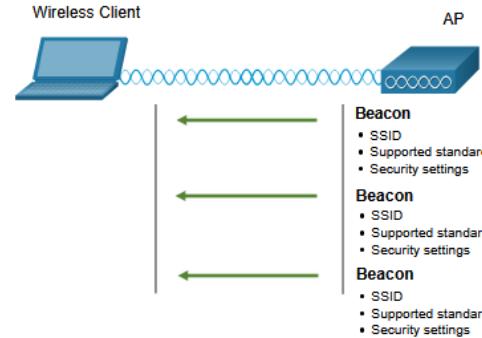
Para lograr una asociación exitosa, un cliente inalámbrico y un AP deben aceptar parámetros específicos:

- **SSID** – El cliente necesita saber el nombre de la red para conectarse.
- **Contraseña** – Esto es necesario para que el cliente se autentique en el AP.
- **Modo de red** – El estándar 802.11 en uso.
- **Modo de Seguridad** – La configuración de los parámetros de seguridad, es decir, WEP, WPA o WPA2.
- **Configuraciones de canal** – Las bandas de frecuencia en uso.

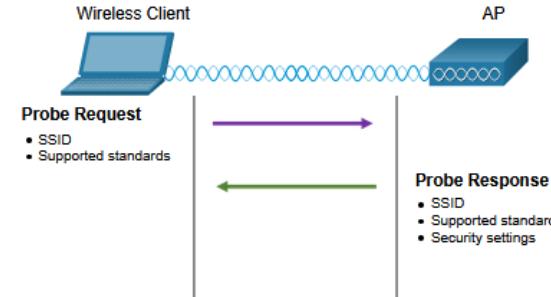
Modo de entrega Pasiva y Activa

Los clientes inalámbricos se conectan al AP mediante un proceso de escaneo (sondeo) pasivo o activo.

- **Modo pasivo:** el AP anuncia abiertamente su servicio enviando periódicamente tramas de señal de difusión que contienen el SSID, los estándares admitidos y la configuración de seguridad.
- **Modo activo :** los clientes inalámbricos deben conocer el nombre del SSID. El cliente inalámbrico inicia el proceso al transmitir por difusión una trama de solicitud de sondeo en varios canales.



Modo pasivo



Modo activo

12.4 - Funcionamiento de la CAPWAP

Operación de la CAPWAP

Video – CAPWAP

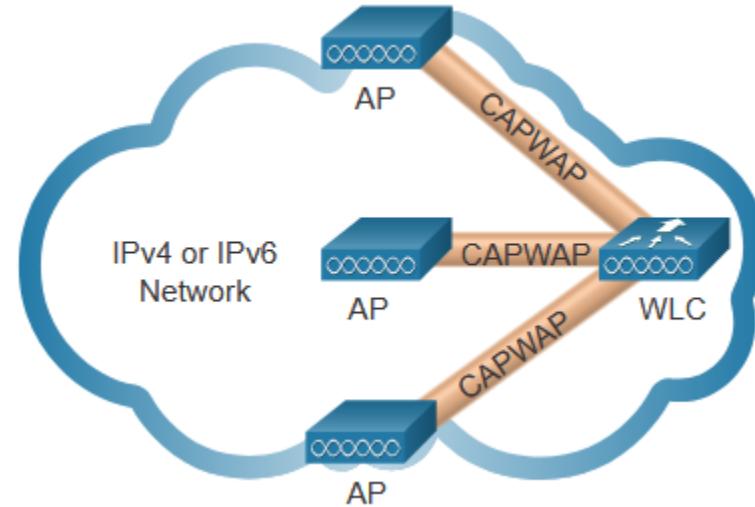
Este video cubrirá lo siguiente:

- Función de control y aprovisionamiento de puntos de acceso inalámbrico (CAPWAP)
- Arquitectura de control de acceso a medios divididos (MAC)
- Encriptación de DTLS
- Conexión flexible a AP

Operación de la CAPWAP

Introducción a CAPWAP

- CAPWAP es un protocolo estándar IEEE que permite que un WLC administre múltiples AP y WLAN.
- Basado en LWAPP pero agrega seguridad adicional con Datagram Transport Layer Security (DLTS).
- Encapsula y reenvía el tráfico del cliente WLAN entre un AP y un WLC a través de túneles utilizando los puertos UDP 5246 y 5247.
- Opera sobre IPv4 e IPv6. IPv4 usa el protocolo IP 17 e IPv6 usa el protocolo IP 136.



Operación de la CAPWAP

Arquitectura MAC dividida

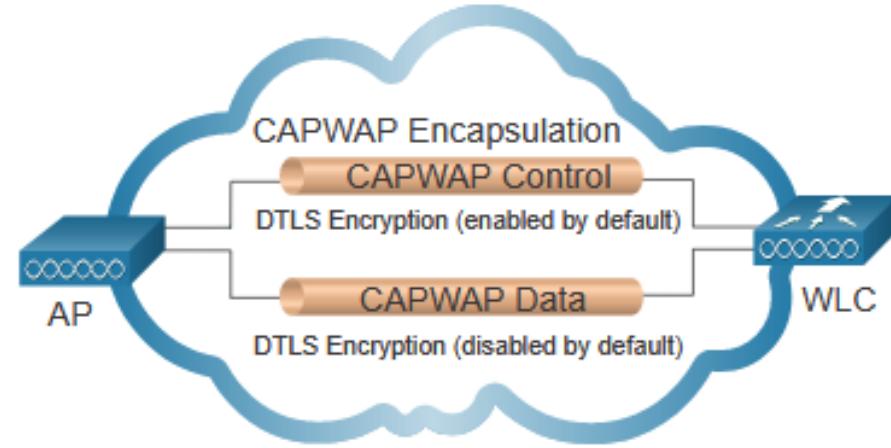
El concepto CAPWAP split MAC realiza todas las funciones que normalmente realizan los AP individuales y las distribuye entre dos componentes funcionales:

- AP Funciones MAC
- Funciones WLC MAC

AP Funciones MAC	Funciones WLC MAC
Beacons y respuestas probe	Autenticación.
Reconocimientos de paquetes y retransmisiones	Asociación y re-asociación de clientes itinerantes.
Cola de Frame y priorización de paquetes	Traducción de Frames a otros protocolos.
Cifrado y descifrado de datos de capa MAC	Terminación del tráfico 802.11 en una interfaz cableada.

Operación de CAPWAP Cifrado DTLS

- DTLS proporciona seguridad entre el AP y el WLC.
- Está habilitado de manera predeterminada para proteger el canal de control CAPWAP y cifrar todo el tráfico de administración y control entre AP y WLC.
- El cifrado de datos está deshabilitado de manera predeterminada y requiere que se instale una licencia DTLS en el WLC antes de que se pueda habilitar en el AP.



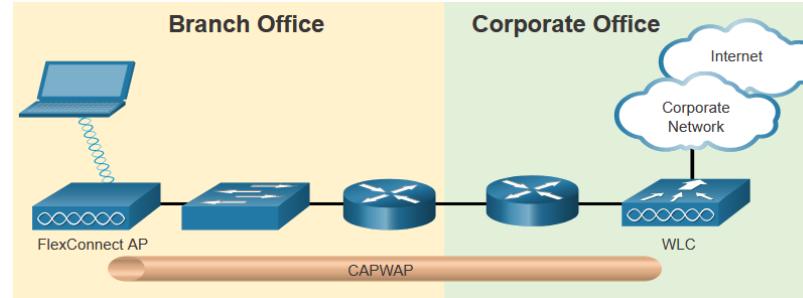
Operación de CAPWAP

Conexión flexible a AP

FlexConnect permite la configuración y el control de Aps a través de un enlace WAN.

Hay dos modos de opción para la Conexión flexible a AP:

- **Modo conectado** – El WLC es accesible. La Conexión flexible a AP tiene conectividad CAPWAP con el WLC a través del túnel CAPWAP. El WLC realiza todas las funciones CAPWAP.
- **Modo independiente** – El WLC es inalcanzable. La Conexión flexible a AP ha perdido la conectividad CAPWAP con el WLC. La Conexión Flexible a AP puede asumir algunas de las funciones de WLC, como cambiar el tráfico de datos del cliente localmente y realizar la autenticación del cliente localmente.



12.5 - Gestión de Canales

Canal de Frecuencia de Saturación

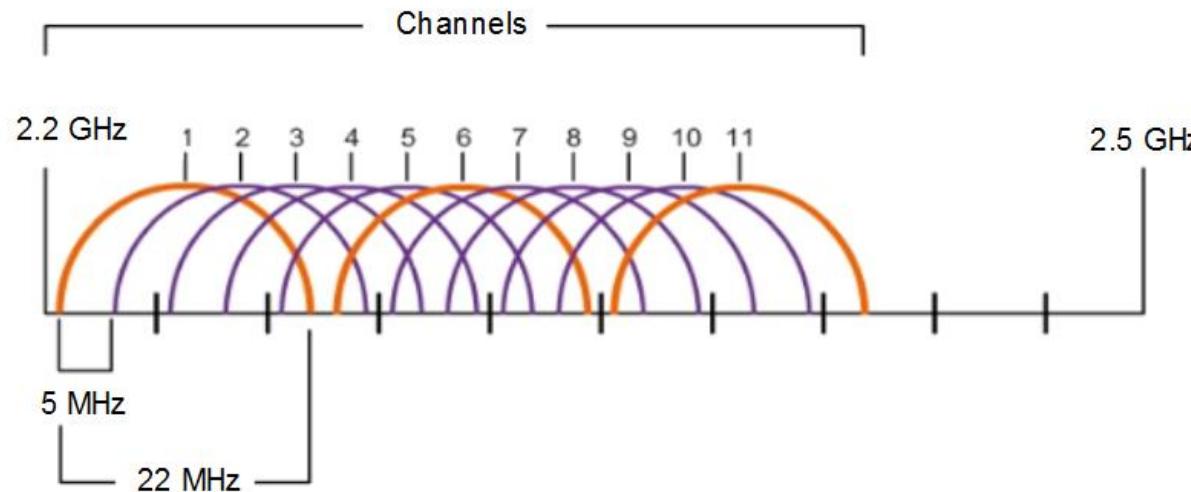
Si la demanda de un canal inalámbrico específico es demasiado alta, el canal puede sobresaturarse, degradando la calidad de la comunicación.

La saturación de canales se puede mitigar utilizando técnicas que usan los canales de manera más eficiente.

- **Direct-Sequence Spread Spectrum (DSSS)** - Una técnica de modulación diseñada para extender una señal sobre una banda de frecuencia más grande. Usado por dispositivos 802.11b para evitar interferencias de otros dispositivos que usan la misma frecuencia de 2.4 GHz.
- **Frequency-Hopping Spread Spectrum (FHSS)** - Transmite señales de radio cambiando rápidamente una señal portadora entre muchos canales de frecuencia. El emisor y el receptor deben estar sincronizados para "saber" a qué canal saltar. Usado por el estándar 802.11 original.
- **Orthogonal Frequency-Division Multiplexing (OFDM)** - Subconjunto de multiplexación por división de frecuencia en el que un solo canal utiliza múltiples subcanales en frecuencias adyacentes. Una serie de sistemas de comunicación, incluidos los estándares 802.11a/g/n/ac, usa OFDM.

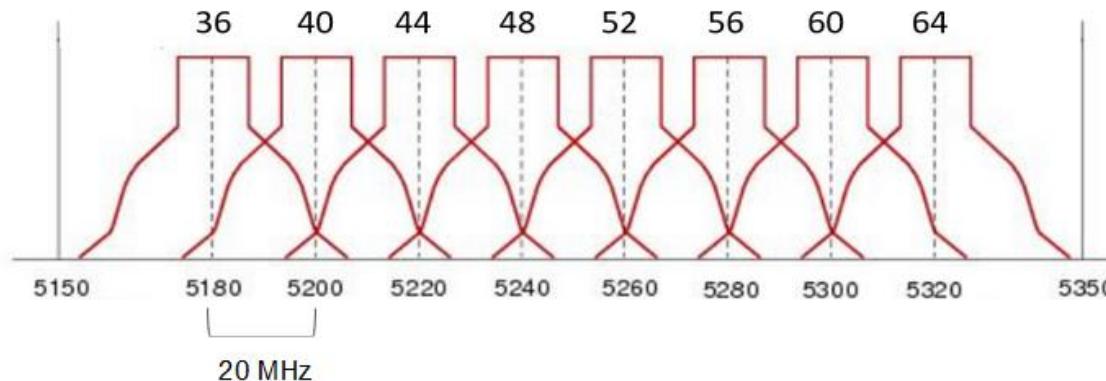
Selección del canal

- La banda de 2,4 GHz se subdivide en múltiples canales, cada uno de los cuales tiene un ancho de banda de 22 MHz y se separa del siguiente canal en 5 MHz.
- Una práctica recomendada para las WLAN 802.11b/g/n que requieren múltiples AP es utilizar canales no superpuestos, como 1, 6 y 11.



Selección de canales (Cont.)

- Para los estándares de 5 GHz 802.11a/n/ac, hay 24 canales. Cada canal está separado del siguiente canal por 20 MHz
- Los canales no superpuestos son 36, 48 y 60.

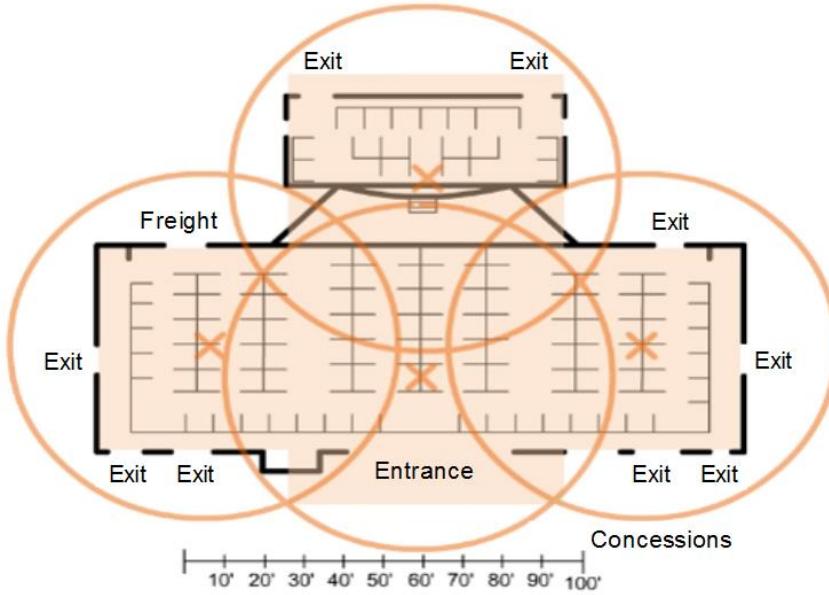


Planifique la Implementación de WLAN

El número de usuarios admitidos por una WLAN depende de lo siguiente:

- El diseño geográfico de la instalación.
- La cantidad de cuerpos y dispositivos que pueden caber en un espacio.
- Las tasas de datos que los usuarios esperan.
- El uso de canales no superpuestos por múltiples AP y configuraciones de potencia de transmisión.

Al planificar la ubicación de los puntos de acceso, el área de cobertura circular aproximada es importante.



12.6 – Amenazas en la WLAN

Video – Amenazas en la WLAN

Este video cubrirá lo siguiente:

- Intercepción de datos.
- Intrusos Inalámbricos.
- Ataques de Denegación de Servicio (DoS).
- AP Dudosos.

Resumen de seguridad inalámbrica

Una WLAN está abierta a cualquier persona dentro del alcance de un AP con las credenciales correspondientes para asociarse a él.

Las personas ajenas a la empresa, los empleados insatisfechos e incluso otros empleados, involuntariamente, pueden generar los ataques. Las Redes Inalámbricas son específicamente susceptibles a varias amenazas, incluidas las siguientes:

- Intercepción de datos.
- Intrusos inalámbricos.
- Ataques de denegación de servicio (DoS).
- AP dudosos.

Amenazas en la WLAN

Ataques DoS

Los ataques DoS inalámbricos pueden ser el resultado de lo siguiente:

- Dispositivos mal configurados
- Un usuario malintencionado que interfiere intencionalmente con la comunicación inalámbrica
- Interferencia accidental.

Para minimizar el riesgo de un ataque DoS debido a dispositivos mal configurados y ataques maliciosos, fortalezca todos los dispositivos, mantenga las contraseñas seguras, cree copias de seguridad y asegúrese de que todos los cambios de configuración se incorporen fuera de horario.

Puntos de acceso no autorizados

- Un AP falso es un AP o un router inalámbrico que se ha conectado a una red corporativa sin autorización explícita y en contra de la política corporativa.
- Una vez conectado, el AP falso puede ser usado por el atacante para capturar direcciones MAC, capturar paquetes de datos, obtener acceso a recursos de red o lanzar un ataque intermedio.
- Un punto de acceso a la red personal también podría usarse como un AP no autorizado. Por ejemplo, un usuario con acceso seguro a la red habilita su host de Windows autorizado para que se convierta en un AP Wi-Fi.
- Para evitar la instalación de puntos de acceso no autorizados, las organizaciones deben configurar WLC con políticas de puntos de acceso no autorizados y utilizar software de monitoreo para monitorear activamente el espectro de radio en busca de puntos de acceso no autorizados.

Ataques intermediarios

En un ataque intermedio (MITM por su sigla en inglés), el pirata informático se coloca entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes. Un popular ataque MITM inalámbrico se denomina “ataque con AP de red intrusa”, en el que un atacante introduce un AP no autorizado y lo configura con el mismo SSID que el de un AP legítimo.

La derrota de un ataque MITM comienza con la identificación de dispositivos legítimos en la WLAN. Para hacer esto, se deben autenticar los usuarios. Una vez que se conocen todos los dispositivos legítimos, se puede monitorear la red para detectar los dispositivos o el tráfico anormal.

12.7 – WLAN seguras

Video – WLAN Seguras

Este video cubrirá lo siguiente:

- Encubrimiento SSID.
- Filtrado de direcciones MAC.
- Sistemas de autenticación y encriptación (Autenticación abierta y autenticación de clave compartida).

Encubrimiento SSID y filtrado de direcciones MAC

Para abordar las amenazas de mantener alejados a los intrusos inalámbricos y proteger los datos, se utilizaron dos características de seguridad tempranas que aún están disponibles en la mayoría de los enrutadores y puntos de acceso:

Encubrimiento SSID

- Los AP y algunos enrutadores inalámbricos permiten deshabilitar la trama de baliza SSID, (Beacon frame SSID). Los clientes inalámbricos deben configurarse manualmente con el SSID para conectarse a la red.

Filtrado de Direcciones MAC

- Un administrador puede permitir o denegar manualmente el acceso inalámbrico de los clientes en función de su dirección física de hardware MAC. En la figura, el router está configurado para permitir dos direcciones MAC. Los dispositivos con diferentes direcciones MAC no podrán unirse a la WLAN de 2.4GHz.

802.11 Métodos de Autenticación Originales

La mejor manera de proteger una red inalámbrica es utilizar sistemas de autenticación y cifrado. Se introdujeron dos tipos de autenticación con el estándar 802.11 original:

Autenticación abierta

- No se requiere contraseña. Normalmente se usa para proporcionar acceso gratuito a Internet en áreas públicas como cafeterías, aeropuertos y hoteles.
- El cliente es responsable de proporcionar seguridad, como a través de una VPN.

Autenticación de clave compartida

- Proporciona mecanismos, como WEP, WPA, WPA2 y WPA3 para autenticar y cifrar datos entre un cliente inalámbrico y AP. Sin embargo, la contraseña se debe compartir previamente entre las dos partes para que estas se conecten.

Métodos de autenticación de clave compartida

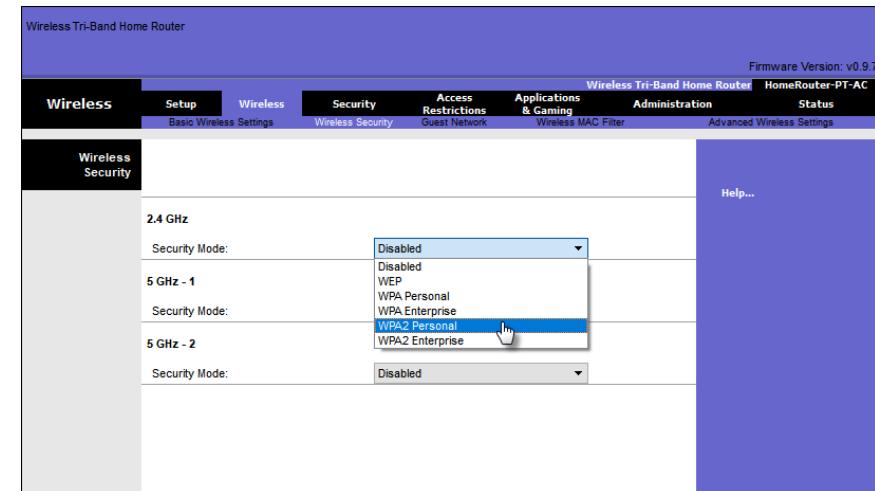
Actualmente hay cuatro técnicas de autenticación de clave compartida disponibles, como se muestra en la tabla.

Método de Autenticación	Descripción
Privacidad Equivalente al Cableado (WEP)	La especificación original 802.11 diseñada para proteger los datos utilizando el método de cifrado Rivest Cipher 4 (RC4) con una clave estática. WEP ya no se recomienda y nunca debe usarse.
Acceso Protegido Wi-Fi (WPA)	Un estándar de Wi-Fi Alliance que usa WEP pero asegura los datos con el algoritmo de cifrado del Protocolo de integridad de clave temporal (TKIP) mucho más fuerte. El TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar.
WPA2	Utiliza el Estándar de Cifrado Avanzado (AES) para el cifrado. AES actualmente se considera el protocolo de cifrado más sólido.
WPA3	Esta es la próxima generación de seguridad Wi-Fi. Todos los dispositivos habilitados para WPA3 utilizan los últimos métodos de seguridad, no permiten protocolos heredados obsoletos y requieren el uso de marcos de administración protegidos (PMF).

Autenticando a un Usuario Doméstico

Los routers domésticos suelen tener dos opciones de autenticación: WPA y WPA2. Con WPA2 tenemos dos métodos de autenticación.

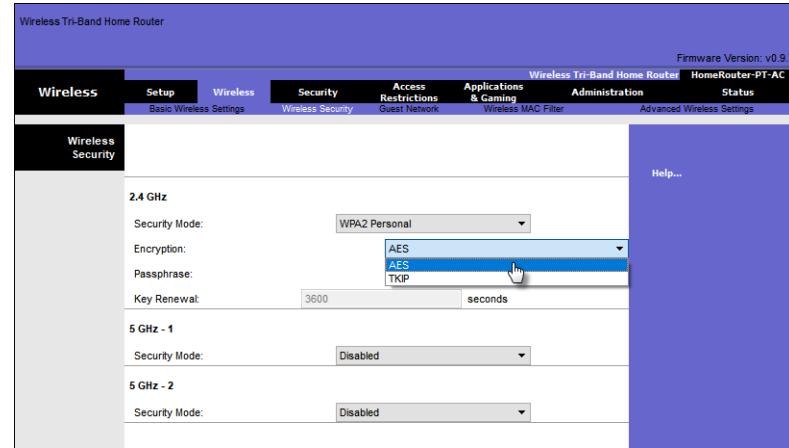
- **Personal** – Destinados a redes domésticas o de pequeñas oficinas, los usuarios se autentican utilizando una clave precompartida (PSK). Los clientes inalámbricos se autentican con el enrutador inalámbrico utilizando una contraseña previamente compartida. No se requiere ningún servidor de autenticación especial.
- **Empresa** – Destinado a redes empresariales. Requiere un servidor de autenticación de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). El servidor RADIUS debe autenticar el dispositivo y, a continuación, se deben autenticar los usuarios mediante el estándar 802.1X, que usa el protocolo de autenticación extensible (EAP).



Métodos de encriptación

WPA y WPA2 incluyen dos protocolos de encriptación:

- **Protocolo de integridad de clave temporal (Temporal Key Integrity Protocol (TKIP))** – Utilizado por WPA y proporciona soporte para equipos WLAN heredados. Hace uso de WEP pero encripta la carga útil de Capa 2 usando TKIP.
- **Estándar de cifrado avanzado (Advanced Encryption Standard (AES))** – Utilizado por WPA2 y utiliza el modo de cifrado de contador con el protocolo de código de autenticación de mensajes de encadenamiento de bloque (CCMP) que permite a los hosts de destino reconocer si los bits cifrados y no cifrados han sido alterados.

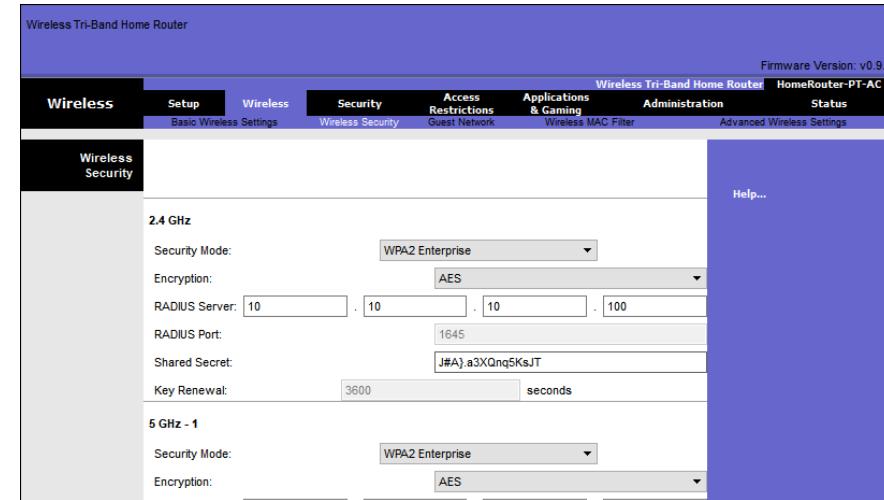


Autenticación en la empresa

La elección del modo de seguridad empresarial requiere un servidor RADIUS de autenticación, autorización y contabilidad (AAA).

Allí se requieren piezas de información:

- **Dirección IP del servidor RADIUS** – Dirección IP del servidor.
- **Números de puerto UDP**–Los puertos UDP 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS, pero también pueden funcionar utilizando los puertos UDP 1645 y 1646.
- **Llave compartida** – Se utiliza para autenticar el AP con el servidor RADIUS.



Nota: La autenticación y autorización del usuario se maneja mediante el estándar 802.1X, que proporciona una autenticación centralizada basada en el servidor de los usuarios finales.

Debido a que WPA2 ya no se considera seguro, se recomienda WPA3 cuando esté disponible. WPA3 incluye cuatro características:

- **WPA3 - Personal:** Frustra los ataques de fuerza bruta mediante el uso de la autenticación simultánea de iguales (Simultaneous Authentication of Equals, SAE).
- **WPA3 - Empresa:** Utiliza la autenticación 802.1X / EAP. Sin embargo, requiere el uso de una suite criptográfica de 192 bits y elimina la combinación de protocolos de seguridad para los estándares 802.11 anteriores.
- **Redes Abiertas:** No usa ninguna autenticación. Sin embargo, utiliza el cifrado inalámbrico oportunista (OWE) para cifrar todo el tráfico inalámbrico.
- **Incorporación de IoT :** Utiliza el Protocolo de aprovisionamiento de dispositivos (DPP) para incorporar rápidamente dispositivos IoT.

12.8 Módulo de Práctica y Cuestionario

¿Qué aprendí en este módulo?

- Las LAN inalámbricas (WLAN) se basan en los estándares IEEE y se pueden clasificar en cuatro tipos principales: WPAN, WLAN, WMAN y WWAN.
- Para enviar y recibir datos, la tecnología inalámbrica usa el espectro de radio sin licencia. Ejemplos de esta tecnología son Bluetooth, WiMAX, Banda Ancha Celular y Banda Ancha Satelital.
- Las redes WLAN operan en la banda de frecuencia de 2,4 GHz y la banda de 5 GHz.
- Las tres organizaciones que influyen en los estándares de WLAN son ITU-R, IEEE y Wi-Fi Alliance.
- CAPWAP es un protocolo estándar IEEE que permite que un WLC administre múltiples AP y WLAN.
- DTLS es un protocolo que proporciona seguridad entre el AP y el WLC.
- Los dispositivos de LAN inalámbricos tienen transmisores y receptores sintonizados a frecuencias específicas de ondas de radio para comunicarse. Los rangos se dividen en rangos más pequeños llamados canales: DSSS, FHSS y OFDM.
- Los estándares 802.11b/g/n operan en el espectro de 2.4 GHz a 2.5GHz. La banda de 2,GHz se subdivide en varios canales. Cada canal tiene un ancho de banda de 22 MHz y está separado del siguiente canal por 5 MHz.
- Las redes inalámbricas son susceptibles a amenazas, que incluyen: interceptación de datos, intrusos inalámbricos, ataques DoS y puntos de acceso no autorizados.
- Para mantener alejados a los intrusos inalámbricos y proteger los datos, dos características de seguridad tempranas todavía están disponibles en la mayoría de los enrutadores y puntos de acceso: ocultamiento de SSID y filtrado de direcciones MAC.
- Hay cuatro técnicas de autenticación de clave compartida disponibles: WEP, WPA, WPA2 y WPA3.



VLANs

UMG – Quetzaltenango

Ingeniería en Sistemas

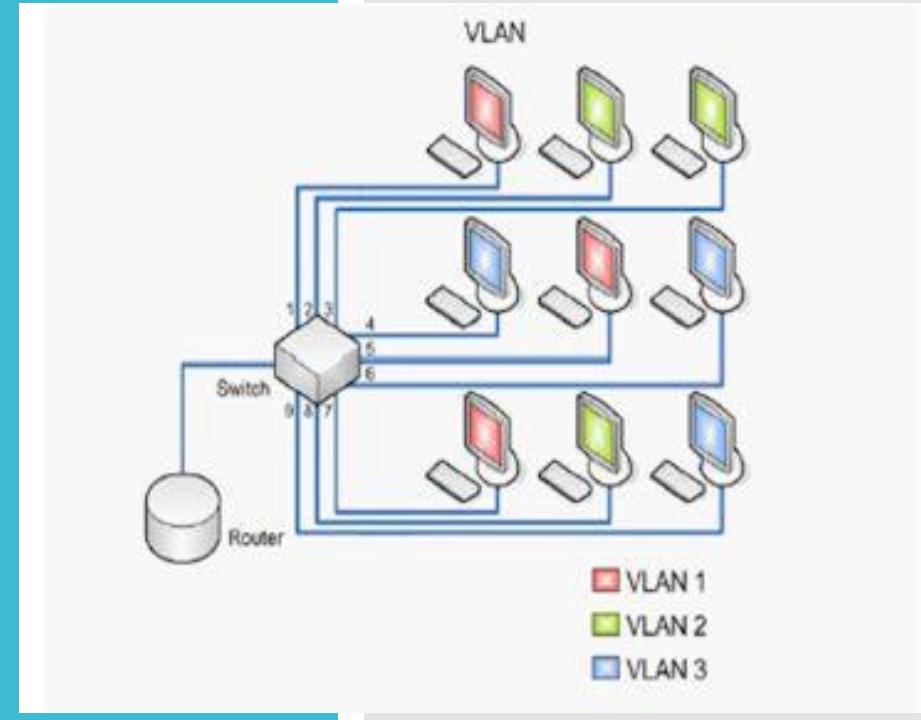
2023 - Redes de Computadoras 2



VLANs

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión.

Además las VLAN se utilizan para separar distintas LAN dentro de una red física, teniendo la capacidad de utilizar un mismo equipo, un mismo canal de enlace WAN, pero conectando directamente equipos acorde a las áreas a las que pertenezcan.



Seguridad LAN (Capa 2)

Comandos de switchport

La seguridad de la LAN puede comenzar por la capa de Enlace de Datos, mediante la revisión de la tabla de direcciones físicas (ARP)

- switchport port-security mac-address sticky
- switchport port-security violation 3 opciones: protect / restrict / shutdown
- switchport port-security maximum
- switchport port-security // tabla se actualiza al momento de generar trafico

Un puerto de Switch se puede configurar básicamente en éstos 2 modos

- switchport mode Access permite acceso a tráfico de datos
- switchport mode Trunk permite tráfico troncal (de cualquier vlan)
- (switchport mode Dynamic) se usa para negociar dinámicamente si el puerto se autoconfigura en modo acceso o troncal, no es recomendable por seguridad.

Tipos de VLAN

Podemos utilizar de la VLAN 1 a la 1005 para asignar las que consideremos convenientes de acuerdo a cada caso.

- VLAN de datos
 - La VLAN que contendrá el tráfico de datos de acuerdo a la configuración sólo se podrá comunicar con equipos de la misma VLAN
- VLAN de voz
 - Cuando utilizamos telefonía IP el tráfico específico de llamadas y la planta telefónica debe utilizar una VLAN específica para separar el tráfico de datos con el de voz y que no se produzcan retrasos o saturación.
- VLAN predeterminada
 - De manera predeterminada es la VLAN 1, aunque cuando hace configuración de VLANs se recomienda ya no utilizar ésta VLAN para ninguna aplicación.
- VLAN nativa
 - Asignada a un puerto troncal es la VLAN por la cual se va a manejar el tráfico que no está etiquetado con alguna VLAN asignada
- VLAN de administración
 - Se utiliza por el administrador de redes para realizar configuraciones remotas de los equipos, nunca se asignan equipos terminales dentro de esta VLAN por seguridad. En todos los equipos de la red se debe crear la misma VLAN administrativa para poder tener acceso a los equipos a través de los enlaces troncales

Configuración de puertos

- Interfaz configurada en modo troncal
 - **Switchport mode trunk**
 - modo troncal permite que el tráfico de cualquier VLAN pase por esta interfaz.
- Interfaz configurada en modo acceso
 - **switchport mode Access**
 - **switchport Access vlan <id vlan>**
 - modo acceso solamente permite que el tráfico de la VLAN idvlan definida se reciba por esa interfaz, y el tráfico que salga por ella será etiquetado con ese número de VLAN.
- VLAN configurada para VoIP
 - **switchport Voice VLAN <id vlan>**
 - Solamente ésta VLAN utilizará el protocolo de Voice Over IP
- Configuración de la VLAN nativa
 - **switchport mode trunk**
 - **switchport trunk native vlan <id vlan>**
 - modo troncal solamente, permite que el tráfico que no tiene ninguna etiqueta de VLAN configurada se le asigne la VLAN nativa.
- Configuración de la VLAN administrativa
 - **Vlan <id vlan>**
 - **Interface vlan <id vlan>**
 - **Ip address x.x.x.x s.s.s.s**
 - Se crea una VLAN y se accede a la interfaz creada con el número de VLAN para configurar una IP correspondiente a la VLAN administrativa de toda la red.
 - **Ip default-Gateway x.x.x.x**
 - Se debe configurar la ruta predeterminada en el switch hacia el equipo principal de la red, para que éste se pueda comunicar por el enlace troncal con los equipos que necesita.

Creación de una VLAN y ver la configuración de VLANs

Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	S1# configure terminal
Cree una VLAN con un número de ID válido.	S1 (config)#vlan id-vlan
Especifique un nombre único para identificar la VLAN.	S1 (config-vlan)#name nombre-vlan
Vuelva al modo EXEC privilegiado.	S1 (config-vlan)# end

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
20	student	active	



Módulo 2: Switch básico y configuración del dispositivo final

Introducciones a las redes v7.0
(ITN)



Objetivos del módulo

Título de módulo: Configuración básica de conmutador y dispositivo final

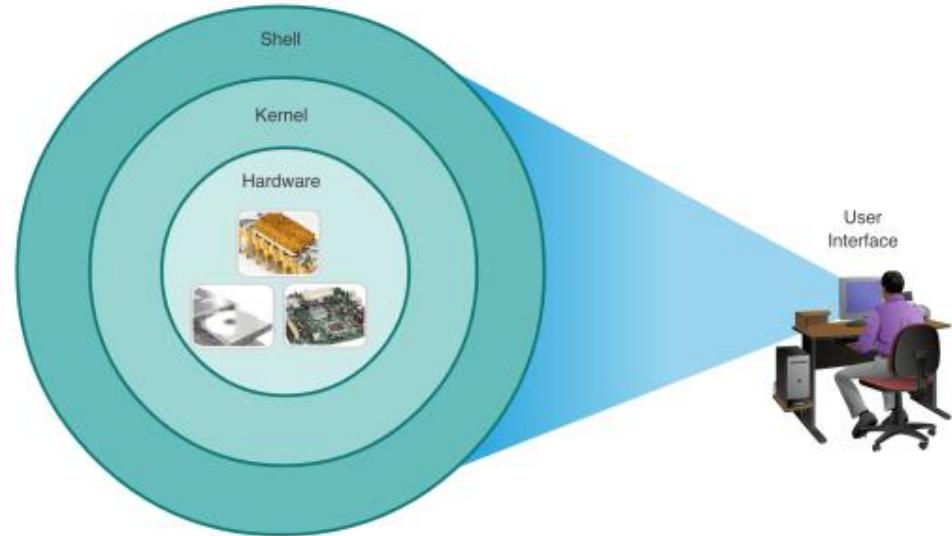
Objetivo del módulo: Implemente configuraciones iniciales que incluyen contraseñas, direccionamiento IP y parámetros de puerta de enlace predeterminados en un conmutador de red y dispositivos finales.

Título del tema	Objetivo del tema
Acceso Cisco IOS	Explicar cómo acceder a un dispositivo Cisco IOS para fines de configuración.
Navegación IOS	Explicar cómo navegar Cisco IOS para configurar dispositivos de red.
La estructura de comando	Describa la estructura de comandos del software Cisco IOS.
Configuración básica del dispositivo	Configure un dispositivo Cisco IOS usando CLI.
Guardar configuraciones	Utilice los comandos de IOS para guardar la configuración en ejecución.
Puertos y Direcciones	Explicar cómo se comunican los dispositivos a través de los medios de red.
Configurar direccionamiento IP	Configure un dispositivo host con una dirección IP.
Verificar conectividad	Verifique la conectividad entre dos dispositivos finales.

2.1 Acceso Cisco IOS

Sistemas operativos

- **Shell**- La interfaz de usuario que permite a los usuarios solicitar tareas específicas de la computadora. Estas solicitudes pueden hacerse a través de las interfaces CLI o GUI.
- **Kernel** - Se comunica entre el hardware y el software de una computadora y gestiona cómo se utilizan los recursos de hardware para cumplir con los requisitos de software.
- **Hardware** - La parte física de una computadora, incluida la electrónica subyacente.



GUI

- Una GUI permite al usuario interactuar con el sistema utilizando un entorno de iconos gráficos, menús y ventanas.
- Una GUI es más fácil de usar y requiere menos conocimiento de la estructura de comandos subyacente que controla el sistema.
- Ejemplos de estos son: Windows, macOS, Linux KDE, Apple iOS y Android.
- Las GUI pueden fallar, bloquearse o simplemente no funcionar como se especifica. Por estas razones, a los dispositivos de red generalmente se accede a través de una CLI.



Propósito de un SO

El sistema operativo de la PC permite al usuario hacer lo siguiente:

- Use un mouse para hacer selecciones y ejecutar programas
- Ingrese texto y comandos basados en texto



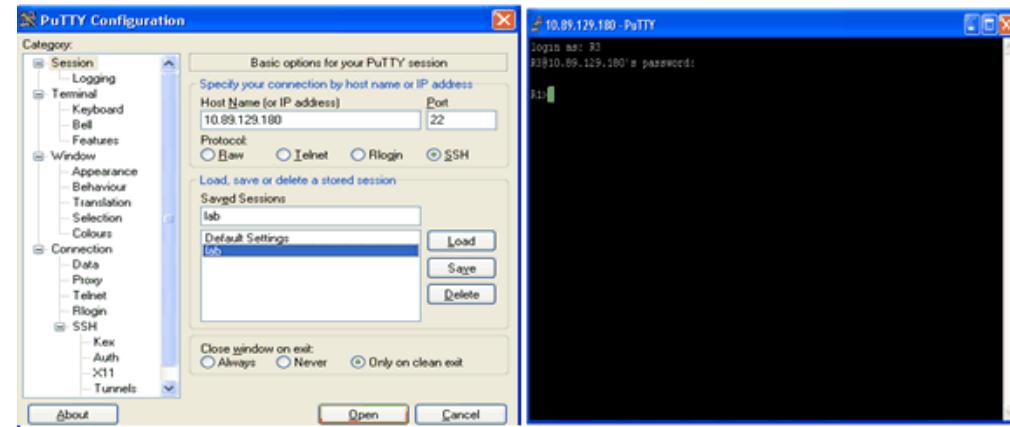
El sistema operativo de red basado en CLI permite que un técnico de red haga lo siguiente:

- Use un teclado para ejecutar programas de red basados en CLI
- Use un teclado para ingresar texto y comandos basados en texto
- Ver salida en un monitor

```
analyst@secOps ~]$ ls
Desktop Downloads lab.support.files second_drive
[analyst@secOps ~]$
```

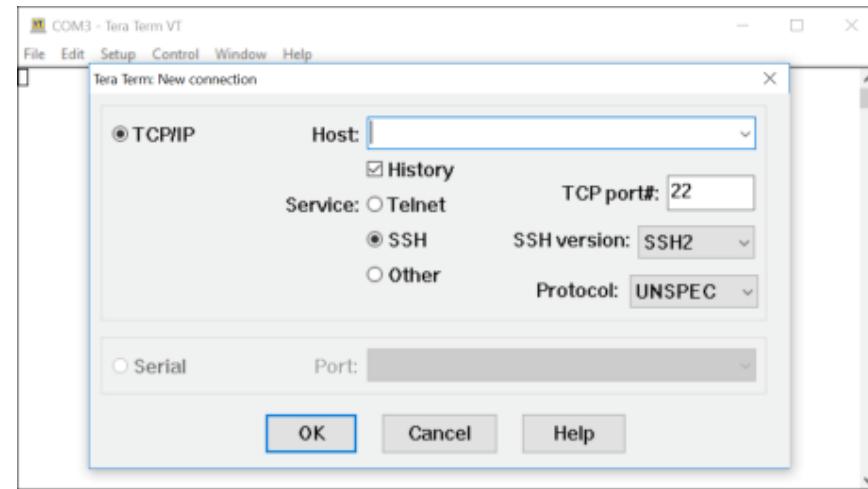
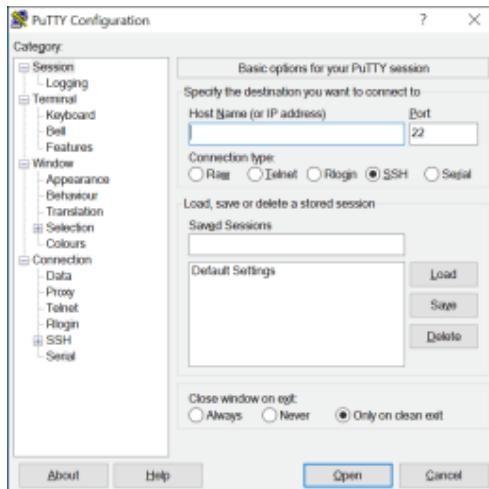
Métodos de acceso

- **Consola** - Un puerto de administración física utilizado para acceder a un dispositivo con el fin de proporcionar mantenimiento, como realizar las configuraciones iniciales.
- **Shell seguro (SSH)** - Establece una conexión CLI remota segura a un dispositivo, a través de una interfaz virtual, a través de una red. (Nota: Este es el método recomendado para conectarse de forma remota a un dispositivo).
- **Telnet** - Establece una conexión CLI remota insegura a un dispositivo a través de la red. (Nota: la autenticación del usuario, las contraseñas y los comandos se envían a través de la red en texto sin formato).



Programas de emulación de terminal

- Los programas de emulación de terminal se utilizan para conectarse a un dispositivo de red mediante un puerto de consola o mediante una conexión SSH / Telnet.
- Hay varios programas de emulación de terminal para elegir, como PuTTY, Tera Term y SecureCRT.



2.2 Navegación IOS

Modos de comando primario

Modo EXEC de usuario:

- Permite el acceso a solo un número limitado de comandos básicos de monitoreo
- Identificado por la solicitud de CLI que termina con el símbolo >

```
Router>  
  
Switch>
```

Modo EXEC privilegiado:

- Permite el acceso a todos los comandos y funciones
- Identificado por la solicitud de CLI que termina con el símbolo #

```
Router#  
  
Switch#
```

Modo de configuración y modos de subconfiguración

Modo de configuración global:

- Se usa para acceder a las opciones de configuración en el dispositivo

```
Switch(config) #
```

Modo de configuración de línea:

- Se usa para configurar el acceso a la consola, SSH, Telnet o AUX

```
Switch(config-line) #
```

Modo de configuración de interfaz:

- Se utiliza para configurar un puerto de comutador o una interfaz de enrutador

```
Switch(config-if) #
```

Video - Modos de comandos principales de la CLI de IOS

Este video cubrirá lo siguiente:

- Modo EXEC de usuario
- Modo EXEC privilegiado
- Modo de configuración global

Navegación entre modos IOS

▪ Modo EXEC privilegiado:

- Para pasar del modo EXEC del usuario al modo EXEC privilegiado, use el **habilitado** mando.

```
Switch> enable  
Switch#
```

▪ Modo de configuración global:

- Para entrar y salir del modo de configuración global, use el **configurar terminal** mando. Para volver al modo EXEC privilegiado, use el mando EXIT.

```
Switch(config)#  
Switch(config)#exit  
Switch#
```

▪ Modo de configuración de línea:

- Para entrar y salir del modo de configuración de línea, use el comando **lín**e seguido del tipo de línea de administración. Para volver al modo de configuración global, use el mando EXIT.

```
Switch(config)#line console 0  
Switch(config-line)#exit  
Switch(config)#
```

Navegación entre modos IOS (Cont.)

Subconfiguración Modos:

- Para salir de cualquier modo de subconfiguración para volver al modo de configuración global, use el **salida** mando. Para volver al modo EXEC privilegiado, use el **final** comando o combinación de teclas **Ctrl + Z**.
- Para pasar directamente de un modo de subconfiguración a otro, escriba el comando del modo de subconfiguración deseado. En el ejemplo, el símbolo del sistema cambia de(**línea de configuración**) # a (**config-if**) #.

```
Switch(config)#line console 0  
Switch(config-line)#end  
Switch#
```

```
Switch(config-line)#interface FastEthernet 0/1  
Switch(config-if)#{
```

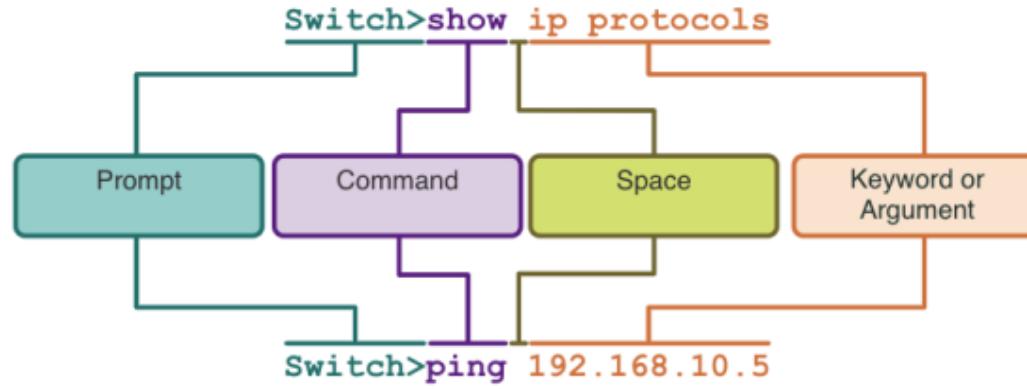
Video - Navegación entre modos IOS

Este video cubrirá lo siguiente:

- enable
- disable
- configure terminal
- exit
- end
- Control + Z on keyboard
- Otros comandos para ingresar a los modos de subconfiguración

2.3 La estructura del comando

Estructura básica del comando IOS



- **Palabra clave** - Este es un parámetro específico definido en el sistema operativo (en la figura, **protocolos ip**)
- **Argumento** - Esto no está predefinido; Es un valor o variable definida por el usuario (en la figura, **192.168.10.5**)

Comprobación de la sintaxis del comando IOS

Un comando puede requerir uno o más argumentos. Para determinar las palabras clave y los argumentos necesarios para un comando, consulte la sintaxis del comando.

- El texto en negrita indica los comandos y las palabras clave que se ingresan como se muestra.
- El texto en cursiva indica un argumento para el cual el usuario proporciona el valor.

Convención	Descripción
negrita	El texto en negrita indica los comandos y las palabras clave que ingresa literalmente como se muestra.
<i>cursiva</i>	El texto en cursiva indica argumentos para los que proporciona valores.
[X]	Los corchetes indican un elemento opcional (palabra clave o argumento).
{X}	Las llaves indican un elemento requerido (palabra clave o argumento).
[x {y z }]	Las llaves y las líneas verticales entre corchetes indican una elección requerida dentro de un elemento opcional. Los espacios se utilizan para delinejar claramente partes del comando.

Comprobación de la sintaxis del comando IOS (Cont.)

- La sintaxis del comando proporciona el patrón, o formato, que debe usarse al ingresar un comando.
- El comando es **ping** y el argumento definido por el usuario es el *ip-address* dispositivo de destino. Por ejemplo,**ping 10.10.10.5**.


```
ping ip-address
```
- El comando es **traceroute** y el argumento definido por el usuario es el *ip-address* del dispositivo de destino.
Por ejemplo,**traceroute 192.168.254.254**.


```
traceroute ip-address
```
- Si un comando es complejo con múltiples argumentos, puede verlo representado así:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

Funciones de ayuda de iOS

El IOS tiene dos formas de ayuda disponibles: ayuda contextual y verificación de sintaxis de comandos.

- La ayuda sensible al contexto le permite encontrar rápidamente respuestas a estas preguntas:
 - ¿Qué comandos están disponibles en cada modo de comando?
 - ¿Qué comandos comienzan con caracteres específicos o grupo de caracteres?
 - ¿Qué argumentos y palabras clave están disponibles para comandos particulares?
- La verificación de sintaxis de comandos verifica que el usuario haya ingresado un comando válido.
 - Si el intérprete no puede entender el comando que se está ingresando, proporcionará comentarios que describan qué está mal con el comando.

```
Router#ping ?  
WORD Ping destination address or hostname  
ip IP echo  
ipv6 IPv6 echo
```

```
Switch#interface fastEthernet 0/1  
^  
% Invalid input detected at '^' marker.
```

La estructura de comando

Video: ayuda sensible al contexto y verificador de sintaxis de comandos

Este video cubrirá lo siguiente:

- Use el comando de ayuda en el usuario EXEC, EXEC privilegiado y el modo de configuración global
- Termina comandos y argumentos con el comando de ayuda
- Use el verificador de sintaxis de comandos para corregir errores de sintaxis y comandos incompletos

Teclas de acceso rápido y atajos

- La CLI de IOS proporciona teclas de acceso rápido y accesos directos que facilitan la configuración, el monitoreo y la solución de problemas.
- Los comandos y las palabras clave se pueden acortar al número mínimo de caracteres que identifican una selección única. Por ejemplo, el**configurar** el comando se puede acortar a **conf** porque **configure** es el único comando que comienza con **conf**.

```
Router#con  
% Ambiguous command: "con"  
Router#con?  
configure connect
```

```
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#
```

Teclas de acceso rápido y atajos (Cont.)

- La siguiente tabla es una breve lista de pulsaciones de teclas para mejorar la edición de la línea de comandos..

Golpe de teclado	Descripción
Tab	Completa una entrada de nombre de comando parcial.
Backspace	Borra el carácter a la izquierda del cursor.
Left Arrow or Ctrl+B	Mueve el cursor un carácter a la izquierda.
Right Arrow or Ctrl+F	Mueve el cursor un carácter a la derecha.
Up Arrow or Ctrl+P	Recupera los comandos en el búfer de historial, comenzando con los comandos más recientes.

Teclas de acceso rápido y atajos (Cont.)

- Cuando una salida de comando produce más texto del que se puede mostrar en una ventana de terminal, el IOS mostrará un "**--More--**" rápido. La siguiente tabla describe las pulsaciones de teclas que se pueden utilizar cuando se muestra este mensaje.
- La siguiente tabla enumera los comandos que se pueden usar para salir de una operación.

Golpe de teclado	Descripción
Enter Key	Muestra la siguiente línea.
Space Bar	Muestra la siguiente pantalla.
Any other key	Finaliza la cadena de visualización, volviendo al modo EXEC privilegiado.

Golpe de teclado	Descripción
Ctrl-C	En cualquier modo de configuración, finaliza el modo de configuración y vuelve al modo EXEC privilegiado.
Ctrl-Z	En cualquier modo de configuración, finaliza el modo de configuración y vuelve al modo EXEC privilegiado.
Ctrl-Shift-6	Secuencia de interrupción de uso múltiple utilizada para abortar búsquedas DNS, traceroutes, pings, etc.

Nota: Para ver más teclas de acceso rápido y accesos directos, consulte 2.3.5.

Video - Teclas de acceso rápido y accesos directos

Este video cubrirá lo siguiente:

- Tecla de tabulación (finalización de tabulación)
- Acortamiento de comandos
- Tecla de flecha arriba y abajo
- CTRL + C
- CTRL + Z
- CTRL + Mayús + 6
- CTRL + R

Packet Tracer: navega por el IOS

En este Packet Tracer, hará lo siguiente:

- Establezca conexiones básicas, acceda a la CLI y explore la ayuda
- Explore los modos EXEC
- Pon el reloj

Laboratorio: navegue por el IOS utilizando Tera Term para la conectividad de la consola

En este laboratorio, completa los siguientes objetivos:

- Acceda a un Switch Cisco a través del puerto de consola serie
- Mostrar y configurar ajustes básicos del dispositivo
- (Opcional) Acceda a un Switch Cisco mediante un cable de consola mini-USB

2.4 Configuración básica del dispositivo

Nombres de dispositivos

- El primer comando de configuración en cualquier dispositivo debe ser darle un nombre de host único.
- Por defecto, a todos los dispositivos se les asigna un nombre predeterminado de fábrica. Por ejemplo, un switch Cisco IOS es "Switch".
- Pauta para nombrar dispositivos:
 - Comience con una letra
 - No contienen espacios
 - Termina con una letra o dígito
 - Use solo letras, dígitos y guiones
 - Tener menos de 64 caracteres de longitud

```
Switch# configure terminal  
Switch(config)# hostname Sw-Floor-1  
Sw-Floor-1(config)#
```

Nota: Para devolver el interruptor al indicador predeterminado, use el **no hostname** en configuración global.

Pautas de contraseña

- El uso de contraseñas débiles o fáciles de adivinar es un problema de seguridad.
- Todos los dispositivos de red deben limitar el acceso administrativo asegurando EXEC privilegiado, EXEC de usuario y acceso remoto de Telnet con contraseñas. Además, todas las contraseñas deben estar encriptadas y se deben proporcionar notificaciones legales.
- Pautas de contraseña:
 - Use contraseñas que tengan más de ocho caracteres de longitud.
 - Use una combinación de letras mayúsculas y minúsculas, números, caracteres especiales y / o secuencias numéricas.
 - Evite usar la misma contraseña para todos los dispositivos.
 - No use palabras comunes porque se adivinan fácilmente.



Nota: La mayoría de los laboratorios en este curso usan contraseñas simples como **cisco** o **class**. Estas contraseñas se consideran débiles y fáciles de adivinar y deben evitarse en entornos de producción.

Configurar contraseñas

Asegurar el acceso al modo EXEC del usuario:

- Primero ingrese al modo de configuración de la consola de línea usando el comando **line console 0** en modo de configuración global.
- A continuación, especifique la contraseña del modo EXEC del usuario utilizando **password contraseña**
- Finalmente, habilite el acceso EXEC del usuario usando el comando **login**.

Asegurar el acceso al modo EXEC privilegiado:

- Primero ingrese al modo de configuración global.
- A continuación, use el comando **enable secret contraseña**

```
Sw-Floor-1# configure terminal  
Sw-Floor-1(config)# line console 0  
Sw-Floor-1(config-line)# password cisco  
Sw-Floor-1(config-line)# login  
Sw-Floor-1(config-line)# end  
Sw-Floor-1#
```

```
Sw-Floor-1# configure terminal  
Sw-Floor-1(config)# enable secret class  
Sw-Floor-1(config)# exit  
Sw-Floor-1#
```

Configurar contraseñas (cont.)

Asegurar el acceso a la línea VTY:

- Primero ingrese al modo de configuración de línea VTY usando el comando **Línea vty 0 15** en modo de configuración global.
- A continuación, especifique la contraseña de VTY utilizando **password contraseña**
- Finalmente, habilite el acceso VTY usando el comando **login**
 - Nota: las líneas VTY permiten el acceso remoto mediante Telnet o SSH al dispositivo. Muchos conmutadores Cisco admiten hasta 16 líneas VTY numeradas del 0 al 15.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Cifrar contraseñas

- Los archivos startup-config y running-config muestran la mayoría de las contraseñas en texto sin formato.
- Para cifrar todas las contraseñas de texto sin formato, use el comando **service password-encryption** en configuración global.
- Utilizar el comando **show running-config** para verificar que las contraseñas del dispositivo estén ahora encriptadas.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

```
Sw-Floor-1# show running-config
!
!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

Mensajes de banner

- Un mensaje de banner es importante para advertir al personal no autorizado que intente acceder al dispositivo.
- Para crear un mensaje de banner del día en un dispositivo de red, use el comando **banner motd # mensaje del dia #** en configuración global.

Nota: El "#" en la sintaxis del comando se llama carácter delimitador. Se ingresa antes y después del mensaje.

```
Sw-Floor-1# configure terminal  
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

El banner se mostrará cuando intente acceder al dispositivo.



```
Press RETURN to get started.
```

```
Authorized Access Only!
```

```
User Access Verification
```

```
Password:
```

Video: acceso administrativo seguro a un conmutador

Este video cubrirá lo siguiente:

- Acceda a la línea de comando para asegurar el interruptor
- Acceso seguro al puerto de la consola
- Acceso seguro a la terminal virtual para acceso remoto
- Cifrar contraseñas en el conmutador
- Configurar el mensaje de banner
- Verificar cambios de seguridad

2.5 Guardar configuraciones

Guardar configuraciones

Archivos de configuración

- Hay dos archivos del sistema que almacenan la configuración del dispositivo:
 - **startup-config**- Este es el archivo de configuración guardado que se almacena en NVRAM. Contiene todos los comandos que utilizará el dispositivo al iniciar o reiniciar. Flash no pierde su contenido cuando el dispositivo está apagado.
 - **running-config**- Esto se almacena en la memoria de acceso aleatorio (RAM). Refleja la configuración actual. La modificación de una configuración en ejecución afecta la operación de un dispositivo Cisco de inmediato. RAM es memoria volátil. Pierde todo su contenido cuando el dispositivo se apaga o se reinicia.
 - Para guardar los cambios realizados en la configuración en ejecución en el archivo de configuración de inicio, use el comando **copy running-config startup-config** en modo EXEC privilegiado.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

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

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

Guardar configuraciones

Alterar las configuraciones en ejecución

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado y la configuración en ejecución aún no se ha guardado, puede restaurar el dispositivo a su configuración anterior. Para hacer esto puedes:

- Elimine los comandos modificados individualmente.
- Vuelva a cargar el dispositivo usando el comando **reload** modo EXEC privilegiado. *Nota: Esto hará que el dispositivo se desconecte brevemente, lo que provocará un tiempo de inactividad de la red.*

Si los cambios no deseados se guardaron en la configuración de inicio, puede ser necesario borrar todas las configuraciones utilizando **erase startup-config** comando en modo EXEC privilegiado.

- Después de borrar la configuración de inicio, vuelva a cargar el dispositivo para borrar el archivo de configuración en ejecución de la RAM.

```
Router# reload  
Proceed with reload? [confirm]  
Initializing Hardware ...
```

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

Video: alterar la configuración en ejecución

Este video cubrirá lo siguiente:

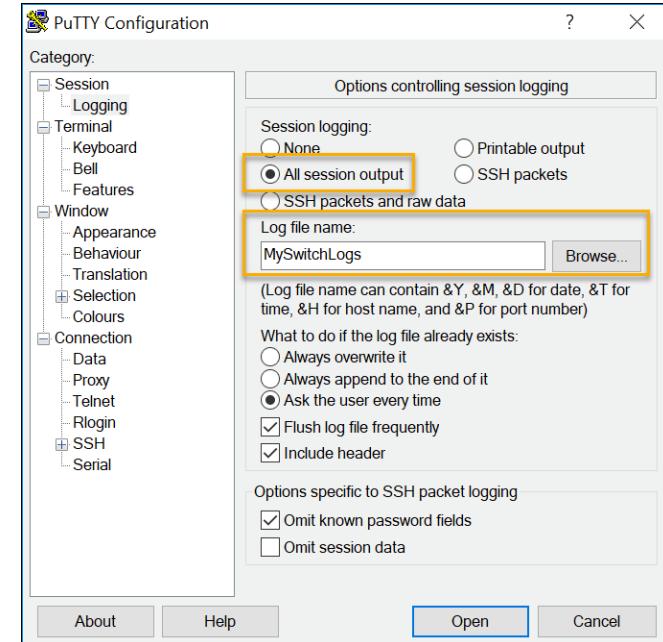
- Copie el archivo running-config en el archivo startup-config
- Mostrar los archivos en el directorio flash o NVRAM
- Usar acortamiento de comandos
- Borrar el archivo de configuración de inicio
- Copie el archivo start-config al archivo running-config

Guardar configuraciones

Capture la configuración a un archivo de texto

Los archivos de configuración también se pueden guardar y archivar en un documento de texto.

- **Paso 1.** Abra el software de emulación de terminal, como PuTTY o Tera Term, que ya está conectado a un conmutador.
- **Paso 2.** Habilite el inicio de sesión en el software del terminal y asigne un nombre y una ubicación de archivo para guardar el archivo de registro. La figura muestra que **Todos los resultados de la sesión** será capturado en el archivo especificado (es decir, MySwitchLogs).



Guardar configuraciones

Capture la configuración en un archivo de texto (Cont.)

- Paso 3.** Ejecutar el **show running-config** o **show startup-config** en el indicador EXEC privilegiado. El texto que se muestra en la ventana del terminal se colocará en el archivo elegido.
- Paso 4.** Deshabilite el inicio de sesión en el software del terminal. La figura muestra cómo deshabilitar el registro seleccionando e **none** opción de registro de sesión

Nota: El archivo de texto creado se puede usar como un registro de cómo se implementa actualmente el dispositivo. El archivo podría requerir edición antes de ser utilizado para restaurar una configuración guardada en un dispositivo.



Packet Tracer: configure los ajustes iniciales del interruptor

En este Packet Tracer, hará lo siguiente:

- Verifique la configuración predeterminada del interruptor
- Configurar una configuración básica de conmutador
- Configurar un banner MOTD
- Guardar archivos de configuración en NVRAM
- Configurar un segundo interruptor

2.6 Puertos y direcciones

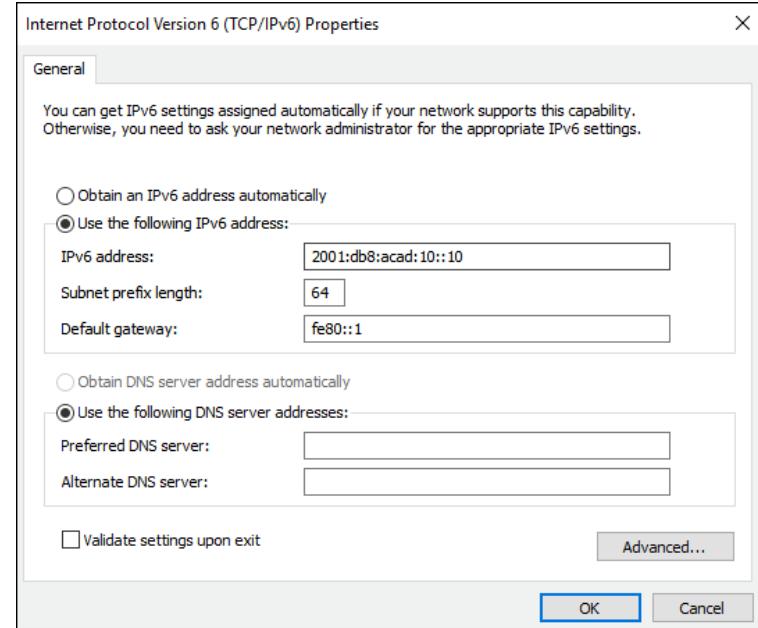
Direcciones IP

- El uso de direcciones IP es el medio principal para permitir que los dispositivos se ubiquen entre sí y establezcan una comunicación de extremo a extremo en Internet.
- La estructura de una dirección IPv4 se denomina notación decimal con puntos y está representada por cuatro números decimales entre 0 y 255.
- Una máscara de subred IPv4 es un valor de 32 bits que diferencia la porción de red de la dirección de la porción del host. Junto con la dirección IPv4, la máscara de subred determina a qué subred pertenece el dispositivo.
- La dirección de puerta de enlace predeterminada es la dirección IP del enrutador que el host usará para acceder a redes remotas, incluida Internet.



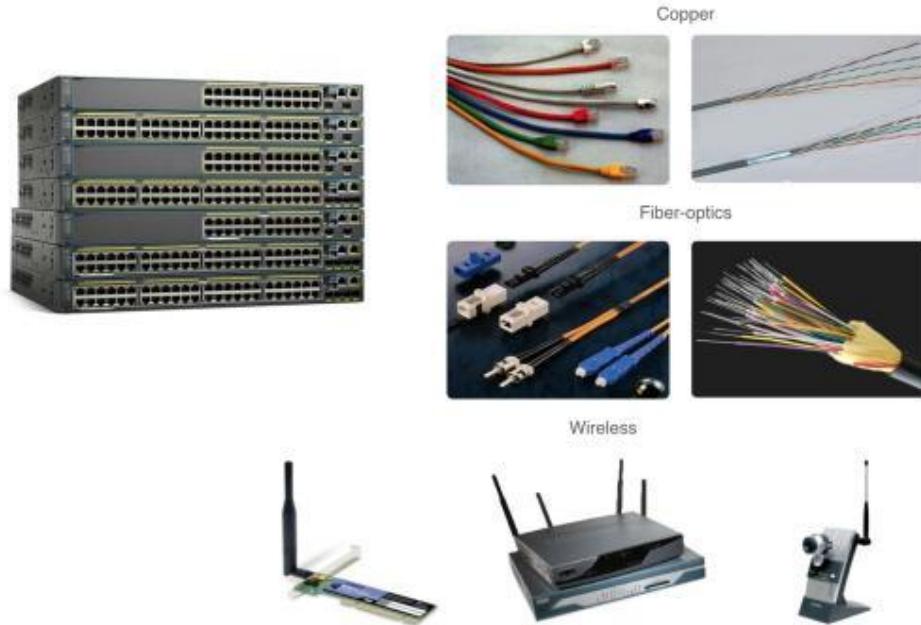
Direcciones IP (Cont.)

- Las direcciones IPv6 tienen 128 bits de longitud y están escritas como una cadena de valores hexadecimales. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Los grupos de cuatro dígitos hexadecimales están separados por dos puntos ":".
 - Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas y pueden escribirse en minúsculas o mayúsculas.
- Nota:** IP en este curso se refiere a los protocolos IPv4 e IPv6. IPv6 es la versión más reciente de IP y está reemplazando al IPv4 más común.



Interfaces y puertos

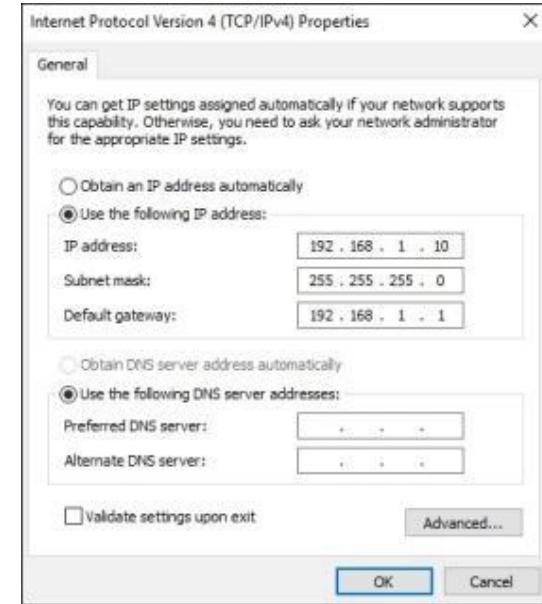
- Las comunicaciones de red dependen de las interfaces del dispositivo del usuario final, las interfaces del dispositivo de red y los cables que las conectan.
- Los tipos de medios de red incluyen cables de cobre de par trenzado, cables de fibra óptica, cables coaxiales o inalámbricos.
- Los diferentes tipos de medios de red tienen diferentes características y beneficios. Algunas de las diferencias entre varios tipos de medios incluyen:
 - Distancia a la que los medios pueden transportar una señal con éxito
 - Entorno en el que se instalarán los medios
 - Cantidad de datos y la velocidad a la que deben transmitirse



2.7 Configurar direcccionamiento IP

Configuración manual de la dirección IP para dispositivos finales

- Los dispositivos finales en la red necesitan una dirección IP para comunicarse con otros dispositivos en la red.
- La información de la dirección IPv4 se puede ingresar en los dispositivos finales de forma manual o automática mediante el Protocolo de configuración dinámica de host (DHCP).
 - Para configurar manualmente una dirección IPv4 en una PC con Windows, abra el **Panel de control > Centro de uso compartido de red > Cambiar la configuración del adaptador** elige el adaptador. Luego haga clic derecho y seleccione**Propiedades** para mostrar el **Propiedades de conexión de área local**.
 - Luego haga clic **Propiedades** para abrir el **Propiedades de Protocolo de Internet versión 4 (TCP / IPv4)** ventana. Luego configure la dirección IPv4 y la información de la máscara de subred, y la puerta de enlace predeterminada.

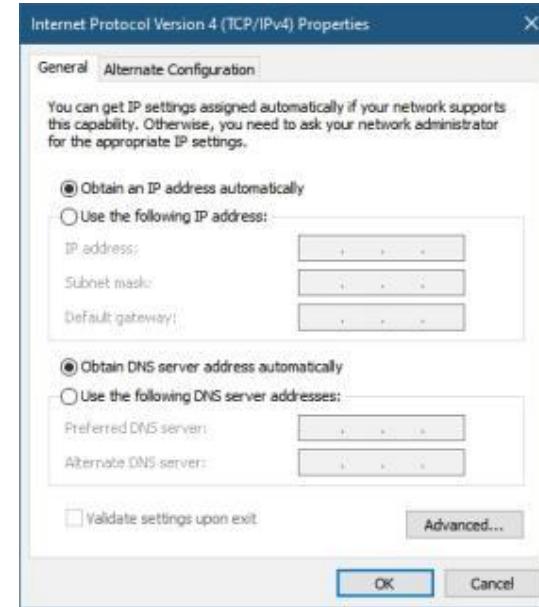


Nota: El direccionamiento IPv6 y las opciones de configuración son similares a IPv4.

Configurar direccionamiento IP

Configuración automática de dirección IP para dispositivos finales

- DHCP habilita la configuración automática de la dirección IPv4 para cada dispositivo final habilitado para DHCP.
- Por lo general, los dispositivos finales usan DHCP para la configuración automática de la dirección IPv4.
- Para configurar DHCP en una PC con Windows, abra el **Panel de control > Centro de uso compartido de red > Cambiar la configuración del adaptador** elige el adaptador. Luego haga clic derecho y seleccione **Propiedades** para mostrar el **Propiedades de conexión de área local**.
- Luego haga clic **Propiedades** para abrir el **Propiedades de Protocolo de Internet versión 4 (TCP / IPv4)** ventana, luego seleccione **Obtenga una dirección IP automáticamente** y **Obtenga la dirección del servidor DNS automáticamente**.



Nota: IPv6 utiliza DHCPv6 y SLAAC (configuración automática de direcciones sin estado) para la asignación dinámica de direcciones.

Cambiar la configuración de la interfaz virtual

Para acceder al conmutador de forma remota, se debe configurar una dirección IP y una máscara de subred en el SVI.

Para configurar un SVI en un conmutador:

- Introducir el **interface vlan 1** comando en modo de configuración global.
- Luego asigne una dirección IPv4 usando el **ip address ip-address subnet-mask**.
- Finalmente, habilite la interfaz virtual usando el **no shutdown** mando.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Packet Tracer - Implemente la conectividad básica

En este Packet Tracer, hará lo siguiente:

- Realizar una configuración básica en dos comutadores
- Configure las PC
- Configure la interfaz de administración del conmutador

2.8 Verificar la conectividad

Video - Probar la asignación de interfaz

Este video cubrirá lo siguiente:

- Conecte un cable de consola desde la PC al interruptor
- Use el programa de emulación de terminal y acepte los valores predeterminados para llevarlo a la línea de comando
- Utilice enable para ingresar al modo EXEC privilegiado
- Use el modo de configuración global y el modo de configuración de la interfaz para ingresar el comando no shutdown

Video: prueba de conectividad de extremo a extremo

Este video cubrirá el uso del comando ping para probar la conectividad en ambos conmutadores y ambas PC.

2.9 Módulo de práctica y cuestionario

Packet Tracer: configuración básica del interruptor y del dispositivo final

En este Packet Tracer, hará lo siguiente:

- Configure nombres de host y direcciones IP en dos comutadores
- Use los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones del dispositivo
- Use los comandos de IOS para guardar la configuración en ejecución
- Configure dos dispositivos host con direcciones IP
- Verifique la conectividad entre los dos dispositivos finales de la PC

Módulo de Práctica y Prueba

Laboratorio: configuración básica del interruptor y del dispositivo final

En este laboratorio, completa los siguientes objetivos:

- Configurar la topología de red
- Configurar hosts de PC
- Configurar y verificar la configuración básica del interruptor

¿Qué aprendí en este módulo?

- Todos los dispositivos finales y dispositivos de red requieren un sistema operativo (SO).
- El software Cisco IOS separa el acceso de administración en los siguientes dos modos de comando: Modo EXEC de usuario y Modo EXEC privilegiado.
- Se accede al modo de configuración global antes que otros modos de configuración específicos. Desde el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración.
- Cada comando IOS tiene un formato o una sintaxis específicos y solo se puede ejecutar en el modo apropiado.
- Configuraciones básicas del dispositivo: nombre de host, contraseña, cifrar contraseñas y banner.
- Hay dos archivos del sistema que almacenan la configuración del dispositivo: startup-config y running-config.
- Las direcciones IP permiten a los dispositivos ubicarse entre sí y establecer una comunicación de extremo a extremo en Internet. Cada dispositivo final en una red debe configurarse con una dirección IP.





Enrutamiento estático



**Conceptos y protocolos de enrutamiento.
Capítulo 2**

Cisco | Networking Academy®
Mind Wide Open™



Objetivos

- Definir la función general que desempeña un router en las redes.
- Describir las redes conectadas directamente y las distintas interfaces del router.
- Analizar las redes conectadas directamente en la tabla de enrutamiento y utilizar el protocolo CDP.
- Describir las rutas estáticas con interfaces de salida.
- Describir la ruta por defecto y la sumarizada.
- Analizar cómo se reenvían los paquetes cuando se usan rutas estáticas.
- Identificar cómo administrar las rutas estáticas y cómo resolver problemas relacionados con ellas.

Función general del router

- Funciones de un router:

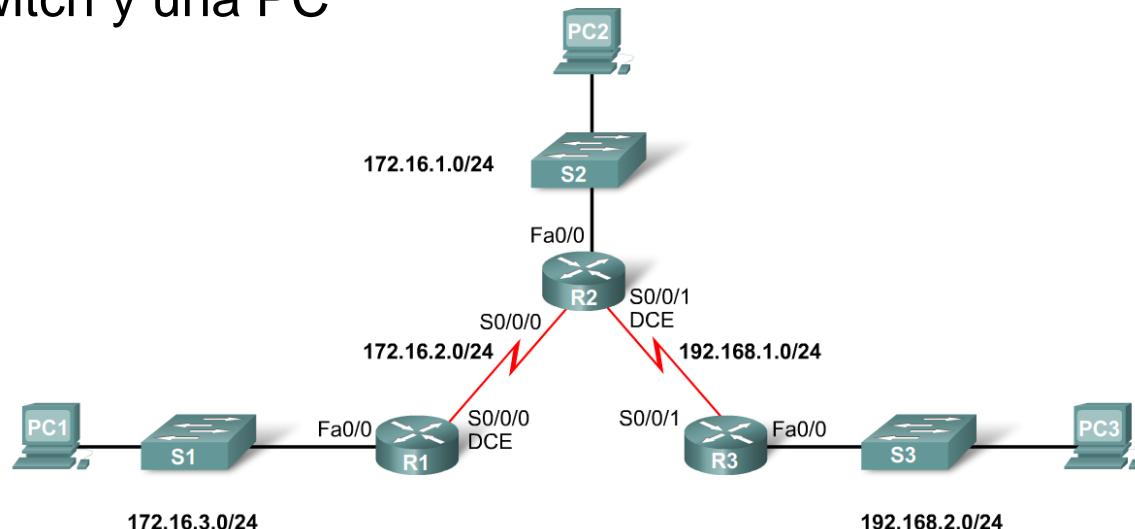
- Selecciones de la mejor ruta

- Reenvío de paquetes al destino

- Presentación de la topología:

- Tres routers serie 1800 conectados por medio de enlaces WAN

- Cada router está conectado a una LAN representada por un switch y una PC





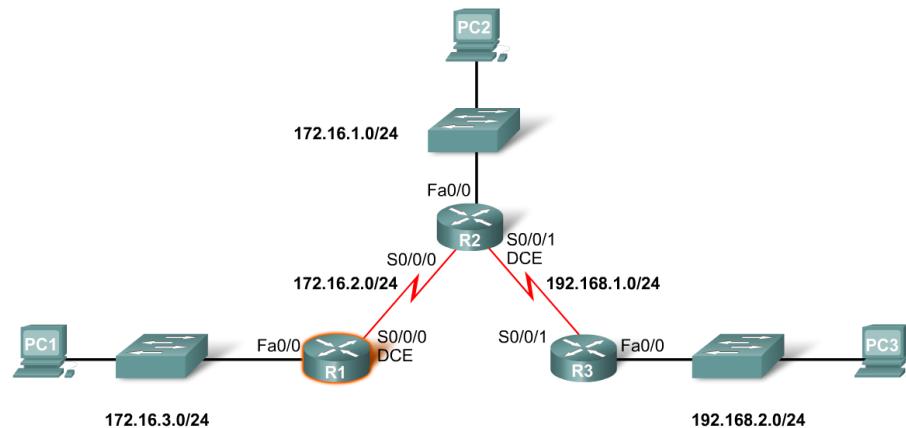
Función general del router

- Conexiones de un router para WAN
 - Un router tiene un puerto DB-60 que puede admitir 5 estándares de cableado diferentes
- Conexiones de un router para Ethernet
 - Pueden usarse 2 tipos de conectores: directos o cruzados.
 - Los conectores directos se usan para conectar:
 - Switch con router, switch con PC, router con servidor, hub con PC, hub con servidor
 - Los conectores cruzados se usan para conectar:
 - Switch con switch, PC con PC, switch con hub, hub con hub, router con router

Interfaces

■ Análisis de interfaces del router

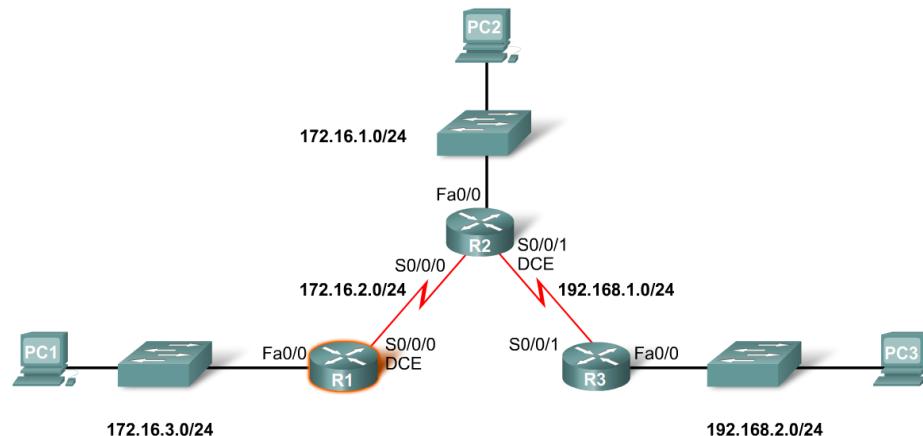
- El comando **show IP router** se usa para ver la tala de enrutamiento
- El comando **show interfaces** se usa para mostrar el estado de una interfaz
- El comando **show IP interface brief** muestra una parte de la información de interfaz
- El comando **show running-config** muestra el archivo de configuración de la RAM



Interfaces

■ Configuración de una interfaz Ethernet

- Por defecto, todas las interfaces seriales y Ethernet están inhabilitadas
- Para habilitar una interfaz, use el comando **no shutdown**



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set
```

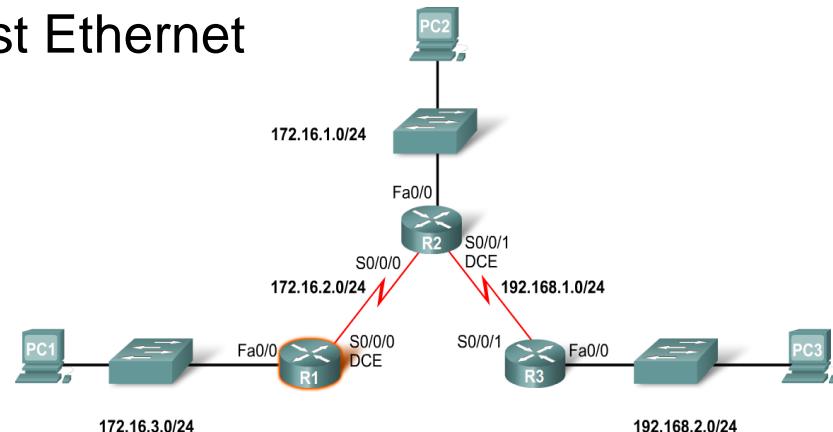
```
R1#
```

Interfaces

■ Verificación de la interfaz Ethernet

- El comando **show interfaces for fastEthernet 0/0** muestra el estado del puerto de Fast Ethernet
- **show ip interface brief**
- **show running-config**

■ Las interfaces Ethernet participan en ARP



Verificando las direcciones MAC en interfaces Ethernet

```
R1#show interfaces fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  Internet address is 172.16.3.1/24
<output omitted>
R1#
```

Las interfaces Ethernet tienen direcciones MAC.



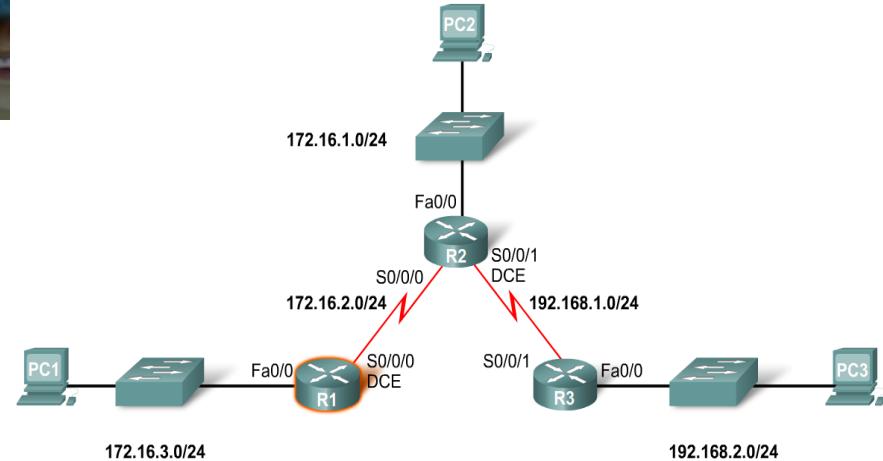
Interfaces

- **Configuración de una interfaz serial**

- Escriba el modo de configuración de interfaz
- Escriba la dirección IP y la máscara de subred
- Escriba el comando **no shutdown**

- Ejemplo:

- R1(config)#interface serial 0/0
- R1(config-if)#ip address 172.16.2.1 255.255.255.0
- R1(config-if)#no shutdown



La interfaz Serial con down y down

```
R1#show interfaces serial 0/0/0
Serial0/0/0 is down, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 172.16.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
<output omitted>
```

La interfaz Serial es down y down aunque tiene una dirección IP y fue habilitada con el comando **no shutdown**.



Interfaces

■ Análisis de interfaces del router

- Conexión física de una interfaz WAN
- Una conexión WAN de capa física tiene dos lados:
 - El equipo de terminación del circuito de datos (DCE): es el proveedor de servicios. Las CSU/DSU se consideran dispositivos DCE
 - El equipo terminal de datos (DTE): en general, el router es el dispositivo DTE



Interfaces

■ Configuración de enlaces seriales en un entorno de laboratorio

- Un lado de una conexión serial debe considerarse un DCE
- Esto requiere colocar una señal de temporización: use el comando `clockrate`
- Ejemplo:
 - `R1(config)#interface serial 0/0`
 - `R1(config-if)#clockrate 64000`
- Las interfaces seriales necesitan una señal de temporización para controlar las comunicaciones



Protocolo CDP y tabla de enrutamiento

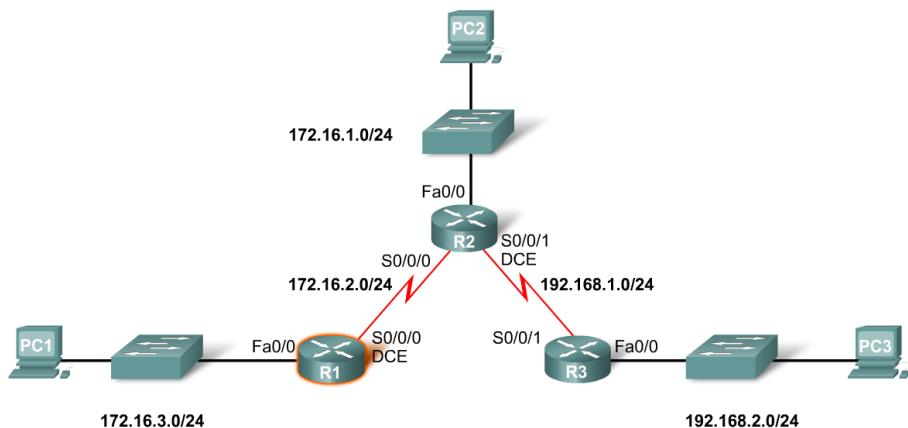
■ Función del comando **debug ip routing**

- Le permite ver los cambios que realiza el router cuando incorpora o elimina rutas
- Ejemplo:
 - R2#debug ip routing
 - Está habilitada la depuración de enrutamiento IP

Protocolo CDP y tabla de enrutamiento

- Para configurar una interfaz Ethernet
 - Ejemplo:

- R2(config)#interface fastethernet 0/0
- R2(config-if)#ip address 172.16.1.1 255.255.255.0
- R2(config-if)#no shutdown



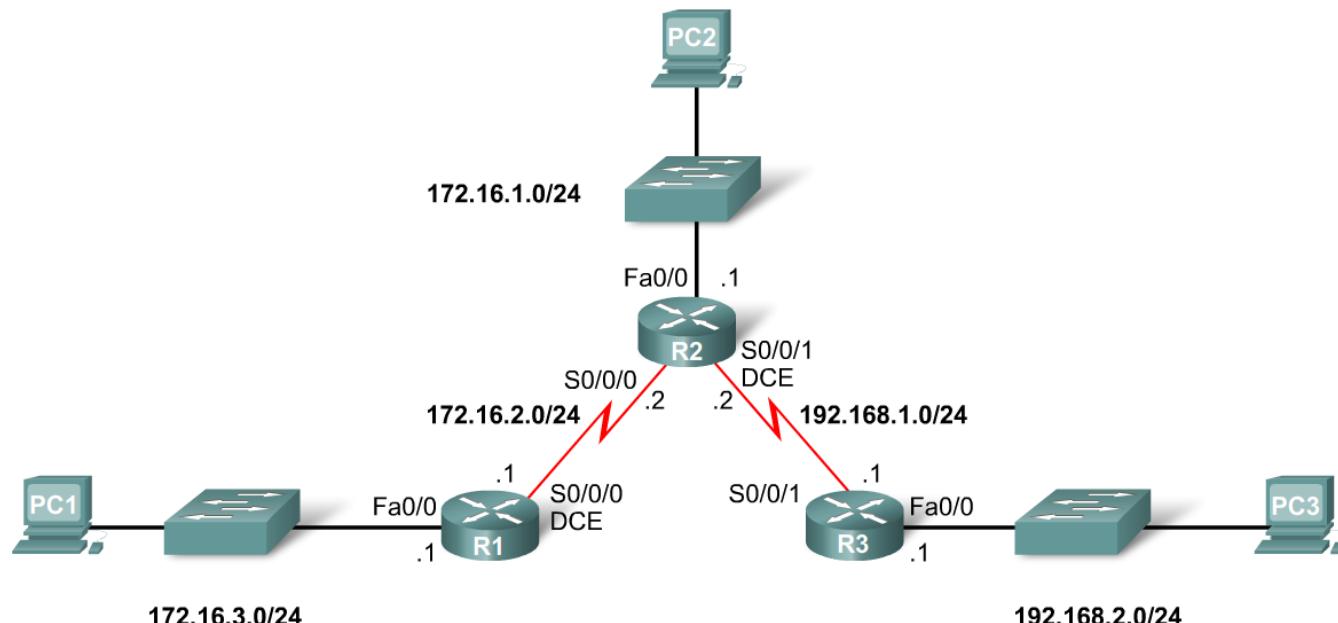
```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

R1#
```

Protocolo CDP y tabla de enrutamiento

- Cuando un **router** sólo tiene sus **interfaces configuradas** y no hay otros protocolos de enrutamiento configurados:
 - La **tabla de enrutamiento** contiene sólo las redes conectadas directamente
 - Solamente los dispositivos en las redes conectadas directamente pueden alcanzarse



Protocolo CDP y tabla de enrutamiento

Con show ip interface brief se puede acceder al resumen del estado de la interfaz

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
FastEthernet0/0    unassigned      YES manual administratively down down
Serial0/0/0        unassigned      YES unset   administratively down down
FastEthernet0/1    unassigned      YES unset   administratively down down
Serial0/0/1        unassigned      YES unset   administratively down down
```

La tabla de enrutamiento no tiene rutas

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

R1#
```

```
R1#show running-config
!
version 12.3
!
hostname R1
!
!
enable secret 5 $1$3ROSVLUOdBF2OqNBn0EjQBvR./
!
!
interface FastEthernet0/0
  mac-address 00c.3010.9260
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface FastEthernet0/1
```

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
```

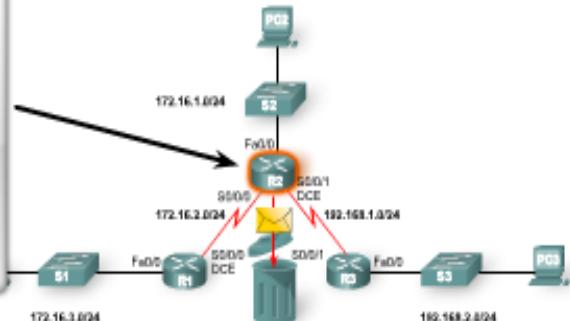
```
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
```

Protocolo CDP y tabla de enrutamiento

- Verificación de cada una de las rutas:

El comando ping se usa para verificar la conectividad de extremo a extremo

```
R2#ping 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1,
    timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#
```



```
R2#show ip route
<output omitted>

      172.16.0.0/24 is subnetted, 2 subnets
C        172.16.1.0 is directly connected, FastEthernet0/0
C        172.16.2.0 is directly connected, Serial0/0/0
C  192.168.1.0/24 is directly connected, Serial0/0/1
R2#
```

Dirección IP de destino 172.16.3.1 10101100.00010000.00000011.00000001
Primera ruta en la tabla de enrutamiento 172.16.1.0 10101100.00010000.00000001.00000000 No hay coincidencia

Dirección IP de destino	172.16.3.1	10101100.00010000.00000011.00000001	No hay coincidencia
Segunda ruta en la tabla de enrutamiento	172.16.3.0	10101100.00010000.00000010.00000000	

Dirección IP de destino 172.16.3.1 10101100.00010000.00000011.00000001
Tercera ruta en la tabla de enrutamiento 192.168.1.0 11000000.10101000.00000001.00000000 No hay coincidencia

Protocolo CDP y tabla de enrutamiento

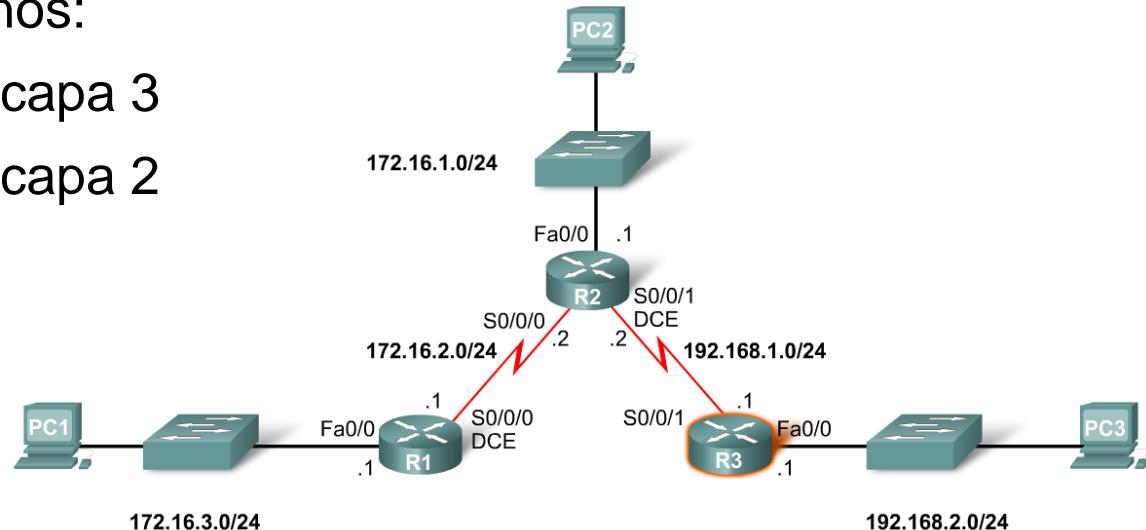
■ Función de CDP

Es una herramienta (propiedad de Cisco) de capa 2 y se usa para reunir información acerca de otros dispositivos Cisco **conectados directamente**.

■ Concepto de vecinos

- 2 tipos de vecinos:

- Vecinos de capa 3
- Vecinos de capa 2





Protocolo CDP y tabla de enrutamiento

- Comandos show de CDP
 - El comando **show cdp neighbors**
 - Muestra la siguiente información:
 - ID del dispositivo vecino
 - Interfaz local
 - Valor del tiempo de espera, en segundos
 - Código de capacidad del dispositivo vecino
 - Plataforma de hardware del vecino
 - ID del puerto remoto del vecino
 - El comando **show cdp neighbors detail**
 - Útil para determinar si se produjo un error de configuración de dirección IP



Protocolo CDP y tabla de enrutamiento

■ Inhabilitación de CDP

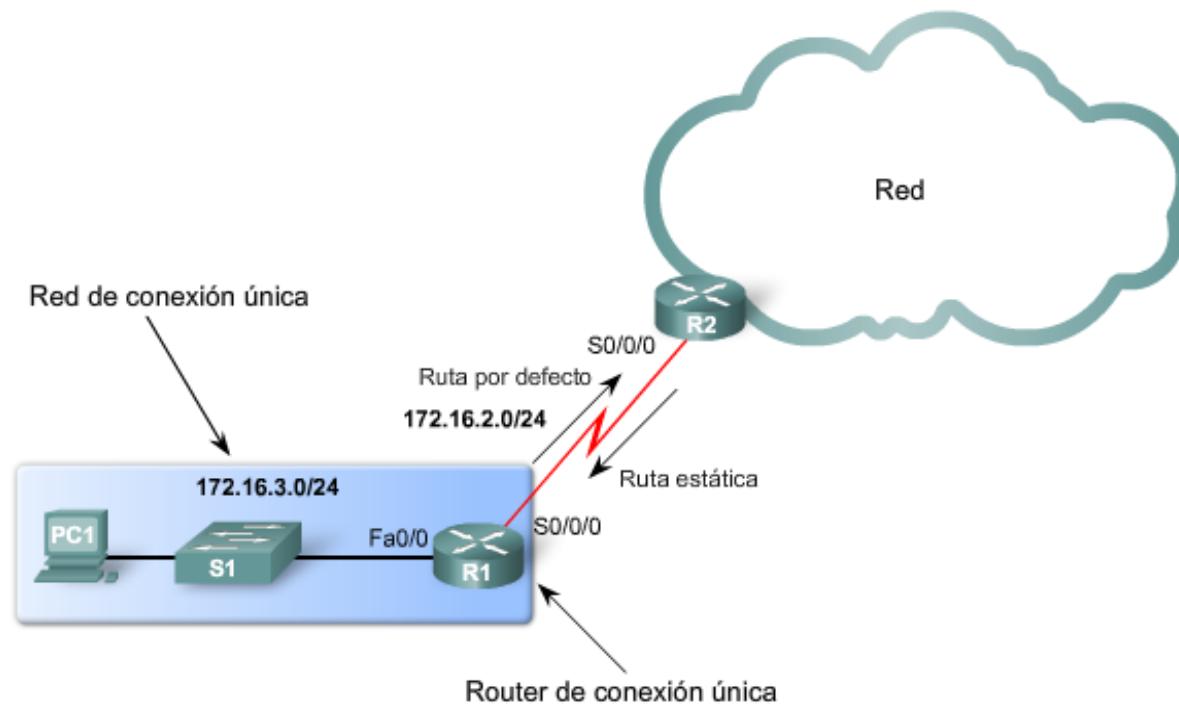
Para deshabilitar CDP globalmente, use el siguiente comando:

```
Router(config)#no cdp run
```

Rutas estáticas con interfaces de salida

■ Función de una ruta estática

Una ruta configurada manualmente que se usa para el enrutamiento desde una red hasta una red de conexión única



Rutas estáticas con interfaces de salida

■ Comando **IP route**

- Para configurar una ruta estática, utilice el siguiente comando:
ip route
- Ejemplo:
 - Router(config)# ip route dirección_red máscara_subred {dirección ip | interfaz de salida}

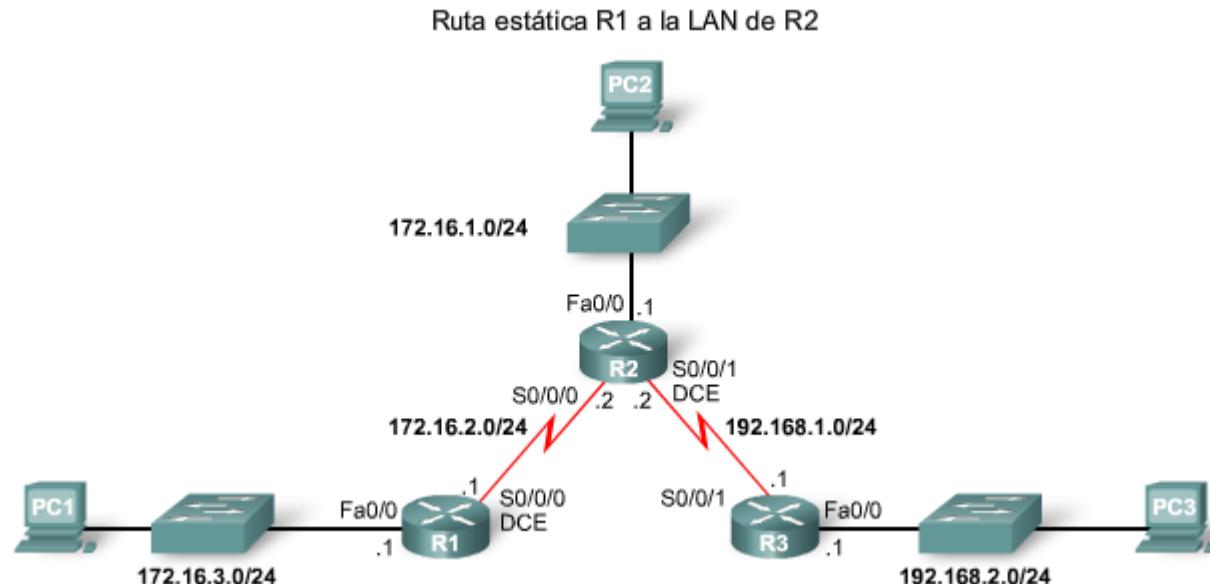
```
Router(config)# ip route network-address subnet-mask  
{ip-address | exit-interface }
```

Parámetro	Descripción
network-address	Dirección de la red de destino de la red remota que será agregada a la tabla de enrutamiento.
subnet-mask	Máscara de subred de la red remota que será agregada a la tabla de enrutamiento. La máscara de subred puede ser modificada para resumir un grupo de redes.
ip-address	Se la denomina comúnmente como dirección IP del router del siguiente salto.
exit-interface	Interfaz de salida utilizada para enviar paquetes a la red de destino.

Rutas estáticas con interfaces de salida

■ Desglose de la sintaxis de la ruta estática

- ip route: comando de la ruta estática
- 172.16.1.0: dirección de la red de destino
- 255.255.255.0: máscara de subred de la red de destino
- 172.16.2.2: dirección IP de la interfaz 0/0/0 serial del R2, que es el “siguiente salto” a esta red

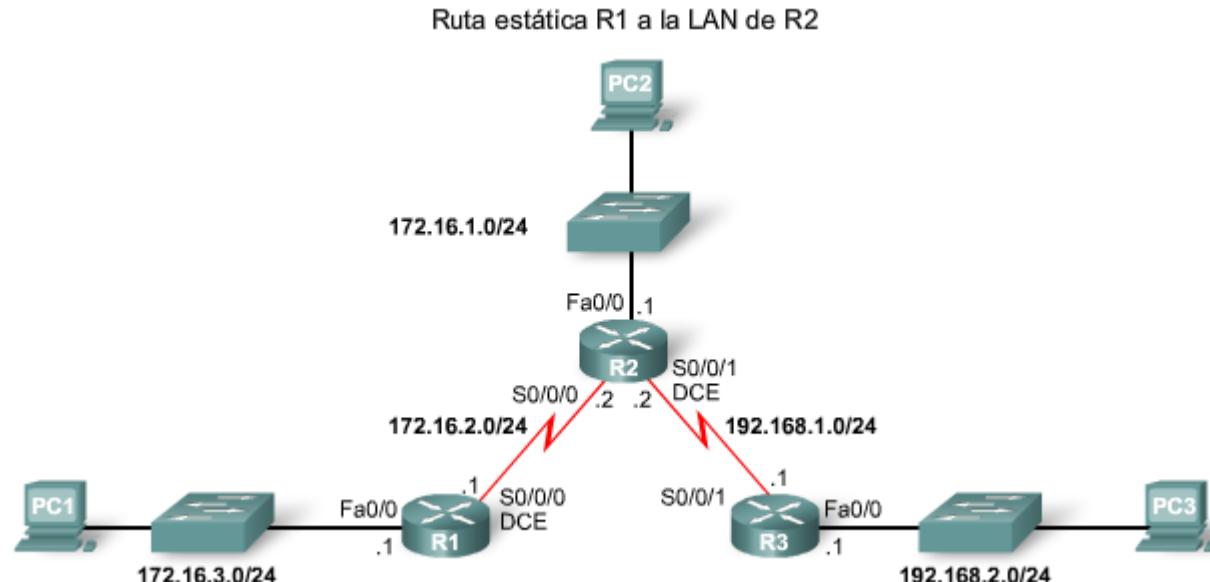


Rutas estáticas con interfaces de salida

- Configuración de las rutas hacia 2 redes remotas o más

Use los siguientes comandos para R1:

- R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
- R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2





Rutas estáticas con interfaces de salida

■ **Los tres principios de enrutamiento de Zinin**

- **Principio 1:** “Cada router toma decisiones de forma independiente, sobre la base de la información que contiene en la tabla de enrutamiento”.
- **Principio 2:** “El hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los demás routers contengan la misma información”.
- **Principio 3:** “La información de enrutamiento acerca de una ruta que va desde una red hasta otra no proporciona información de enrutamiento acerca de la ruta en sentido contrario o ruta de regreso”.

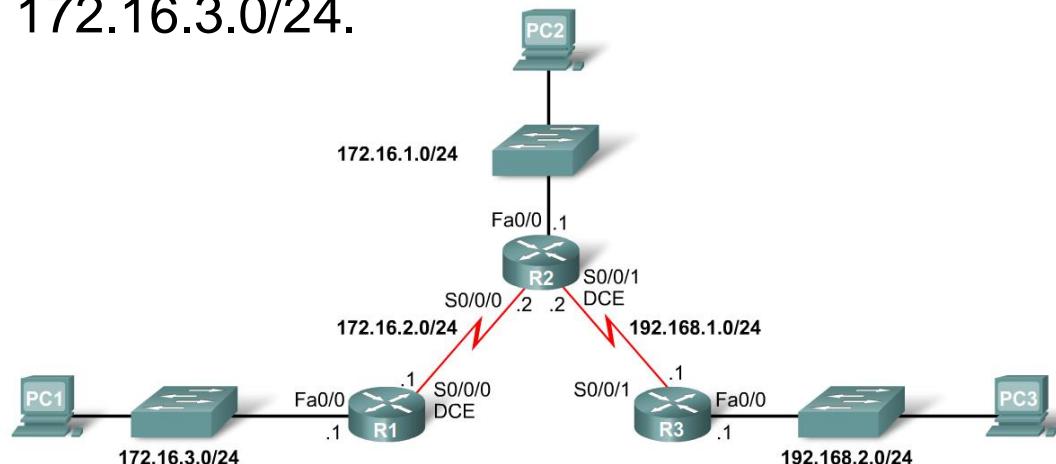
Rutas estáticas con interfaces de salida

- A partir de los 3 principios de enrutamiento de Zinin, ¿cómo respondería lo siguiente?
 - ¿Los paquetes de PC1 llegarán a su destino?

Sí, los paquetes con destino a las redes 172.16.1.0/24 y 192.168.1.0/24 llegarán a sus destinos.

- ¿Esto significa que todos los paquetes de estas redes con destino a la red 172.16.3.0/24 llegarán a su destino?

No, porque ni el router R2 ni el R3 tienen una ruta hacia la red 172.16.3.0/24.

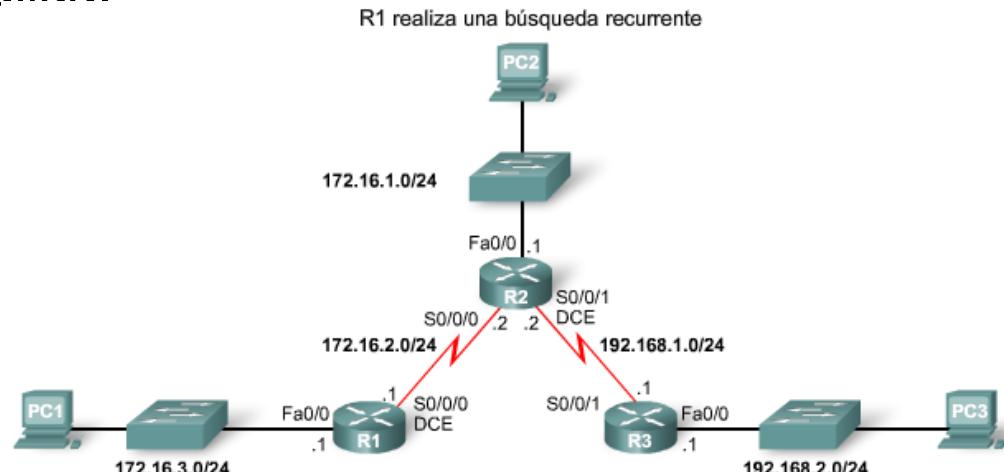


Rutas estáticas con interfaces de salida

- Asociación a una interfaz de salida

- **Búsqueda recursiva de rutas:** ocurre cuando el router tiene que realizar varias búsquedas en la tabla de enrutamiento antes del reenvío de un paquete. Una ruta estática que reenvía todos los paquetes a la dirección IP del siguiente salto atraviesa el proceso que se muestra a continuación (búsqueda aislada de rutas).

- Primero, el router debe hacer coincidir la dirección IP de destino de la ruta estática con la dirección del siguiente salto.
 - Luego, la dirección del siguiente salto se compara con una interfaz de salida.



Rutas estáticas con interfaces de salida

- Configuración de una ruta estática con una interfaz de salida
 - Las rutas estáticas configuradas con una interfaz de salida son **más eficaces** debido al enrutamiento
 - La tabla de enrutamiento puede resolver la interfaz de salida en una sola búsqueda en vez de resolverla en 2
 - Ejemplo de una sintaxis necesaria para configurar una ruta estática con una interfaz de salida

Las rutas R1 dependen de la interfaz de salida

```
R1#debug ip routing
IP routing debugging is on
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#shutdown
R1(config-if)#end

is up: 0 state: 6 sub state: 1 line: 0
RT: interface Serial0/0/0 removed from routing table
RT: del 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: delete subnet route to 172.16.2.0/24
RT: del 192.168.1.0 via 172.16.2.2, static metric [1/0]
RT: delete network route to 192.168.1.0
RT: del 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
RT: delete subnet route to 172.16.1.0/24

R1#show ip route
<output omitted>
```

Se eliminan cuatro rutas.
Sólo queda una ruta en la tabla.

Rutas estáticas con interfaces de salida

■ Modificación de rutas estáticas

- Las rutas estáticas existentes **no pueden** modificarse. Debe eliminarse la ruta estática anterior mediante la colocación de **no** antes de **ip route**
- Ejemplo:
 - **no ip route 192.168.2.0 255.255.255.0 172.16.2.2**
- Una ruta estática nueva debe reescribirse en la configuración

```
R1(config) #no ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config) #ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config) #no ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config) #ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

```
R2(config) #no ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config) #ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config) #no ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config) #ip route 192.168.2.0 255.255.255.0 serial 0/0/1
```

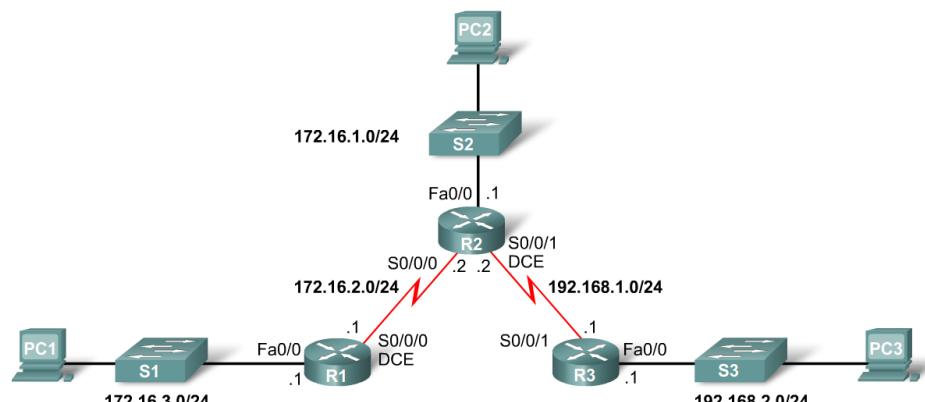
```
R3(config) #no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config) #ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config) #no ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config) #ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config) #no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config) #ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Rutas estáticas con interfaces de salida

■ Verificación de la configuración de rutas estáticas

- Utilice los siguientes comandos:

- Paso 1: **show running-config**
- Paso 2: **verifique** que la ruta estática se haya escrito correctamente
- Paso 3: **show ip route**
- Paso 4: **verifique** que la ruta se haya configurado en la tabla de enrutamiento
- Paso 5: ejecute el comando **ping** para **verificar** que los paquetes puedan llegar al destino y que la ruta de regreso funcione



Rutas estáticas con interfaces de salida

■ Interfaces Ethernet y ARP

— Si se configura una ruta estática en un enlace Ethernet

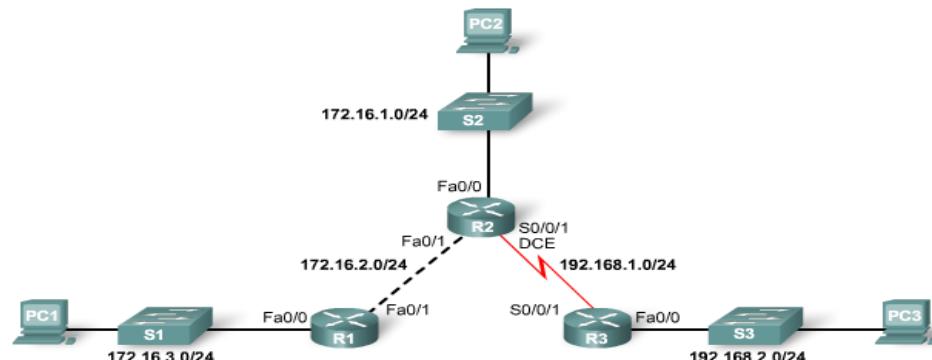
- Si el paquete se envía al router del siguiente salto,

la dirección MAC de destino será la dirección de la interfaz Ethernet del siguiente salto.

El router descubre esto mediante la consulta de la tabla ARP.

Si no se encuentra una entrada, se enviará una solicitud ARP.

Interfaz de salida y dirección del siguiente salto





Ruta por defecto y summarizada

- **El resumen de rutas** **reduce** el tamaño de la tabla de enrutamiento.
- **La summarización de ruta** es el proceso de combinación de una cantidad de rutas estáticas en una sola ruta estática.

Ruta por defecto y summarizada

■ Configuración de una ruta summarizada

Paso 1: elimine la ruta estática actual

Paso 2: configure la ruta estática summarizada

Paso 3: verifique la ruta estática nueva

```
R3#show ip route
<output omitted>

Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 3 subnets
 S   172.16.1.0 is directly connected, Serial0/0/1
 S   172.16.2.0 is directly connected, Serial0/0/1
 S   172.16.3.0 is directly connected, Serial0/0/1
 C 192.168.1.0/24 is directly connected, Serial0/0/1
 C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R3#show ip route
<output omitted>

Gateway of last resort is not set

 172.16.0.0/22 is subnetted, 1 subnets
 S   172.16.0.0 is directly connected, Serial0/0/1
 C 192.168.1.0/24 is directly connected, Serial0/0/1
 C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R3#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R3#ping 172.16.2.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3#ping 172.16.3.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3#
```

Ruta por defecto y summarizada

■ Rutas estáticas por defecto

- Ésta es una ruta que coincidirá con todos los paquetes.

Los routers de conexión única que tienen una cantidad de rutas estáticas con la misma interfaz de salida son buenos candidatos para una ruta por defecto.

- Al igual que la summarización de ruta, esto ayudará a reducir el tamaño de la tabla de enrutamiento.

■ Configuración de una ruta estática por defecto

- Es similar a configurar una ruta estática. Excepto que la dirección IP de destino y la máscara de subred son todos ceros.

- Ejemplo:

- Router(config)#ip route 0.0.0.0 0.0.0.0 [interfaz de salida | dirección ip]



Ruta por defecto y summarizada

- **Rutas estáticas y máscaras de subred**

El proceso de búsqueda de la tabla de enrutamiento **usará la concordancia más específica** cuando compare la dirección IP de destino y la máscara de subred.

- **Rutas estáticas por defecto y máscaras de subred**

Como la máscara de subred usada en la ruta estática por defecto es 0.0.0.0, todos los paquetes coincidirán.

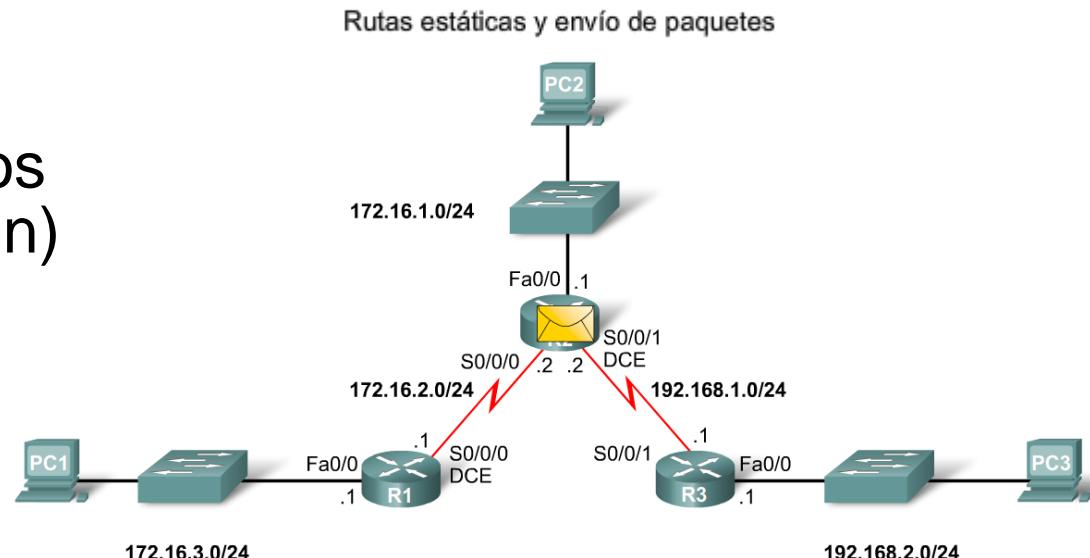
Rutas estáticas y reenvío de paquetes

- Reenvío de paquetes con rutas estáticas (recuerde los 3 principios de enrutamiento de Zinin)
- Router 1

El paquete llega a la interfaz Fastethernet 0/0 del R1

El R1 no tiene una ruta hacia la red de destino, 192.168.2.0/24

El R1 usa la ruta estática por defecto



R1#show ip route

<output omitted>

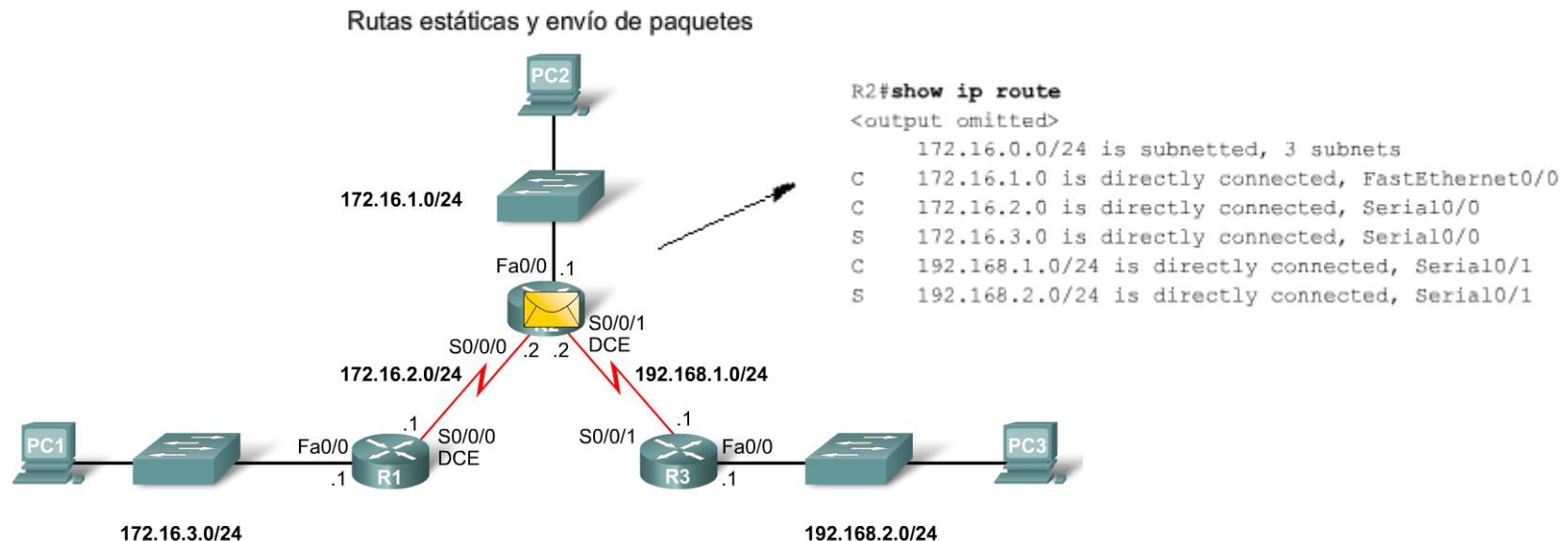
```
    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.2.0 is directly connected, Serial0/0
C      172.16.3.0 is directly connected, FastEthernet0/0
S*     0.0.0.0/0 is directly connected, Serial0/0
```

Rutas estáticas y reenvío de paquetes

- Reenvío de paquetes con rutas estáticas (recuerde los 3 principios de enrutamiento de Zinin)
- Router 2

El paquete llega a la interfaz serial 0/0/0 en el R2

El R2 tiene una ruta estática hacia 192.168.2.0/24 a través de Serial0/0/1

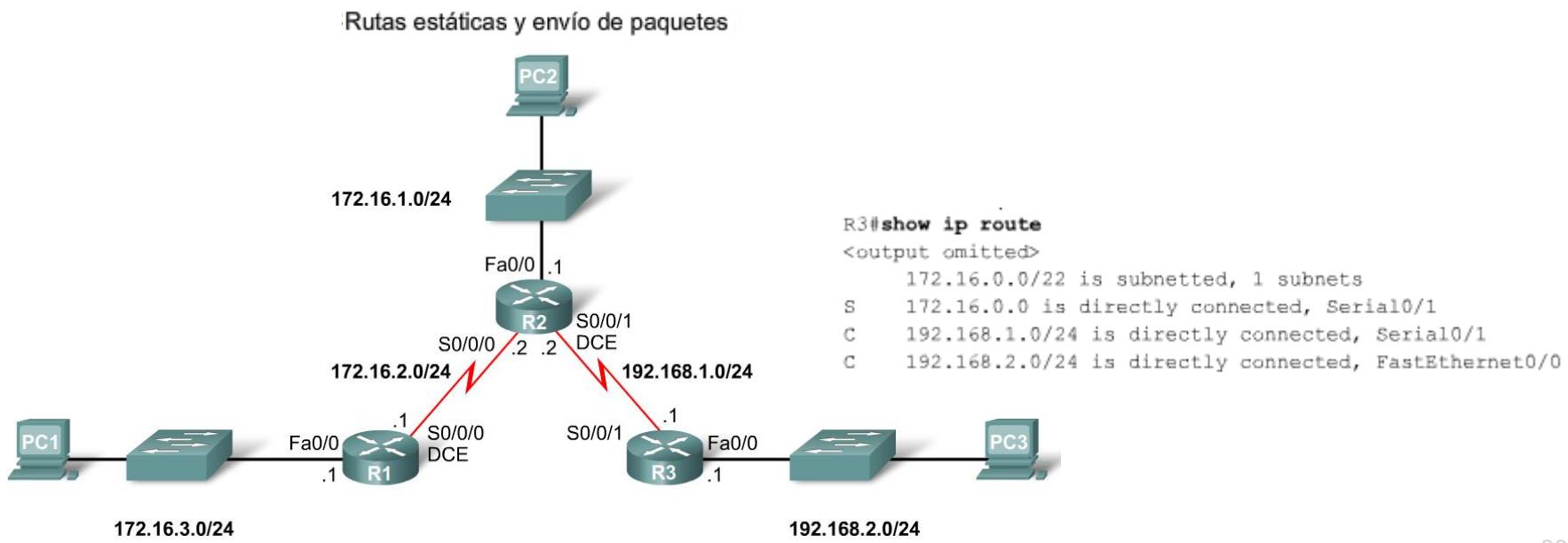


Rutas estáticas y reenvío de paquetes

- Reenvío de paquetes con rutas estáticas (recuerde los 3 principios de enrutamiento de Zinin)
- Router 3

El paquete llega a la interfaz serial 0/0/1 en el R3

El R3 tiene una ruta conectada con 192.168.2.0/24 a través de Fastethernet 0/1



Rutas estáticas y reenvío de paquetes

- Resolución de problemas causados por la falta de una ruta
- Las herramientas que pueden usarse para aislar los problemas de enrutamiento incluyen:
 - **Ping:** prueba la conectividad de extremo a extremo
 - **Traceroute:** detecta todos los saltos (routers) a lo largo del camino entre dos puntos
 - **Show IP route:** muestra la tabla de enrutamiento y asegura el proceso de reenvío
 - **Show ip interface brief:** muestra el estado de las interfaces del router
 - **Show cdp neighbors detail:** recopila información de configuración de los vecinos conectados directamente



Rutas estáticas y reenvío de paquetes

- Resolución de la ruta que falta
- Encontrar una ruta que falta o está mal configurada requiere el uso metódico de las herramientas adecuadas
 - Comience con **PING**. Si ping no funciona, use traceroute para determinar a dónde no llegan los paquetes
- Ejecute **show IP route** para analizar la tabla de enrutamiento
 - Si hay un problema con una ruta estática mal configurada, elimine la ruta estática y luego vuelva a configurar la ruta estática nueva



Rutas estáticas y reenvío de paquetes

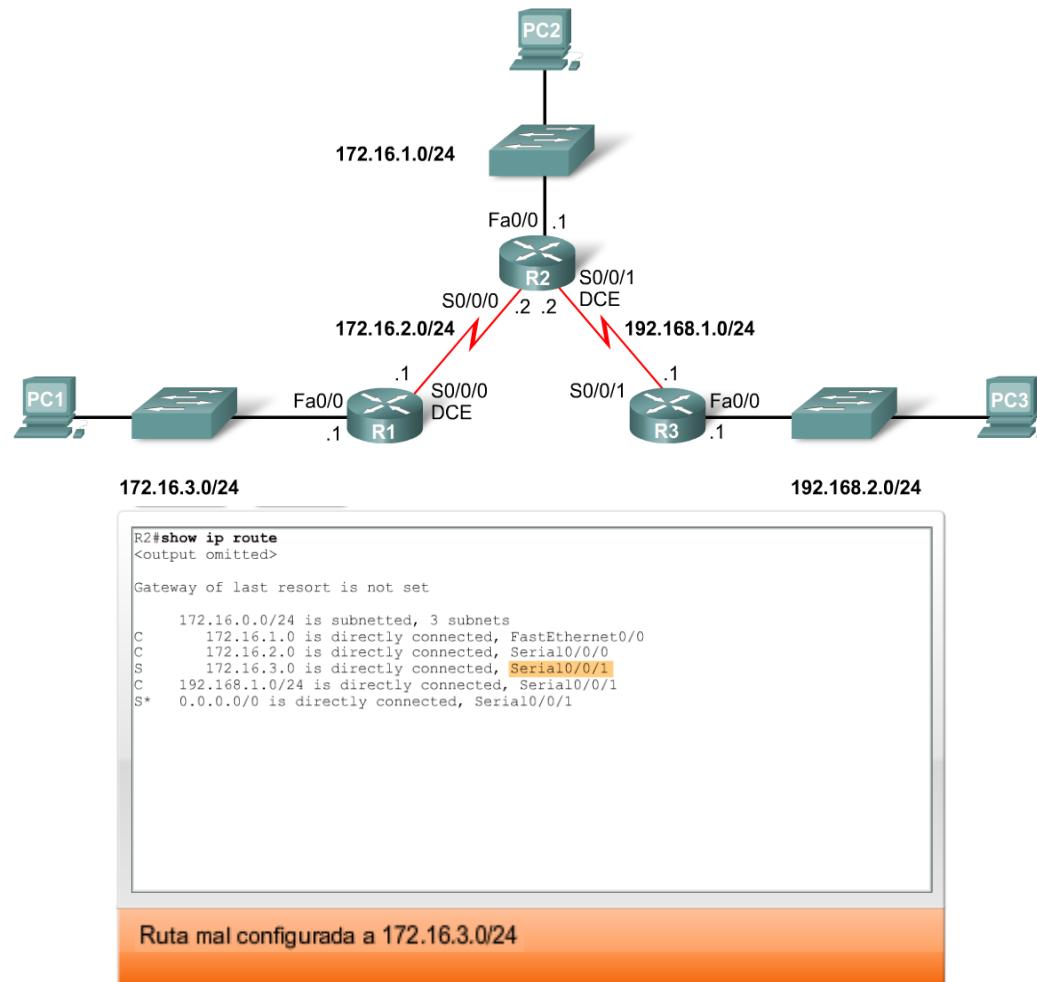
- Resolución de la ruta que falta

Herramientas para la resolución de problemas de conectividad

- **ping**
- **traceroute**
- **show ip route**
- **show ip interface brief**
- **show cdp neighbors detail**

Rutas estáticas y reenvío de paquetes

- Resolución de la ruta que falta





Resumen

■ Routers

- Funcionan en la capa 3
- Las funciones incluyen la selección de la mejor ruta y el reenvío de paquetes

■ Conexión de redes

WAN

Los cables seriales se conectan a los puertos seriales del router
En el entorno de laboratorio, debe configurarse la frecuencia de reloj para DCE

LAN

Los cables de conexión directa o cruzada se utilizan para conectar al puerto fastethernet. (El tipo de cable dependerá de los dispositivos que se vayan a conectar)

■ Cisco Discovery Protocol

Un protocolo privado de capa 2

Se usa para detectar información acerca de los dispositivos **Cisco** conectados en forma directa



Resumen

- **Rutas estáticas**
 - Éstas son rutas configuradas manualmente que especifican cómo llegará el router a un punto determinado por medio de una ruta determinada.
- **Rutas estáticas summarizadas**
 - Son varias rutas estáticas que han sido resumidas en una sola ruta estática.
- **Ruta por defecto**
 - Es la ruta que usan los paquetes si no encuentran otra coincidencia posible para su destino en la tabla de enrutamiento.
- **Reenvío de paquetes cuando se usa la ruta estática**
 - Los tres principios de enrutamiento de Zinin describen cómo se reenvían los paquetes.
- **La resolución de problemas de rutas estáticas** puede requerir alguno de los siguientes comandos:
 - Ping
 - Traceroute
 - Show IP route
 - Show ip interface brief
 - Show cdp neighbors detail



Introducción al enrutamiento y envío de paquetes



**Conceptos y protocolos de enrutamiento.
Capítulo 1**

Cisco | Networking Academy®
Mind Wide Open™



Objetivos

- Identificar un router como una computadora con SO y hardware diseñados para el proceso de enrutamiento.
- Demostrar la capacidad de configurar dispositivos y aplicar direcciones.
- Describir la estructura de una tabla de enrutamiento.
- Describir el proceso por medio del cual un router determina la ruta y commuta paquetes.

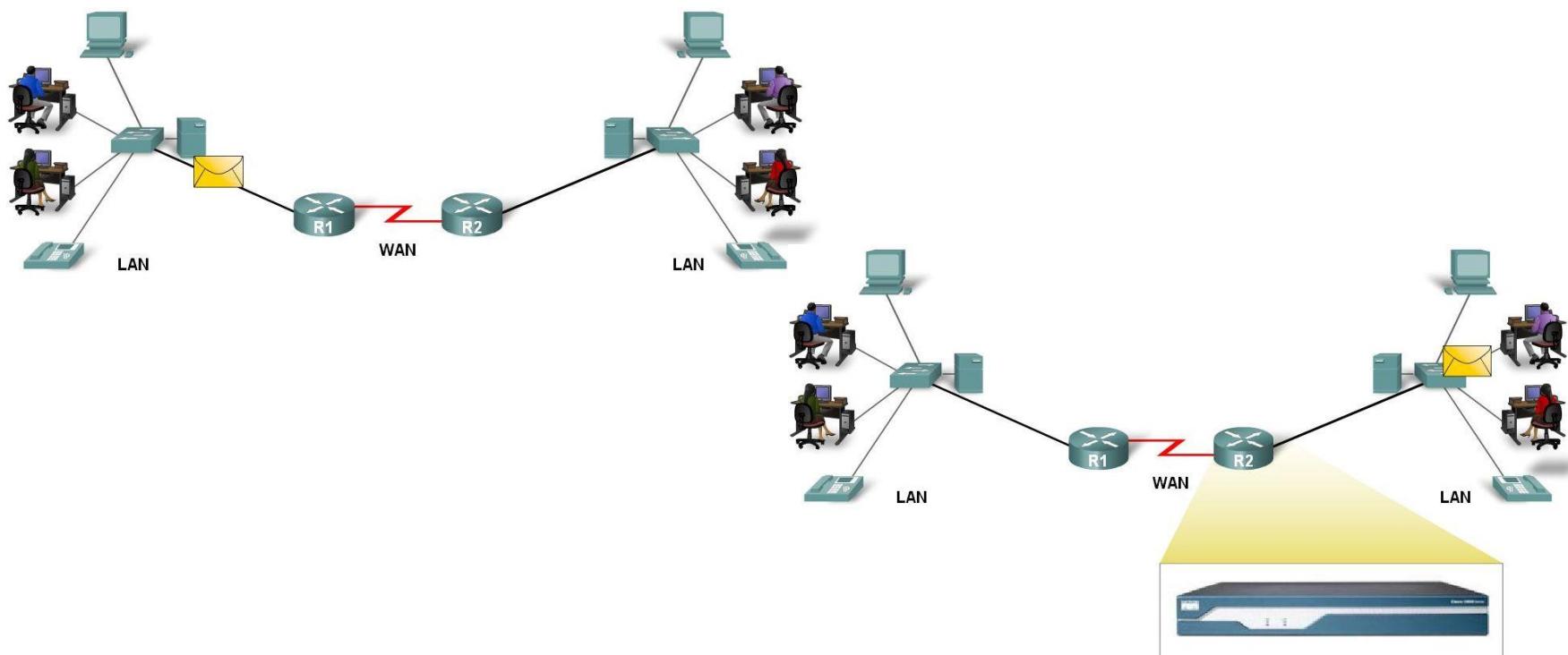


El router como una computadora

- Describa la función básica de un router
 - Son computadoras que se especializan en el envío de paquetes a través de redes de datos. Son los responsables de la interconexión de las redes: seleccionan la mejor ruta para transmitir los paquetes y los reenvían al destino.
- Los routers son el centro de una red
 - Por lo general, los routers tienen 2 conexiones:
 - Conexión WAN (conexión a un ISP)
 - Conexión LAN

El router como una computadora

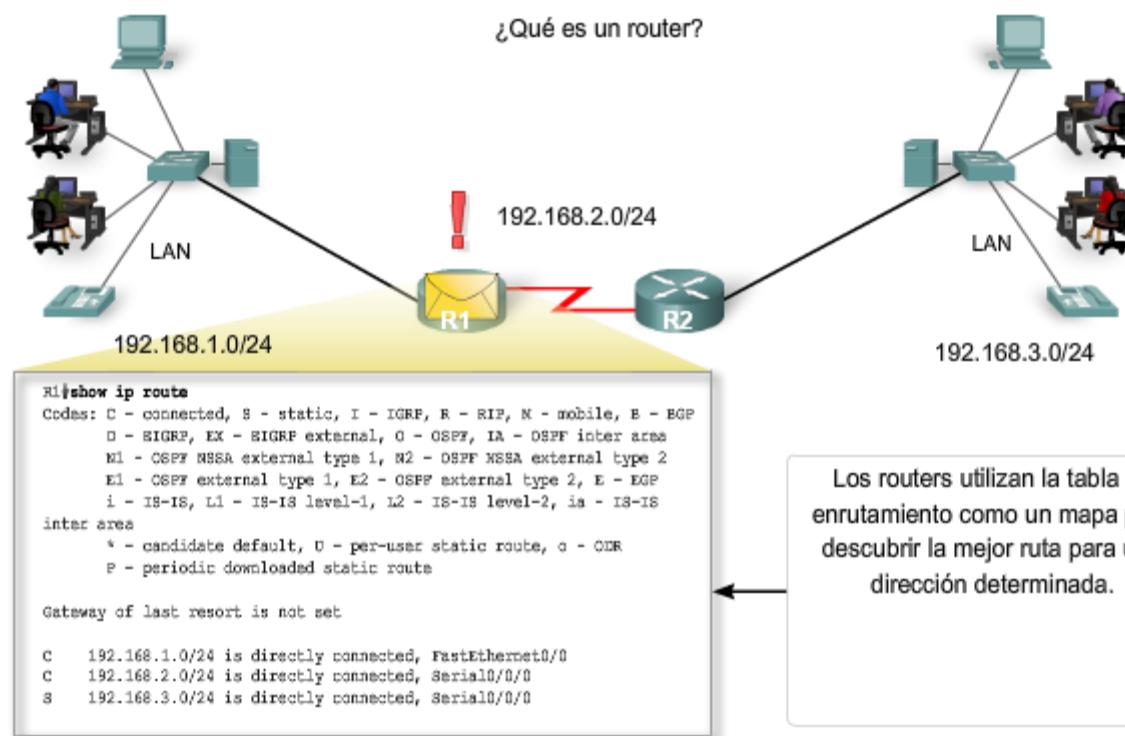
- Los datos se envían en paquetes entre 2 dispositivos finales
- Los routers se usan para dirigir los paquetes hacia los destinos



Los routers dirigen paquetes hacia el destino correspondiente. Los routers conectan diferentes medios.

El router como una computadora

- Los routers examinan la dirección IP de destino del paquete y, con la ayuda de una tabla de enruteamiento, determinan cuál es la mejor ruta

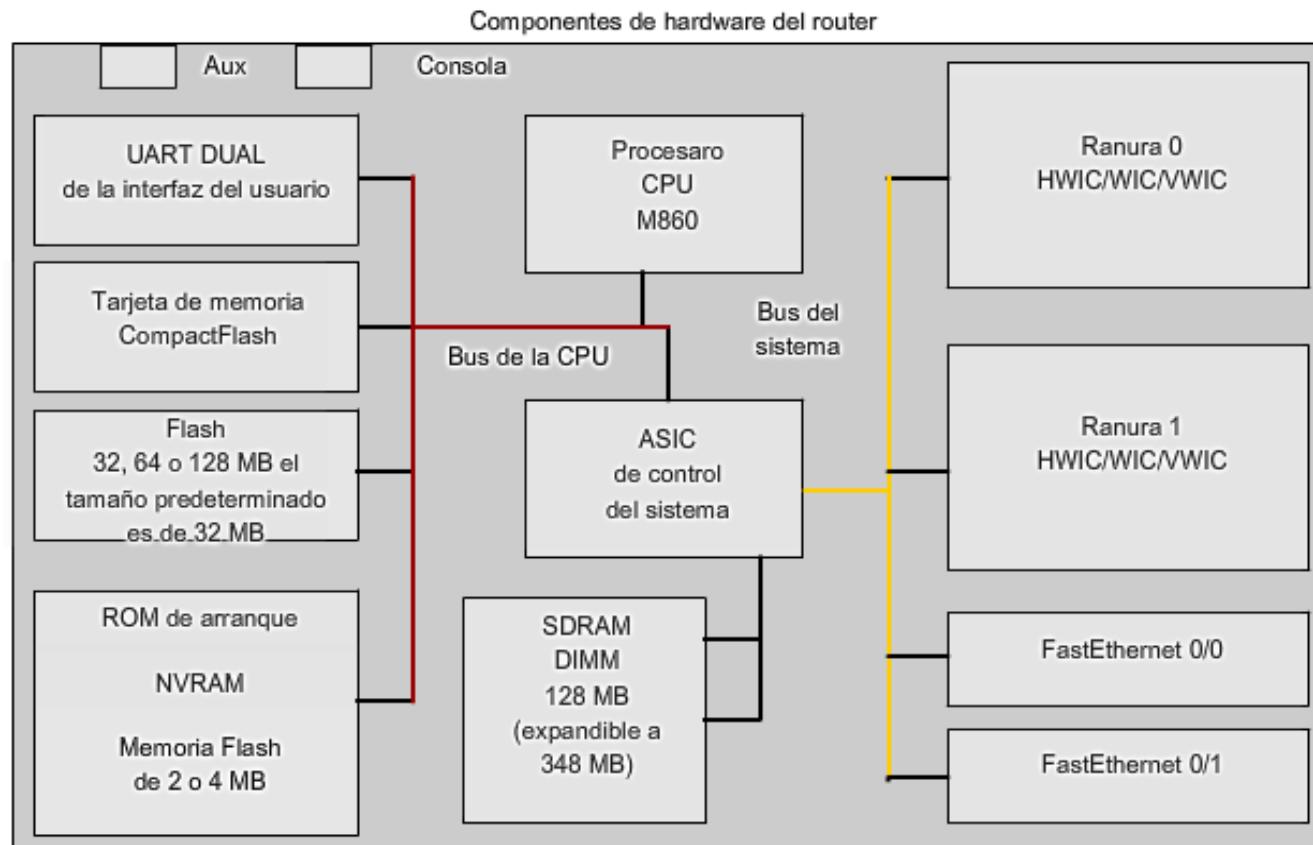


El router como una computadora

- Los componentes de los routers y sus funciones:
 - **CPU:** Ejecuta las instrucciones del sistema operativo
 - **Memoria de acceso aleatorio (RAM):** Contiene la copia en ejecución del archivo de configuración. Almacena la tabla de enrutamiento. Los contenidos de la RAM se pierden cuando se apaga el equipo
 - **Memoria de sólo lectura (ROM):** Almacena software de diagnóstico que se usa cuando se enciende el router. Contiene el programa bootstrap
 - **RAM no volátil (NVRAM):** Almacena la configuración de inicio. Esta configuración puede incluir direcciones IP (protocolo de enrutamiento, nombre de host del router)
 - **Memoria flash:** Contiene el sistema operativo (IOS de Cisco).
 - **Interfaces:** Hay varias interfaces físicas que se usan para conectar redes. Ejemplos de tipos de interfaces:
 - Interfaces Ethernet/Fast Ethernet
 - Interfaces seriales
 - Interfaces de administración

El router como una computadora

■ Componentes del router



El router como una computadora

- Fases principales del proceso de inicio del router

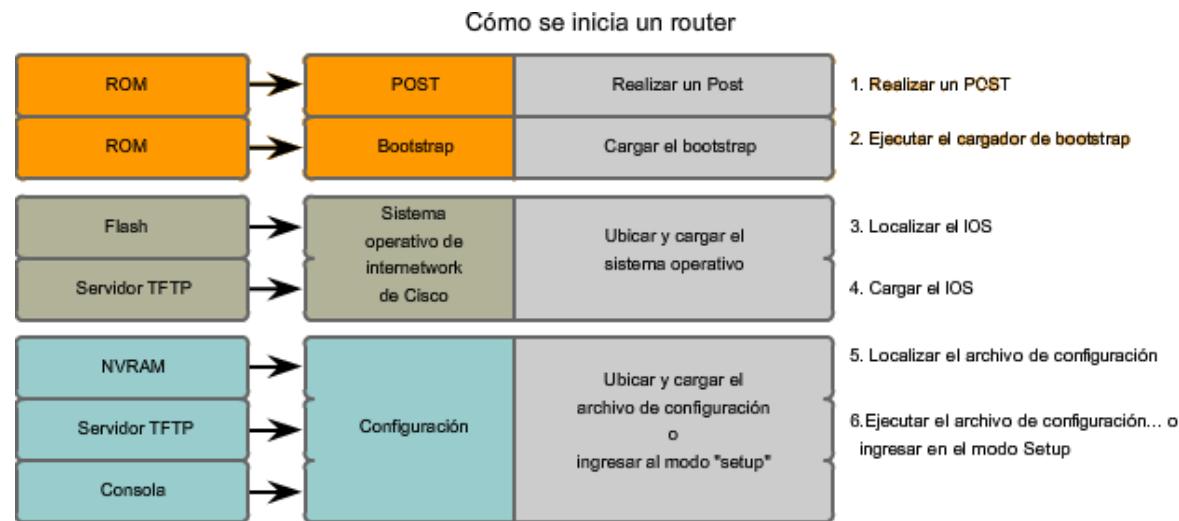
- Prueba del hardware del router

Autodiagnóstico al encender (POST)

Ejecución del cargador de bootstrap

- Búsqueda y carga del software IOS de Cisco
 - Búsqueda del IOS
 - Carga del IOS

- Búsqueda y carga del archivo de configuración de inicio o ingreso al modo Setup
 - El programa bootstrap busca el archivo de configuración.





El router como una computadora

- Verificación del proceso de inicio del router:
 - El comando `show version` se usa para visualizar información del router durante el proceso de inicio. Esta información incluye:
 - Número del modelo de plataforma
 - Nombre de la imagen y versión del IOS
 - Versión del programa bootstrap almacenado en la ROM
 - Nombre del archivo de imagen y ubicación del lugar de carga
 - Cantidad y tipo de interfaces
 - Cantidad de NVRAM
 - Cantidad de memoria flash
 - Registro de configuración

El router como una computadora

Cómo se inicia un router

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (c2600-i-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC
ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
CDATA[Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-i-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.

2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/asynch) network interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
Router#
```

Versión de IOS ←

Versión del bootstrap ←

Modelo y CPU ←

Cantidad de RAM ←

Cantidad y tipo de interfaces ←

Cantidad de NVRAM ←

Cantidad de Flash ←

El router como una computadora

- La interfaz del router es un conector físico que permite que el router envíe o reciba paquetes
- Cada interfaz se conecta a una red diferente
- Consiste en un socket o jack ubicado en el exterior del router
- Tipos de interfaces del router:
 - Ethernet
 - Fastethernet
 - Serial
 - DSL
 - ISDN
 - Cable

Cada interfaz individual se conecta a una red diferente. Por lo tanto, cada interfaz tiene una máscara/dirección IP de dicha red.

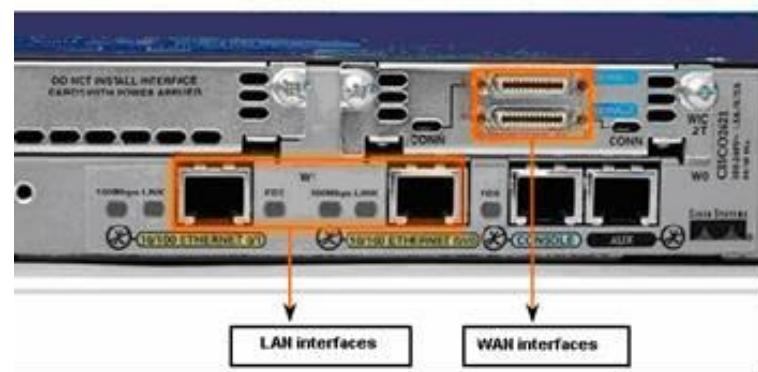


El router como una computadora

- Hay dos grupos principales de interfaces del router

Interfaces LAN:

- Se usan para conectar el router a la red LAN
- Tienen una dirección MAC de capa 2
- Se les puede asignar una dirección IP de capa 3
- Por lo general, se componen de un jack RJ-45



- Interfaces WAN:

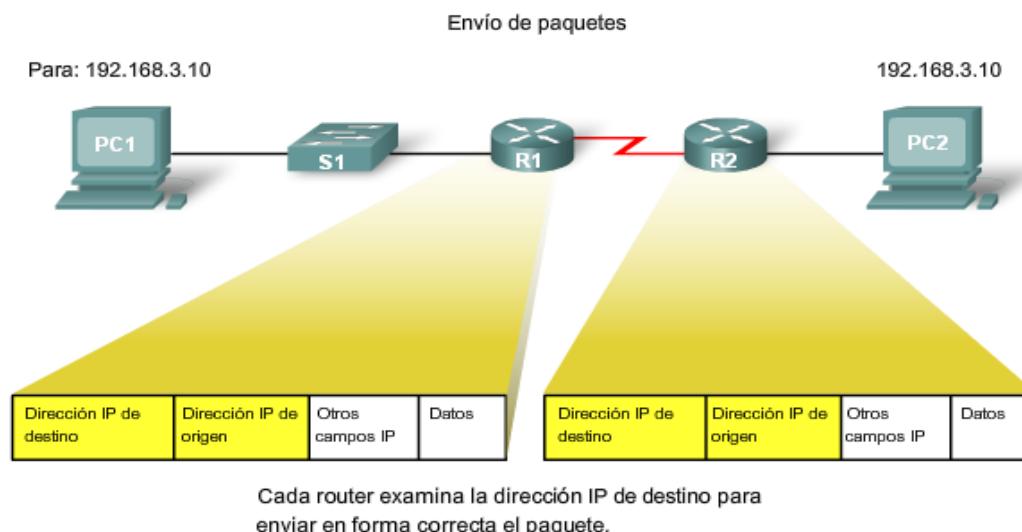
- Se usan para conectar routers a redes externas que interconectan redes LAN
- Según la tecnología WAN usada, es posible utilizar una dirección de capa 2
- Usan una dirección IP de capa 3

El router como una computadora

■ Los routers y la capa de red

Los routers usan direcciones IP de destino para reenviar paquetes

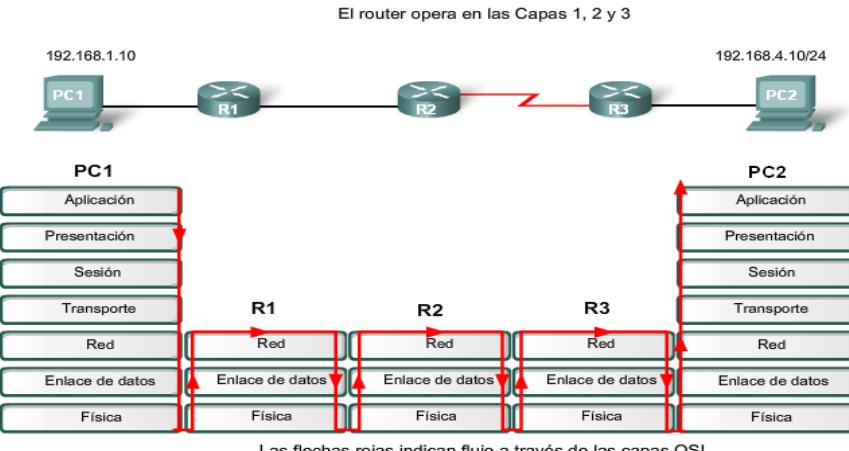
- El router determina la ruta por la que se transmitirá un paquete después de consultar la información de la tabla de enrutamiento
- El router determina cuál es la mejor ruta
- Se encapsula el paquete dentro de una trama
- Luego, se coloca la trama, en forma de bits, en un medio de red



El router como una computadora

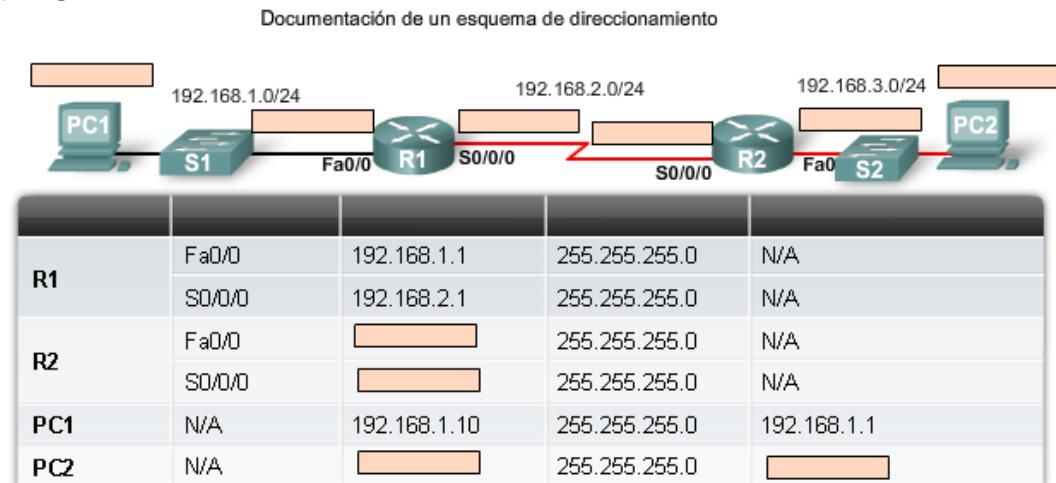
■ Los routers funcionan en las capas 1, 2 y 3

- El router recibe un stream de bits codificados
- Se decodifican los bits y se transmiten a la capa 2
- El router desencapsula la trama
- El paquete resultante se transmite a la capa 3
 - Para tomar las decisiones de enrutamiento de esta capa, se examina la dirección IP de destino
- Luego, el paquete se vuelve a encapsular y se envía a la interfaz de salida



Configuración de dispositivos y aplicación de direcciones

- Implementación de esquemas de direccionamiento básicos
- Cuando se diseña una nueva red o se realizan asignaciones de una red existente, se debe proporcionar la siguiente información en un documento:
 - Un diseño de topología que muestre la conectividad física
 - Una tabla de direcciones que contenga la siguiente información:
 - Nombre del dispositivo
 - Interfaces usadas
 - Direcciones IP
 - Gateway por defecto

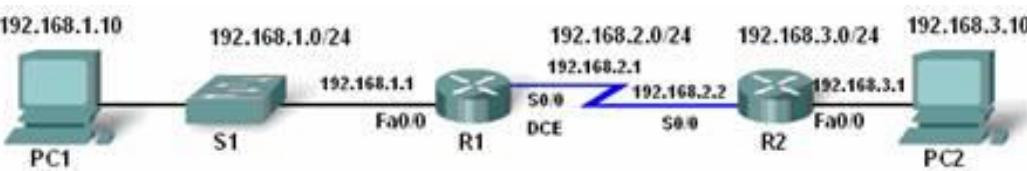




Configuración de dispositivos y aplicación de direcciones

- Configuración básica del router
- Una configuración básica de router debe tener lo siguiente:
 - **Nombre del router**: El nombre de host debe ser único
 - **Título**: Como mínimo, el título debe prohibir el uso no autorizado
 - **Contraséñas**: Se deben usar contraseñas seguras
 - **Configuración de interfaces**: Se debe especificar el tipo de interfaz, la dirección IP y la máscara de subred. Describa la función de la interfaz. Ejecute el comando no shutdown. Para la interfaz serial DCE, ejecute el comando clock rate.
- Después de introducir la configuración básica, deben realizarse las siguientes tareas
 - **Verifique** la configuración básica y el funcionamiento del router
 - **Guarde** los cambios en un router

Configuración de dispositivos y aplicación de direcciones



Sintaxis básica del comando de configuración del router

Denominación del router	Router(config)#hostname name
Configuración de contraseñas	Router(config)#enable secret password Router(config)#line console 0 Router(config-line)#password password Router(config-line)#login Router(config)#line vty 0 4 Router(config-line)#password password Router(config-line)#login
Configuración de un mensaje del día	Router(config)#banner motd # message #
Configuración de una interfaz	Router(config)#interface type number Router(config-if)#ip address address mask Router(config-if)#description description Router(config-if)#no shutdown
Cómo guardar cambios realizados en un router	Router#copy running-config startup-config
Análisis del resultado de los comandos show	Router#show running-config Router#show ip route Router#show ip interface brief Router#show interfaces

Configuración de dispositivos y aplicación de direcciones

- Verificación de la configuración básica del router
 - Ejecute el comando ***show running-config***
 - Ejecute el comando ***copy running-config startup-config*** para guardar la configuración básica del router
 - Estos son comandos adicionales que le permitirán verificar con más detalle la configuración del router:
 - **Show running-config:** muestra la configuración actual de la RAM
 - **Show startup-config:** muestra el archivo de configuración de NVRAM
 - **Show IP route:** muestra la tabla de enrutamiento
 - **Show interfaces:** muestra todas las configuraciones de interfaces
 - **Show ip int brief:** muestra información resumida de las configuraciones de interfaces

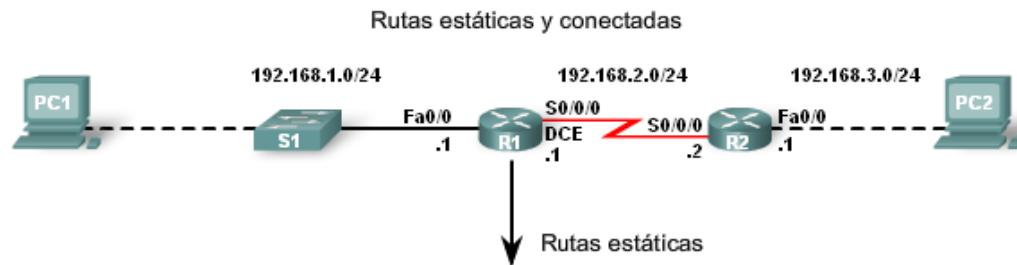


Estructura de la tabla de enrutamiento

- La tabla de enrutamiento se almacena en la RAM y contiene información sobre lo siguiente:
 - **Redes conectadas directamente:** Corresponde a un dispositivo conectado a otra interfaz del router
 - **Redes conectadas de forma remota:** Una red que no está conectada directamente a un router particular
 - **Información detallada** acerca de las redes incluye la fuente de la información, la dirección de red y la máscara de subred, y la dirección IP del router de siguiente salto
- El comando **show ip route** se utiliza para visualizar una tabla de enrutamiento.

Estructura de la tabla de enrutamiento

- Cómo agregar una red conectada a la tabla de enrutamiento
 - Interfaces del router
 - Cada interfaz del router pertenece a una red **distinta**
 - Se activan con el comando ***no shutdown***
 - Para que haya rutas estáticas y dinámicas en la tabla de enrutamiento, debe haber redes conectadas directamente



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

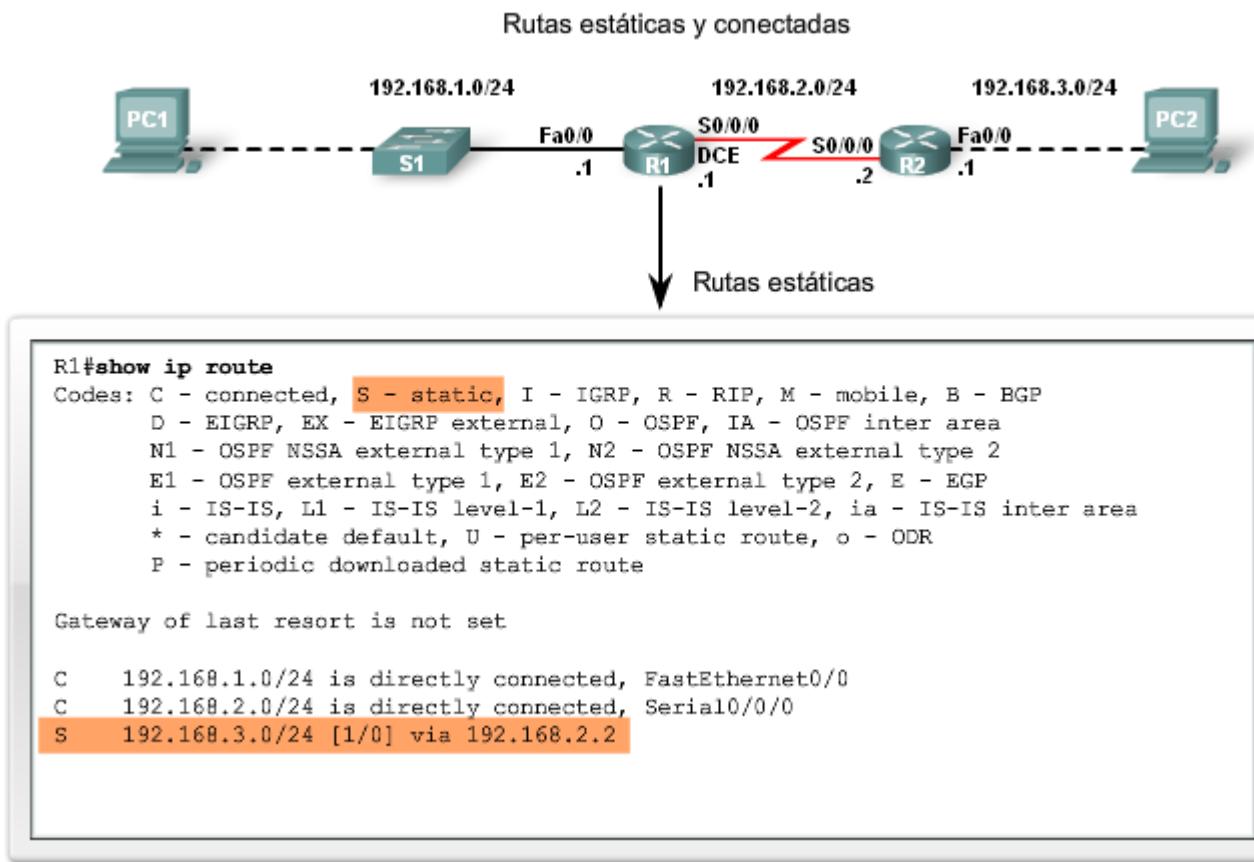


Estructura de la tabla de enrutamiento

- Rutas estáticas de la tabla de enrutamiento
 - Incluyen: la dirección de red, la máscara de subred y la dirección IP del router de siguiente salto o la interfaz de salida
 - Se indican, en la tabla de enrutamiento, con el código **S**
 - Antes de poder usar el enrutamiento estático o dinámico, las tablas de enrutamiento deben tener redes conectadas directamente usadas para conectar redes remotas
- Cuándo usar las rutas estáticas
 - Cuando la red tiene sólo unos pocos routers
 - Cuando la red está conectada a Internet sólo a través de un ISP
 - Cuando se usa una topología hub-and-spoke en una red de gran tamaño

Estructura de la tabla de enrutamiento

- Rutas estáticas y conectadas



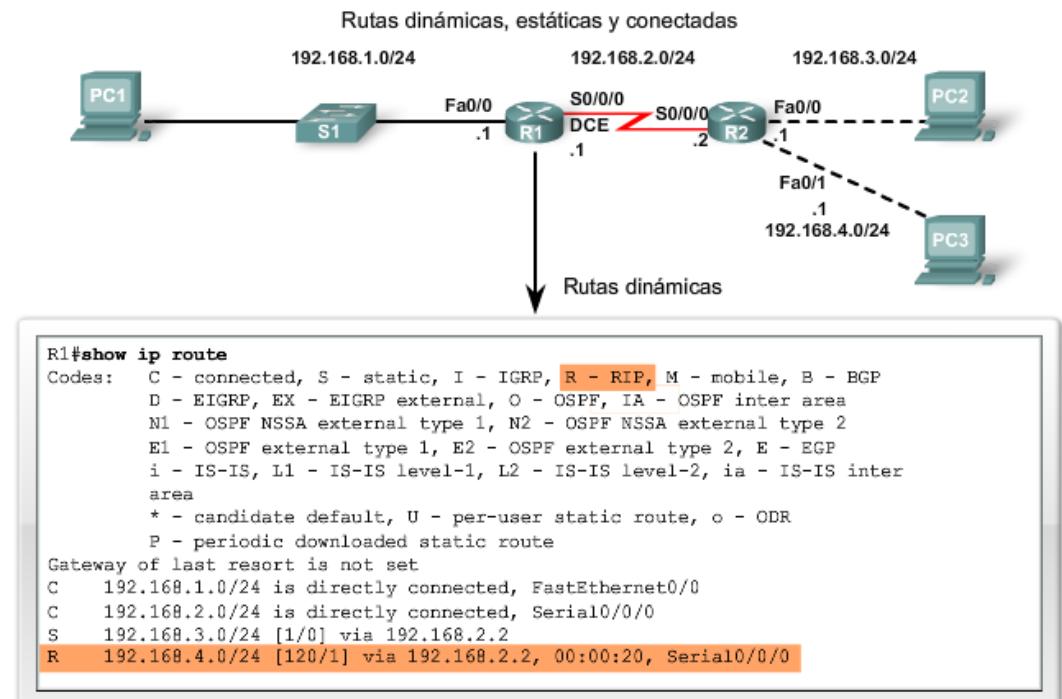


Estructura de la tabla de enrutamiento

- Protocolos de enrutamiento dinámico
 - Se usan para agregar redes remotas a una tabla de enrutamiento
 - Se usan para detección de redes
 - Se usan para la actualización y el mantenimiento de las tablas de enrutamiento
- Detección automática de redes
 - Los routers pueden detectar nuevas redes mediante el uso compartido de la información de las tablas de enrutamiento

Estructura de la tabla de enrutamiento

- Mantenimiento de las tablas de enrutamiento
 - Los protocolos de enrutamiento dinámico se usan para compartir información de enrutamiento entre routers y para mantener las tablas de enrutamiento actualizadas
- Protocolos de enrutamiento IP. Ejemplos de protocolos de enrutamiento:
 - RIP
 - IGRP
 - EIGRP
 - OSPF



Estructura de la tabla de enrutamiento

- Principios de la tabla de enrutamiento
 - Hay 3 principios en lo que respecta a las tablas de enrutamiento:
 - Cada router toma decisiones en forma independiente, sobre la base de la información que posee en la tabla de enrutamiento
 - Cada tabla de enrutamiento puede contener información diferente
 - Una tabla de enrutamiento tiene información sobre cómo llegar a un destino, pero no sobre cómo regresar

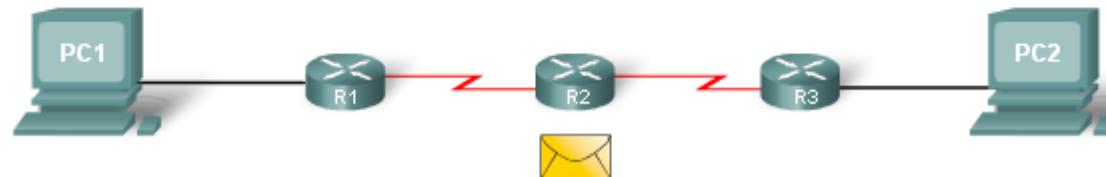
Principio de enrutamiento 3 en acción



Estructura de la tabla de enrutamiento

- Efectos de los 3 principios de la tabla de enrutamiento
 - Los paquetes se reenvían a través de la red de un router a otro, de salto a salto
 - Los paquetes pueden transmitirse al destino por la ruta “X” y regresar por la ruta “Y” (enrutamiento asimétrico)

Principio de enrutamiento 3 en acción



Rutas de routers y conmutación de paquetes

- El formato de paquete protocolo de internet (IP) contiene campos que proporcionan información sobre el paquete y sobre los hosts emisores y receptores.
- Campos importantes para los estudiantes de CCNA:
 - Dirección IP de destino
 - Dirección IP de origen
 - Versión y TTL
 - Longitud del encabezado IP
 - Prioridad y tipo de servicio
 - Longitud del paquete

Campos de paquetes IP



Rutas de routers y conmutación de paquetes

- Formato de la trama de capa MAC
- Las tramas MAC también se dividen en campos. Incluyen:
 - Preámbulo
 - Delimitador de inicio de trama
 - Dirección MAC de destino
 - Dirección MAC de origen
 - Tipo/longitud
 - Datos y pad
 - Secuencia de verificación de tramas

Campos de trama Ethernet

Ethernet

Longitud del campo en bytes						
8	6	6	2	46-1500	4	
Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	FCS	

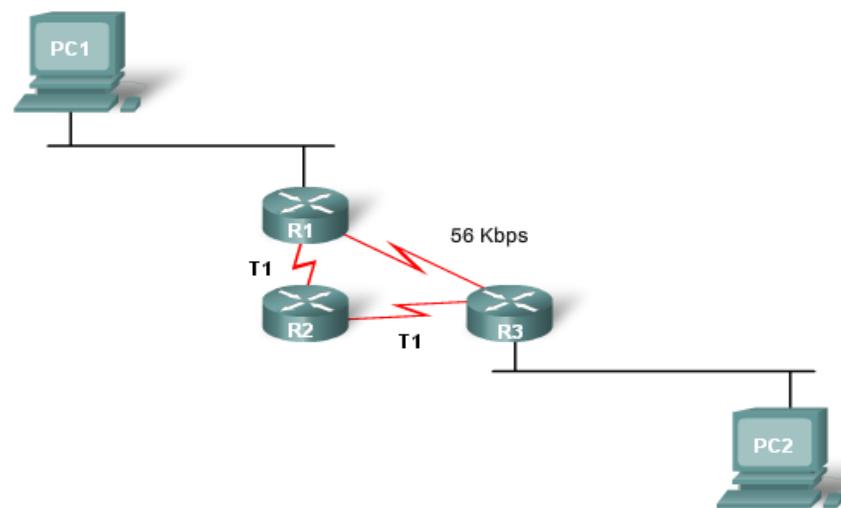
IEEE 802.3

Longitud del campo en bytes						
7	1	6	6	2	46-1500	4
Preámbulo	S O F	Dirección de destino	Dirección de origen	Longitud	Encabezado y datos 802.2	FCS

Rutas de routers y conmutación de paquetes

- Una **métrica** es **un valor numérico** que usan los protocolos de enrutamiento para determinar cuál es la mejor ruta a un destino
 - Cuanto menor sea el valor de la métrica, **mejor será** la ruta
- Dos tipos de métricas que usan los protocolos de enrutamiento son:
 - **Conteo de saltos:** la cantidad de routers que un paquete debe atravesar antes de llegar al destino
 - **Ancho de banda:** la “velocidad” de un enlace. También se conoce como “capacidad de datos” de un enlace

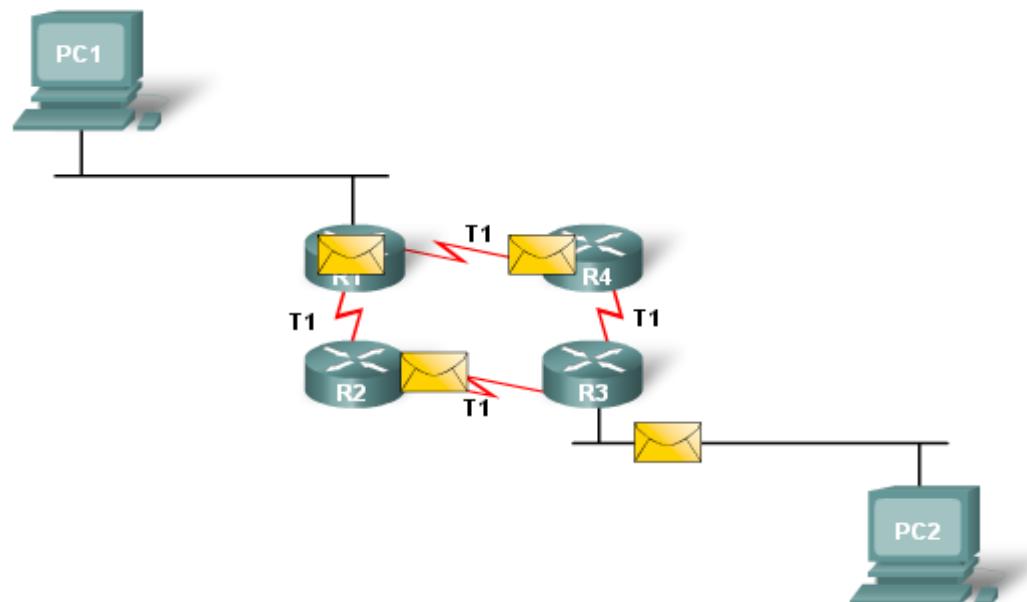
Conteo de saltos en comparación con el ancho de banda como métrica



Rutas de routers y conmutación de paquetes

- **Métrica del mismo costo:** condición en la que un router tiene varias rutas al mismo destino con la misma métrica.
- Para solucionar este dilema, el router usará el **balanceo de carga de mismo costo**. Esto significa que el router enviará los paquetes a través de las múltiples interfaces de salida enumeradas en la tabla de enrutamiento.

Balanceo de carga de mismo costo



Rutas de routers y conmutación de paquetes

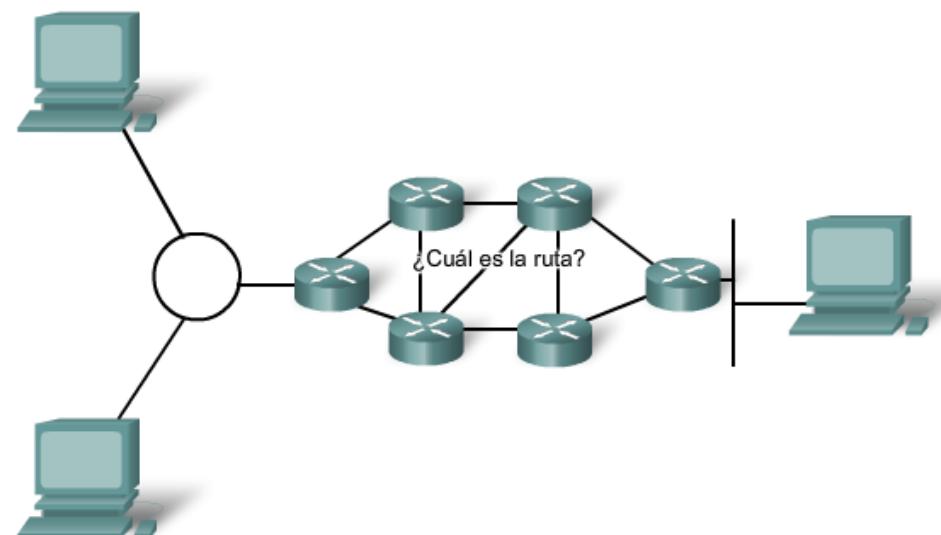
- La determinación de la ruta es un proceso que usa el router para seleccionar la mejor ruta a un destino
- La búsqueda de la mejor ruta tiene como resultado **una de tres determinaciones de ruta:**

Red conectada directamente

Red remota

No se determina una ruta

Cómo encontrar la mejor ruta



Los routers determinan la mejor ruta hacia el destino

Rutas de routers y conmutación de paquetes

- **La función de conmutación** de un router es el proceso que usa un router para conmutar un paquete de una interfaz de entrada a una interfaz de salida en el mismo router.
 - Cuando un router recibe un paquete, sucede lo siguiente:
 - Se eliminan los encabezados de capa 2
 - Se analiza la dirección IP de destino ubicada en el encabezado de capa 3 para encontrar la mejor ruta al destino
 - Se vuelve a encapsular el paquete de capa 3 en una trama de capa 2
 - Se reenvía la trama a través de la interfaz de salida

Rutas de routers y conmutación de paquetes

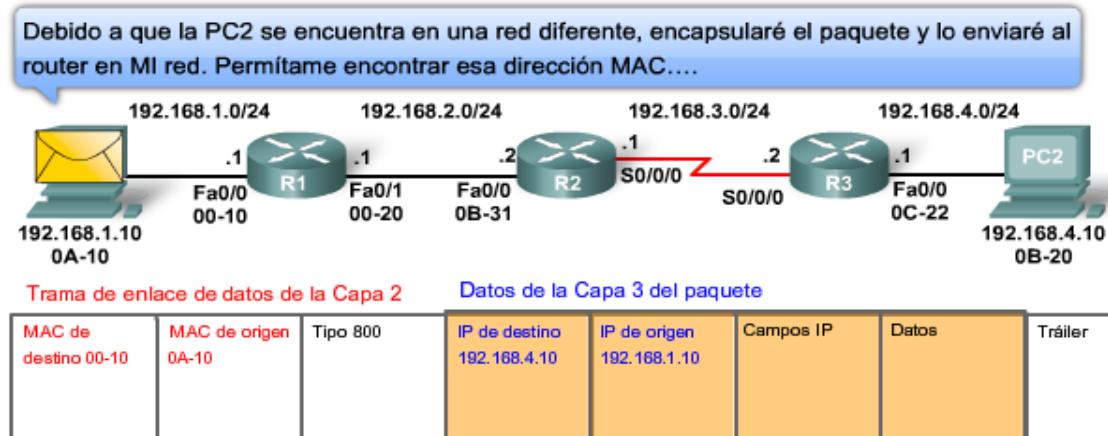
- Mientras un paquete se transmite de un dispositivo de networking a otro:
 - Las **direcciones IP** de origen y destino **NO** cambian
 - Las **direcciones MAC** de origen y destino **CAMBIAN** cuando el paquete se reenvía de un router a otro
 - El campo TTL disminuye de a un número hasta llegar a un valor de cero. En ese momento, el router descarta el paquete (este mecanismo evita que los paquetes se transmitan a través de la red de forma indefinida)

Rutas de routers y conmutación de paquetes

- Información sobre la función de conmutación y determinación de rutas. A continuación, se muestra parte de lo que ocurre cuando la PC1 desea enviar un paquete a la PC2:

Paso 1: la PC1 encapsula el paquete en una trama. La trama tiene la dirección MAC de destino del R1

Funcionamiento diario de un paquete: Paso 1



Caché ARP de la PC1 para R1

Dirección IP	Dirección MAC
192.168.1.1	00-10



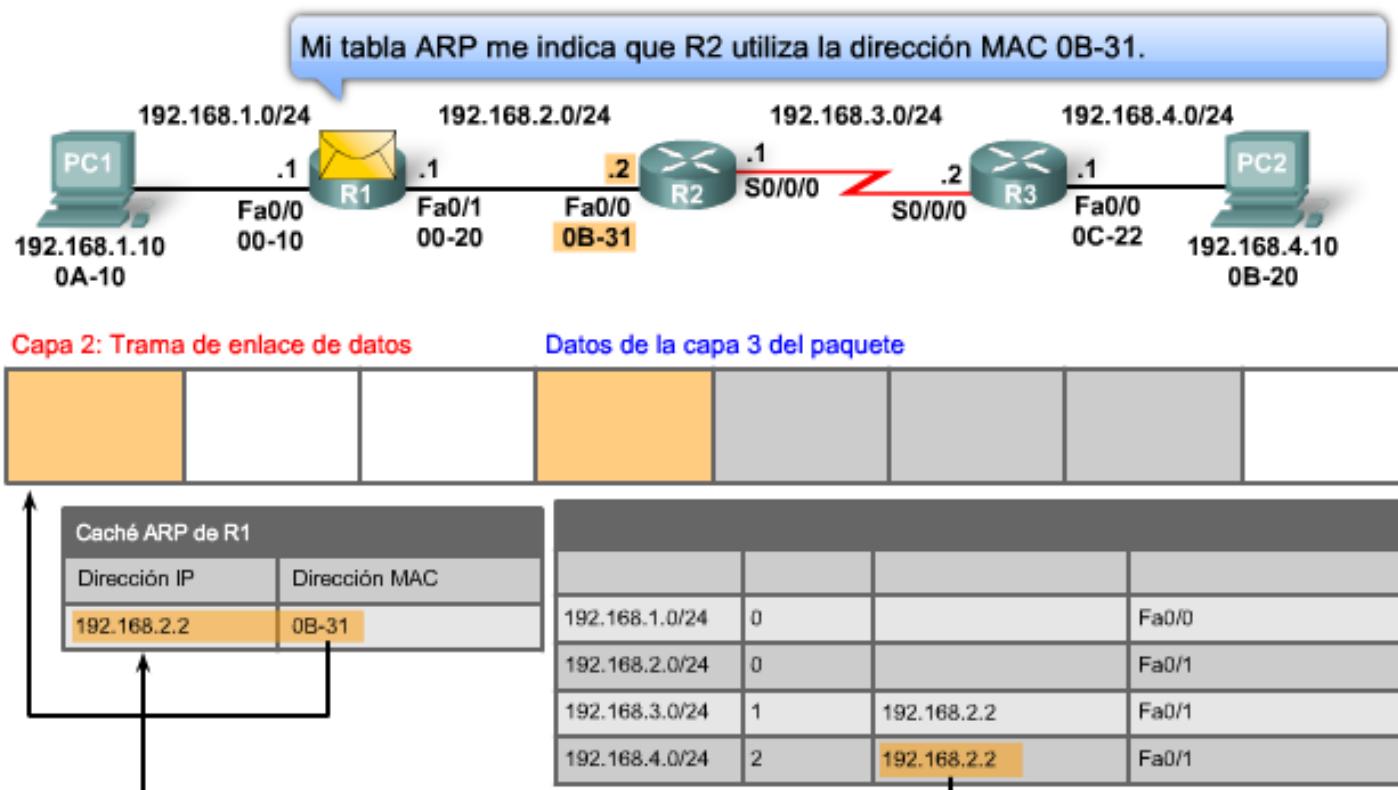
Rutas de routers y conmutación de paquetes

Paso 2: el R1 recibe la trama de Ethernet.

- El R1 reconoce que la dirección MAC de destino coincide con la dirección MAC propia.
- Luego, el R1 elimina la trama de Ethernet.
- El R1 examina la IP de destino.
- El R1 busca la IP de destino en la tabla de enrutamiento.
- Una vez que encontró la IP de destino en la tabla de enrutamiento, el R1 busca la dirección IP de siguiente salto.
- El R1 vuelve a encapsular el paquete IP con una nueva trama de Ethernet.
- El R1 reenvía el paquete Ethernet a través de la interfaz Fa0/1.

Rutas de routers y conmutación de paquetes

Funcionamiento diario de un paquete: Paso 2



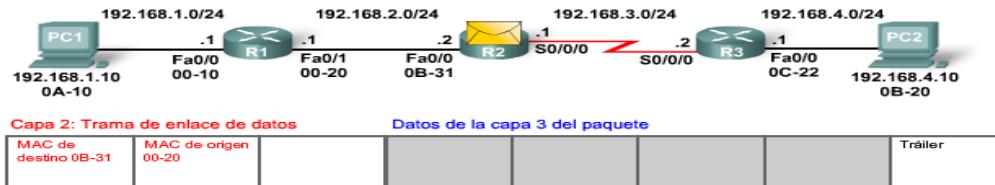
Rutas de routers y conmutación de paquetes

- Información sobre la función de conmutación y determinación de rutas.
A continuación, se muestra parte de lo que ocurre cuando la PC1 desea enviar un paquete a la PC2:

Paso 3: el paquete llega al R2

- El R2 recibe la trama de Ethernet
- El R2 reconoce que la dirección MAC de destino coincide con la dirección MAC propia
- Luego, el R2 elimina la trama de Ethernet
- El R2 examina la IP de destino
- El R2 busca la IP de destino en la tabla de enrutamiento
- Una vez que encontró la IP de destino en la tabla de enrutamiento, el R2 busca la dirección IP de siguiente salto
- El R2 vuelve a encapsular el paquete IP con una nueva trama de enlace de datos
- El R2 reenvía el paquete Ethernet a través de la interfaz S0/0

Funcionamiento diario de un paquete: Paso 3





Rutas de routers y conmutación de paquetes

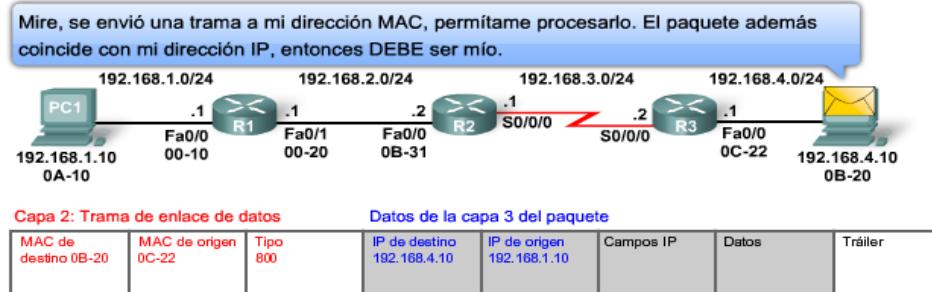
- Información sobre la función de conmutación y determinación de rutas.
A continuación, se muestra parte de lo que ocurre cuando la PC1 desea enviar un paquete a la PC2

Paso 4: el paquete llega al R3

- R3 recibe la trama de PPP
- Luego, el R3 elimina la trama de PPP
- El R3 examina la IP de destino
- El R3 busca la IP de destino en la tabla de enrutamiento
- Una vez que encontró la IP de destino en la tabla de enrutamiento, el R3 se conecta directamente al destino a través de la interfaz Fast Ethernet
- El R3 vuelve a encapsular el paquete IP con una nueva trama de Ethernet
- El R3 reenvía el paquete Ethernet a través de la interfaz Fa0/0

Paso 5: el paquete IP llega a la PC2. Se desencapsula la trama y la procesan los protocolos de capa superior

Funcionamiento diario de un paquete: Paso 4





Resumen

- Los routers son computadoras que se especializan en el envío de datos a través de redes
- Los routers están formados por:
 - Hardware, es decir, la CPU, la memoria, el bus del sistema y las interfaces
 - Software que administra el proceso de enrutamiento
 - IOS
 - Archivo de configuración
- Es necesario configurar los routers. Las configuraciones básicas son:
 - El nombre del router
 - El título del router
 - Las contraseñas
 - Las configuraciones de interfaz, es decir, la dirección IP y la máscara de subred
- Las tablas de enrutamiento contienen la siguiente información:
 - Redes conectadas directamente
 - Redes conectadas de forma remota
 - Direcciones de red y máscaras de subred
 - Dirección IP de la dirección de siguiente salto



Resumen

- Los routers determinan qué ruta debe tomar un paquete para llegar al destino, de la siguiente forma:
 - Reciben una trama encapsulada y analizan la dirección MAC de destino.
 - Si la dirección MAC coincide, se desencapsula la trama para que el router pueda analizar la dirección IP de destino.
 - Si la dirección IP de destino está en la tabla de enrutamiento o si hay una ruta estática, el router determina la dirección IP de siguiente salto. El router vuelve a encapsular el paquete con la trama de capa 2 adecuada y la envía al destino siguiente.
 - El proceso continúa hasta que el paquete llega al destino.
 - Nota: Sólo cambian las direcciones MAC; las direcciones IP de origen y de destino no cambian.

