

Módulo 8: SLAAC y DHCPv6

Switching, Routing y Wireless
Essentials (SRWE)



Objetivos del módulo

Título del módulo: SLAAC y DHCPv6

Objetivo del módulo: configurar la asignación dinámica de direcciones en redes IPv6.

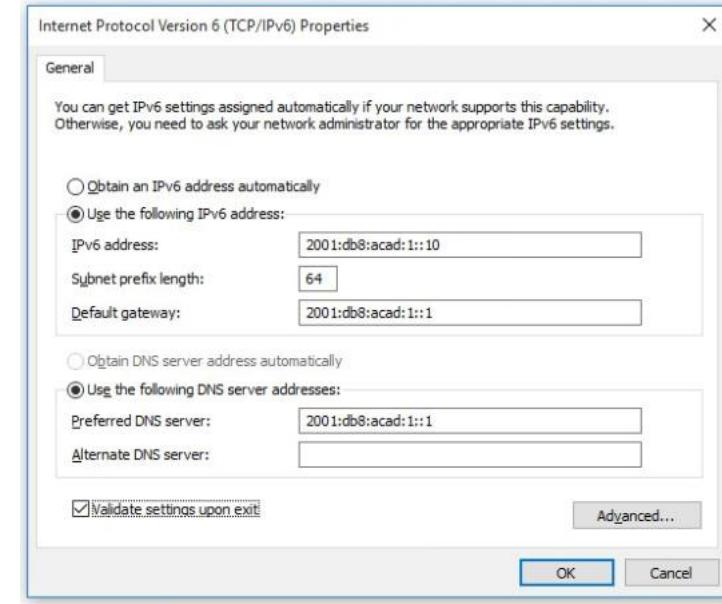
Título del tema	Objetivo del tema
Asignación de direcciones de unidifusión global IPv6	Explicar cómo un host IPv6 puede adquirir su configuración IPv6.
SLAAC	Explicar el funcionamiento de SLAAC.
DHCPv6	Explicar el funcionamiento de DHCPv6.
Configurar servidor DHCPv6	Configurar servidor DHCPv6 stateful y stateless.

8.1 Asignación de GUA IPv6

Configuración de host IPv6

En un router, una dirección global de unidifusión (GUA) **IPv6 se configura manualmente** mediante el comando de *configuración _ipv6-address__prefix-length_ interface*.

- Un host de Windows también se puede configurar manualmente con una configuración de dirección IPv6 GUA, como se muestra en la figura.
- Sin embargo, introducir manualmente una GUA IPv6 puede llevar mucho tiempo y ser algo propenso a errores.
- Por lo tanto, la mayoría de los hosts de Windows están habilitados para adquirir dinámicamente una configuración GUA IPv6.



Dirección local de enlace de host IPv6

Si se selecciona el direccionamiento IPv6 automático, el host utilizará un mensaje de anuncio de enrutador (RA) del protocolo de mensajes de control de Internet versión 6 (ICMPv6) para ayudarle a configurar automáticamente una configuración IPv6.

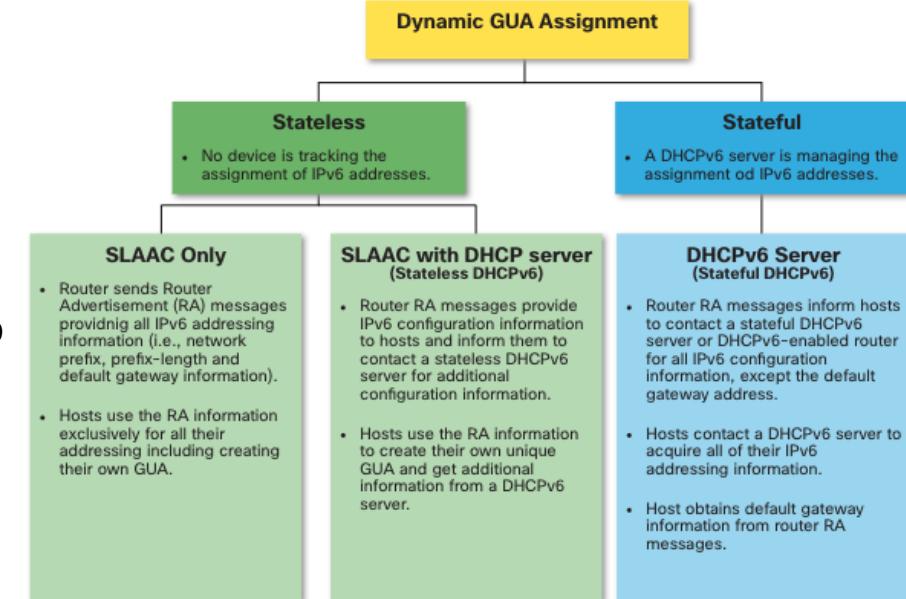
- El host crea automáticamente la dirección local del vínculo IPv6 cuando se inicia y la interfaz Ethernet está activa.
- La interfaz no creó un GUA IPv6 en la salida porque el segmento de red no tenía un enrutador para proporcionar instrucciones de configuración de red para el host.
- **Nota:** El «%» y el número al final de la dirección local del vínculo se conocen como identificador de zona o identificador de ámbito y el sistema operativo utiliza para asociar la LLA a una interfaz específica.
- **Nota:** DHCPv6 se define en RFC 3315.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . :
  IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
  Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
  IPv4 Address . . . . . : 169.254.202.140
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :
C:\>
```

Asignación de IPv6 GUA

De forma predeterminada, un enrutador habilitado para IPv6 envía periódicamente RA ICMPv6, lo que simplifica la forma en que un host puede crear o adquirir dinámicamente su configuración IPv6.

- A un host se le puede asignar dinámicamente un GUA mediante servicios sin estado y con estado.
- Todos los métodos sin estado y con estado de este módulo utilizan mensajes de RA ICMPv6 para sugerir al host cómo crear o adquirir su configuración IPv6.
- Aunque los sistemas operativos del host siguen la sugerencia de la RA, la decisión real depende en última instancia del host

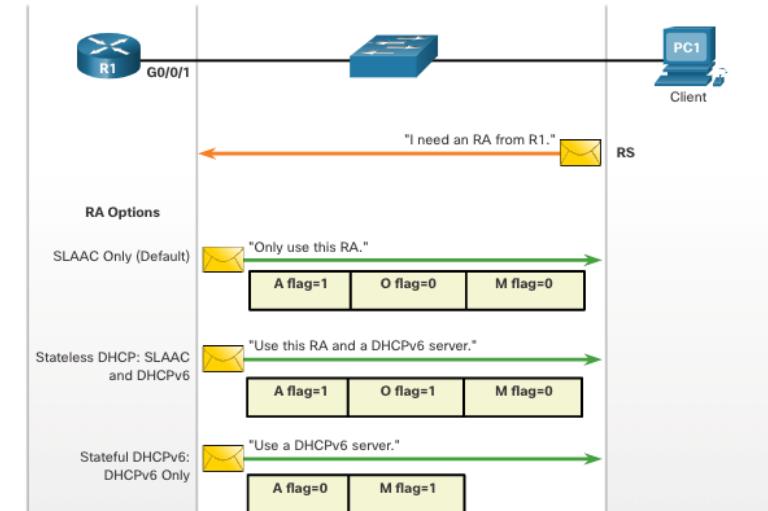


Tres indicadores de mensaje RA

La forma en que un cliente obtiene un GUA IPv6 depende de la configuración del mensaje RA.

Un mensaje de ICMPv6 RA incluye los tres indicadores siguientes:

- **Un indicador (flag):** el indicador de configuración automática de direcciones significa utilizar la configuración automática de direcciones sin estado (SLAAC) para crear un GUA de IPv6
- **El Indicador 0 (flag O)-** El otro indicador de configuración se utiliza para informarle al cliente que hay información adicional disponible de un servidor de DHCPv6 stateless.
- **Indicador M :** el indicador Configuración de dirección administrada significa usar un servidor DHCPv6 con estado para obtener una GUA IPv6.



Mediante diferentes combinaciones de los indicadores A, O y M, los mensajes RA informan al host sobre las opciones dinámicas disponibles.

8.2 SLAAC

Descripción general de SLAAC SLAAC

No todas las redes tienen acceso a un servidor DHCPv6, pero todos los dispositivos de una red IPv6 necesitan un GUA. El método SLAAC permite a los hosts crear su propia dirección única global IPv6 sin los servicios de un servidor DHCPv6.

- SLAAC es un servicio sin estado, lo que significa que no hay ningún servidor que mantenga información de direcciones de red para saber qué direcciones IPv6 se están utilizando y cuáles están disponibles.
- SLAAC envía mensajes periódicos de RA ICMPv6 (es decir, cada 200 segundos) proporcionando direcciones y otra información de configuración para que los hosts configuren automáticamente su dirección IPv6 en función de la información del RA.
- Un host también puede enviar un mensaje de solicitud de enrutador (RS) solicitando una RA.
- SLAAC sólo se puede implementar como SLAAC, o SLAAC con DHCPv6.

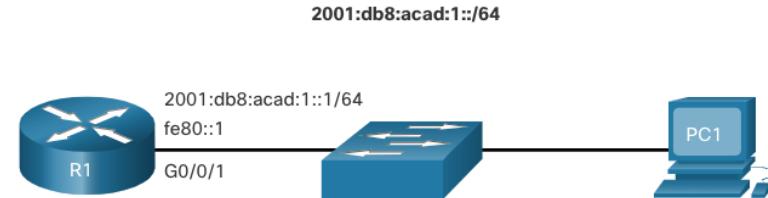
Activación de SLAAC

R1 G0/0/1 se ha configurado con la GUA IPv6 indicada y las direcciones locales de enlace.

Las direcciones IPv6 R1 G0/0/1 incluyen:

- **Link-local IPv6 address** - fe80::1
- **GUA/subred** - 2001:db8:acad:1::1, 2001:db8:acad:1::/64
- **Grupo de todos los nodos IPv6** - ff02::1

R1 está configurado para unirse al grupo de multidifusión IPv6 y comenzar a enviar mensajes RA que contienen información de configuración de direcciones a hosts que utilizan SLAAC.



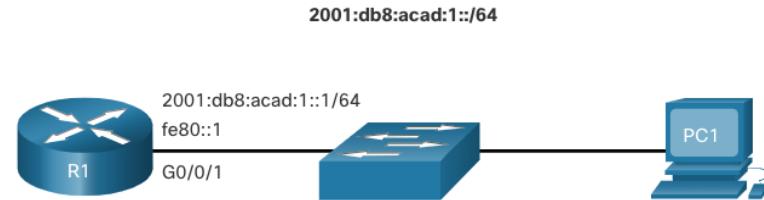
```
R1# show ipv6 interface G0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
  (output omitted)
R1#
```

```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
```

Activación de SLAAC (cont.)

El grupo de todos los routers IPv6 responde a la dirección de multidifusión IPv6 ff02 :: 2.

- El comando **show ipv6 interface** verifica que R1 se haya unido al grupo de todos los routers IPv6 (es decir, ff02::2).
- R1 comenzará ahora a enviar mensajes de RA cada 200 segundos a la dirección de multidifusión IPv6 de todos los nodos ff02::1.

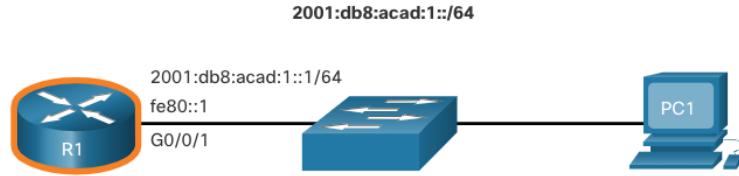


```
R1# show ipv6 interface G0/0/1 | section Joined  
Joined group address(es):  
FF02::1  
FF02::2  
FF02::1:FF00:1  
R1#
```

Método SLAAC SLAAC

Los mensajes RA de R1 tienen los siguientes indicadores establecidos:

- **A = 1**: informa al cliente que use el prefijo IPv6 GUA en la RA y cree dinámicamente su propio ID de interfaz.
- **O = 0 y M = 0**: informa al cliente que utilice también la información adicional en el mensaje RA (es decir, servidor DNS, MTU e información de puerta de enlace predeterminada).
- El comando **ipconfig** Windows confirma que PC1 ha generado un GUS IPv6 utilizando el RA R1.
- La dirección de puerta de enlace predeterminada es LLA de la interfaz R1 G0/0/1.



RA Message	
Flag	value
A	1
O	0
M	0

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
  Link-local IPv6 Address . . . . : fe80::fb:1d54:839f:f595%21
  IPv4 Address. . . . . : 169.254.202.140
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : fe80::1%6
C:\>
```

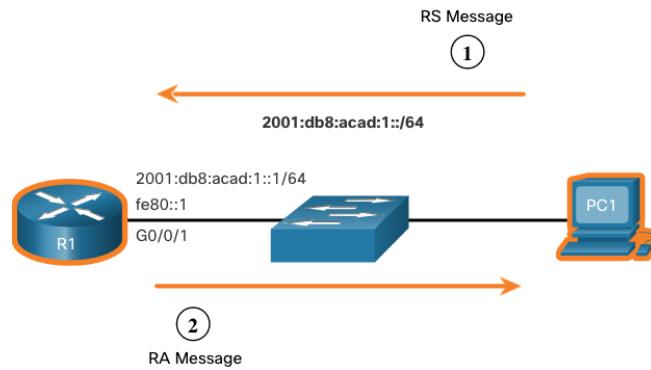
Mensajes SLAAC ICMPv6 RS

Un router envía mensajes RA cada 200 segundos o cuando recibe un mensaje RS de un host.

- Los hosts habilitados para IPv6 que deseen obtener información de direccionamiento IPv6 envían un mensaje RS a la dirección de multidifusión de IPv6 para todos los routers ff02::2.

La figura ilustra cómo un host inicia el método SLAAC.

- PC1 acaba de arrancar y envía un mensaje RS a la dirección de multidifusión IPv6 de todos los routers ff02::2 solicitando una RA.
- R1 genera un RA y, a continuación, envía el mensaje RA a la dirección de multidifusión IPv6 de todos los nodos ff02::1. PC1 utiliza esta información para crear una GUA IPv6 única.



Proceso de host SLAAC para generar ID de interfaz

Mediante SLAAC, un host adquiere la información de la subred IPv6 de 64 bits del RA del router y debe generar el identificador de interfaz (ID) de 64 bits restante mediante:

- **De generación aleatoria** - La identificación de la interfaz de 64 bits es generada aleatoriamente por el sistema operativo del cliente. Este es el método utilizado ahora por los hosts de Windows 10.
- **EUI-64** - El host crea un ID de interfaz utilizando su dirección MAC de 48 bits e inserta el valor hexadecimal de fffe en el medio de la dirección. Algunos sistemas operativos utilizan por defecto el ID de interfaz generado aleatoriamente en lugar del método EUI-64, debido a problemas de privacidad. Esto se debe a que EUI-64 utiliza la dirección MAC Ethernet del host para crear el ID de interfaz.

Nota: Windows, Linux y Mac OS permiten al usuario modificar la generación del ID de interfaz para que se genere aleatoriamente o utilice EUI-64.

Detección de direcciones duplicadas

Un host SLAAC puede utilizar el siguiente proceso de detección de direcciones duplicadas (DAD) para asegurarse de que IPv6 GUA es único.

- El host envía un mensaje ICMPv6 Neighbor Solicitation (NS) con una dirección de multidifusión de nodo solicitado especialmente construida que contiene los últimos 24 bits de dirección IPv6 del host.
- Si ningún otro dispositivo responde con un mensaje Neighbor Advertisement (NA), prácticamente se garantiza que la dirección es única y puede ser utilizada por la PC.
- Si el host recibe un NA, entonces la dirección no es única y el host debe generar un nuevo ID de interfaz para utilizarlo.

Nota: DAD realmente no es necesario porque un ID de interfaz de 64 bits proporciona 18 quintillion de posibilidades. Por lo tanto, la posibilidad de una dirección duplicada es remota. Sin embargo, Internet Engineering Task Force (IETF) recomienda que se utilice DAD. Por lo tanto, la mayoría de los sistemas operativos realizan DAD en todas las direcciones de unidifusión IPv6, independientemente de cómo se configure la dirección.

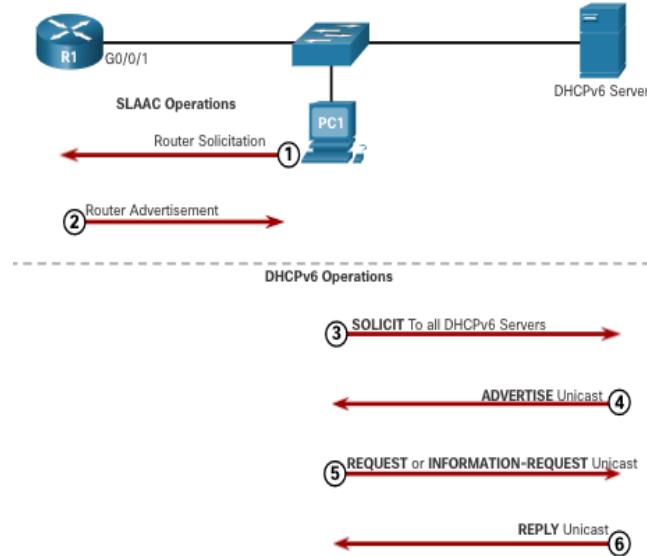
8.3 DHCPv6

Pasos de operación DHCPv6

DHCPv6 con estado no requiere SLAAC mientras que DHCPv6 sin estado lo hace.

Sin embargo, cuando un RA indica que debe usar DHCPv6 o DHCPv6 con estado:

1. El host envía un mensaje RS.
2. El router responde con un mensaje RA.
3. El host envía un mensaje DHCPv6 SOLIT.
4. El servidor DHCPv6 responde con un mensaje ADVERTISE.
5. El host responde al servidor DHCPv6.
6. El servidor DHCPv6 envía un mensaje de respuesta.



Nota: Los mensajes DHCPv6 de servidor a cliente utilizan el puerto de destino UDP 546, mientras que los mensajes DHCPv6 de cliente a servidor utilizan el puerto de destino UDP 547.

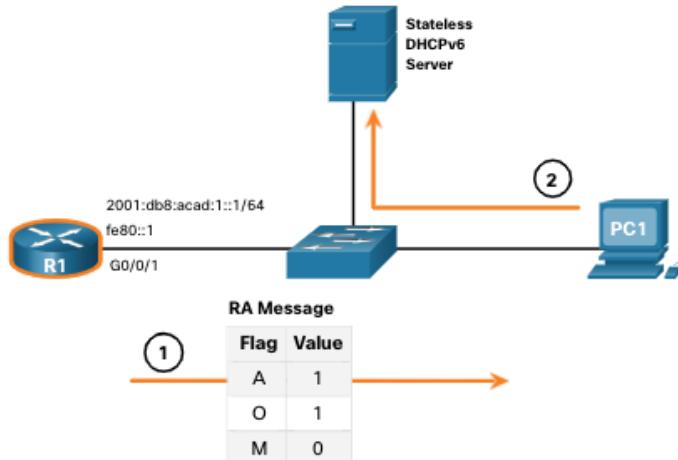
Operación DHCPv6 sin estado DHCPv6

Si un RA indica el método DHCPv6 sin estado, el host utiliza la información del mensaje RA para direccionamiento y se pone en contacto con un servidor DHCPv6 para obtener información adicional.

Nota: El servidor DHCPv6 sólo proporciona parámetros de configuración para clientes y no mantiene una lista de enlaces de direcciones IPv6 (es decir, sin estado).

Por ejemplo, PC1 recibe un mensaje de RA sin estado que contiene:

- El prefijo de red IPv6 GUA y la longitud del prefijo.
- Un indicador establecido en 1 que informa al host de usar SLAAC.
- Indicador O establecido en 1 para informar al host que busque esa información de configuración adicional de un servidor DHCPv6.
- Indicador M establecido en el valor predeterminado 0.
- PC1 envía un mensaje DHCPv6 SOLCIT buscando información adicional de un servidor DHCPv6 sin estado.



Habilitar DHCPv6 sin estado en una interfaz

DHCPv6 sin estado está habilitado mediante el comando de configuración de interfaz **ipv6 nd other-config-flag** estableciendo el indicador O en 1.

La salida resaltada confirma que el RA indicará a los hosts receptores que utilicen autoconfigure sin estado (indicador A = 1) y que se ponga en contacto con un servidor DHCPv6 para obtener otra información de configuración (indicador O = 1).

Nota: Puede utilizar el **indicador no ipv6 nd other-config-flag** para restablecer la interfaz a la opción predeterminada de sólo SLAAC (O flag = 0).

```
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Hosts use DHCP to obtain other configuration.
R1#
```

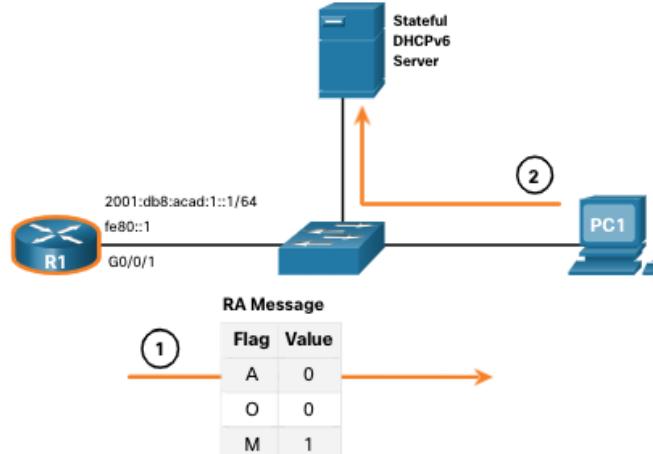
Operación DHCPv6 sin estado

Si un RA indica el método DHCPv6 con estado, el host se pone en contacto con un servidor DHCPv6 para obtener toda la información de configuración.

- **Nota:** El servidor DHCPv6 tiene estado y mantiene una lista de enlaces de direcciones IPv6.

Por ejemplo, PC1 recibe un mensaje de RA con estado que contiene:

- El prefijo de red IPv6 GUA y la longitud del prefijo.
- Indicador establecido en 0 que informa al host de ponerse en contacto con un servidor DHCPv6.
- Indicador O establecido en 0 para informar al host de ponerse en contacto con un servidor DHCPv6.
- Indicador M establecido en el valor 1.
- PC1 envía un mensaje DHCPv6 SOLCIT buscando información adicional de un servidor DHCPv6 con estado.



Habilitar DHCPv6 con estado en una interfaz

DHCPv6 con estado está habilitado mediante el comando de configuración de interfaz **ipv6 nd managed-config-flag**, estableciendo el indicador M en 1.

El resultado resaltado en el ejemplo confirma que RA indicará al host que obtenga toda la información de configuración IPv6 de un servidor DHCPv6 (indicador M = 1).

```
R1(config)# int g0/0/1
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
R1#
```

8.4 Configurar el servidor DHCPv6

Configurar las funciones de enrutador como servidor DHCPv6

Los routers IOS de Cisco son dispositivos potentes. En redes más pequeñas, no es necesario tener dispositivos separados para tener un servidor DHCPv6, un cliente o un agente de retransmisión. Se puede configurar un router Cisco para proporcionar servicios DHCPv6.

Especificamente, se puede configurar para que sea uno de los siguientes:

- **Servidor DHCPv6** - Router proporciona servicios DHCPv6 sin estado o con estado.
- **Cliente DHCPv6** : la interfaz del enrutador adquiere una configuración IP IPv6 de un servidor DHCPv6.
- **Agente de retransmisión DHCPv6** - Router proporciona servicios de reenvío DHCPv6 cuando el cliente y el servidor se encuentran en diferentes redes.

Configurar un servidor DHCPv6 sin estado

La opción de servidor DHCPv6 sin estado requiere que el enrutador anuncie la información de direccionamiento de red IPv6 en los mensajes RA.

Hay cinco pasos para configurar y verificar un enrutador como servidor DHCPv6 sin estado:

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Defina un nombre de grupo DHCPv6 mediante el comando **ipv6 dhcp pool POOL-NAME** global config.
3. Configure el grupo DHCPv6 con opciones. Las opciones comunes incluyen **dns-server X:X:X:X:X:X** y **nombre de dominio** .
4. Enlazar la interfaz al grupo mediante el comando **ipv6 dhcp server POOL-NAME** interface config.
 - El indicador O debe cambiarse de 0 a 1 mediante el comando de interfaz `ipv6 nd other-config-flag`. Los mensajes RA enviados en esta interfaz indican que hay información adicional disponible de un servidor de DHCPv6 sin estado. El indicador A es 1 de forma predeterminada, indicando a los clientes que usen SLAAC para crear su propio GUA.
5. Compruebe que los hosts han recibido información de direccionamiento IPv6 mediante el comando **ipconfig /all** .

Configurar un cliente DHCPv6 sin estado

Un enrutador también puede ser un cliente DHCPv6 y obtener una configuración IPv6 de un servidor DHCPv6, como un enrutador que funcione como servidor DHCPv6.

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Configure el enrutador cliente para crear una LLA. Una dirección local de vínculo IPv6 se crea en una interfaz de enrutador cuando se configura una dirección de unidifusión global, o sin una GUA mediante el comando de configuración de interfaz **ipv6 enable**. Cisco IOS utiliza EUI-64 para crear el ID de interfaz.
3. Configure el enrutador cliente para que utilice SLAAC mediante el comando **ipv6 address autoconfig**.
4. Compruebe que el router cliente tiene asignado un GUA mediante el comando **show ipv6 interface brief**.
5. Verifique que el enrutador cliente haya recibido otra información DHCPv6 necesaria. El comando **show ipv6 dhcp interface g0/0/1** confirma que el cliente ha recibido información de opciones DHCP, como el servidor DNS y el nombre de dominio.

Configurar un servidor DHCPv6 con estado

La opción de servidor DHCP con estado requiere que el enrutador habilitado para IPv6 indique al host que se ponga en contacto con un servidor DHCPv6 para obtener toda la información de direccionamiento de red IPv6 necesaria.

Hay cinco pasos para configurar y verificar un enrutador como un servidor DHCPv6 con estado:

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Defina un nombre de grupo DHCPv6 mediante el comando **ipv6 dhcp pool POOL-NAME** global config.
3. Configure el grupo DHCPv6 con opciones. Las opciones comunes incluyen el comando **address prefix**, el nombre de dominio, la dirección IP del servidor DHS y más.
4. Enlazar la interfaz al grupo mediante el comando **ipv6 dhcp server POOL-NAME interface config**.
 - El indicador O debe cambiarse de 0 a 1 mediante el comando de interfa **ipv6 nd other-config-flag**.
 - Cambie manualmente el indicador A de 1 a 0 mediante el comando **ipv6 nd prefix default no-autoconfig** interface para informar al cliente de que no utilice SLAAC para crear un GUA. El router responde a las solicitudes de DHCPv6 con la información incluida en el pool.
5. Compruebe que los hosts han recibido información de direccionamiento IPv6 mediante el comando **ipconfig /all**.

Configurar un cliente DHCPv6 con estado

Un router también puede ser un cliente DHCPv6. El enrutador cliente debe tener habilitado el enrutamiento **unicast-routing ipv6** y una dirección local de enlace IPv6 para enviar y recibir mensajes IPv6.

Hay cinco pasos para configurar y verificar un enrutador como cliente DHCPv6 sin estado.

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Configure el router cliente para crear una LLA. Una dirección local de vínculo IPv6 se crea en una interfaz de enrutador cuando se configura una dirección de unidifusión global, o sin una GUA mediante el comando de configuración de interfaz **ipv6 enable**. Cisco IOS utiliza EUI-64 para crear un ID de interfaz.
3. Configure el enrutador cliente para que utilice DHCPv6 mediante el comando **ipv6 address dhcp interface config**.
4. Compruebe que el router cliente tiene asignado un GUA mediante el comando **show ipv6 interface brief**.
5. Compruebe que el router cliente recibió otra información DHCPv6 necesaria mediante el comando **show ipv6 dhcp interface g0/0/1**.

Comandos de verificación del servidor DHCPv6

En la figura 1 el comando **show ipv6 dhcp pool** verifica el nombre del pool de DHCPv6 y sus parámetros. El comando también identifica el número de clientes activos.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:ACAD:1::/64 valid 172800 preferred 86400 (2 in use, 0
  conflicts)
    DNS server: 2001:4860:4860::8888
    Domain name: example.com
    Active clients: 2
R1#
```

Comandos de verificación del servidor DHCPv6 (cont.)

Utilice el resultado del comando **show ipv6 dhcp binding** para mostrar la dirección local del vínculo IPv6 del cliente y la dirección de unidifusión global asignada por el servidor.

- Esta información la mantiene un servidor de DHCPv6 stateful.
- Un servidor DHCPv6 sin estado no mantendría esta información.

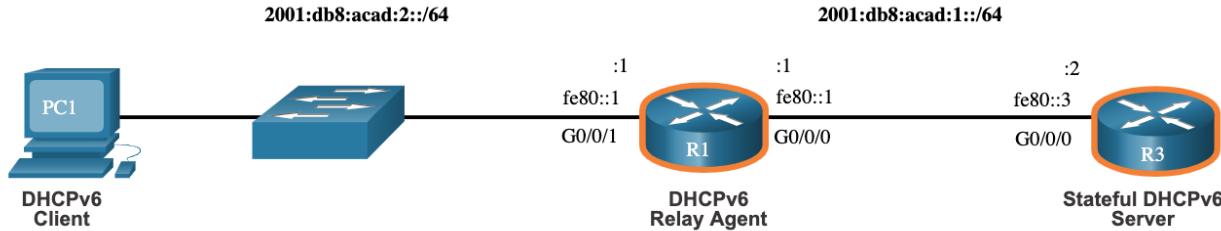
```
R1# show ipv6 dhcp binding
Client: FE80::192F:6FBC:9DB:B749
    DUID: 0001000125148183005056B327D6
    Username : unassigned
    VRF : default
    IA NA: IA ID 0x03000C29, T1 43200, T2 69120
        Address: 2001:DB8:ACAD:1:A43C:FD28:9D79:9E42
                    preferred lifetime 86400, valid lifetime 172800
                    expires at Sep 27 2019 09:10 AM (171192 seconds)
Client: FE80::2FC:BAFF:FE94:29B1
    DUID: 0003000100FCBA9429B0
    Username : unassigned
    VRF : default
    IA NA: IA ID 0x00060001, T1 43200, T2 69120
        Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C
                    preferred lifetime 86400, valid lifetime 172800
                    expires at Sep 27 2019 09:29 AM (172339 seconds)
```

R1#

Configurar un agente de retransmisión DHCPv6

Si el servidor de DHCPv6 está ubicado en una red distinta de la del cliente, el router IPv6 puede configurarse como agente de retransmisión DHCPv6.

- La configuración de un agente de retransmisión DHCPv6 es similar a la configuración de un router IPv4 como retransmisor DHCPv4.
- Este comando se configura en la interfaz que enfrenta a los clientes DHCPv6 y especifica la dirección del servidor DHCPv6 y la interfaz de salida para llegar al servidor, como se muestra en la salida. La interfaz de salida sólo es necesaria cuando la dirección de salto siguiente es una LLA.



```
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 dhcp relay destination 2001:db8:acad:1::2 G0/0/0
R1(config-if)# exit
R1(config)#
```

Verificar el agente de retransmisión DHCPv6

Compruebe que el agente de retransmisión DHCPv6 esté operativo con los comandos **show ipv6 dhcp interface** y **show ipv6 dhcp binding**.

```
R1# show ipv6 dhcp interface
GigabitEthernet0/0/1 is in relay mode
  Relay destinations:
    2001:DB8:ACAD:1::2
    2001:DB8:ACAD:1::2 via GigabitEthernet0/0/0
R1#
```

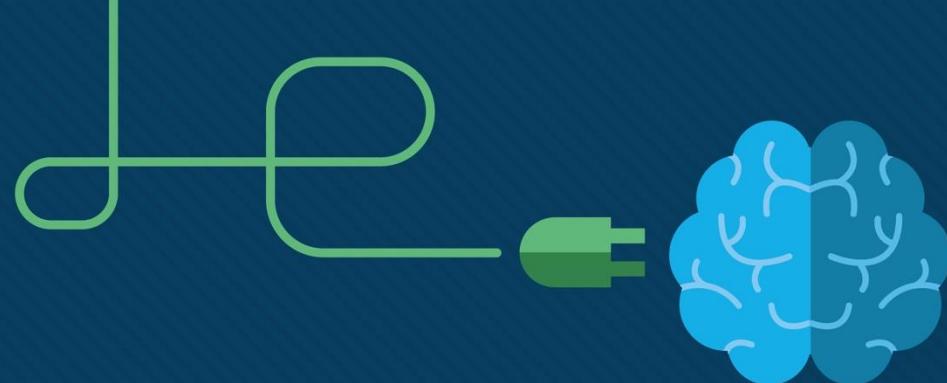
```
R3# show ipv6 dhcp binding
Client: FE80::5C43:EE7C:2959:DA68
  DUID: 0001000124F5CEA2005056B3636D
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x03000C29, T1 43200, T2 69120
  Address: 2001:DB8:ACAD:2:9C3C:64DE:AADA:7857
            preferred lifetime 86400, valid lifetime 172800
            expires at Sep 29 2019 08:26 PM (172710 seconds)
R3#
```

Compruebe que los hosts de Windows hayan recibido información de direccionamiento IPv6 con el comando **ipconfig /all**.

New Terms and Commands

- | | |
|---|--|
| <ul style="list-style-type: none">• Stateless Address Autoconfiguration (SLAAC)• Global Unicast Address (GUA)• Link Local Address (LLA)• Zone ID• Scope ID• Address Autoconfiguration Flag• Other Configuration Flag• Managed Address Configuration Flag• Router Solicitation (RS)• Router Advertisement (RA)• ipv6 unicast-routing• EUI-64• Duplicate Address Detection (DAD)• Neighbor Solicitation (NS)• Neighbor Advertisement (NA)• DHCPv6 SOLICIT• DHCPv6 ADVERTISE• DHCPv6 REPLY | <ul style="list-style-type: none">• Stateless DHCPv6 Client• Stateful DHCPv6 Client• ipv6 nd other-config-flag• ipv6 nd managed-config-flag• DHCPv6 Relay Agent• ipv6 dhcp pool pool-name• ipv6 dhcp server pool-name• ipv6 enable• ipv6 address autoconfig• show ipv6 dhcp interface• address prefix X:X:X:X:X:X:X:YY• dns-server X:X:X:X:X:X:X:X• domain-name name• ipv6 nd prefix default no-autoconfig• ipv6 address dhcp• show ipv6 dhcp pool• show ipv6 dhcp binding• ipv6 dhcp relay destination ipv6-address [interface-type interface-number] |
|---|--|





Módulo 7: DHCPv4

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



Objetivos del módulo

Título del módulo: DHCPv4

Objetivo del módulo: Implemente DHCPv4 para operar en varias LAN.

Título del tema	Objetivo del tema
Conceptos DHCP4	Explicar la forma en la que funciona DHCPv4 en la red de una pequeña o mediana empresa.
Configurar un servidor DHCP4 del IOS de Cisco	Configurar un router como servidor DHCPv4.
Configurar un cliente DHCP4	Configurar un router como cliente DHCPv4.

7.1 Conceptos DHCPv4

Conceptos DHCPv4

Servidor y cliente

- Dynamic Host Configuration Protocol v4 (DHCPv4) asigna direcciones IPv4 y otra información de configuración de red dinámicamente. Dado que los clientes de escritorio suelen componer gran parte de los nodos de red, DHCPv4 es una herramienta extremadamente útil para los administradores de red y que ahorra mucho tiempo.
- Un servidor de DHCPv4 dedicado es escalable y relativamente fácil de administrar. Sin embargo, en una sucursal pequeña o ubicación SOHO, se puede configurar un router Cisco para proporcionar servicios DHCPv4 sin necesidad de un servidor dedicado. El software Cisco IOS admite un servidor DHCPv4 con funciones completas opcional.

Servidor y cliente (Cont.)

- El servidor DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.
- Los clientes arriendan la información del servidor durante un período definido administrativamente. Los administradores configuran los servidores de DHCPv4 para establecer los arrendamientos, a fin de que caduquen a distintos intervalos. El arrendamiento típicamente dura de 24 horas a una semana o más. Cuando caduca el arrendamiento, el cliente debe solicitar otra dirección, aunque generalmente se le vuelve a asignar la misma.

Conceptos DHCPv4

OperaciónDHCPv4

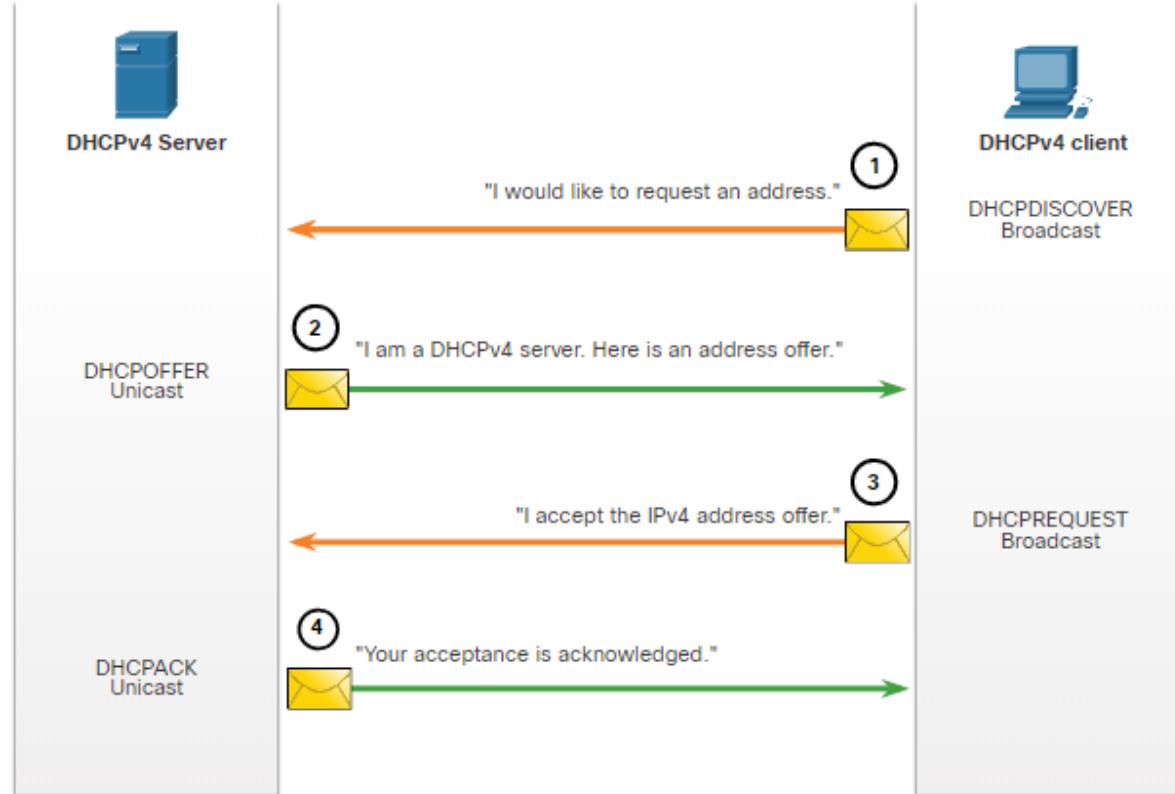
DHCPv4 funciona en un modo cliente/servidor. Cuando un cliente se comunica con un servidor de DHCPv4, el servidor asigna o arrienda una dirección IPv4 a ese cliente.

- El cliente se conecta a la red con esa dirección IPv4 arrendada hasta que caduque el arrendamiento. El cliente debe ponerse en contacto con el servidor de DHCP periódicamente para extender el arrendamiento.
- Este mecanismo de arrendamiento asegura que los clientes que se trasladan o se desconectan no mantengan las direcciones que ya no necesitan.
- Cuando caduca un arrendamiento, el servidor de DHCP devuelve la dirección al conjunto, donde se puede volver a asignar según sea necesario.

Pasos para obtener una concesión

Cuando el cliente arranca (o quiere unirse a una red), comienza un proceso de cuatro pasos para obtener un arrendamiento:

- 1. Detección de DHCP (DHCPDISCOVER)**
- 2. Oferta de DHCP (DHCPOFFER)**
- 3. Solicitud de DHCP (DHCPREQUEST)**
- 4. Acuse de recibo de DHCP (DHCPACK)**



Pasos para renovar una concesión

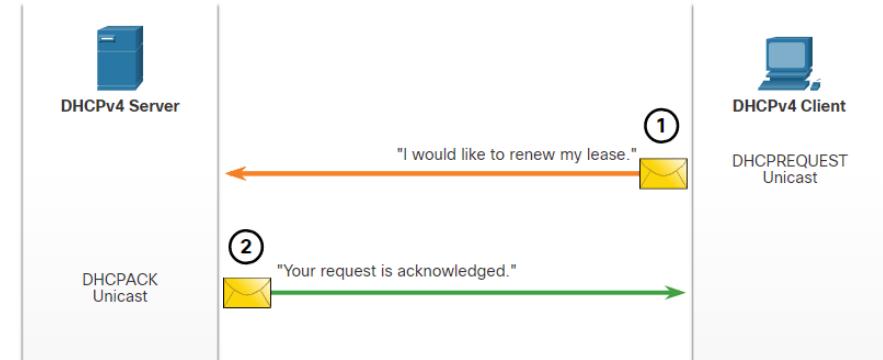
Antes de la expiración de la concesión, el cliente inicia un proceso de dos pasos para renovar la concesión con el servidor DHCPv4, como se muestra en la figura:

1. Solicitud de DHCP (DHCPREQUEST)

Antes de que caduque el arrendamiento, el cliente envía un mensaje DHCPREQUEST directamente al servidor de DHCPv4 que ofreció la dirección IPv4 en primera instancia. Si no se recibe un mensaje DHCPACK dentro de una cantidad de tiempo especificada, el cliente transmite otro mensaje DHCPREQUEST de modo que uno de los otros servidores de DHCPv4 pueda extender el arrendamiento.

2. Acuse de recepción de DHCP (DHCPACK)

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento al devolver un DHCPACK.



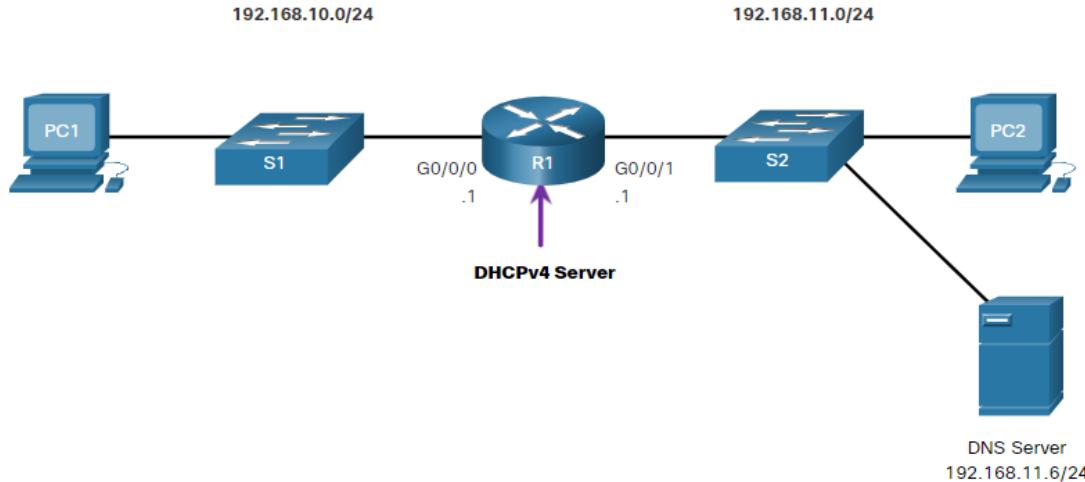
Nota: Estos mensajes (principalmente DHCPOFFER y DHCPACK) se pueden enviar como unidifusión o difusión según la IETF RFC 2131.

7.2 Configurar un servidor DHCPv4 del IOS de Cisco

Configurar un servidor DHCPv4 del IOS de Cisco

Servidor DHCPv4

Ahora usted tiene una comprensión básica de cómo funciona DHCPv4 y cómo puede hacer su trabajo un poco más fácil. Un router Cisco que ejecuta el software IOS de Cisco puede configurarse para que funcione como servidor de DHCPv4. El servidor de DHCPv4 que utiliza IOS de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4.



Pasos para configurar un servidor DHCPv4 de Cisco IOS

Utilice los siguientes pasos para configurar un servidor DHCPv4 del IOS de Cisco:

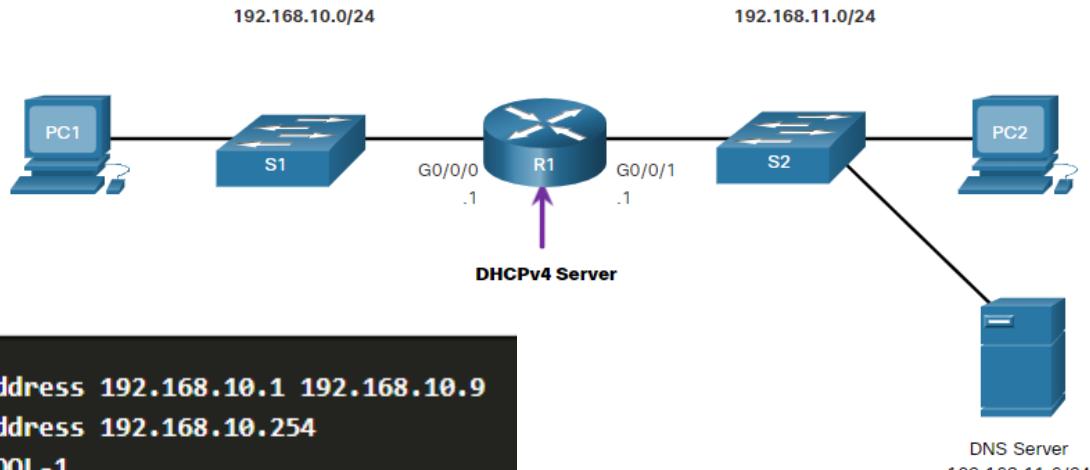
- **Paso 1.** Excluir direcciones IPv4 Se puede excluir una única dirección o un rango de direcciones especificando la *dirección más baja* y la *dirección más alta* del rango. Las direcciones excluidas deben incluir las direcciones asignadas a los routers, a los servidores, a las impresoras y a los demás dispositivos que se configuraron o se configurarán manualmente. También puede introducir el comando varias veces. El comando es **ip dhcp excluded-address *low-address [high-address]***
- **Paso 2.** Defina un nombre de grupo DHCPv4. El comando **ip dhcp pool *pool-name*** crea un conjunto con el nombre especificado y coloca al router en el modo de configuración de DHCPv4, que se identifica con el indicador **Router(dhcp-config)#[**.

Pasos para configurar un servidor DHCPv4 de Cisco IOS (Cont.)

- Paso 3.** Configure el grupo DHCPv4. El conjunto de direcciones y el router de gateway predeterminado deben estar configurados. Utilice la instrucción **network** para definir el rango de direcciones disponibles. Utilice el comando **default-router** para definir el router de gateway predeterminado. Estos comandos y otros comandos opcionales se muestran en la tabla.

Tarea	Comando de IOS
Definir el conjunto de direcciones.	<code>network network-number [mask /prefix-length]</code>
Definir el router o gateway predeterminado.	<code>default-router address [address2...address8]</code>
Definir un servidor DNS.	<code>dns-server address [address2...address8]</code>
Definir el nombre de dominio.	<code>domain-name domain</code>
Definir la duración de la concesión DHCP.	<code>lease {days [hours [minutes]] infinite}</code>
Definir el servidor WINS con NetBIOS.	<code>netbios-name-server address [address2...address8]</code>

Ejemplo de configuración de servidor DHCPv4 de Cisco IOS



```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

DNS Server
192.168.11.6/24

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique que DHCPv4 esté activo

Utilice los comandos de la tabla para verificar que el servidor DHCPv4 del IOS de Cisco esté operativo.

Comando	Descripción
show running-config section dhcp	Muestra los comandos DHCPv4 configurados en el router.
show ip dhcp binding	Muestra una lista de todos los enlaces de dirección IPv4 a dirección MAC proporcionadas por el servicio de DHCPv4.
show ip dhcp server statistics	Muestra información relacionada al numero de mensajes DHCPv4 que han sido mandados y recibidos.

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique la configuración DHCPv4

Como se muestra en el ejemplo, la salida del comando **show running-config | section dhcp** muestra los comandos DHCPv4 configurados en R1. El parámetro **| section** muestra solamente los comandos asociados a la configuración de DHCPv4.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 192.168.11.5
  domain-name example.com
```

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique los enlaces DHCPv4

Como se muestra en el ejemplo, el funcionamiento de DHCPv4 se puede verificar utilizando el comando **show ip dhcp binding**. Este comando muestra una lista de todas las vinculaciones de la dirección IPv4 con la dirección MAC que fueron proporcionadas por el servicio DHCPv4.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration        Type      State       Interface
                  Hardware address/
                  User name
192.168.10.10   0100.5056.b3ed.d8    Sep 15 2019 8:42 AM  Automatic  Active
GigabitEthernet0/0/0
```

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique las estadísticas de DHCPv4

La salida de **show ip dhcp server statistics** es utilizada para verificar que los mensajes están siendo recibidos o enviados por el router. Este comando muestra información de conteo con respecto a la cantidad de mensajes DHCPv4 que se enviaron y recibieron.

```
R1# show ip dhcp server statistics
Memory usage          19465
Address pools          1
Database agents         0
Automatic bindings      2
Manual bindings         0
Expired bindings        0
Malformed messages      0
Secure arp entries      0
Renew messages          0
Workspace timeouts       0
Static routes           0
Relay bindings           0
Relay bindings active     0
Relay bindings terminated   0
Relay bindings selecting    0
Message                Received
BOOTREQUEST              0
DHCPDISCOVER               4
DHCPREQUEST                 2
DHCPDECLINE                  0
DHCPRELEASE                  0
DHCPINFORM                   0
```

Configurar un servidor DHCPv4 del IOS de Cisco

Verificar el direccionamiento IPv4 recibido del cliente DHCPv4

El comando ipconfig /all, cuando se emite en PC1, muestra los parámetros TCP/IP, como se muestra en el ejemplo. Dado que la PC1 se conectó al segmento de red 192.168.10.0/24, recibió automáticamente un sufijo DNS, una dirección IPv4, una máscara de subred, un gateway predeterminado y una dirección del servidor DNS de ese pool. No se requiere ninguna configuración de interfaz del router específica de DHCP. Si una computadora está conectada a un segmento de red que tiene un pool de DHCPv4 disponible, la computadora puede obtener una dirección IPv4 del pool adecuado de manera automática.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration
  Host Name . . . . . : ciscolab
  Primary Dns Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No
  Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . : example.com
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : 00-05-9A-3C-7A-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained . . . . . : Saturday, September 14, 2019 8:42:22AM
    Lease Expires . . . . . : Sunday, September 15, 2019 8:42:22AM
    Default Gateway . . . . . : 192.168.10.1
    DHCP Server . . . . . : 192.168.10.1
    DNS Servers . . . . . : 192.168.11.5
```



Configurar un servidor DHCPv4 del IOS de Cisco

Desactivar el servidor DHCPv4

El servicio DHCPv4 está habilitado de manera predeterminada. Para deshabilitar el servicio, use el comando **no service dhcp** global configuration mode. Utilice el comando del modo de configuración del global **service dhcp** para volver a activar el proceso del servidor de DHCPv4. Si los parámetros no se configuran, active el servicio no tiene ningún efecto.

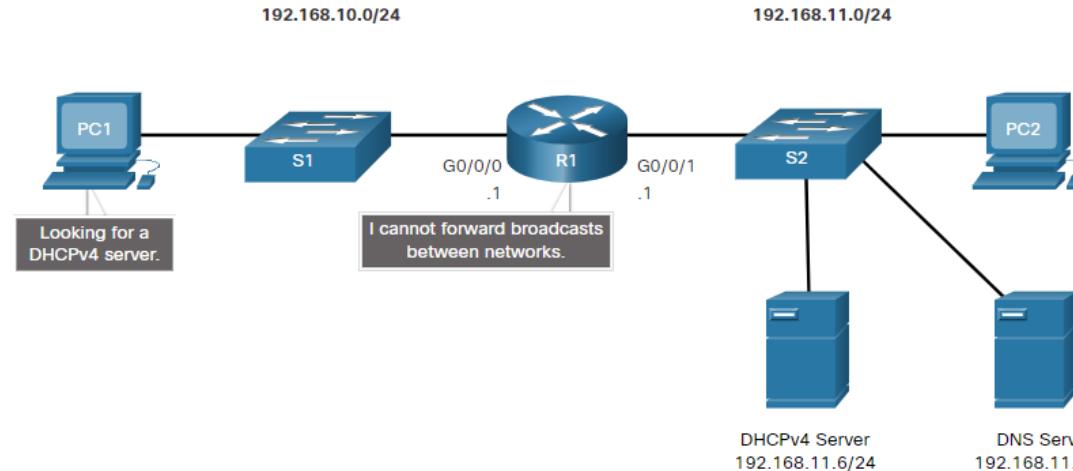
Nota: Si se borra los enlaces DHCP o se detiene y reinicia el servicio DHCP, se pueden asignar direcciones IP duplicadas en la red.

```
R1(config)# no service dhcp  
R1(config)# service dhcp  
R1(config)#{
```

Configurar un servidor DHCPv4 del IOS de Cisco

Relay DHCPv4

- En una red jerárquica compleja, los servidores empresariales suelen estar ubicados en una central. Estos servidores pueden proporcionar servicios DHCP, DNS, TFTP y FTP para la red. Generalmente, los clientes de red no se encuentran en la misma subred que esos servidores. Para ubicar los servidores y recibir servicios, los clientes con frecuencia utilizan mensajes de difusión.
- En la figura, la PC1 intenta adquirir una dirección IPv4 de un servidor de DHCPv4 mediante un mensaje de difusión. En esta situación, el router R1 no está configurado como servidor de DHCPv4 y no reenvía el mensaje de difusión. Dado que el servidor de DHCPv4 está ubicado en una red diferente, la PC1 no puede recibir una dirección IP mediante DHCP. R1 debe configurarse para retransmitir mensajes DHCPv4 al servidor DHCPv4.



Configurar un servidor DHCPv4 del IOS de Cisco Relay DHCPv4

- Configure R1 con el comando de configuración **ip helper-address address interface**. Esto hará que R1 retransmita transmisiones DHCPv4 al servidor DHCPv4. Como se muestra en el ejemplo, la interfaz en R1 que recibe la difusión desde PC1 está configurada para retransmitir la dirección DHCPv4 al servidor DHCPv4 en 192.168.11.6.
- Cuando se configura el R1 como agente de retransmisión DHCPv4, acepta solicitudes de difusión para el servicio DHCPv4 y, a continuación, reenvía dichas solicitudes en forma de unidifusión a la dirección IPv4 192.168.11.6. El administrador de red puede utilizar el comando **show ip interface** para verificar la configuración.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
  (output omitted)
```

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```



Otras transmisiones de servicio retransmitidas

DHCPv4 no es el único servicio que puede configurarse para que retransmita el router. De manera predeterminada, el comando **ip helper-address** reenvía los siguientes ocho siguientes servicios UDP:

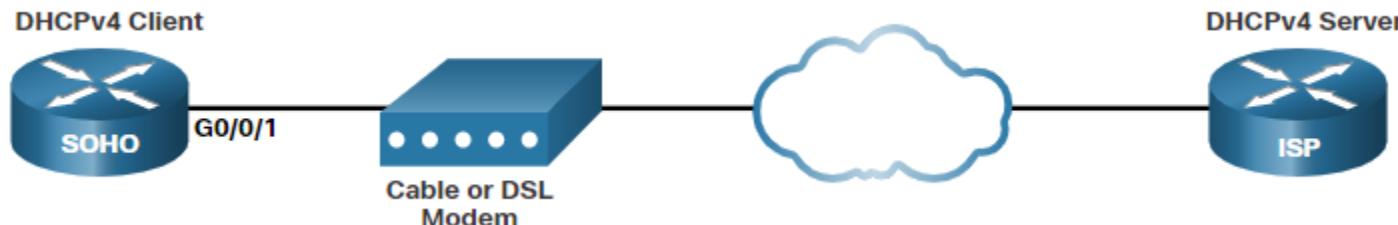
- **Puerto 37:** Tiempo
- **Puerto 49:** TACACS
- **Puerto 53:** DNS
- **Puerto 67:** servidor de DHCP/BOOTP
- **Puerto 68:** cliente DHCP/BOOTP
- **Puerto 69:** TFTP
- **Puerto 137:** servicio de nombres NetBIOS
- **Puerto 138:** servicio de datagrama NetBIOS

7.3 Configurar un cliente DHCPv4

Router Cisco como cliente DHCPv4.

Hay escenarios en los que puede tener acceso a un servidor DHCP a través de su ISP. En estos casos, puede configurar un router Cisco IOS como cliente DHCPv4.

- En ocasiones, los routers Cisco en oficinas pequeñas y oficinas domésticas (SOHO) y en los sitios de sucursales deben configurarse como clientes DHCPv4 de manera similar a los equipos cliente. El método específico utilizado depende del ISP. Sin embargo, en su configuración más simple, se utiliza la interfaz Ethernet para conectarse a un cable módem o a un módem DSL.
- Para configurar una interfaz Ethernet como cliente DHCP, utilice el comando del modo de configuración de interfaz **ip address dhcp**.
- En la figura, suponga que un ISP ha sido configurado para proporcionar a clientes seleccionados direcciones IP del rango de red 209.165.201.0/27 después de que la interfaz G0/0/1 es configurada con el comando **ip address dhcp**.



Ejemplo de Configuración de Cliente DHCPv4

- Para configurar una interfaz Ethernet como cliente DHCP, utilice comando del modo de configuración de interfaz **ip address dhcp** como se muestra en el ejemplo. Esta configuración supone que el ISP se ha configurado para proporcionar a los clientes seleccionados información de direcciones IPv4.
- El comando **show ip interface g0/1** confirma que la interfaz está activa y que la dirección fue asignada por un servidor DHCPv4.

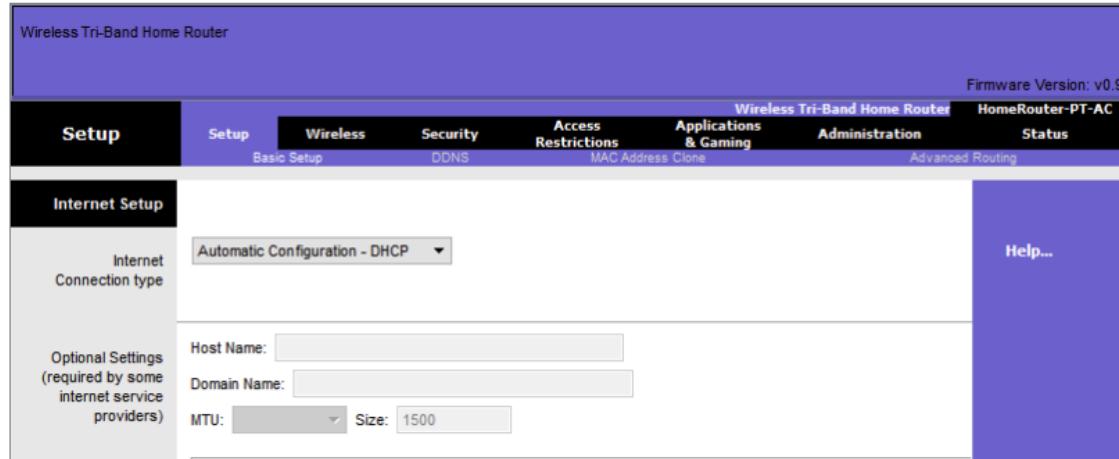
```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address
209.165.201.12, mask 255.255.255.224, hostname SOHO
```

```
SOHO# show ip interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  (output omitted)
```

Router Cisco como cliente DHCPv4.

Los routers de los hogares se configuran para recibir información de asignación de dirección IPv4 automáticamente desde el ISP. Esto es para que los clientes puedan configurar fácilmente el enrutador y conectarse a Internet.

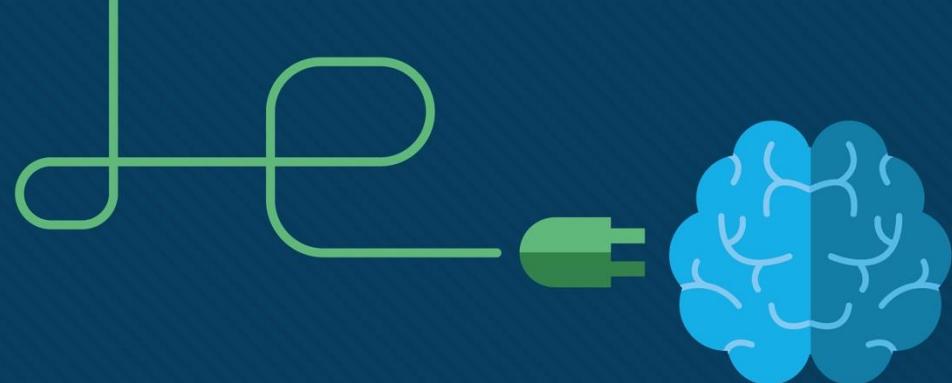
- Por ejemplo, en la ilustración se muestra la página de configuración de WAN predeterminada para un router inalámbrico de Packet Tracer. Notice that the internet connection type is set to **Automatic Configuration - DHCP**. Se utiliza esta selección cuando el router se conecta a un cable módem o DSL y actúa como cliente DHCPv4 y solicita una dirección IPv4 del ISP.
- Varios fabricantes de enrutadores domésticos tendrán una configuración similar.



Nuevos términos y comandos

- Dynamic Host Configuration Protocol (DHCP)
- DHCP Discover (DHCPDISCOVER)
- DHCP Offer (DHCPOFFER)
- DHCP Request (DHCPREQUEST)
- DHCP Acknowledgment (DHCPACK)
- **ip dhcp excluded-address low-address [high-address]**
- **ip dhcp pool name**
- **network network-number [mask | /prefix-length]**
- **default-router address [address2 ... address8]**
- **dns-server address [address2 ... address8]**
- **domain-name domain**
- **lease {days [hours [minutes]] | infinite}**
- **netbios-name-server address [address2 ... address8]**
- **show running-config | section dhcp**
- **show ip dhcp binding**
- **show ip dhcp server statistics**
- **[no] service dhcp**
- **ip helper-address address**
- **ip address dhcp**





Módulo 6: EtherChannel

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



Objetivos del módulo

Título del módulo: EtherChannel

Objetivo del módulo: TResuelva problemas de EtherChannel en enlaces de switches.

Título del tema	Objetivo del tema
Funcionamiento de EtherChannel	Describa la tecnología EtherChannel.
Configuración de EtherChannel	Configure EtherChannel.
Verificación y solución de problemas de EtherChannel	Solucionar problemas de EtherChannel.

6.1 – Funcionamiento de EtherChannel

Funcionamiento de EtherChannel

Etherchannel

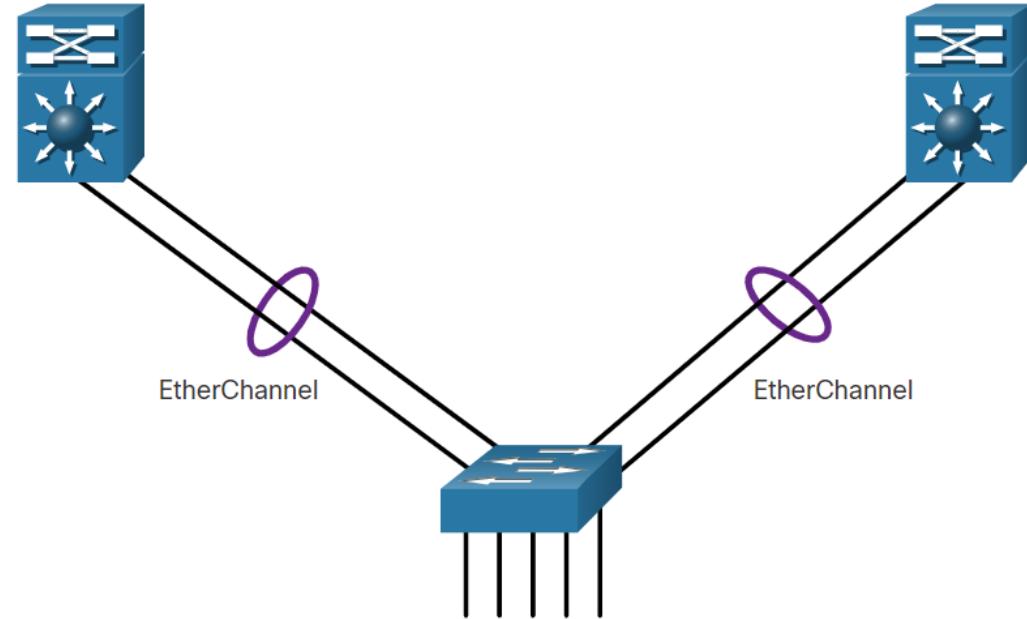
- Hay escenarios en los que se necesita más ancho de banda o redundancia entre dispositivos que lo que puede proporcionar un único enlace. Se pueden conectar varios enlaces entre dispositivos para aumentar el ancho de banda. Sin embargo, el protocolo de árbol de expansión (STP), que está habilitado en dispositivos de capa 2 como switches Cisco de forma predeterminada, bloqueará enlaces redundantes para evitar bucles de conmutación.
- Se necesita una tecnología de agregación de enlaces que permita vínculos redundantes entre dispositivos que no serán bloqueados por STP. Esa tecnología se conoce como EtherChannel.
- EtherChannel es una tecnología de agregación de enlaces que agrupa varios enlaces físicos Ethernet en un único enlace lógico. Se utiliza para proporcionar tolerancia a fallos, uso compartido de carga, mayor ancho de banda y redundancia entre switches, routers y servidores.
- La tecnología de EtherChannel hace posible combinar la cantidad de enlaces físicos entre los switches para aumentar la velocidad general de la comunicación switch a switch.

Funcionamiento de EtherChannel

EtherChannel

En los inicios, Cisco desarrolló la tecnología EtherChannel como una técnica switch a switch LAN para agrupar varios puertos Fast Ethernet o gigabit Ethernet en un único canal lógico.

Cuando se configura un EtherChannel, la interfaz virtual resultante se denomina “canal de puertos”. Las interfaces físicas se agrupan en una interfaz de canal de puertos, como se muestra en la figura.



Ventajas de la operación EtherChannel

La tecnología EtherChannel tiene muchas ventajas, incluidas las siguientes:

- La mayoría de las tareas de configuración se pueden realizar en la interfaz EtherChannel en lugar de en cada puerto individual, lo que asegura la coherencia de configuración en todos los enlaces.
- EtherChannel depende de los puertos de switch existentes. No es necesario actualizar el enlace a una conexión más rápida y más costosa para tener más ancho de banda.
- El equilibrio de carga ocurre entre los enlaces que forman parte del mismo EtherChannel.
- EtherChannel crea una agregación que se ve como un único enlace lógico. Cuando existen varios grupos EtherChannel entre dos switches, STP puede bloquear uno de los grupos para evitar los bucles de switching. Cuando STP bloquea uno de los enlaces redundantes, bloquea el EtherChannel completo. Esto bloquea todos los puertos que pertenecen a ese enlace EtherChannel. Donde solo existe un único enlace EtherChannel, todos los enlaces físicos en el EtherChannel están activos, ya que STP solo ve un único enlace (lógico).
- EtherChannel proporciona redundancia, ya que el enlace general se ve como una única conexión lógica. Además, la pérdida de un enlace físico dentro del canal no crea ningún cambio en la topología.

Funcionamiento de EtherChannel

Restricciones de implementación

EtherChannel tiene ciertas restricciones de implementación, entre las que se incluyen las siguientes:

- No pueden mezclarse los tipos de interfaz. Por ejemplo, Fast Ethernet y Gigabit Ethernet no se pueden mezclar dentro de un único EtherChannel.
- En la actualidad, cada EtherChannel puede constar de hasta ocho puertos Ethernet configurados de manera compatible. El EtherChannel proporciona un ancho de banda full-duplex de hasta 800 Mbps (Fast EtherChannel) u 8 Gbps (Gigabit EtherChannel) entre un switch y otro switch o host.
- El switch Cisco Catalyst 2960 Layer 2 soporta actualmente hasta seis EtherChannels.
- La configuración de los puertos individuales que forman parte del grupo EtherChannel debe ser coherente en ambos dispositivos. Si los puertos físicos de un lado se configuran como enlaces troncales, los puertos físicos del otro lado también se deben configurar como enlaces troncales dentro de la misma VLAN nativa. Además, todos los puertos en cada enlace EtherChannel se deben configurar como puertos de capa 2.
- Cada EtherChannel tiene una interfaz de canal de puertos lógica. La configuración aplicada a la interfaz de canal de puertos afecta a todas las interfaces físicas que se asignan a esa interfaz.

Protocolos de negociación automática

Los EtherChannels se pueden formar por medio de una negociación con uno de dos protocolos: Port Aggregation Protocol (PAgP) o Link Aggregation Control Protocol (LACP). Estos protocolos permiten que los puertos con características similares formen un canal mediante una negociación dinámica con los switches adyacentes.

Nota: también es posible configurar un EtherChannel estático o incondicional sin PAgP o LACP.

Funcionamiento de EtherChannel

Funcionamiento PAgP

PAgP (pronunciado “Pag - P”) es un protocolo patentado por Cisco que ayuda en la creación automática de enlaces EtherChannel. Cuando se configura un enlace EtherChannel mediante PAgP, se envían paquetes PAgP entre los puertos aptos para EtherChannel para negociar la formación de un canal. Cuando PAgP identifica enlaces Ethernet compatibles, agrupa los enlaces en un EtherChannel. El EtherChannel después se agrega al árbol de expansión como un único puerto.

Cuando se habilita, PAgP también administra el EtherChannel. Los paquetes PAgP se envían cada 30 segundos. PAgP revisa la coherencia de la configuración y administra los enlaces que se agregan, así como las fallas entre dos switches. Cuando se crea un EtherChannel, asegura que todos los puertos tengan el mismo tipo de configuración.

Nota: en EtherChannel, es obligatorio que todos los puertos tengan la misma velocidad, la misma configuración de dúplex y la misma información de VLAN. Cualquier modificación de los puertos después de la creación del canal también modifica a los demás puertos del canal.

Operación de EtherChannel PAgP (Cont.)

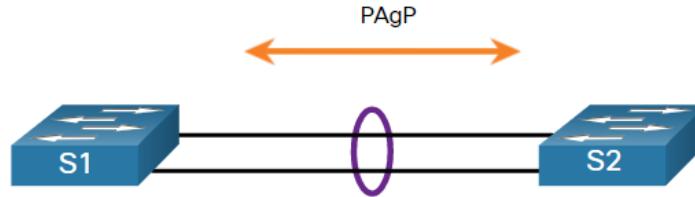
PAgP ayuda a crear el enlace EtherChannel al detectar la configuración de cada lado y asegurarse de que los enlaces sean compatibles, de modo que se pueda habilitar el enlace EtherChannel cuando sea necesario. Los modos de PAgP de la siguiente manera:

- **Encendido:** este modo obliga a la interfaz a proporcionar un canal sin PAgP. Las interfaces configuradas en el modo encendido no intercambian paquetes PAgP.
- **PAgP deseable** - Este modo PAgP coloca una interfaz en un estado de negociación activa en el que la interfaz inicia negociaciones con otras interfaces al enviar paquetes PAgP.
- **PAgP auto** - este modo PAgP coloca una interfaz en un estado de negociación pasiva en el que la interfaz responde a los paquetes PAgP que recibe, pero no inicia la negociación PAgP.

Los modos deben ser compatibles en cada lado. Si se configura un lado en modo automático, se coloca en estado pasivo, a la espera de que el otro lado inicie la negociación del EtherChannel. Si el otro lado se establece en modo automático, la negociación nunca se inicia y no se forma el canal EtherChannel. Si se deshabilitan todos los modos mediante el comando **no** o si no se configura ningún modo, entonces se deshabilita el EtherChannel. El modo encendido coloca manualmente la interfaz en un EtherChannel, sin ninguna negociación. Funciona solo si el otro lado también se establece en modo encendido. Si el otro lado se establece para negociar los parámetros a través de PAgP, no se forma ningún EtherChannel, ya que el lado que se establece en modo encendido no negocia. El hecho de que no haya negociación entre los dos switches significa que no hay un control para asegurarse de que todos los enlaces en el EtherChannel terminen del otro lado o de que haya compatibilidad con PAgP en el otro switch.

Operación de EtherChannel

Ejemplo de configuración del modo PAgP



La tabla muestra las diversas combinaciones de modos PAgP en S1 y S2 y el resultado resultante del establecimiento de canales.

S1	S2	Establecimiento del canal
On	On	Sí
On	Desirable/Auto	No
Desirable	Desirable	Sí
Desirable	Auto	Sí
Auto	Desirable	Sí
Auto	Auto	No

Funcionamiento de EtherChannel

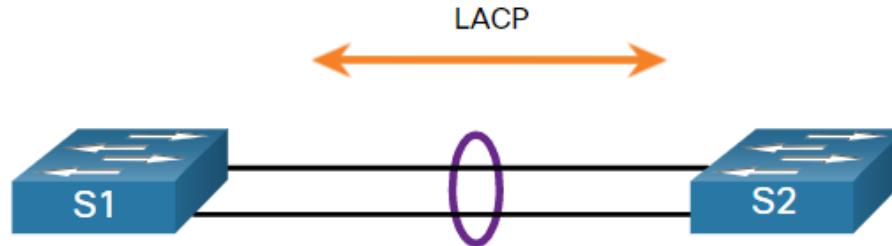
Funcionamiento LACP

LACP forma parte de una especificación IEEE (802.3ad) que permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al otro switch. Realiza una función similar a PAgP con EtherChannel de Cisco. Debido a que LACP es un estándar IEEE, se puede usar para facilitar los EtherChannels en entornos de varios proveedores. En los dispositivos de Cisco, se admiten ambos protocolos.

LACP proporciona los mismos beneficios de negociación que PAgP. LACP ayuda a crear el enlace EtherChannel al detectar la configuración de cada lado y al asegurarse de que sean compatibles, de modo que se pueda habilitar el enlace EtherChannel cuando sea necesario. Los modos para LACP son los siguientes:

- **On** - Este modo obliga a la interfaz a proporcionar un canal sin LACP. Las interfaces configuradas en el modo encendido no intercambian paquetes LACP.
- **LACP active** - Este modo de LACP coloca un puerto en estado de negociación activa. En este estado, el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP.
- **LACP passive** - Este modo de LACP coloca un puerto en estado de negociación pasiva. En este estado, el puerto responde a los paquetes LACP que recibe, pero no inicia la negociación de paquetes LACP.

Ejemplo de configuración del modo LACP



La tabla muestra las diversas combinaciones de modos LACP en S1 y S2 y el resultado resultante del establecimiento de canales.

S1	S2	Establecimiento del canal
On	On	Sí
On	Active/Passive	No
Active	Active	Sí
Active	Passive	Sí
Passive	Active	Sí
Passive	Passive	No

6.2 Configuración de EtherChannel

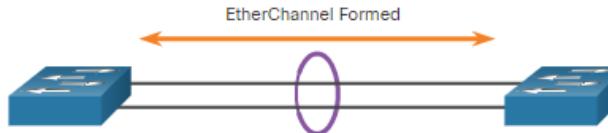
Pautas para la configuración

Las siguientes pautas y restricciones son útiles para configurar EtherChannel:

- **EtherChannel support** - Todas las interfaces Ethernet deben admitir EtherChannel, sin necesidad de que las interfaces sean físicamente contiguas
- **Speed and duplex** - Configure todas las interfaces en un EtherChannel para que funcionen a la misma velocidad y en el mismo modo dúplex.
- **VLAN match** - Todas las interfaces en el grupo EtherChannel se deben asignar a la misma VLAN o se deben configurar como enlace troncal (mostrado en la figura).
- Rango de VLAN: un EtherChannel admite el mismo rango permitido de VLAN en todas las interfaces de un EtherChannel de enlace troncal. Si el rango permitido de VLAN no es el mismo, las interfaces no forman un EtherChannel, incluso si se establecen en modo auto **o desirable** .

Pautas para la configuración (cont.)

- La figura muestra una configuración que permitiría que se forme un EtherChannel entre el S1 y el S2.
- Si se deben modificar estos parámetros, configúrelos en el modo de configuración de interfaz de canal de puertos. Cualquier configuración que se aplique a la interfaz de canal de puertos también afectará a las interfaces individuales. Sin embargo, las configuraciones que se aplican a las interfaces individuales no afectan a la interfaz de canal de puertos. Por ello, realizar cambios de configuración a una interfaz que forma parte de un enlace EtherChannel puede causar problemas de compatibilidad de interfaces.
- El canal de puertos se puede configurar en modo de acceso, modo de enlace troncal (más frecuente) o en un puerto enrutado.



S1 Port Configurations

Speed	1 Gbps
Duplex	Full
VLAN	10

S2 Port Configurations

Speed	1 Gbps
Duplex	Full
VLAN	10

Configuración de EtherChannel

Ejemplo de LACP

La configuración de EtherChannel con LACP requiere tres pasos:

- **Paso 1.** Especifique las interfaces que conforman el grupo EtherChannel mediante el comando **interface range interface** en modo de configuración global. La palabra clave **range** le permite seleccionar varias interfaces y configurarlas a la vez.
- **Paso 2.** Cree la interfaz de canal de puerto con el comando **channel-group identifier mode active** en el modo de configuración de rango de interfaz. El identificador especifica el número del grupo del canal. Las palabras clave **mode active** identifican a esta configuración como EtherChannel LACP.
- **Paso 3.** Para cambiar la configuración de capa 2 en la interfaz de canal de puertos, ingrese al modo de configuración de interfaz de canal de puertos mediante el comando **interface port-channel** seguido del identificador de la interfaz. En el ejemplo, S1 está configurado con un EtherChannel LACP. El canal de puertos está configurado como interfaz de enlace troncal con VLAN permitidas específicas.

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config-if)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```



6.3 – Verificación y solución de problemas de EtherChannel

Verificación y solución de problemas de EtherChannel

Como siempre, al configurar dispositivos en su red, debe verificar su configuración. Si hay problemas, también deberá poder solucionarlos y solucionarlos. Existe una variedad de comandos para verificar una configuración EtherChannel.

- Primero, el comando **show interfaces port-channel** muestra el estado general de la interfaz de canal de puertos.
- El comando **show etherchannel summary** muestra una línea de información por canal de puerto.
- Use el comando **show etherchannel port-channel** para mostrar la información sobre una interfaz de canal de puertos específica.
- Utilice el comando **show interfaces etherchannel** para proporcionar información sobre el rol de la interfaz en EtherChannel.

Verificación y solución de problemas de EtherChannel

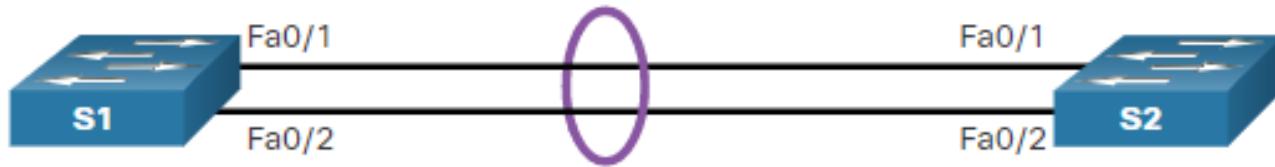
Solución de problemas de EtherChannel

Todas las interfaces dentro de un EtherChannel deben tener la misma configuración de velocidad y modo dúplex, de VLAN nativas y permitidas en los enlaces troncales, y de VLAN de acceso en los puertos de acceso. Garantizar estas configuraciones reducirá significativamente los problemas de red relacionados con EtherChannel. Entre los problemas comunes de EtherChannel se incluyen los siguientes:

- Los puertos asignados en el EtherChannel no son parte de la misma VLAN ni son configurados como enlace troncal. Los puertos con VLAN nativas diferentes no pueden formar un EtherChannel.
- La conexión troncal se configuró en algunos de los puertos que componen el EtherChannel, pero no en todos ellos. No se recomienda que configure el modo de enlace troncal en los puertos individuales que conforman el EtherChannel. Al configurar un enlace troncal en un EtherChannel, compruebe el modo de enlace troncal en EtherChannel.
- Si el rango permitido de VLAN no es el mismo, los puertos no forman un EtherChannel incluso cuando PAgP está configurado en modo **auto** o **desirable** .
- Las opciones de negociación dinámica para PAgP y LACP no se encuentran configuradas de manera compatible en ambos extremos del EtherChannel.

Solución de problemas de EtherChannel (Cont.)

En la figura, las interfaces F0/1 y F0/2 en los switches S1 y S2 se conectan con un EtherChannel. Sin embargo, el EtherChannel no está operativo.



Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

Paso 1. Ver la información de resumen de EtherChannel: la salida del comando show etherchannel summary indica que EtherChannel está inactivado.

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3      L - Layer2
      U - in use      N - not in use, no aggregation
      f - failed to allocate aggregator
      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
      A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group  Port-channel  Protocol    Ports
-----+-----+-----+
 1     Po1(SD)        -       Fa0/1(D)   Fa0/2(D)
```

Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

Paso 2. Ver configuración del canal de puerto: En el **show run | begin interface puerto** salida canal, salida más detallada indica que hay modos PAgP incompatibles configurados en S1 y S2.

```
S1# show run | begin interface port-channel
interface Port-channel1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/2
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode on
=====
S2# show run | begin interface port-channel
interface Port-channel1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/2
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode desirable
```

Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

Paso 3: Corrija la configuración incorrecta: Para corregir el problema, el modo PAgP en el EtherChannel se cambia a deseable.

Nota: EtherChannel y STP deben interoperar. Por este motivo, el orden en el que se introducen los comandos relacionados con EtherChannel es importante, y por ello se puede ver que se quitó el canal de puertos de interfaz1 y después se volvió a agregar con el comando **channel-group** en vez de cambiarse directamente. Si se intenta cambiar la configuración directamente, los errores STP hacen que los puertos asociados entren en estado de bloqueo o errdisabled.

```
S1(config)# no interface port-channel 1
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

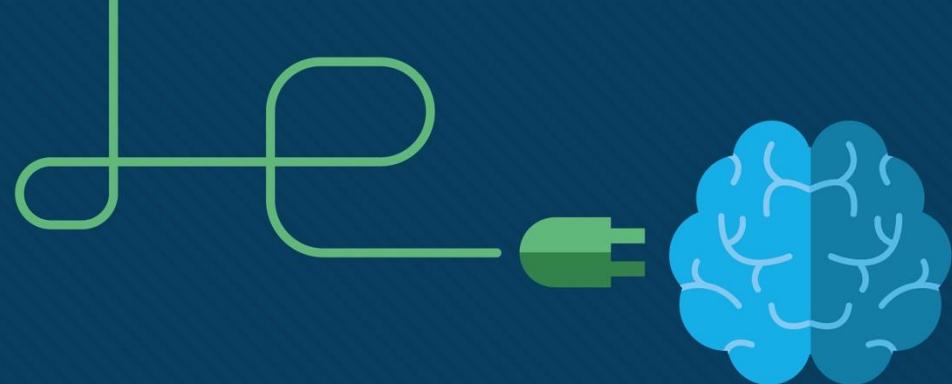
Paso 4. Verifique que EtherChannel esté operativo: el EtherChannel está activo como se ha verificado mediante la salida del comando show etherchannel summary.

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3      S - Layer2
      U - in use       N - not in use, no aggregation
      f - failed to allocate aggregator
      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
      A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1(SU)        PAgP        Fa0/1(P)   Fa0/2(P)
```

Nuevos términos y comandos

- Link Aggregation
- EtherChannel
- Port Channel
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- PAgP desirable
- PAgP auto
- LACP active
- LACP passive
- **channel-group X mode [desirable | auto | active | passive]**
- **interface port-channel X**
- **show interfaces port-channel**
- **show etherchannel summary**
- **show etherchannel port-channel**
- **show interfaces etherchannel**





Módulo 5: Conceptos STP

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



Objetivos del módulo

Título del módulo: Conceptos STP

Objetivo del módulo: Explicar cómo STP permite la redundancia en una red de capa 2.

Título del tema	Objetivo del tema
Propósito del STP	Explique los problemas comunes en una red commutada redundante L2.
Funcionamientos del STP	Explicar cómo opera STP en una red commutada simple.
Evolución del STP	Explique la forma en que funciona PVST+ rápido.

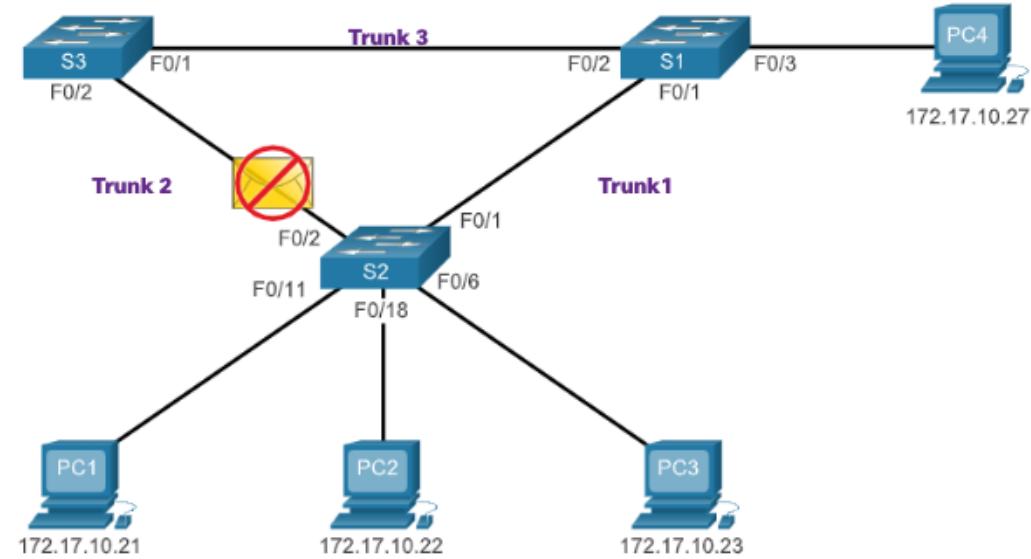
5.1 Propósito de STP

Redundancia en redes conmutadas de capa 2

- En este tema se tratan las causas de los bucles en una red de capa 2 y se explica brevemente cómo funciona el protocolo de árbol de expansión. La redundancia es una parte importante del diseño jerárquico para eliminar puntos únicos de falla y prevenir la interrupción de los servicios de red para los usuarios. Las redes redundantes requieren la adición de rutas físicas, pero la redundancia lógica también debe formar parte del diseño. Tener rutas físicas alternativas para que los datos atraviesen la red permite que los usuarios accedan a los recursos de red, a pesar de las interrupciones de la ruta. Sin embargo, las rutas redundantes en una red Ethernet conmutada pueden causar bucles físicos y lógicos en la capa 2.
- Las LAN Ethernet requieren una topología sin bucles con una única ruta entre dos dispositivos. Un bucle en una LAN Ethernet puede provocar una propagación continua de tramas Ethernet hasta que un enlace se interrumpe y interrumpa el bucle.

Protocolo de árbol de expansión (Spanning Tree Protocol, STP)

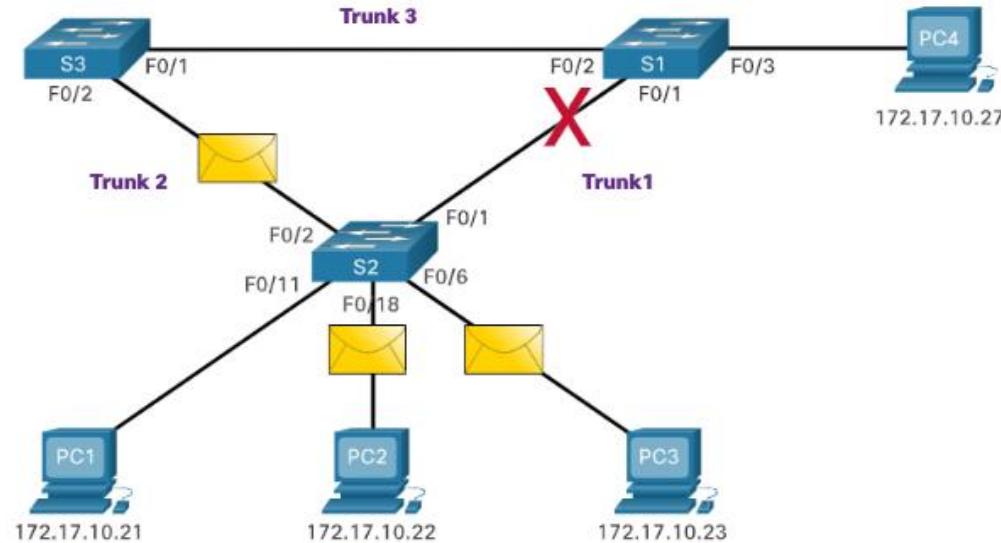
- El protocolo de árbol de expansión (STP) es un protocolo de red de prevención de bucles que permite redundancia mientras crea una topología de capa 2 sin bucles.
- STP bloquea lógicamente los bucles físicos en una red de Capa 2, evitando que las tramas circulen por la red para siempre.



S2 drops the frame because it received it on a blocked port.

Propósito del STP Recálculo STP

STP compensa un error en la red al volver a calcular y abrir los puertos previamente bloqueados.



Problemas con vínculos de switches redundantes

- La redundancia de ruta proporciona múltiples servicios de red al eliminar la posibilidad de un solo punto de falla. Cuando existen múltiples rutas entre dos dispositivos en una red Ethernet, y no hay implementación de árbol de expansión en los switches, se produce un bucle de capa 2. Un bucle de capa 2 puede provocar inestabilidad en la tabla de direcciones MAC, saturación de enlaces y alta utilización de CPU en switch y dispositivos finales, lo que hace que la red se vuelva inutilizable.
- La capa 2 Ethernet no incluye un mecanismo para reconocer y eliminar tramas de bucle sin fin. Tanto IPv4 como IPv6 incluyen un mecanismo que limita la cantidad de veces que un dispositivo de red de Capa 3 puede retransmitir un paquete. Un router disminuirá el TTL (Tiempo de vida) en cada paquete IPv4 y el campo Límite de saltos en cada paquete IPv6. Cuando estos campos se reducen a 0, un router dejará caer el paquete. Los switches Ethernet y Ethernet no tienen un mecanismo comparable para limitar el número de veces que un switch retransmite una trama de Capa 2. STP fue desarrollado específicamente como un mecanismo de prevención de bucles para Ethernet de Capa 2.

Bucles de Capa 2

- Sin STP habilitado, se pueden formar bucles de capa 2, lo que hace que las tramas de difusión, multidifusión y unidifusión desconocidos se reproduzcan sin fin. Esto puede derribar una red rápidamente.
- Cuando se produce un bucle, la tabla de direcciones MAC en un switch cambiará constantemente con las actualizaciones de las tramas de difusión, lo que resulta en la inestabilidad de la base de datos MAC. Esto puede causar una alta utilización de la CPU, lo que hace que el switch no pueda reenviar tramas.
- Una trama de unidifusión desconocida se produce cuando el switch no tiene la dirección MAC de destino en la tabla de direcciones MAC y debe reenviar la trama a todos los puertos, excepto el puerto de ingreso.

Tormenta de difusión (Broadcast Storm)

- Una tormenta de difusión es un número anormalmente alto de emisiones que abruman la red durante un período específico de tiempo. Las tormentas de difusión pueden deshabilitar una red en cuestión de segundos al abrumar los switch y los dispositivos finales. Las tormentas de difusión pueden deberse a un problema de hardware como una NIC defectuosa o a un bucle de capa 2 en la red.
- Las emisiones de capa 2 en una red, como las solicitudes ARP, son muy comunes. Las multidifusión de capa 2 normalmente se reenvían de la misma manera que una difusión por el switch. Los paquetes IPv6 nunca se reenvían como una difusión de Capa 2, ICMPv6 Neighbor Discovery utiliza multidifusión de Capa 2.
- Un host atrapado en un bucle de capa 2 no está accesible para otros hosts en la red. Además, debido a los constantes cambios en su tabla de direcciones MAC, el switch no sabe desde qué puerto reenviar las tramas de unidifusión.
- Para evitar que ocurran estos problemas en una red redundante, se debe habilitar algún tipo de árbol de expansión en los switch. De manera predeterminada, el árbol de expansión está habilitado en los switch Cisco para prevenir que ocurran bucles en la capa 2.

El algoritmo de árbol de expansión (Spanning Tree)

- STP se basa en un algoritmo inventado por Radia Perlman mientras trabajaba para Digital Equipment Corporation, y publicado en el artículo de 1985 "Un algoritmo para la computación distribuida de un árbol de expansión en una LAN extendida". Su algoritmo de árbol de expansión (STA) crea una topología sin bucles al seleccionar un único puente raíz donde todos los demás switch determinan una única ruta de menor costo.
- STP evita que ocurran bucles mediante la configuración de una ruta sin bucles a través de la red, con puertos “en estado de bloqueo” ubicados estratégicamente. Los switch que ejecutan STP pueden compensar las fallas mediante el desbloqueo dinámico de los puertos bloqueados anteriormente y el permiso para que el tráfico se transmita por las rutas alternativas.

El algoritmo de árbol de expansión (cont.)

¿Cómo crea STA una topología sin bucles?

- **Selección de un puente raíz:** Este puente (switch) es el punto de referencia para que toda la red cree un árbol de expansión alrededor.
- **Bloquear rutas redundantes:** STP garantiza que solo haya una ruta lógica entre todos los destinos de la red al bloquear intencionalmente las rutas redundantes que podrían causar un bucle. Cuando se bloquea un puerto, se impide que los datos del usuario entren o salgan de ese puerto.
- **Crear una topología sin bucle:** un puerto bloqueado tiene el efecto de convertir ese vínculo en un vínculo no reenvío entre los dos switch. Esto crea una topología en la que cada switch tiene una única ruta al puente raíz, similar a las ramas de un árbol que se conectan a la raíz del árbol.
- **Vuelva a calcular en caso de falla de enlace:** las rutas físicas todavía existen para proporcionar redundancia, pero estas rutas están deshabilitadas para evitar que ocurran los bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active. Los recálculos STP también pueden ocurrir cada vez que se agrega un nuevo switch o un nuevo vínculo entre switches a la red.

5.2 Operaciones STP

Pasos para una topología sin bucles

Usando STA, STP crea una topología sin bucles en un proceso de cuatro pasos:

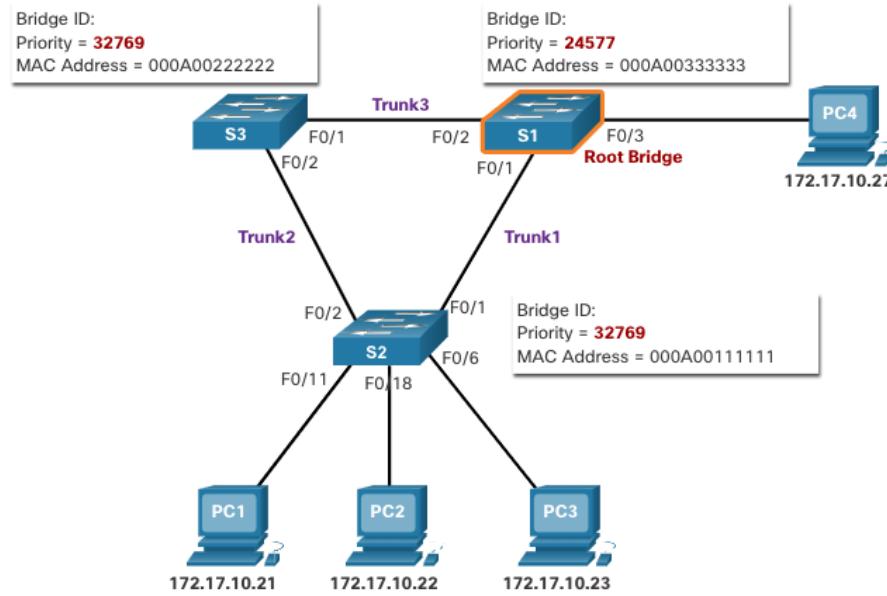
1. Elige el puente raíz.
 2. Seleccione los puertos raíz.
 3. Elegir puertos designados.
 4. Seleccione puertos alternativos (bloqueados).
- Durante las funciones STA y STP, los switch utilizan unidades de datos de protocolo de puente (BPDU) para compartir información sobre sí mismos y sus conexiones. Las BPDU se utilizan para elegir el puente raíz, los puertos raíz, los puertos designados y los puertos alternativos.
 - Cada BPDU contiene una ID de puente (BID) que identifica qué switch envió la BPDU. El BID participa en la toma de muchas de las decisiones STA, incluidos los roles de puente raíz y puerto.
 - El BID contiene un valor de prioridad, la dirección MAC del switch y un ID de sistema extendido. El valor de BID más bajo lo determina la combinación de estos tres campos.

Pasos para una topología sin bucles(cont.)

- **Prioridad de puente:** el valor de prioridad predeterminado para todos los switch Cisco es el valor decimal 32768 El rango va de 0 a 61440 y aumenta de a 4096. Es preferible una prioridad de puente más baja. La prioridad de puente 0 prevalece sobre el resto de las prioridades de puente.
- **ID del sistema extendido:** el valor de ID del sistema extendido es un valor decimal agregado al valor de prioridad del puente en el BID para identificar la VLAN para esta BPDU.
- **Dirección MAC:** cuando dos switch se configuran con la misma prioridad y tienen la misma ID de sistema extendida, el switch que tiene la dirección MAC con el valor más bajo, expresado en hexadecimal, tendrá el BID más bajo.

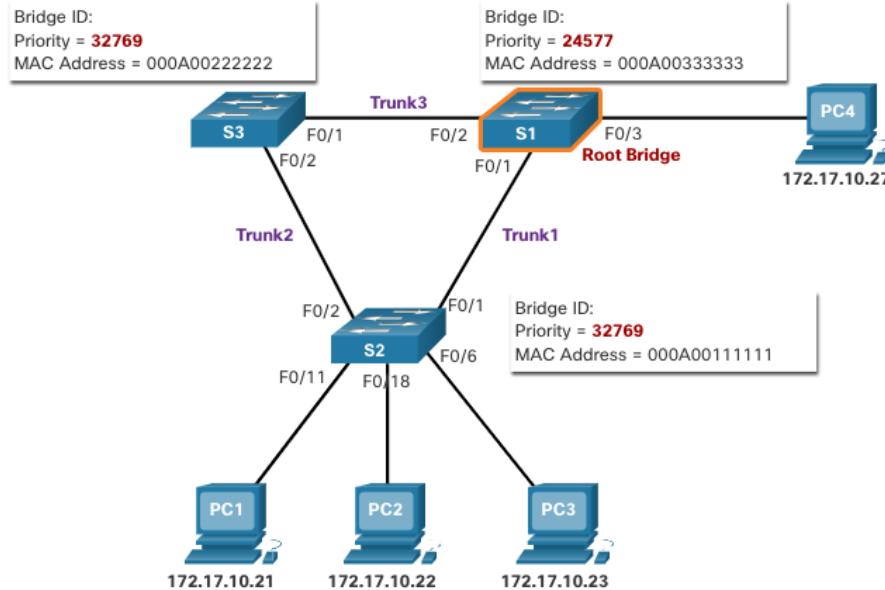
1. Elige el puente raíz

- El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. Los switch intercambian BPDU para crear la topología sin bucles comenzando con la selección del puente raíz.
- Todos los switch del dominio de difusión participan del proceso de elección. Una vez que el switch arranca, comienza a enviar tramas BPDU cada dos segundos. Estas tramas BPDU contienen el BID del switch de envío y el BID del puente raíz, conocido como ID raíz.
- El switch que tiene el BID más bajo se convierte en el puente raíz. Al principio, todos los switch se declaran a sí mismos como el puente raíz con su propio BID establecido como ID raíz. Eventualmente, los switch aprenden a través del intercambio de BPDU qué switch tiene el BID más bajo y acordarán un puente raíz.



Operaciones STP Impacto del BID predeterminado

- Dado que el BID predeterminado es 32768, es posible que dos o más switches tengan la misma prioridad. En este escenario, donde las prioridades son las mismas, el switch con la dirección MAC más baja se convertirá en el puente raíz. El administrador debe configurar el switch de puente raíz deseado con una prioridad inferior.
- En la figura, todos los switch están configurados con la misma prioridad de 32769. Aquí la dirección MAC se convierte en el factor decisivo en cuanto a qué interruptor se convierte en el puente raíz. El switch con el valor de dirección MAC hexadecimal más bajo es el puente raíz preferido. En este ejemplo, S2 tiene el valor más bajo para su dirección MAC y se elige como el puente raíz para esa instancia de árbol de expansión.
- Nota:** La prioridad de todos los switch es 32769. El valor se basa en la prioridad de puente predeterminada 32768 y la ID del sistema extendida (asignación de VLAN 1) asociada con cada switch ($32768 + 1$).



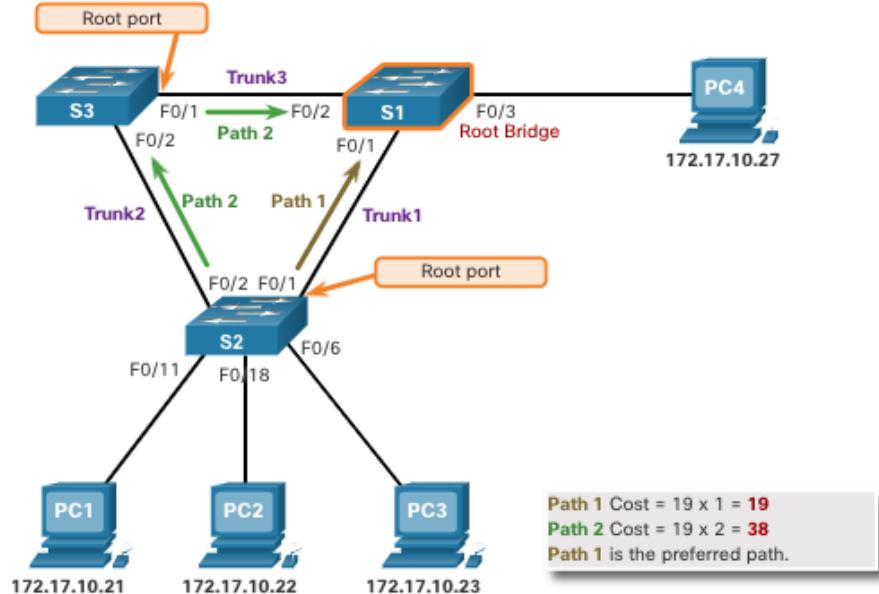
Determinar el costo de la ruta raíz

- Cuando se ha elegido el puente raíz para una instancia de árbol de expansión dado, el STA comienza a determinar las mejores rutas al puente raíz desde todos los destinos en el dominio de difusión. La información de la ruta, conocida como el costo interno de la ruta raíz, está determinada por la suma de todos los costos de los puertos individuales a lo largo de la ruta desde el switch hasta el puente raíz.
- Cuando un switch recibe la BPDU, agrega el costo del puerto de ingreso del segmento para determinar el costo interno de la ruta hacia la raíz.
- Los costos de los puertos predeterminados se definen por la velocidad a la que funcionan los mismos. La tabla muestra los costos de puerto predeterminados sugeridos por IEEE. Los switch Cisco utilizan de forma predeterminada los valores definidos por el estándar IEEE 802.1D, también conocido como costo de ruta corta, tanto para STP como para RSTP.
- Pese a que los puertos de switch cuentan con un costo de puerto predeterminado asociado a los mismos, tal costo puede configurarse. La capacidad de configurar costos de puerto individuales le da al administrador la flexibilidad para controlar de forma manual las rutas de árbol de expansión hacia el puente raíz.

Velocidad de enlace	STP Cost: IEEE 802.1D-1998	Costo de RSTP: IEEE 802.1w-2004
10 Gbps	2	2000
1 Gbps	4	20 000
100 Mbps	19	200 000
10 Mbps	100	2 000 000

2. Elegir los puertos raíz

- Después de determinar el puente raíz, se utiliza el algoritmo STA para seleccionar el puerto raíz. Cada switch que no sea root seleccionará un puerto raíz. El puerto raíz es el puerto más cercano al puente raíz en términos de costo general para el puente raíz. Este costo general se conoce como costo de ruta raíz interna.
- El costo interno de la ruta raíz es igual a la suma de todos los costos del puerto a lo largo de la ruta al puente raíz, como se muestra en la figura. Las rutas con el costo más bajo se convierten en las preferidas, y el resto de las rutas redundantes se bloquean. En el ejemplo, el costo de la ruta raíz interna desde S2 hasta el puente raíz S1 sobre la ruta 1 es 19, mientras que el costo de la ruta raíz interna sobre la ruta 2 es 38. Debido a que la ruta 1 tiene un costo de ruta general más bajo para el puente raíz, es la ruta preferida y F0 / 1 se convierte en el puerto raíz en S2.



Elegir un puerto raíz a partir de múltiples rutas de igual costo

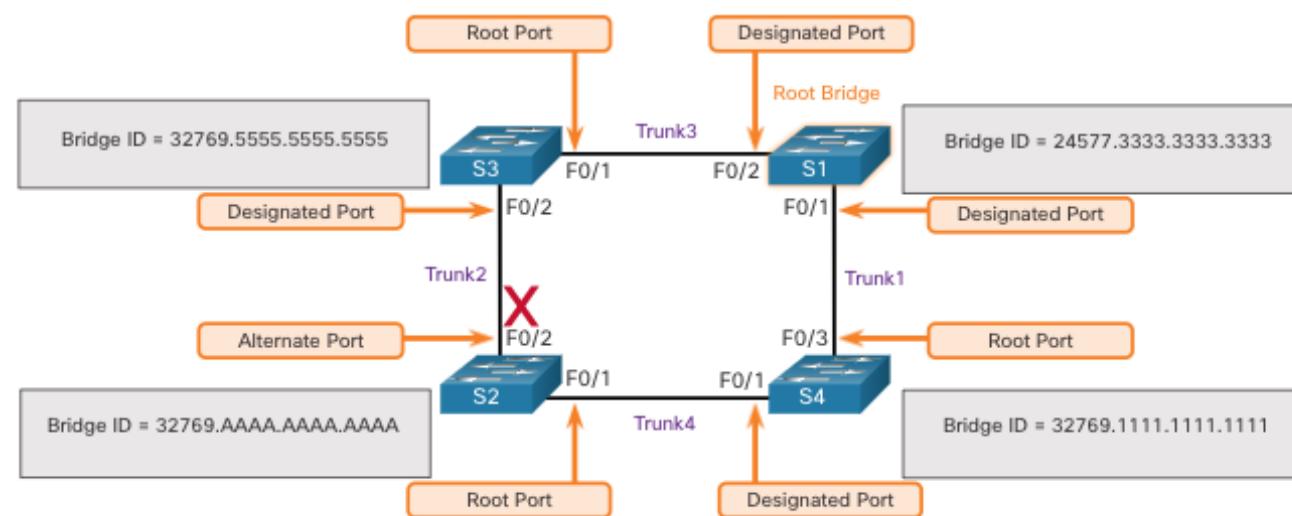
Cuando un switch tiene varias rutas de igual costo al puente raíz, el switch determinará un puerto utilizando los siguientes criterios:

- Oferta de remitente más baja
- Prioridad de puerto del remitente más baja
- ID de puerto del remitente más bajo

Elegir un puerto raíz a partir de varias rutas de igual costo (Cont.)

Oferta más baja del remitente: esta topología tiene cuatro switch con el switch S1 como puente raíz. El puerto F0/1 en el switch S3 y el puerto F0/3 en el switch S4 se han seleccionado como puertos raíz porque tienen el costo de la ruta raíz al puente raíz para sus respectivos switch.

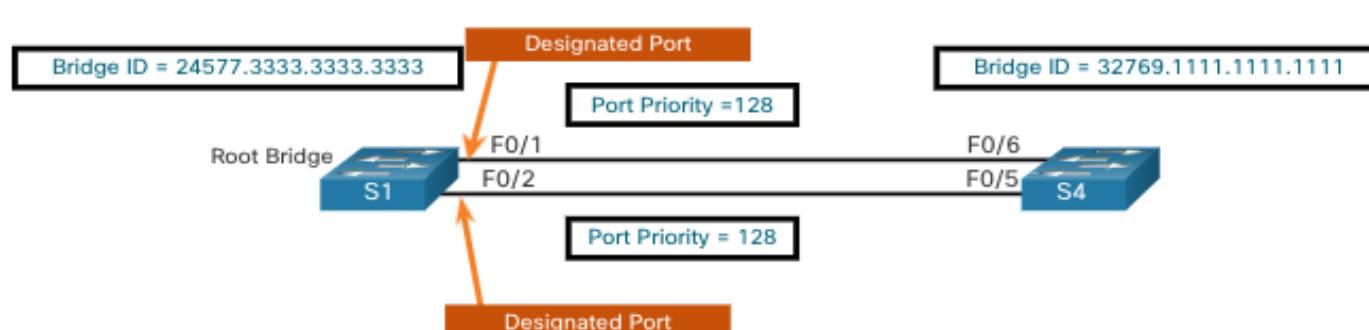
S2 tiene dos puertos, F0/1 y F0/2 con rutas de igual costo al puente raíz. Las ID de puente de S3 y S4 se utilizarán para romper el empate. Esto se conoce como BID del emisor. S3 tiene un BID de 32769.5555.5555.5555 y S4 tiene un BID de 32769.1111.1111.1111. Como S4 tiene un BID más bajo, el puerto F0/1 de S2, que es el puerto conectado a S4, será el puerto raíz.



Elegir un puerto raíz a partir de varias rutas de igual costo (Cont.)

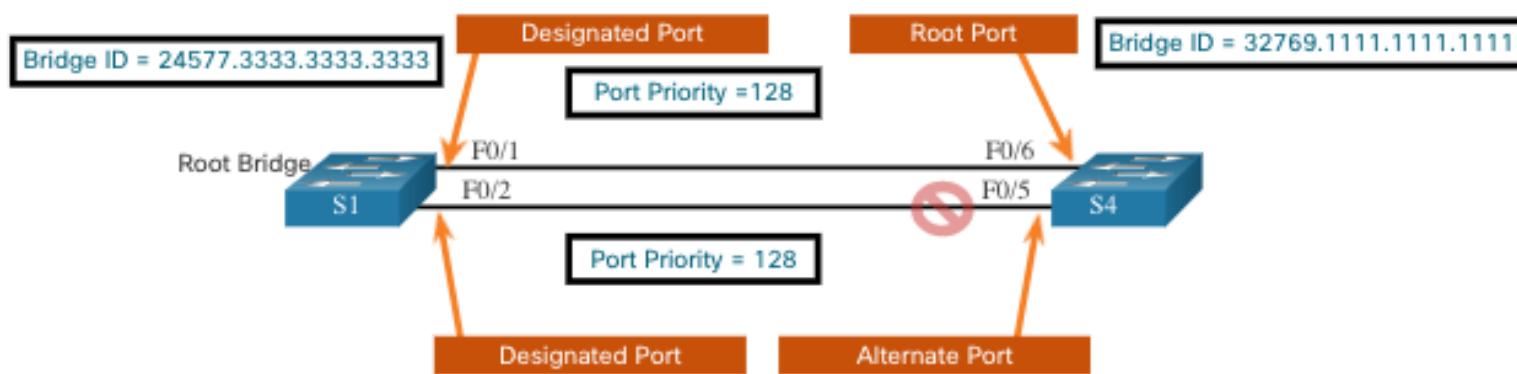
Prioridad de puerto de remitente más baja: Esta topología tiene dos switch que están conectados con dos rutas de igual costo entre ellos. S1 es el puente raíz, por lo que ambos puertos son puertos designados.

- S4 tiene dos puertos con rutas de igual costo al puente raíz. Dado que ambos puertos están conectados al mismo switch, el BID (S1) del remitente es igual. Entonces el primer paso es un empate.
- A continuación, es la prioridad del puerto del remitente (S1). La prioridad de puerto predeterminada es 128, por lo que ambos puertos de S1 tienen la misma prioridad de puerto. Esto también es un empate. Sin embargo, si cualquiera de los puertos de S1 se configuraba con una prioridad de puerto más baja, S4 pondría su puerto adyacente en estado de reenvío. El otro puerto en S4 sería un estado de bloqueo.



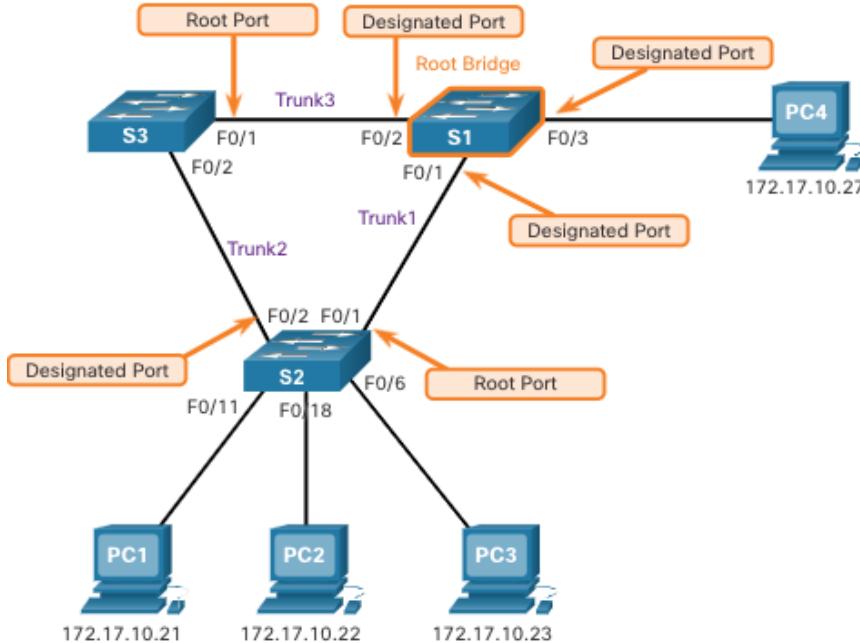
Elegir un puerto raíz a partir de varias rutas de igual coste (Cont.)

- **Id. de puerto del remitente más bajo:** el último desempate es el Id. de puerto del remitente más bajo. El switch S4 ha recibido BPDU desde el puerto F0/1 y el puerto F0/2 en S1. La decisión se basa en el ID del puerto del remitente, no en el ID del puerto del receptor. Dado que el Id. de puerto de F0/1 en S1 es menor que el puerto F0/2, el puerto F0/6 en el switch S4 será el puerto raíz. Este es el puerto de S4 que está conectado al puerto F0/1 de S1.
- El puerto F0/5 en S4 se convertirá en un puerto alternativo y se colocará en el estado de bloqueo.



3. Seleccionar puertos designados

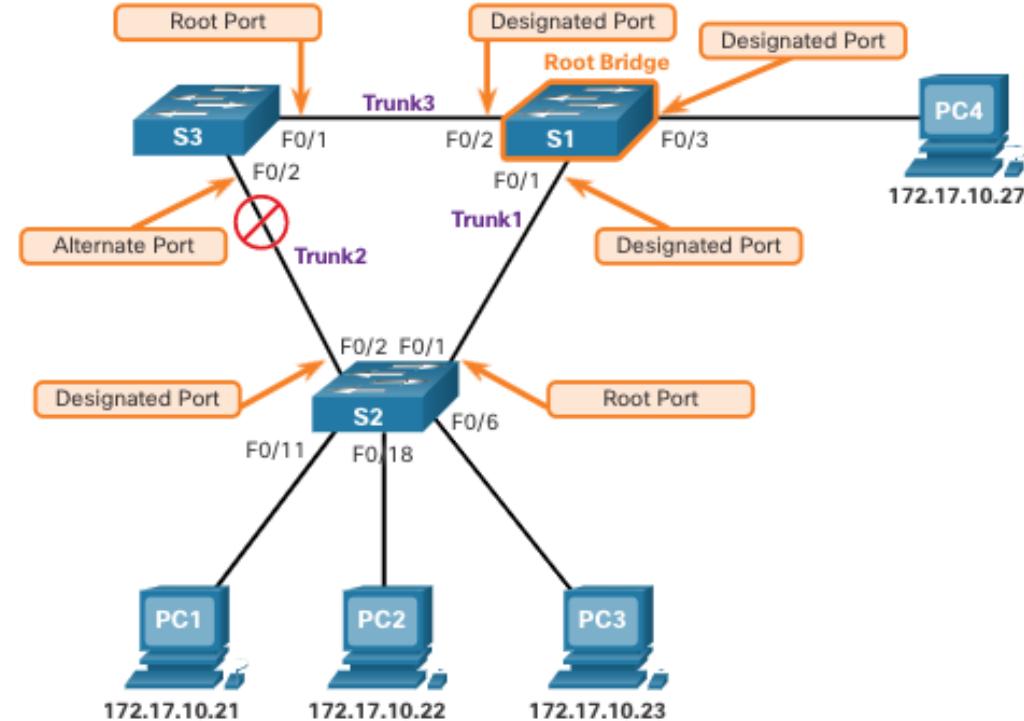
- Cada segmento entre dos switch tendrá un puerto designado. El puerto designado es un puerto en el segmento que tiene el costo de ruta raíz interna para el puente raíz. En otras palabras, el puerto designado tiene la mejor ruta para recibir el tráfico que conduce al puente raíz.
 - Lo que no es un puerto raíz o un puerto designado se convierte en un puerto alternativo o bloqueado.
 - Todos los puertos en el puente raíz son puertos designados.
 - Si un extremo de un segmento es un puerto raíz, el otro extremo es un puerto designado.
 - Todos los puertos conectados a los dispositivos finales son puertos designados.
 - En segmentos entre dos switch donde ninguno de los switch es el puente raíz, el puerto del switch con la ruta de menor costo al puente raíz es un puerto designado.



4. Seleccionar puertos alternativos (bloqueados)

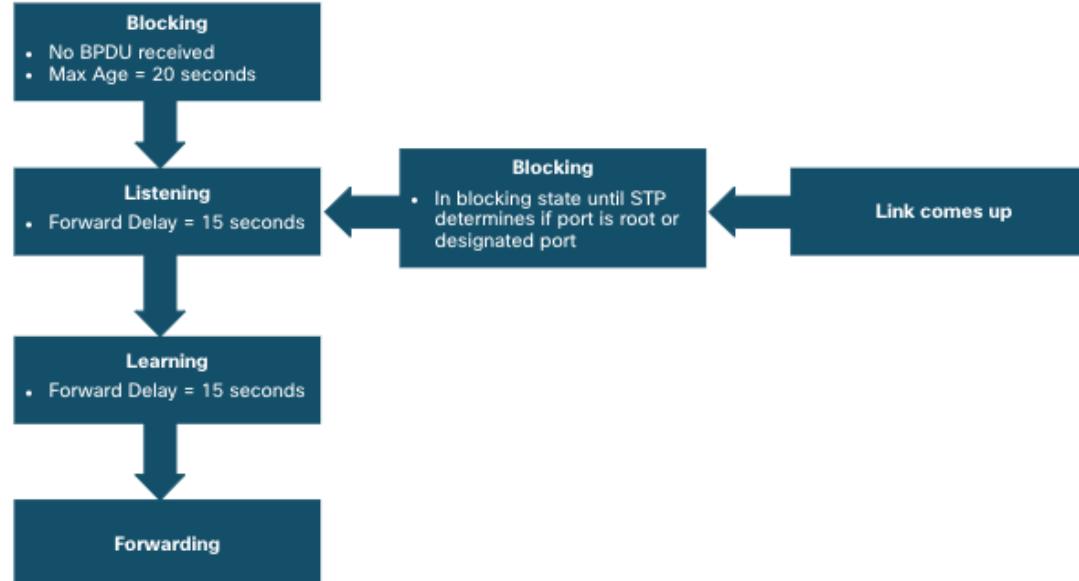
Si un puerto no es un puerto raíz o un puerto designado, se convierte en un puerto alternativo (o de copia de seguridad). Los puertos alternativos están en estado de descarte o bloqueo para evitar bucles.

En la figura, la STA ha configurado el puerto F0/2 en S3 en el rol alternativo. El puerto F0/2 en S3 está en estado de bloqueo y no reenviará tramas Ethernet. Todos los demás puertos entre switch están en estado de reenvío. Esta es la parte de prevención de bucles de STP.



Detalles operativos de cada estado de puerto (cont.)

STP facilita la ruta lógica sin bucles en todo el dominio de difusión. El árbol de expansión se determina a través de la información obtenida en el intercambio de tramas de BPDU entre los switch interconectados. Si un puerto de switch pasa directamente del estado de bloqueo al de reenvío sin información acerca de la topología completa durante la transición, el puerto puede crear un bucle de datos temporal. Por esta razón, STP tiene cinco estados de puertos, cuatro de los cuales son estados de puertos operativos, como se muestra en la figura. El estado deshabilitado se considera no operativo.



Detalles operativos de cada estado de puerto

La tabla resume los detalles operativos de cada estado del puerto

Estado del puerto	BPDU	Tabla de direcciones MAC	Reenvío de tramas de datos
Bloqueo	Recibir solo	No hay actualización	No
Escucha	Recibir y enviar	No hay actualización	No
Aprendizaje	Recibir y enviar	Actualización de la tabla	No
Reenvío	Recibir y enviar	Actualización de la tabla	Sí
Deshabilitado	No se ha enviado ni recibido	No hay actualización	No

Temporizadores STP

La convergencia STP requiere tres temporizadores, como sigue:

- **Hello Timer** - el tiempo de saludo es el intervalo entre BPDU. El valor predeterminado es 2 segundos, pero se puede modificar entre 1 y 10 segundos.
- **Temporizador de demora directa**: la demora directa es el tiempo que se pasa en el estado de escucha y aprendizaje. El valor predeterminado es 15 segundos, pero se puede modificar a entre 4 y 30 segundos.
- **Temporizador de edad máxima**: la antigüedad máxima es la duración máxima de tiempo que un switch espera antes de intentar cambiar la topología STP. El valor predeterminado es 20 segundos, pero se puede modificar entre 6 y 40 segundos.

Nota: Los tiempos predeterminados se pueden cambiar en el puente raíz, que dicta el valor de estos temporizadores para el dominio STP.

Árbol de expansión por VLAN

STP se puede configurar para operar en un entorno con varias VLAN. En el árbol de expansión por VLAN (PVST) versión para STP, hay un puente raíz ha elegir por cada instancia de árbol de expansión.

Esto hace posible tener diferentes puentes raíz para diferentes conjuntos de VLAN. STP opera una instancia independiente de STP para cada VLAN individual. Si todos los puertos de todos los switch pertenecen a la VLAN 1, solo se da una instancia de árbol de expansión.

5.3 Evolución del STP

Diferentes versiones de STP

- Muchos profesionales usan genéricamente árbol de expansión (spanning tree) y STP para referirse a las diversas implementaciones de árbol de expansión, como Rapid Spanning Tree Protocol (RSTP) y Multiple Spanning Tree Protocol (MSTP). Para comunicar los conceptos del árbol de expansión correctamente, es importante hacer referencia a la implementación o al estándar del árbol de expansión en contexto.
- El documento más reciente del IEEE acerca del árbol de expansión (IEEE-802-1D-2004) establece que “STP se reemplazó con el protocolo de árbol de expansión rápido (RSTP)”. El IEEE utiliza “STP” para referirse a la implementación original del árbol de expansión y “RSTP” para describir la versión del árbol de expansión especificada en IEEE-802.1D-2004.
- Debido a que los dos protocolos comparten gran parte de la misma terminología y métodos para la ruta sin bucles, el enfoque principal estará en el estándar actual y las implementaciones propietarias de Cisco de STP y RSTP.
- Los switch de Cisco con IOS 15.0 o posterior ejecutan PVST+ de manera predeterminada. Esta versión incluye muchas de las especificaciones IEEE 802.1D-2004, como puertos alternativos en lugar de los puertos no designados anteriores. Los switch deben configurarse explícitamente para el modo de árbol de expansión rápida para ejecutar el protocolo de árbol de expansión rápida.

Evolución de STP

Diferentes versiones de STP (cont.)

Variedad STP	Descripción
STP	Esta es la versión original IEEE 802.1D (802.1D-1998 y anteriores) que proporciona una topología sin bucles en una red con enlaces redundantes. También llamado Common Spanning Tree (CST), asume una instancia de árbol de expansión para toda la red puenteada, independientemente de la cantidad de VLAN.
PVST+	El árbol de expansión por VLAN (PVST +) es una mejora de Cisco de STP que proporciona una instancia de árbol de expansión 802.1D separada para cada VLAN configurada en la red. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
802.1D-2004	Esta es una versión actualizada del estándar STP, que incorpora IEEE 802.1w.
RSTP	Rapid Spanning Tree Protocol (RSTP) o IEEE 802.1w es una evolución de STP que proporciona una convergencia más rápida que STP.
PVST+ rápido	Esta es una mejora de Cisco de RSTP que utiliza PVST + y proporciona una instancia independiente de 802.1w por VLAN. Cada instancia aparte admite PortFast, protección de BPDU, filtro de BPDU, protección de raíz y protección de bucle.
MSTP	El Protocolo de árbol de expansión múltiple (MSTP) es un estándar IEEE inspirado en la implementación anterior de STP de instancia múltiple (MISTP) de Cisco. MSTP asigna varias VLAN en la misma instancia de árbol de expansión.
Instancia	Multiple Spanning Tree (MST) es la implementación de Cisco de MSTP, que proporciona hasta 16 instancias de RSTP y combina muchas VLAN con la misma topología física y lógica en una instancia RSTP común. Cada instancia admite PortFast, protección BPDU, filtro BPDU, protección de raíz y protección de bucle.

Conceptos de RSTP

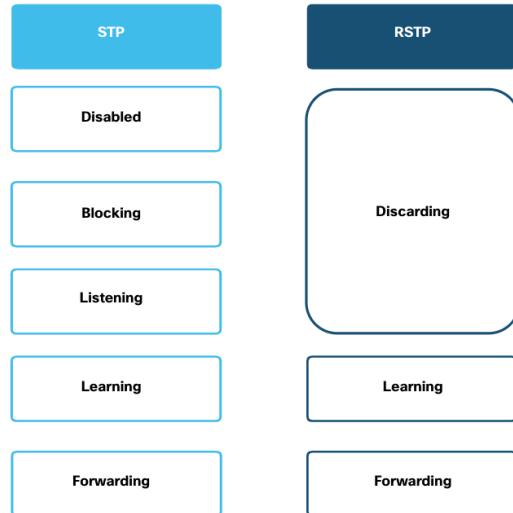
- RSTP (IEEE 802.1w) reemplaza al 802.1D original mientras conserva la compatibilidad con versiones anteriores. La terminología de STP 802.1w sigue siendo fundamentalmente la misma que la de STP IEEE 802.1D original. La mayoría de los parámetros se han dejado sin cambios. Los usuarios que estén familiarizados con el estándar STP original pueden configurar fácilmente RSTP. El mismo algoritmo de árbol de expansión se utiliza tanto para STP como para RSTP para determinar los roles de puerto y la topología.
- RSTP aumenta la velocidad del recálculo del árbol de expansión cuando cambia la topología de la red de Capa 2. RSTP puede lograr una convergencia mucho más rápida en una red configurada en forma adecuada, a veces sólo en unos pocos cientos de milisegundos. Si un puerto está configurado para ser un puerto alternativo, puede cambiar inmediatamente a un estado de reenvío sin esperar a que la red converja.

Nota: Rapid PVST + es la implementación de Cisco de RSTP por VLAN. Con Rapid PVST + se ejecuta una instancia independiente de RSTP para cada VLAN.

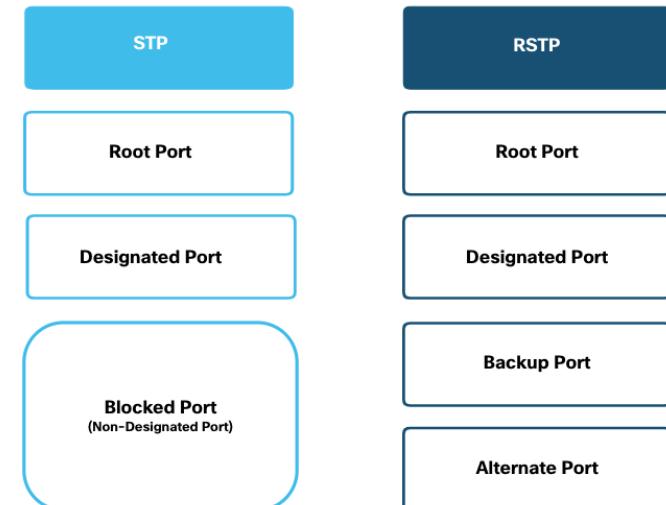
Estados del puerto RSTP y las funciones del puerto

Solo hay tres estados de puerto en RSTP que corresponden a los tres estados operativos posibles en STP.

Los estados de desactivación, bloqueo y escucha 802.1D se fusionan en un único estado de descarte 802.1w.

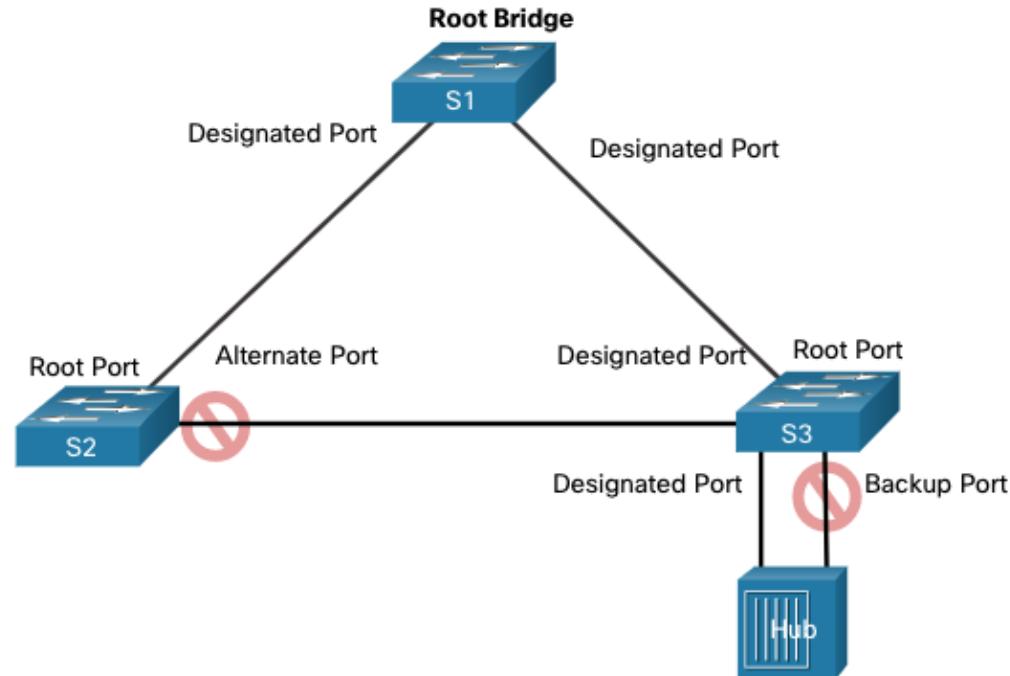


Los puertos raíz y los puertos designados son los mismos para STP y RSTP. Sin embargo, hay dos roles de puerto RSTP que corresponden al estado de bloqueo de STP. En STP, un puerto bloqueado se define como no ser el puerto designado o raíz. RSTP tiene dos funciones de puerto para este propósito.



Estados de puerto RSTP y las funciones de puerto (cont.)

El puerto alternativo tiene una ruta alternativa al puente raíz. El puerto de copia de seguridad es una copia de seguridad en un medio compartido, como un concentrador. Un puerto de copia de seguridad es menos común porque ahora los concentradores se consideran dispositivos heredados.



PortFast y BPDU Guard

- Cuando un dispositivo está conectado a un puerto del switch o cuando un switch se enciende, el puerto del switch pasa por los estados de escucha y aprendizaje, esperando cada vez que expire el temporizador de retardo de reenvío. Este retraso es de 15 segundos para cada estado durante un total de 30 segundos. Esto puede presentar un problema para los clientes DHCP que intentan detectar un servidor DHCP porque el proceso DHCP puede agotarse. El resultado es que un cliente IPv4 no recibirá una dirección IPv4 válida.
- Cuando un puerto de switch está configurado con PortFast, ese puerto pasa de un estado de bloqueo al de reenvío inmediatamente, evitando el retraso de 30 segundos. Puede utilizar PortFast en los puertos de acceso para permitir que los dispositivos conectados a estos puertos accedan a la red inmediatamente. PortFast sólo debe utilizarse en puertos de acceso. Si habilita PortFast en un puerto que se conecta a otro switch, corre el riesgo de crear un bucle de árbol de expansión.
- Un puerto de switch habilitado para PortFast nunca debería recibir BPDU porque eso indicaría que el switch está conectado al puerto, lo que podría causar un bucle de árbol de expansión. Los switch Cisco admiten una característica denominada “protección BPDU”. Cuando está habilitado, inmediatamente pone el puerto del switch en un estado errdisabled (error-disabled) al recibir cualquier BPDU. Esto protege contra posibles bucles al apagar eficazmente el puerto. El administrador debe volver a poner manualmente la interfaz en servicio.

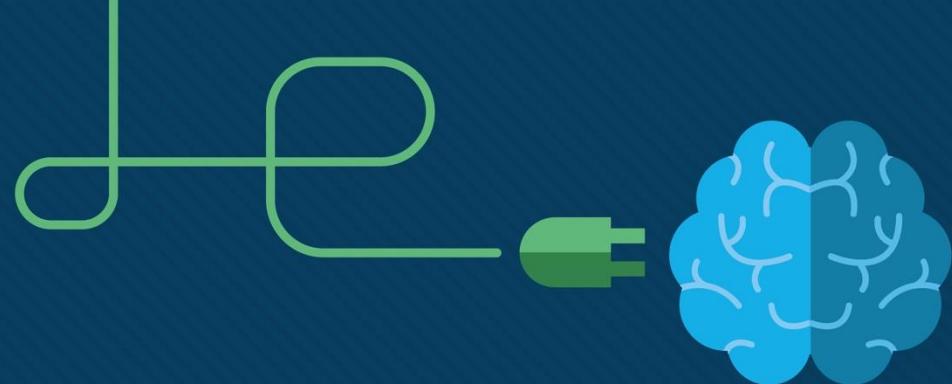
Alternativas a STP

- A lo largo de los años, las organizaciones requerían una mayor resiliencia y disponibilidad en la LAN. Las LAN Ethernet pasaron de unos pocos switch interconectados conectados a un único enrutador, a un sofisticado diseño de red jerárquica que incluía switch de acceso, distribución y capa central.
- Dependiendo de la implementación, la capa 2 puede incluir no solo la capa de acceso, sino también la distribución o incluso las capas principales. Estos diseños pueden incluir cientos de switch, con cientos o incluso miles de VLAN. STP se ha adaptado a la redundancia y complejidad añadida con mejoras, como parte de RSTP y MSTP.
- Un aspecto importante del diseño de red es la convergencia rápida y predecible cuando se produce un error o un cambio en la topología. El árbol de expansión no ofrece las mismas eficiencias y predictibilidades proporcionadas por los protocolos de enrutamiento en la Capa 3.
- El enrutamiento de capa 3 permite rutas y bucles redundantes en la topología, sin bloquear puertos. Por esta razón, algunos entornos están en transición a la capa 3 en todas partes, excepto donde los dispositivos se conectan al switch de capa de acceso. En otras palabras, las conexiones entre los switch de capa de acceso y los switch de distribución serían Capa 3 en lugar de Capa 2.

Nuevos términos y comandos

- Spanning Tree Protocol (STP)
- Spanning Tree Algorithm (STA)
- IEEE 802.1D
- IEEE 802.1w
- Broadcast Storm
- Root Bridge
- Root Port
- Designated Port
- Alternate (Blocked) Port
- Learning
- Listening
- Bridge ID (BID)
- Root ID
- Bridge Protocol Data Unit (BPDU)
- Bridge Priority
- Extended System ID
- short path cost
- long path cost
- root path cost
- Rapid STP (RSTP)
- port priority
- Hello timer
- Max Age timer
- Forward Delay timers
- Blocking
- Forwarding
- Discarding
- Per-VLAN Spanning Tree (PVST)
- PVST+
- Rapid PVST+
- Multiple Spanning Tree Protocol (MSTP)
- Multiple Spanning Tree (MST)
- PortFast
- BPDU Guard





Módulo 4: Inter-VLAN Routing

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



Objetivos del módulo

Título del módulo: Enrutamiento entre VLAN

Objetivo del módulo: Solucionar problemas sobre inter-VLAN routing en dispositivos capa 3

Título del tema	Objetivo del tema
Funcionamiento del routing entre redes VLAN	Describa las opciones para configurar el routing entre redes VLAN.
Routing entre VLAN con router-on-a-stick	Configurar el routing entre redes VLAN con un router-on-a-stick.
Inter-VLAN Routing usando switches de capa 3	Configurar el routing entre redes VLAN mediante switching de capa 3.
Resolución de problemas de routing entre VLAN	Solución de problemas comunes de configuración de inter-VLAN

4.1 Funcionamiento de Inter-VLAN Routing

Funcionamiento de Inter-VLAN Routing Operation

Qué es Inter-VLAN Routing?

Las VLAN se utilizan para segmentar las redes de switch de Capa 2 por diversas razones. Independientemente del motivo, los hosts de una VLAN no pueden comunicarse con los hosts de otra VLAN a menos que haya un router o un switch de capa 3 para proporcionar servicios de enrutamiento.

Inter-VLA routing es el proceso de reenviar el tráfico de red de una VLAN a otra VLAN.

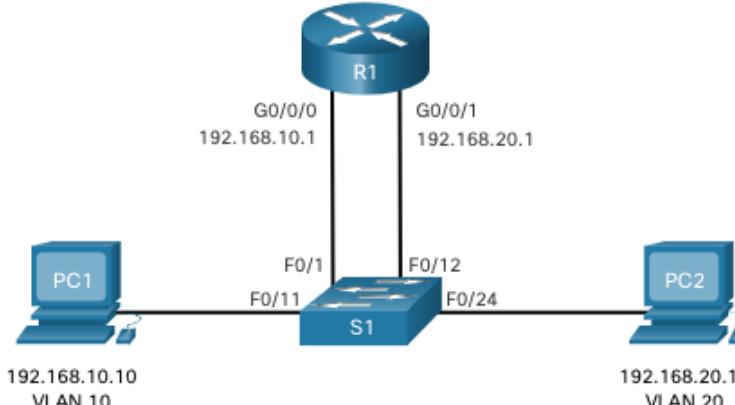
Hay tres opciones inter-VLAN routing:

- **Enrutamiento entre VLAN heredado** - Esta es una solución heredada. No escala bien
- **Router-on-a-stick** - Esta es una solución aceptable para una red pequeña y mediana.
- **Comutador de nivel 3 con interfaces virtuales comutadas (SVIs)** : Esta es la solución más escalable para organizaciones medianas y grandes.

Funcionamiento de Inter-VLAN Routing

Inter-VLAN Routing antiguo

- La primera solución de inter-VLAN routing se basó en el uso de un router con múltiples interfaces Ethernet. Cada interfaz del router estaba conectada a un puerto del switch en diferentes VLAN. Las interfaces del router sirven como default gateways para los hosts locales en la subred de la VLAN.
- Inter-VLAN routing heredado, usa las interfaces físicas funciona, pero tiene limitaciones significantes. No es razonablemente escalable porque los routers tienen un número limitado de interfaces físicas. Requerir una interfaz física del router por VLAN agota rápidamente la capacidad de la interfaz física del router
- **Nota:** Este método de inter-VLAN routing ya no se implementa en redes de switches y se incluye únicamente con fines explicativos.



Router-on-a-Stick Inter-VLAN Routing

El método ‘router-on-a-stick’ inter-VLAN routing supera la limitación del método de enruteamiento interVLAN heredado. Solo requiere una interfaz Ethernet física para enrutar el tráfico entre varias VLAN de una red.

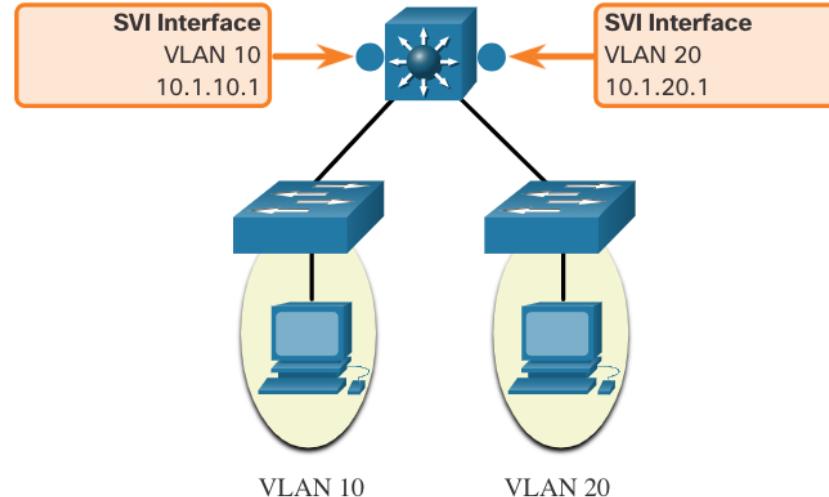
- Una interfaz Ethernet del router Cisco IOS se configura como un troncal 802.1Q y se conecta a un puerto troncal en un switch de capa 2. Específicamente, la interfaz del router se configura mediante subinterfaces para identificar VLAN enruteables.
- Las subinterfaces configuradas son interfaces virtuales basadas en software. Cada uno está asociado a una única interfaz Ethernet física. Estas subinterfaces se configuran en el software del router. Cada una se configura de forma independiente con sus propias direcciones IP y una asignación de VLAN. Las subinterfaces se configuran para subredes diferentes que corresponden a su asignación de VLAN. Esto facilita el enruteamiento lógico.
- Cuando el tráfico etiquetado de VLAN entra en la interfaz del router, se reenvía a la subinterfaz de VLAN. Después de tomar una decisión de enruteamiento basada en la dirección de red IP de destino, el router determina la interfaz de salida del tráfico. Si la interfaz de salida está configurada como una subinterfaz 802.1q, las tramas de datos se etiquetan VLAN con la nueva VLAN y se envían de vuelta a la interfaz física

Nota: el método de routing entre VLAN de router-on-a-stick no es escalable más allá de 50.

Inter-VLAN Routing en el Switch capa 3

El método moderno para realizar inter-VLAN routing es utilizar switches de capa 3 e interfaces virtuales del switch (SVI). Una SVI es una interfaz virtual configurada en un switch multicapa, como se muestra en la figura.

Nota: Un conmutador de capa 3 también se denomina conmutador multicapa ya que funciona en la capa 2 y la capa 3. Sin embargo, en este curso usamos el término Layer 3 switch.



Inter-VLAN Routing en el Switch capa 3 (Cont.)

Los SVIs entre VLAN se crean de la misma manera que se configura la interfaz de VLAN de administración. El SVI se crea para una VLAN que existe en el switch. Aunque es virtual, el SVI realiza las mismas funciones para la VLAN que lo haría una interfaz de router. Específicamente, proporciona el procesamiento de Capa 3 para los paquetes que se envían hacia o desde todos los puertos de switch asociados con esa VLAN.

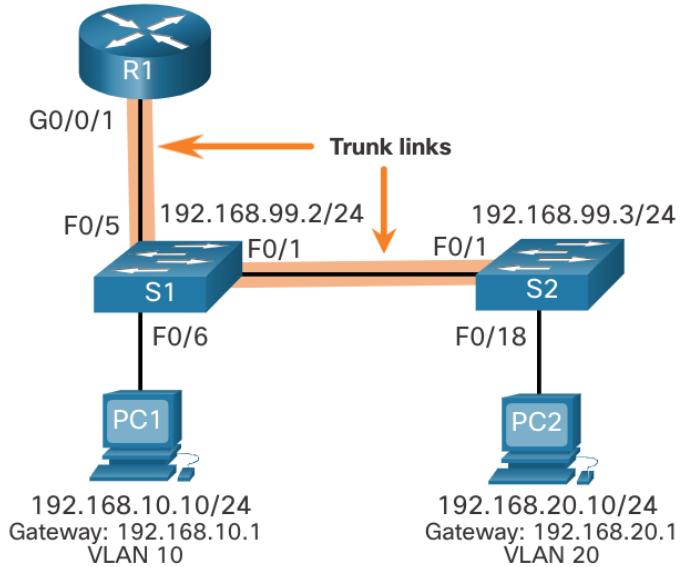
A continuación se presentan las ventajas del uso de switches de capa 3 para inter-VLAN routing:

- Es mucho más veloz que router-on-a-stick, porque todo el switching y el routing se realizan por hardware.
- El routing no requiere enlaces externos del switch al router.
- No se limitan a un enlace porque los EtherChannels de Capa 2 se pueden utilizar como enlaces troncal entre los switches para aumentar el ancho de banda.
- La latencia es mucho más baja, dado que los datos no necesitan salir del switch para ser enrutados a una red diferente.
- Se implementan con mayor frecuencia en una LAN de campus que en enrutadores.
- La única desventaja es que los switches de capa 3 son más caros.

4.2 Router-on-a-Stick Inter-VLAN Routing

Escenario de enrutamiento entre VLAN de Router-on-a-stickde Router-on-a-stick

- En la figura, la interfaz R1 GigabitEthernet 0/0/1 está conectada al puerto S1 FastEthernet 0/5. El puerto S1 FastEthernet 0/1 está conectado al puerto S2 FastEthernet 0/1. Estos son enlaces troncales necesarios para reenviar tráfico dentro de las VLAN y entre ellas.
- Para enrutar entre VLAN, la interfaz R1 GigabitEthernet 0/0/1 se divide lógicamente en tres subinterfaces, como se muestra en la tabla. La tabla también muestra las tres VLAN que se configurarán en los switches.
- Suponga que R1, S1 y S2 tienen configuraciones básicas iniciales. Actualmente, PC1 y PC2 no pueden **hacer ping** entre sí porque están en redes separadas. Solo S1 y S2 pueden **hacer ping** entre sí, pero son inalcanzables por PC1 o PC2 porque también están en diferentes redes.
- Para permitir que los dispositivos se hagan ping entre sí, los comutadores deben configurarse con VLAN y trunking, y el enrutador debe configurarse para el enrutamiento entre VLAN.



Subinterfaz	VLAN	Dirección IP
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

Configuración de conexión troncal y VLANS2 de enrutamiento entre VLAN y enrutamiento entre VLAN S2

La configuración para S2 es similar a S1.

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar  1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

Configuración de la subinterfaz R1 de Router-on-a-stick entre VLAN

Routing

Para el método de router-on-a-stick, se requieren subinterfaces configuradas para cada VLAN que se pueda enrutar. Se crea una subinterfaz mediante el comando **interface interface_id subinterface_id** global configuration mode. La sintaxis de la subinterfaz es la interfaz física seguida de un punto y un número de subinterfaz. Aunque no es obligatorio, es costumbre hacer coincidir el número de subinterfaz con el número de VLAN.

A continuación, cada subinterfaz se configura con los dos comandos siguientes:

- **encapsulation dot1q vlan_id [native]** - Este comando configura la subinterfaz para responder al tráfico encapsulado 802.1Q desde el *vlan-id* especificado. La opción de palabra clave **nativa** solo se agrega para establecer la VLAN nativa en algo distinto de la VLAN 1.
- **ip address ip-address subnet-mask** - Este comando configura la dirección IPv4 de la subinterfaz. Esta dirección normalmente sirve como default gateway para la VLAN identificada.

Repita el proceso para cada VLAN que se vaya a enrutar. Es necesario asignar una dirección IP a cada subinterfaz del router en una subred única para que se produzca el routing. Cuando se hayan creado todas las subinterfaces, habilite la interfaz física mediante el comando de configuración **no shutdown**. Si la interfaz física está deshabilitada, todas las subinterfaces están deshabilitadas.

Configuración de la subinterfaz R1 de Router-on-a-stick entre VLAN Routing (Cont.)

En la configuración, las subinterfaces R1 G0/0/1 se configuran para las VLAN 10, 20 y 99.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```



Verificar la Conectividad entre PC1 y PC2

La configuración del router-on-a-stick se completa después de configurar los enlaces troncales del switch y las subinterfaces del router. La configuración se puede verificar desde los hosts, el router y el switch.

Desde un host, compruebe la conectividad con un host de otra VLAN mediante el comando **ping**. Es una buena idea verificar primero la configuración IP del host actual mediante el comando **ipconfig** Windows host.

A continuación, utilice **ping** para verificar la conectividad con PC2 y S1, como se muestra en la figura. La salida de **ping** confirma correctamente que el enrutamiento entre VLAN está funcionando.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

Verificación de enrutamiento entre VLAN Router-on-a-stick entre VLAN Router-on-a-stick

Además de utilizar **ping** entre dispositivos, se pueden utilizar los siguientes comandos **show** para verificar y solucionar problemas de la configuración del router-on-a-stick.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

4.3 Inter-VLAN Routing using Layer 3 Switches

Enrutamiento entre VLAN del conmutador de capa 3

El inter-VLAN routing, mediante el método router-on-a-stick es fácil de implementar para una organización pequeña y mediana. Sin embargo, una gran empresa requiere un método más rápido y mucho más escalable para proporcionar inter-VLAN routing.

Las LAN de campus empresariales utilizan switches de capa 3 para proporcionar enrutamiento entre VLAN. Los switches de capa 3 utilizan switching basado en hardware para lograr velocidades de procesamiento de paquetes más altas que los routers. Los switches de capa 3 también se implementan comúnmente en armarios de cableado de capa de distribución empresarial.

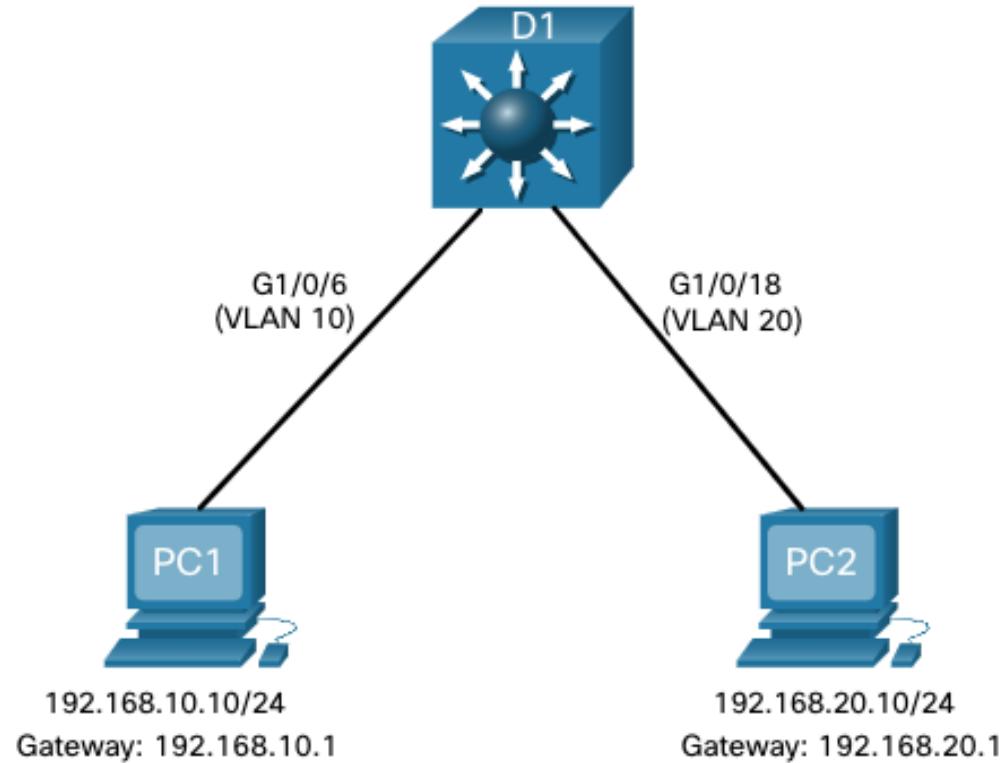
Las capacidades de un switch de capa 3 incluyen la capacidad de hacer lo siguiente:

- Ruta de una VLAN a otra mediante múltiples interfaces virtuales conmutadas (SVIs).
- Convierta un puerto de conmutación de capa 2 en una interfaz de capa 3 (es decir, un puerto enrutado). Un puerto enrutado es similar a una interfaz física en un router Cisco IOS.
- Para proporcionar enrutamiento entre VLAN, los switches de capa 3 utilizan SVIs. Los SVIs se configuran utilizando el mismo comando **interface vlan vlan-id** utilizado para crear el SVI de administración en un conmutador de capa 2. Se debe crear un SVI de Capa 3 para cada una de las VLAN enrutables.

Enrutamiento entre VLAN mediante comutadores de capa 3

Escenario de comutador de capa 3

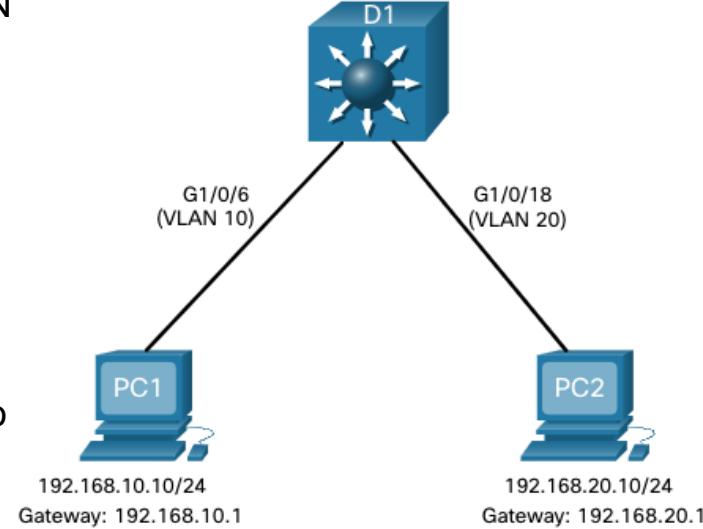
En la figura, el switch de capa 3, D1, está conectado a dos hosts en diferentes VLAN. PC1 está en VLAN 10 y PC2 está en VLAN 20, como se muestra. El switch de capa 3 proporcionará servicios inter-VLAN routing a los dos hosts.



Enrutamiento entre VLAN mediante Conmutadores de Capa 3 **Configuración de Conmutadores de Capa 3**

Complete los siguientes pasos para configurar S1 con VLAN y trunking :

- **Paso 1.** Cree las VLAN. En el ejemplo, se utilizan VLAN 10 y 20.
- **Paso 2.** Cree las interfaces VLAN SVI. La dirección IP configurada servirá como puerta de enlace predeterminada para los hosts de la VLAN respectiva.
- **Paso 3.** Configure puertos de acceso. Asigne el puerto apropiado a la VLAN requerida.
- **Paso 4.** Habilitar routing IP. Ejecute el comando **ip routing** global configuration para permitir el intercambio de tráfico entre las VLAN 10 y 20. Este comando debe configurarse para habilitar el enrutamiento inter-VAN en un conmutador de capa 3 para IPv4.



Verificación de enrutamiento entre VLAN del switch de nivel 3

El Inter-VLAN Routing mediante un switch de capa 3 es más sencillo de configurar que el método router-on-a-stick. Una vez completada la configuración, la configuración se puede verificar probando la conectividad entre los hosts.

- Desde un host, compruebe la conectividad con un host de otra VLAN mediante el comando **ping**. Es una buena idea verificar primero la configuración IP del host actual mediante el comando **ipconfig** Windows host.
- A continuación, verifique la conectividad con PC2 mediante el comando **ping** de host de Windows. La salida **de ping** correcta confirma que el enrutamiento entre VLAN está funcionando.

Enrutamiento en un conmutador de capa 3

Si se quiere que otros dispositivos de Capa 3 puedan acceder a las VLAN, deben anunciarse mediante enrutamiento estático o dinámico. Para habilitar el enrutamiento en un switch de capa 3, se debe configurar un puerto enrutado.

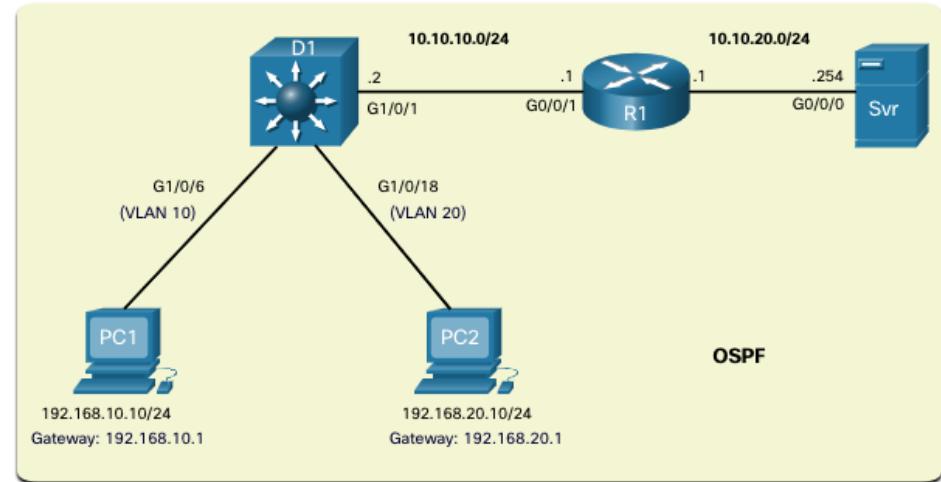
Un puerto enrutado se crea en un switch de Capa 3 deshabilitando la función `switchport` de un switch de Capa 2 que está conectado a otro dispositivo de Capa 3.

Específicamente, al configurar el comando de configuración de **no switchport** en un puerto de Capa 2, se convierte en una interfaz de Capa 3. A continuación, la interfaz se puede configurar con una configuración IPv4 para conectarse a un enrutador u otro conmutador de capa 3.

Escenario de enrutamiento en un commutador de capa 3

En la figura, el switch de capa 3 D1 previamente configurado ahora está conectado a R1. R1 y D1 están ambos en un dominio de protocolo de enrutamiento Open Shortest Path First (OSPF). Supongamos que Inter-VLAN se ha implementado correctamente en D1. La interfaz G0/0/1 de R1 también ha sido configurada y habilitada. Además, R1 está utilizando OSPF para anunciar sus dos redes, 10.10.10.0/24 y 10.20.20.0/24.

Nota: La configuración de ruteo OSPF está cubierta en otro curso. En este módulo, se le darán comandos de configuración OSPF en todas las actividades y evaluaciones. No es necesario que comprenda la configuración para habilitar el enrutamiento OSPF en el commutador de capa 3.



Configuración de enrutamiento de switches de capa 3

Complete los siguientes pasos para configurar D1 para enrutar con R1:

- **Paso 1.** Configurar el puerto enrutado. Utilice el **comando no switchport** para convertir el puerto en un puerto enrutado y, a continuación, asigne una dirección IP y una máscara de subred. Habilite el puerto.
- **Paso 2.** Activar el routing. Use el comando de modo de configuración global **ip routing** para habilitar el routing
- **Paso 3.** Configurar el enrutamiento Utilice un método de enrutamiento adecuado. En este ejemplo, se configura **OSPFv2 de área única**
- **Paso 4.** Verificar enrutamiento. Use el comando **show ip route** .
- **Paso 5.** Verificar la conectividad Use el comando **ping** para verificar la conectividad.

4.4 - Resolución de problemas Inter-VLAN Routing

Solucionar problemas comunes de enrutamiento entre VLAN

Hay varias razones por las que una configuración entre VLANs puede no funcionar. Todos están relacionados con problemas de conectividad. En primer lugar, compruebe la capa física para resolver cualquier problema en el que un cable pueda estar conectado al puerto incorrecto. Si las conexiones son correctas, utilice la lista de la tabla para otras razones comunes por las que puede fallar la conectividad entre VLAN.

Tipo de problema	Cómo arreglar	Cómo verificar
VLAN faltantes	<ul style="list-style-type: none">Cree (o vuelva a crear) la VLAN si no existe.Asegúrese de que el puerto host está asignado a la VLAN correcta.	show vlan [brief] show interfaces switchport ping
Problemas con el puerto troncal del switch	<ul style="list-style-type: none">Asegúrese de que los enlaces troncales estén configurados correctamente.Asegúrese de que el puerto es un puerto troncal y está habilitado.	show interface trunk show running-config
Problemas en los puertos de acceso de switch	<ul style="list-style-type: none">Asigne el puerto a la VLAN correcta.Asegúrese de que el puerto es un puerto de acceso y está habilitado.El host está configurado incorrectamente en la subred incorrecta.	show interfaces switchport show running-config interface ipconfig
Temas de configuración del router	<ul style="list-style-type: none">La dirección IPv4 de la subinterfaz del router está configurada incorrectamente.La subinterfaz del router se asigna al ID de VLAN.	show ip interface brief show interfaces

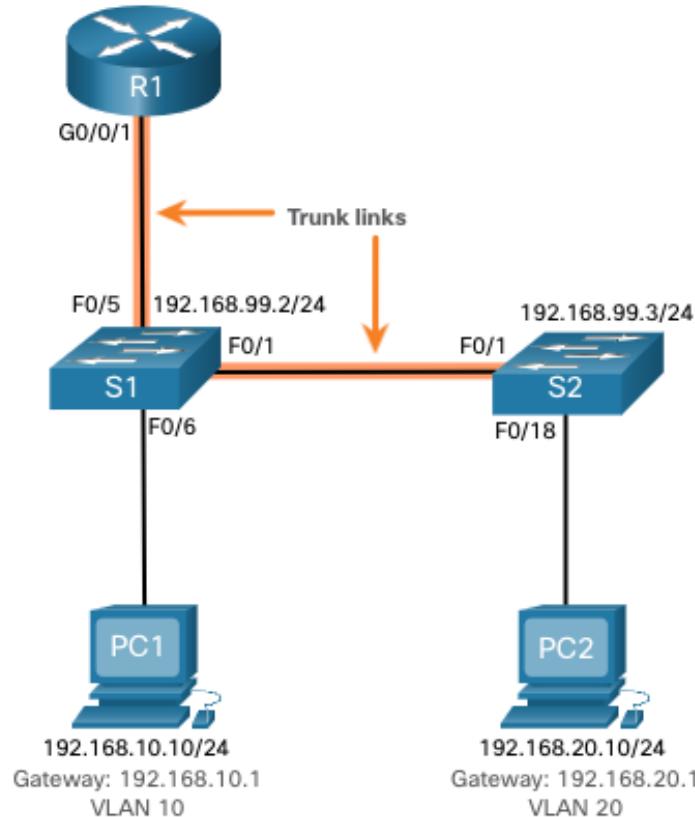
Solucionar problemas de enrutamiento entre VLAN

Solucionar problemas de escenario de enrutamiento entre VLAN

Los ejemplos de algunos de estos problemas de Inter-VLAN Routing ahora se tratarán con más detalle. Esta topología se utilizará para todos estos problemas.

Subinterfaces R1 del router

Subinterfaz	VLAN	Dirección IP
G0/0/0.10	10	192.168.10.1/24
G0/0/0.20	20	192.168.20.1/24
G0/0/0.30	99	192.168.99.1/24



Resolución de problemas de Inter-VLAN Routing VLAN faltantes

Un problema de conectividad entre VLAN podría deberse a la falta de una VLAN. La VLAN podría faltar si no se creó, se eliminó accidentalmente o no se permite en el enlace troncal.

Cuando se elimina una VLAN, cualquier puerto asignado a esa VLAN queda inactivo. Permanecen asociados con la VLAN (y, por lo tanto, inactivos) hasta que los asigne a una nueva VLAN o vuelva a crear la VLAN que falta. Si se vuelve a crear la VLAN que falta, se reasignarán automáticamente los hosts a ella.

Utilice el comando **show interface***interface-id***switchport** para verificar la membresía de VLAN del puerto.

CISCO

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

Puerto troncal del switch

Otro problema para el enrutamiento entre VLAN incluye puertos de switch mal configurados. En una solución interVLAN heredada, esto podría deberse a que el puerto del router de conexión no está asignado a la VLAN correcta.

Sin embargo, con una solución router-on-a-stick, la causa más común es un puerto troncal mal configurado.

- Compruebe que el puerto que se conecta al enrutador esté configurado correctamente como enlace troncal mediante el comando **show interface trunk** .
- Si falta ese puerto en la salida, examine la configuración del puerto con el comando **show running-config interface X** para ver cómo está configurado el puerto.

```
S1# show interface trunk
  Port      Mode          Encapsulation  Status        Native vlan
  Fa0/1     on            802.1q         trunking      1
  Port      Vlans allowed on trunk
  Fa0/1     1-4094
  Port      Vlans allowed and active in management domain
  Fa0/1     1,10,20,99
  Port      Vlans in spanning tree forwarding state and not pruned
  Fa0/1     1,10,20,99
S1#
```

Puerto de acceso del switch

Cuando sospeche que hay un problema con una configuración del switch, utilice los distintos comandos de verificación para examinar la configuración e identificar el problema.

Un indicador común de este problema es el equipo que tiene la configuración de dirección correcta (dirección IP, máscara de subred, puerta de enlace predeterminada), pero no puede hacer ping a su puerta de enlace predeterminada.

- Utilice el comando **show vlan brief**, **show interface X switchport** o **show running-config interface X** para verificar la asignación de interfaz VLAN.

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Problemas de configuración del Router

Los problemas de configuración del router-on-a-stick suelen estar relacionados con configuraciones incorrectas de la subinterfaz.

- Puede verificar el estado de los puertos del switch emitiendo el comando **show ip interface brief**.
- Compruebe en qué VLAN se encuentra cada una de las subinterfaces. Para ello, el comando **show interfaces** es útil, pero genera una gran cantidad de resultados adicionales no requeridos. La salida del comando se puede reducir utilizando filtros de comando IOS. En este ejemplo, utilice la palabra clave **include** para identificar que sólo las líneas que contienen las letras «Gig» o «802.1Q»

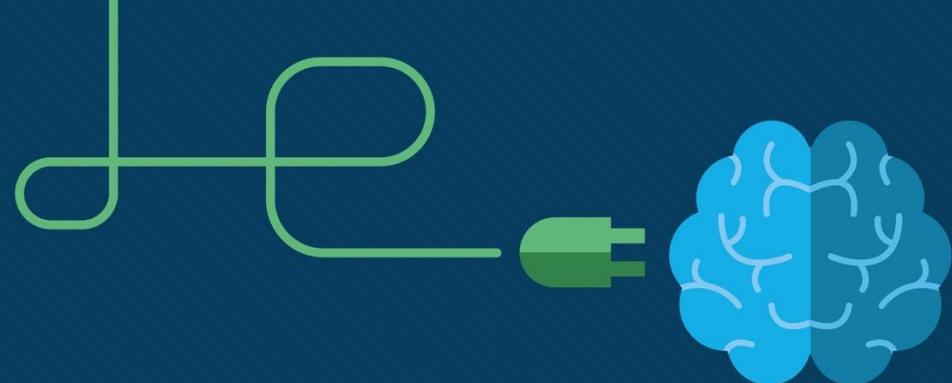
```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

Módulo 4:

Nuevos términos y comandos de configuración básica del dispositivo

- Enrutamiento entre VLAN
- Router-on-a-stick
- **encapsulation dot1q X [native]**
- **El comando no switchport**
- **router ospf**
- **ip routing**





Módulo 3: VLAN

Comunicación, enrutamiento y
Wireless Essentials v7.0
(SRWE)



Objetivos del módulo

Título del módulo: Protocolos y modelos

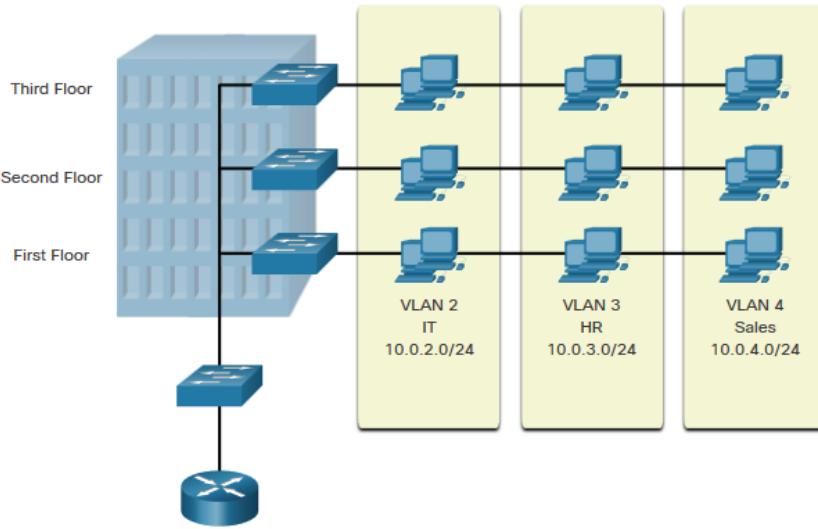
Objetivo del módulo: Explicar cómo los protocolos de red permiten que los dispositivos accedan a recursos de red locales y remotos.

Título del tema	Objetivo del tema
Descripción general de las VLAN	Explique la finalidad de las VLAN en una red conmutada.
Redes VLAN en un entorno conmutado múltiple	Explique cómo un switch reenvía tramas según la configuración de VLAN en un entorno conmutado múltiple.
Configuración de VLAN	Configure un puerto para switch que se asignará a una VLAN según los requisitos.
Enlaces troncales de la VLAN	Configure un puerto de enlace troncal en un switch LAN.
Protocolo de enlace troncal dinámico	Configure el protocolo de enlace troncal dinámico (DTP).

3.1 Descripción general de las VLAN

Descripción general de las VLAN

Definiciones de VLAN



Las VLAN son conexiones lógicas con otros dispositivos similares.

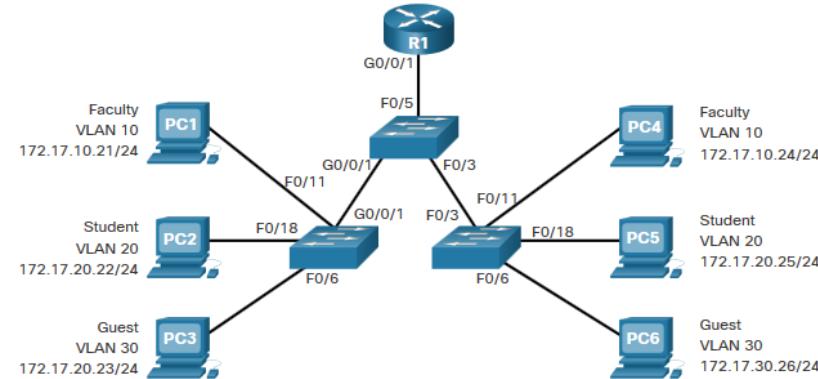
La colocación de dispositivos en varias VLAN tienen las siguientes características:

- Proporciona segmentación de los diversos grupos de dispositivos en los mismos switches
- Proporciona una organización más manejable
 - Difusiones, multidifusión y unidifusión se aíslan en la VLAN individual
 - Cada VLAN tendrá su propia gama única de direcciones IP
 - Dominios de difusión más pequeños

Descripción general de las VLAN

Beneficios de un diseño de VLAN

Los beneficios de usar VLAN son los siguientes:



Beneficios	Descripción
Dominios de difusión más pequeños	Dividir la LAN reduce el número de dominios de difusión
Seguridad mejorada	Solo los usuarios de la misma VLAN pueden comunicarse juntos
Eficiencia de TI mejorada	Las VLAN pueden agrupar dispositivos con requisitos similares, por ejemplo, profesores frente a estudiantes
Reducción de costos	Un switch puede admitir varios grupos o VLAN
Mejor rendimiento	Pequeños dominios de difusión reducen el tráfico y mejoran el ancho de banda
Gestión Simple	Grupos similares necesitarán aplicaciones similares y otros recursos de red

Descripción general de las VLAN

Tipos de VLAN

VLAN predeterminada – VLAN 1

- La VLAN predeterminada
- La VLAN nativa predeterminada
- La VLAN de administración predeterminada
- No se puede eliminar ni cambiar el nombre

Switch# 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
1002	fdci-default		act/unsup
1003	token-ring-default		act/unsup
1004	fddinet-default		act/unsup
1005	trnet-default		act/unsup

Nota: Aunque no podemos eliminar VLAN1, Cisco recomendará que asignemos estas características predeterminadas a otras VLAN

Tipos de VLAN (Cont.)

VLAN de datos

- Dedicado al tráfico generado por el usuario (correo electrónico y tráfico web).
- VLAN 1 es la VLAN de datos predeterminada porque todas las interfaces están asignadas a esta VLAN.

VLAN nativa

- Esto se utiliza sólo para enlaces troncales.
- Todas las tramas están etiquetadas en un enlace troncal 802.1Q excepto las de la VLAN nativa.

VLAN de administración

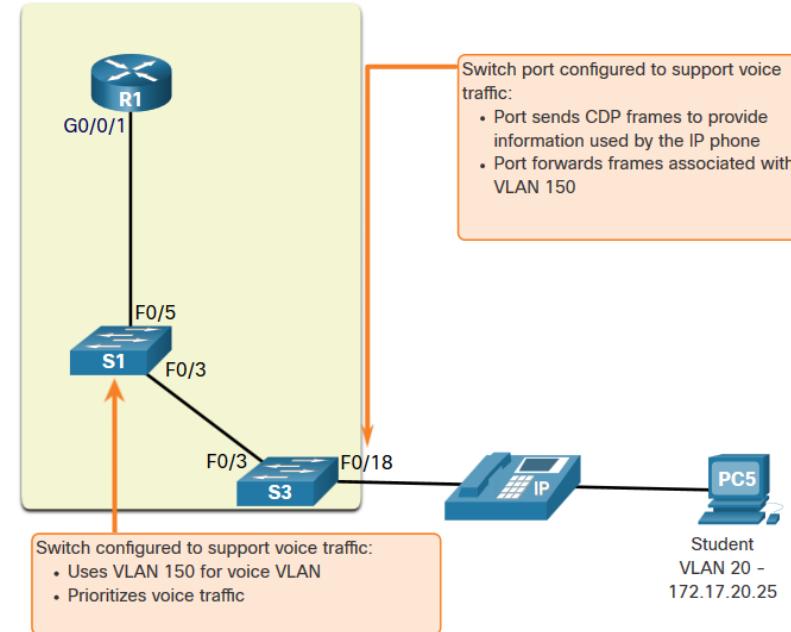
- Esto se utiliza para el tráfico SSH/Telnet VTY y no debe ser llevado con el tráfico de usuario final.
- Normalmente, la VLAN que es el SVI para el switch de capa 2.

Descripción general de las VLAN

Tipos de VLAN (Cont.)

VLAN de voz

- Se requiere una VLAN separada porque el tráfico de voz requiere:
 - Ancho de banda asegurado
 - Alta prioridad de QoS
 - Capacidad para evitar la congestión
 - Retraso menos de 150 ms desde el origen hasta el destino
- Toda la red debe estar diseñada para admitir la voz.



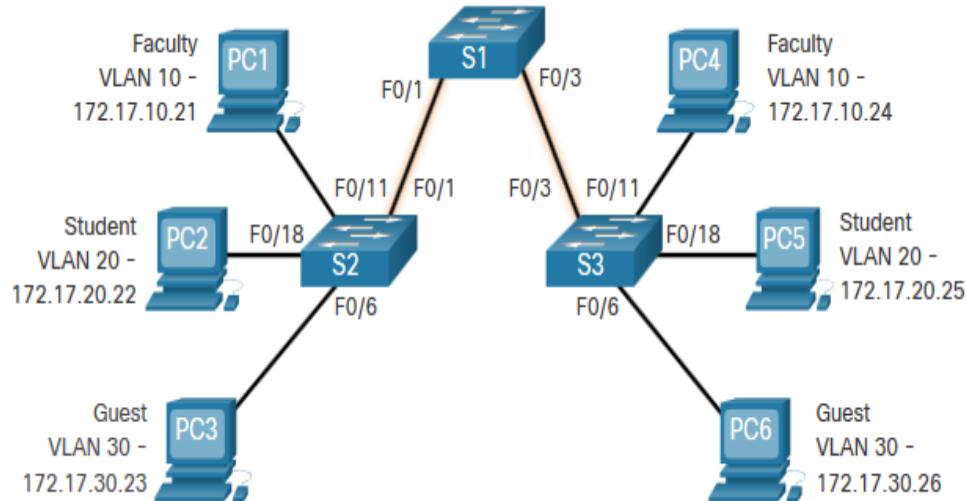
3.2 VLAN en un entorno de comunicación múltiple

Definición de troncales de VLAN

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red.

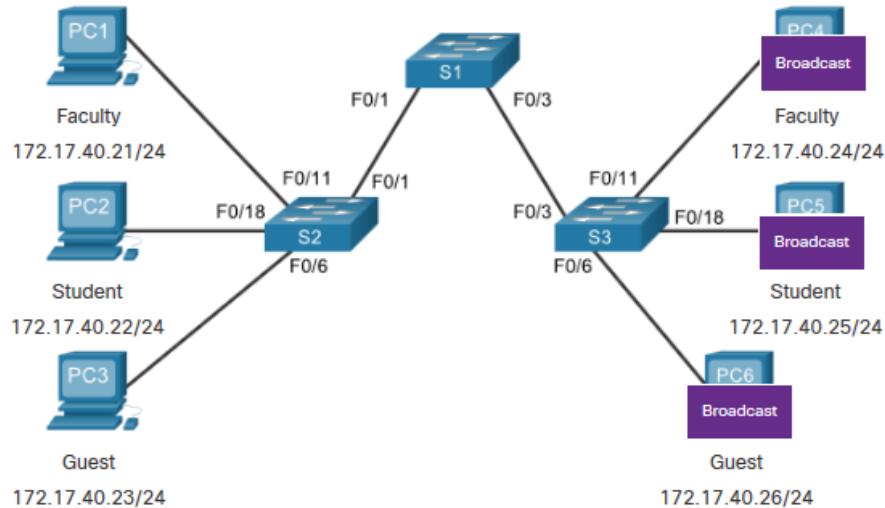
Funciones troncales de Cisco:

- Permitir más de una VLAN
- Extender la VLAN a través de toda la red
- De forma predeterminada, admite todas las VLAN
- Soporta enlace troncal 802.1Q



Redes sin VLAN

Sin VLAN, todos los dispositivos conectados a los switches recibirán todo el tráfico de unidifusión, multidifusión y difusión.

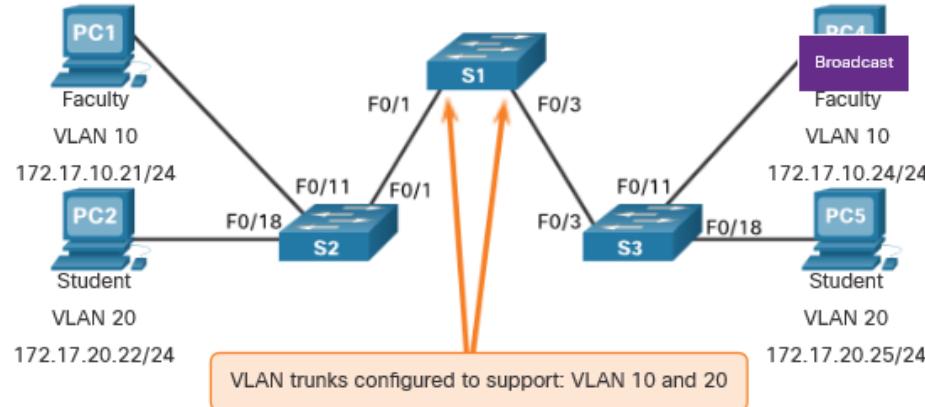


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

VLAN en un entorno de commutación múltiple

Redes con VLAN

Con las VLAN, el tráfico de unidifusión, multidifusión y difusión se limita a una VLAN. Sin un dispositivo de capa 3 para conectar las VLAN, los dispositivos de diferentes VLAN no pueden comunicarse.

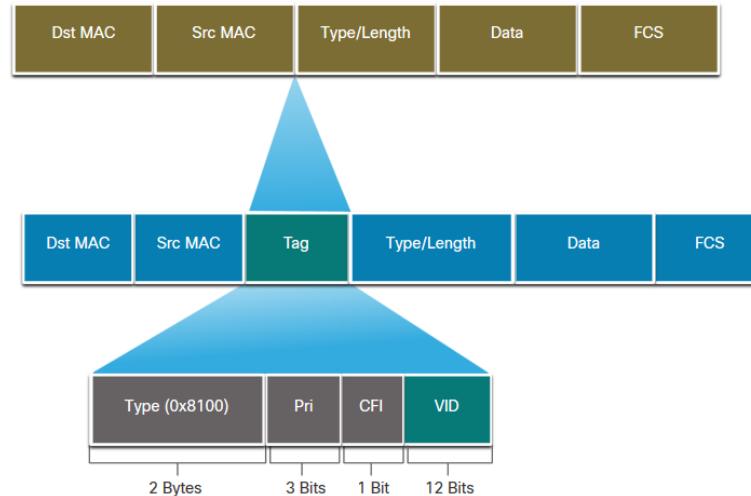


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

VLAN en un Entorno de Comutación Múltiple

Identificación de VLAN con una etiqueta

- El encabezado IEEE 802.1Q es de 4 Bytes
- Cuando se crea la etiqueta, se debe volver a calcular el FCS.
- Cuando se envía a los dispositivos finales, esta etiqueta debe eliminarse y el FCS vuelve a calcular su número original.

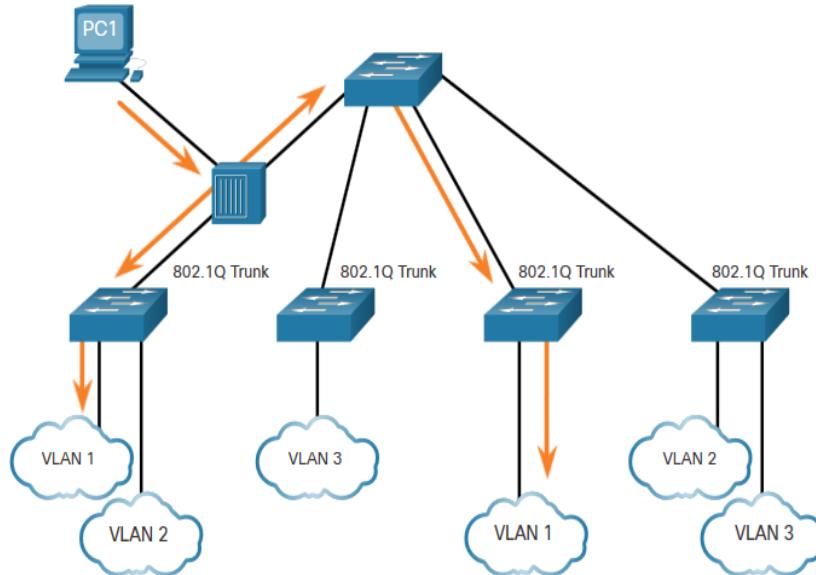


Campo de etiqueta VLAN 802.1Q	Función
Tipo	<ul style="list-style-type: none">• Campo de 2 bytes con hexadecimal 0x8100• Esto se conoce como ID de Protocolo de Etiqueta (TPID)
Prioridad de usuario	<ul style="list-style-type: none">• Valor de 3 bits que admite
Identificador de formato canónico (CFI)	<ul style="list-style-type: none">• Valor de 1 bit que puede admitir tramas de Token Ring en Ethernet
VLAN ID (VID)	<ul style="list-style-type: none">• Identificador de VLAN de 12 bits que puede admitir hasta 4096 VLAN

VLAN nativas y etiquetado 802.1Q

Conceptos básicos de 802.1Q:

- El etiquetado se realiza normalmente en todas las VLAN.
- El uso de una VLAN nativa se diseñó para uso heredado, como el Switch en el ejemplo.
- A menos que se modifique, VLAN1 es la VLAN nativa.
- Ambos extremos de un enlace troncal deben configurarse con la misma VLAN nativa.
- Cada troncal se configura por separado, por lo que es posible tener una VLAN nativa diferente en troncales separados.

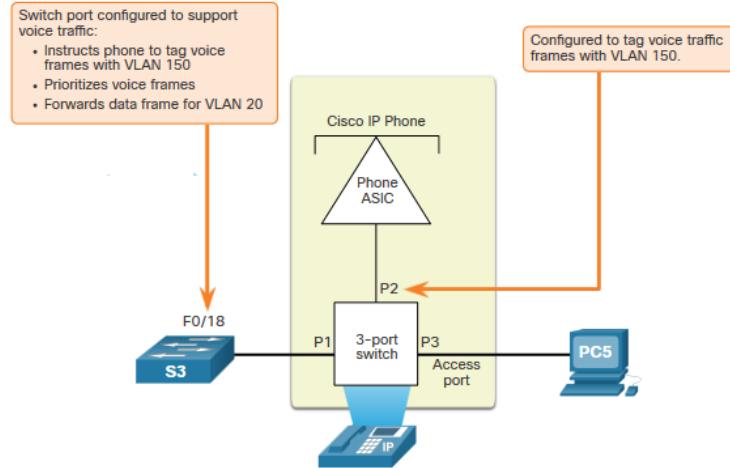


Etiquetado de VLAN de voz

El teléfono VoIP es un switch de tres puertos:

- El switch utilizará CDP para informar al teléfono de la VLAN de voz.
- El teléfono etiquetará su propio tráfico (Voz) y puede establecer el coste de servicio (CoS). CoS es QoS para la capa 2.
- El teléfono puede o no etiquetar tramas de la PC.

Tráfico	Función de etiquetado
VLAN de voz	etiquetado con un valor de prioridad de clase de servicio (CoS) de capa 2 apropiado
VLAN de acceso	también se puede etiquetar con un valor de prioridad CoS de capa 2
VLAN de acceso	no está etiquetado (sin valor de prioridad CoS de capa 2)



Ejemplo de verificación de VLAN de voz

El comando **show interfaces fa0/18 switchport** puede mostrarnos las VLAN de datos y voz asignadas a la interfaz.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

3.3 Configuración de VLAN

Configuración de VLAN

Rangos de VLAN en Catalyst

Los switches Catalyst 2960 y 3650 admiten más de 4000 VLAN.

- Rango normal VLAN 1-1005, utilizado en pequeñas y medianas empresas. Se guardan en `vlan.dat` en flash.
- Rango extendido VLAN 1006-4094, usado por los proveedores de servicios. Menos opciones que las VLAN de rango normal. Se guardan en `running-config`. No admite VTP

```
Switch# 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
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdninet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN ID	Tipo	Uso
0 y 4095	Reservado	Para uso exclusivo del sistema.
1	Utilizable	VLAN nativa por defecto para todos los puertos. Se crea automáticamente y no puede ser modificada o eliminada.
2 – 1001	Utilizable	Rango de uso general. Pueden ser creadas, modificadas o eliminadas.
1002 - 1005	Utilizable	Están reservados para VLAN heredadas. VLANs por defecto en dispositivos para FDDI y Token Ring. Se crean automáticamente y no pueden ser eliminadas.

Comandos de creación de VLAN

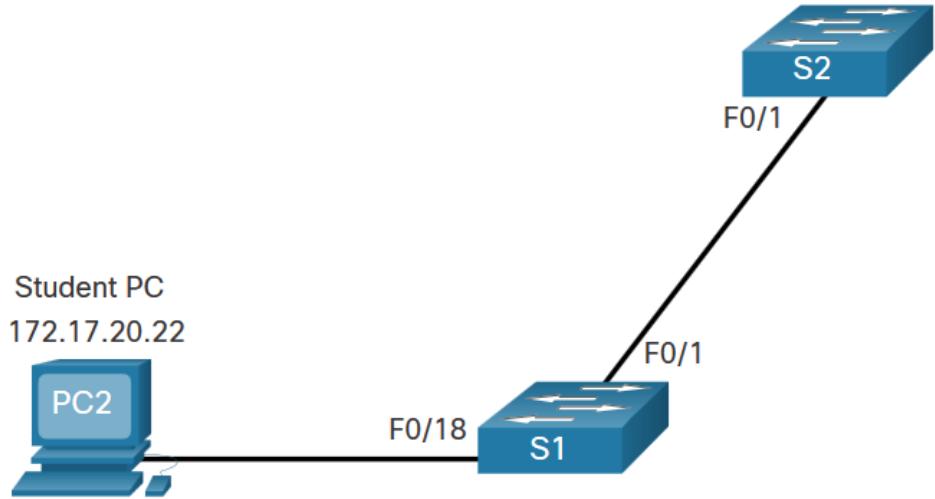
Los detalles de la VLAN se almacenan en el archivo `vlan.dat`. Crea VLAN en el modo de configuración global.

Tarea	Comando de IOS
Ingresar al modo de configuración global.	Switch# configure terminal
Crear una VLAN con un número de identificación válido.	Switch(config)# vlan vlan-id
Especificar un nombre único para identificar la VLAN.	Switch(config-vlan)# name vlan-name
Volver al modo EXEC con privilegios.	Switch (config-vlan) # end

Configuración de VLAN

Ejemplo de creación de VLAN

- Si el Student PC va a estar en VLAN 20, primero crearemos la VLAN y luego la nombraremos.
- Si no lo nombra, Cisco IOS le dará un nombre predeterminado de `vlan` y el número de cuatro dígitos de la VLAN. Por ejemplo, `vlan0020` para VLAN 20.



Indicador	Comando
S1#	configure terminal
S1(config)#	vlan 20
S1(config-vlan)#	name student
S1(config-vlan)#	end

Comandos de asignación de puertos de VLAN

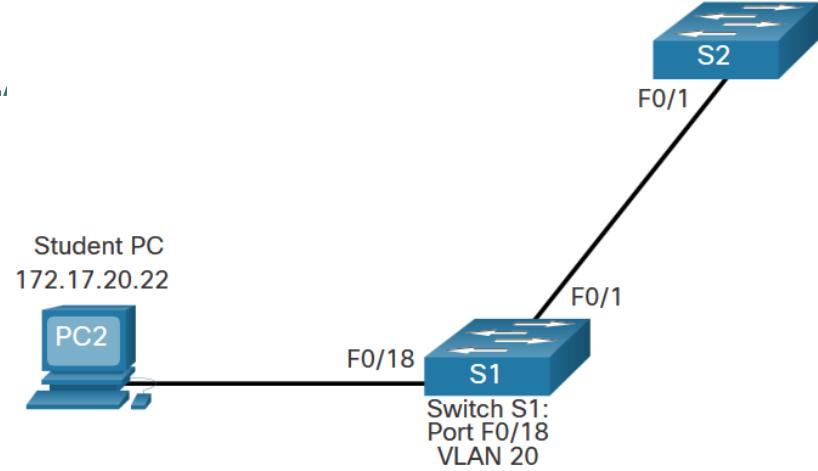
Una vez creada la VLAN, podemos asignarla a las interfaces correctas.

Tarea	Comando
Ingresar al modo de configuración global.	Switch# configure terminal
Ingresa al modo de configuración de interfaz.	Switch(config)# interface interface-id
Establezca el puerto en modo de acceso.	Switch(config-if)# switchport mode access
Asigna el puerto a una VLAN.	Switch(config-if)# switchport access vlan vlan-id
Vuelve al modo EXEC con privilegios.	Switch(config-if)# end

Ejemplo de asignación de puerto VL.

Podemos asignar la VLAN a la interfaz del puerto.

- Una vez que el dispositivo se asigna la VLAN, el dispositivo final necesitará la información de dirección IP para esa VLAN
- Aquí, Student PC recibe 172.17.20.22

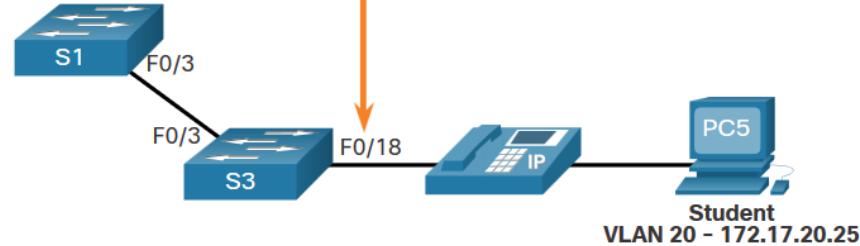


Indicador	Comando
S1#	configure terminal
S1(config)#	interface fa0/18
S1(config-if)#	switchport mode Access
S1(config-if)#	switchport access vlan 20
S1(config-if)#	end

Datos de configuración de VLAN y VLAN de voz

Un puerto de acceso solo se puede asignar a una VLAN de datos. Sin embargo, también se puede asignar a una VLAN de voz para cuando un teléfono y un dispositivo final estén fuera del mismo puerto de commutación.

Switchport must support VLAN traffic for:
• Voice traffic to the IP phone
• Data traffic to PC5



Ejemplo de VLAN de voz y datos

- Queremos crear y nombrar VLAN de voz y datos.
- Además de asignar la VLAN de datos, también asignaremos la VLAN de voz y activaremos QoS para el tráfico de voz a la interfaz.
- El switch Catalyst más reciente creará automáticamente la VLAN, si aún no existe, cuando se asigne a una interfaz.

Nota: QoS está más allá del alcance de este curso. Aquí mostramos el uso del comando mls qos trust [cos | device cisco-phone | dscp | ip-precedence].

```
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# vlan 150
S1(config-vlan)# name VOICE
S1(config-vlan)# exit
S1(config)# interface fa0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# mls qos trust cos
S1(config-if)# switchport voice vlan 150
S1(config-if)# end
```

```
% Access VLAN does not exist. Creating vlan 30
```

Configuración de VLAN

Verifique la información de VLAN

Use el comando **show vlan** . La sintaxis completa es:

show vlan [brief | id *vlan-id* | name *vlan-name* | summary]

```
S1# show vlan summary
Number of existing VLANs : 7
Number of existing VTP VLANs : 7
Number of existing extended VLANs : 0
```

```
S1# show interface vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001f.6ddb.3ec1 (bia 001f.6ddb.3ec1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

(Output omitted)
```

Tarea	Opción de comando
Muestra el nombre de VLAN, el estado y sus puertos una VLAN por linea.	brief
Muestra información sobre el número de ID de VLAN identificado.	id <i>vlan-id</i>
Muestra información sobre el número de ID de VLAN identificado. El <i>nombre de vlan</i> es una cadena ASCII de 1 a 32 caracteres.	name <i>vlan-name</i>
Muestra el resumen de información de la VLAN.	resume

Configuración de VLAN

Cambiar pertenencia al puerto VLAN

Hay varias formas de cambiar la membresía de VLAN:

- vuelva a ingresar el comando **switchport access vlan *vlan-id***
- use **no switchport access vlan** para volver a colocar la interfaz en la VLAN 1

Utilice los comandos **show vlan brief** o **show interface fa0/18 switchport** para verificar la asociación correcta de VLAN.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
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
1002 fddi-default    act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default   act/unsup
```

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Eliminar VLAN

Elimine las VLAN con el comando **no vlan *vlan-id***.

Precaución: antes de eliminar una VLAN, reasigne todos los puertos miembros a una VLAN diferente..

- Elimine todas las VLAN con los comandos **delete flash:vlan.dat** o **delete vlan.dat** .
- Vuelva a cargar el switch al eliminar todas las VLAN.

Nota: Para restaurar el valor predeterminado de fábrica, desconecte todos los cables de datos, borre la configuración de inicio y elimine el archivo *vlan.dat* y, a continuación, vuelva a cargar el dispositivo.

3.4 Troncales VLAN

Comandos de configuración troncal

Configure y verifique las troncales VLAN. Los troncales son capa 2 y transportan tráfico para todas las VLAN.

Tarea	Comando de IOS
Ingresar al modo de configuración global.	Switch# configure terminal
Ingresa al modo de configuración de interfaz.	Switch(config)# interface interface-id
Establece el puerto en modo de enlace permanente.	Switch(config-if)# switchport mode trunk
Cambia la configuración de la VLAN nativa a otra opción que no sea VLAN 1.	Switch(config-if)# switchport trunk native vlan vlan-id
Especifica la lista de VLAN que se permitirán en el enlace troncal.	Switch(config-if)# switchport trunk allowed vlan vlan-list
Vuelve al modo EXEC con privilegios.	Switch(config-if)# end

Troncales VLAN

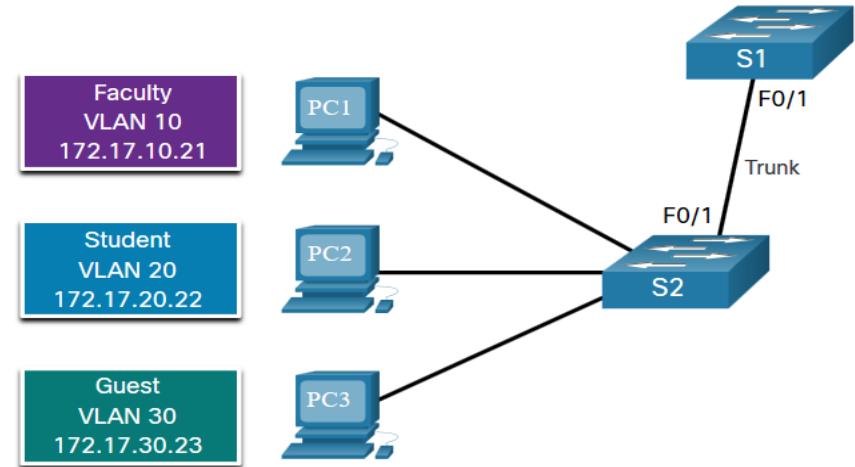
Ejemplo de configuración

Las subredes asociadas a cada VLAN son:

- VLAN 10 - Faculty/Staff - 172.17.10.0/24
- VLAN 20 - Students - 172.17.20.0/24
- VLAN 30 - Guests - 172.17.30.0/24
- VLAN 99 - Native - 172.17.99.0/24

El puerto F0/1 en S1 está configurado como un puerto troncal.

Nota: Se asume un switch 2960 que utiliza el etiquetado 802.1q. Los switches de capa 3 requieren que la encapsulación se configure antes del modo troncal.



Indicador	Comando
S1(config)#	interface fa0/1
S1(config-if)#	switchport mode trunk
S1(config-if)#	switchport trunk native vlan 99
S1(config-if)#	switchport trunk allowed vlan 10,20,30,99
S1(config-if)#	end

Verifique la configuración de troncales

- Establezca el modo troncal y la VLAN nativa.
- Observe el comando **sh int fa0/1 switchport** :
 - Se establece en troncal administrativamente
 - Se establece como troncal operacionalmente (en funcionamiento)
 - La encapsulación es dot1q.
 - VLAN nativa establecida en VLAN 99.
 - Todas las VLAN creadas en el switch pasarán tráfico en este troncal.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Restablezca el troncal al estado predeterminado

- Restablezca la configuración predeterminada del troncal con el comando no.
 - Todas las VLAN permitidas para pasar tráfico
 - VLAN nativa = VLAN 1
 - Verifique la configuración predeterminada.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Restablezca el troncal al estado predeterminado (Cont.)

Restablezca el troncal a modo de acceso con el comando **switchport mode access** :

- Se establece en una interfaz de acceso administrativamente
- Se establece como una interfaz de acceso operacionalmente (en funcionamiento)

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

3.5 Protocolo de Enlace Dinámico (DTP)

Protocolo de Enlace Dinámico

Introducción al DTP

El Protocolo de Enlace Troncal Dinámico (DTP) es un protocolo propietario de Cisco.

Las características de DTP son las siguientes:

- Activado de forma predeterminada en switches Catalyst 2960 y 2950.
- Dynamic-Auto es el valor predeterminado en los switches 2960 y 2950.
- Puede desactivarse con el comando `nonegotiate`.
- Puede volver a activarse configurando la interfaz en dinámico automático.
- Establecer un switch en un troncal estático o acceso estático evitará problemas de negociación con los comandos **switchport mode trunk** o **switchport mode access** .

```
S1(config-if)# switchport mode trunk  
S1(config-if)# switchport nonegotiate
```

```
S1(config-if)# switchport mode dynamic auto
```

Modos de interfaz negociados

El comando **switchport mode** tiene opciones adicionales.

Utilice el comando **switchport nonegotiate** interface configuration para detener la negociación DTP.

Opción	Descripción
Acceso	Modo de acceso permanente y negocia para convertir la interfaz vecina en un enlace de acceso
Dinámico automático	Se convertirá en una interfaz troncal si la interfaz vecina se configura en modo troncal o deseable.
Dinámico deseable	Busca activamente convertirse en un troncal negociando con otras interfaces automáticas o deseables.
Enlace troncal	Modo de enlace permanente y negocia para convertir el enlace vecino en un enlace troncal.

Resultados del protocolo de enlace troncal dinámico de una configuración DTP

Las opciones de configuración de DTP son las siguientes:

	Dinámico automático	Dinámico deseado	Troncal	Acceso
Dinámico automático	Acceso	Troncal	Troncal	Acceso
Dinámico deseado	Troncal	Troncal	Troncal	Acceso
Troncal	Troncal	Troncal	Troncal	Conectividad limitada
Acceso	Acceso	Acceso	Conectividad limitada	Acceso

Protocolo de enlace dinámico

Verifique el modo DTP

La configuración predeterminada de DTP depende de la versión y plataforma del IOS de Cisco.

- Utilice el comando **show dtp interface** para determinar el modo DTP actual.
- La práctica recomienda que las interfaces se configuren para acceder o troncal y para desconectarse DTP.

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

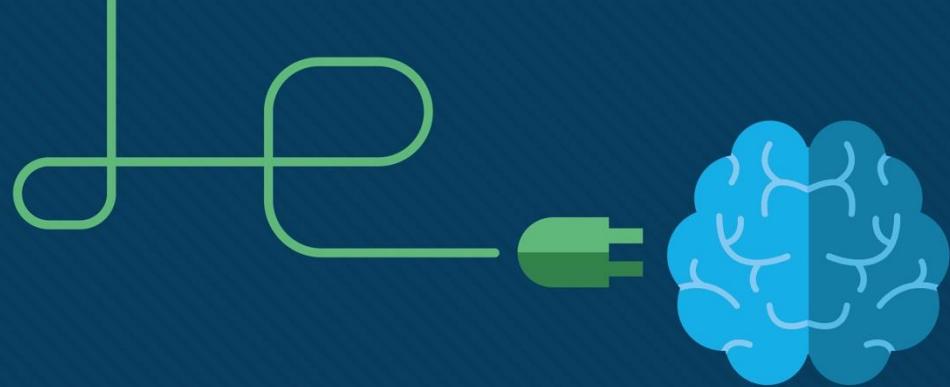
Nuevos Términos y Comandos

- | | |
|--|--|
| <ul style="list-style-type: none">• VLAN• Dominio de difusión lógico• VLAN de datos• VLAN predeterminada• VLAN nativa• VLAN de administración• show vlan brief• VLAN de voz• Enlace troncal de VLAN• Segmentación de VLAN• IEEE 802.1Q• Etiquetado de VLAN• Identificador de formato canónico (CFI) | <ul style="list-style-type: none">• Prioridad del usuario• ID de VLAN• Tipo• show interfaces <i>int</i> switchport |
|--|--|

Nuevos Términos y Comandos

<ul style="list-style-type: none">• Redes VLAN de rango normal• Redes VLAN de rango extendido• vlan <i>vlan-id</i>• name <i>vlan-name</i>• switchport mode access• switchport access vlan <i>vlan-id</i>• interface range• no switchport access vlan <i>vlan-id</i>• no vlan <i>vlan-id</i>• delete flash:vlan.dat	<ul style="list-style-type: none">• delete vlan.dat• show vlan• show interfaces• show vlan summary• show interfaces vlan <i>vlan_id</i>• switchport mode trunk• switchport trunk allowed <i>vlan_list</i>• switchport trunk native <i>vlan vlan_id</i>• no switchport trunk allowed <i>vlan</i>	<ul style="list-style-type: none">• no switchport trunk native <i>vlan</i>• show interfaces switchport• no switchport access vlan <i>vlan_id</i>• show interfaces trunk• show interfaces <i>int_id</i> trunk
---	--	---





Módulo 2: Conceptos de Commutación (Switching)

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



Objetivos del módulo

Titulo del Módulo: Conceptos de Comutación (Switching)

Objetivo del módulo: Explicar cómo la capa 2 envía la data.

Título del tema	Objetivo del tema
Reenvío de tramas	Explique la forma en la que las tramas se reenvían en una red comutada.
Dominios de switching	Compare un dominio de colisiones con un dominio de difusión.

2.1 Reenvío de tramas (Frame Forwarding)

Reenvío de Tramas

Comutación en redes

Se asocian dos términos con tramas que entran o salen de una interfaz:

- **Entrada** — entrar en la interfaz
- **Salida** : salida de la interfaz

Un switch reenvía basado en la interfaz de entrada y la dirección MAC de destino.

Un switch Ethernet de capa 2 utiliza direcciones MAC para tomar decisiones de reenvío.

Nota: Un switch nunca permitirá que el tráfico se reenvíe fuera de la interfaz en la que recibió el tráfico.



Port Table	
Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

Tabla de direcciones MAC del switch

Un switch utilizará la dirección MAC de destino para determinar la interfaz de salida.

Antes de que un switch pueda tomar esta decisión, debe saber qué interfaz se encuentra el destino.

Un switch crea una tabla de direcciones MAC, también conocida como tabla de memoria direccionable por contenido (CAM), grabando la dirección MAC de origen en la tabla junto con el puerto en el que se recibió.

El método de aprendizaje y reenvío del switch

El switch utiliza un proceso de dos pasos:

Paso 1. Explora– Examinar la dirección MAC de origen

- Agrega el MAC de origen si no está en la tabla
- Restablece la configuración de tiempo de espera de nuevo a 5 minutos si el origen está en la tabla

Paso 2. Reenvía – Examinar la dirección MAC de destino

- Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado.
- Si un MAC de destino no está en la tabla, se saturan todas las interfaces excepto la que se recibió.

Métodos de reenvío de un switch

Los switches utilizan software en circuitos integrados específicos de la aplicación (ASIC) para tomar decisiones muy rápidas.

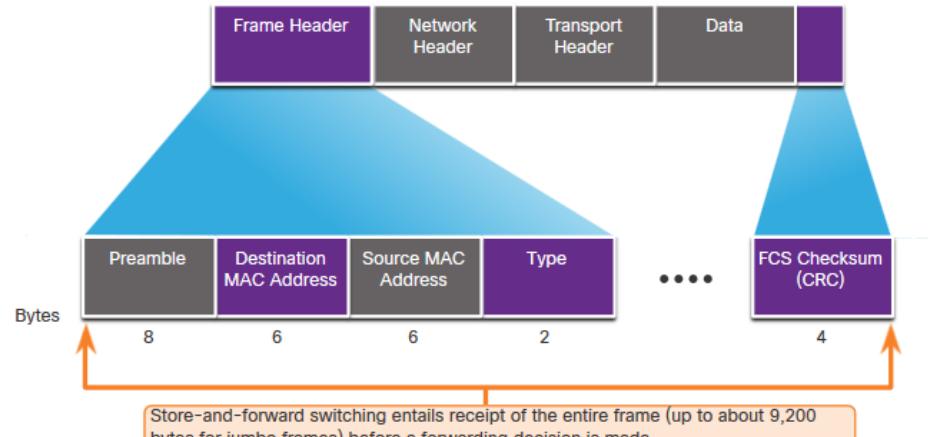
Un switch utilizará uno de estos dos métodos para tomar decisiones de reenvío después de recibir un frame:

- **Conmutación de almacenamiento y reenvío** : recibe toda la trama y garantiza que la trama es válida. Conmutación de almacenamiento y reenvío es el método principal de switching LAN de Cisco.
- **Conmutación de corte** : reenvía la trama inmediatamente después de determinar la dirección MAC de destino de una trama entrante y el puerto de salida.

Comutación de almacenamiento y reenvío

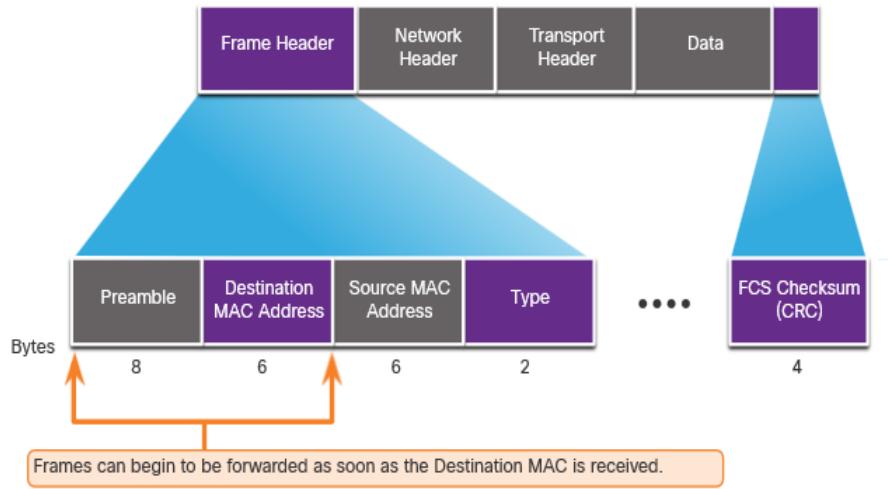
Almacenamiento y envío tienen dos características principales:

- **Comprobación de errores** - El switch comprobará si hay errores CRC en la secuencia de comprobación de cuadros (FCS). Las tramas defectuosas se descartarán.
- **Almacenamiento en búfer** - La interfaz de entrada almacenará en búfer la trama mientras comprueba el FCS. Esto también permite que el switch se ajuste a una diferencia potencial en velocidades entre los puertos de entrada y salida.



Reenvío de tramas

Switching de corte



- El corte reenvía la trama inmediatamente después de determinar el MAC de destino.
- El método Fragment (Frag) Free comprobará el destino y se asegurará de que la trama sea de al menos 64 Bytes. Esto eliminará a los runts.

Conceptos de switching por método de corte:

- Es apropiado para los switches que necesitan latencia de menos de 10 microsegundos.
- No comprueba el FCS, por lo que puede propagar errores.
- Puede provocar problemas de ancho de banda si el switch propaga demasiados errores.
- No es compatible con puertos con velocidades diferentes que van desde la entrada hasta la salida.

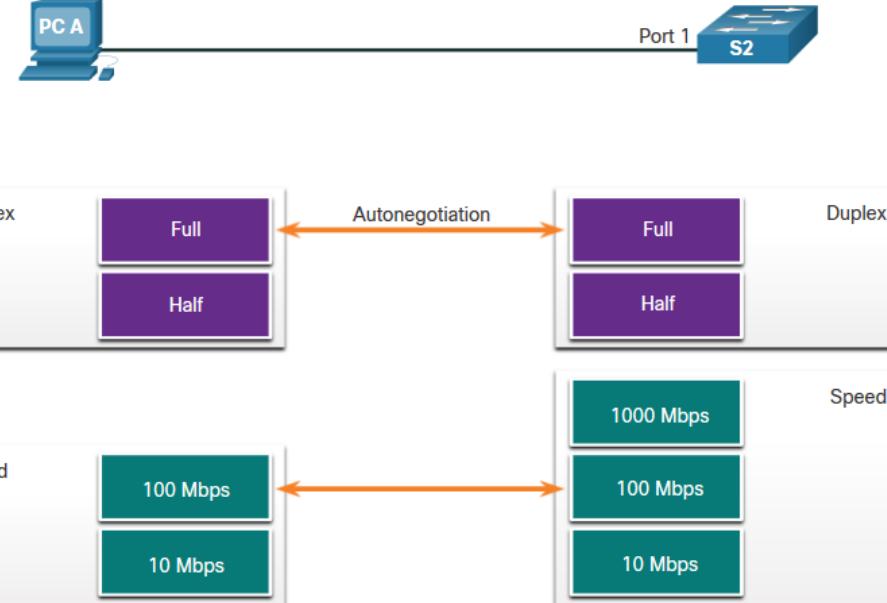
2.2 Dominios de switching

Dominios de switching

Dominios de colisiones

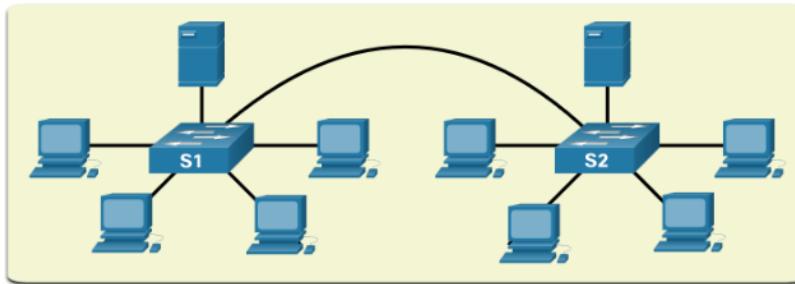
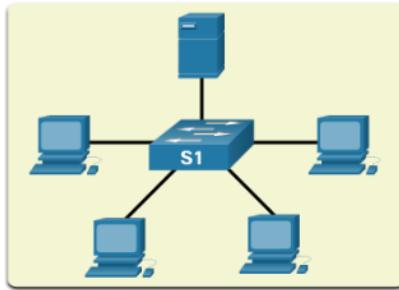
Los switch eliminan los dominios de colisión y reducen la congestión.

- Cuando hay dúplex completo en el enlace, se eliminan los dominios de colisión.
- Cuando hay uno o más dispositivos en semidúplex, ahora habrá un dominio de colisión.
 - Ahora habrá contención por el ancho de banda.
 - Las colisiones son ahora posibles.
- La mayoría de los dispositivos, incluidos Cisco y Microsoft, utilizan la negociación automática como configuración predeterminada para dúplex y velocidad.



Dominios de Difusión (Broadcast Domains)

- Un dominio de difusión se extiende a todos los dispositivos de Capa 1 o Capa 2 de una LAN.
- Sólo un dispositivo de capa 3 (enrutador) romperá el dominio de difusión, también llamado dominio de difusión MAC.
- El dominio de difusión consta de todos los dispositivos en la LAN que reciben el tráfico de difusión.
- Cuando el switch de capa 2 recibe la difusión, saturará todas las interfaces excepto la interfaz de entrada.
- Demasiadas emisiones pueden causar congestión y un rendimiento deficiente de la red.
- El aumento de los dispositivos en la capa 1 o en la capa 2 hará que el dominio de difusión se expanda.



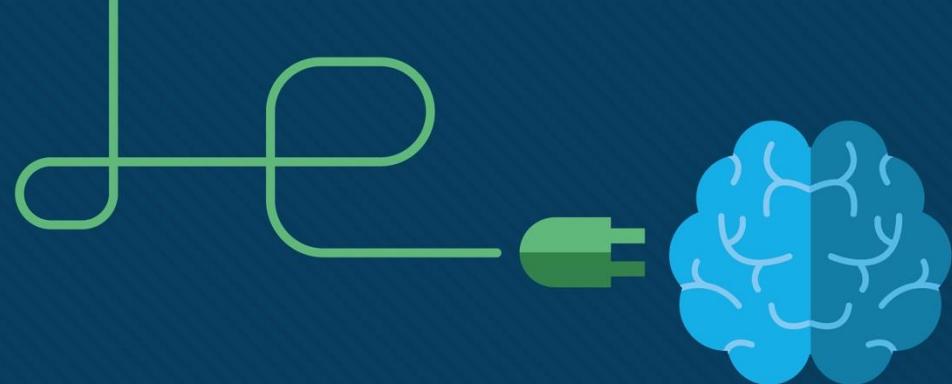
Alivio de la congestión en la red

Los switches utilizan la tabla de direcciones MAC y dúplex completo para eliminar colisiones y evitar la congestión.

Las características del comutador que alivian la congestión son las siguientes:

Característica	Función
Velocidades de puertos rápidos	Dependiendo del modelo, los switch pueden tener velocidades de puerto de hasta 100 Gbps.
Switching interno rápido	Esto utiliza un bus interno rápido o memoria compartida para mejorar el rendimiento.
Búferes para tramas grandes	Esto permite el almacenamiento temporal mientras se procesan grandes cantidades de tramas.
Alta densidad del puerto	Esto proporciona muchos puertos para que los dispositivos se conecten a LAN con menos costo. Esto también proporciona más tráfico local con menos congestión.





Módulo 1: Configuración básica del dispositivo

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



Objetivos del módulo

Título del módulo: Configuración básica del dispositivo

Objetivo del módulo: Configurar dispositivos utilizando las mejores prácticas de seguridad.

Título del tema	Objetivo del tema
Configuración de parámetros iniciales de un switch	Configure los parámetros iniciales en un switch Cisco.
Configuración de puertos de un switch	Configurar los puertos de un switch para cumplir con los requisitos de red.
Acceso remoto seguro	Configure el acceso de administración seguro en un switch.
Configuración Básica de un router	Configure los parámetros básicos en un router para enrutar entre dos redes conectadas directamente, mediante la CLI.
Verificar redes conectadas directamente	Verifique la conectividad entre dos redes que están conectadas directamente a un router.

1.1 Configurar un switch con parámetros iniciales

Secuencia de arranque de un switch

Después de encender un switch Cisco, pasa por la siguiente secuencia de inicio de cinco pasos:

Paso 1: Primero, el switch carga un programa de autocomprobación de encendido (POST) almacenado en la ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.

Paso 2: A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.

Paso 3: El gestor de arranque realiza la inicialización de CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.

Paso 4: El cargador de arranque inicializa el sistema de archivos flash en la placa del sistema.

Paso 5: Finalmente, el cargador de arranque localiza y carga una imagen de software

del sistema operativo IOS predeterminado en la memoria y le da el control del cambio al IOS.

El comando boot system

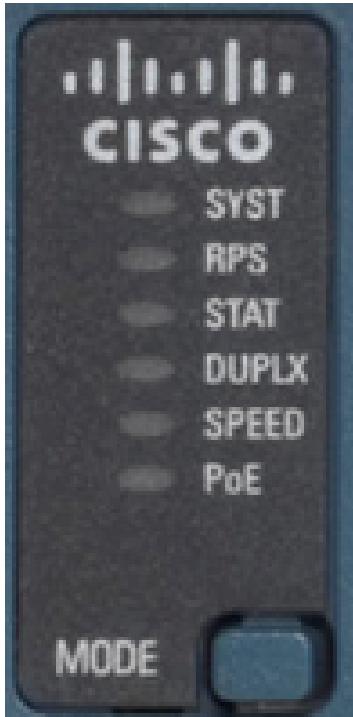
- Después de encender un switch Cisco, pasa por la siguiente secuencia de inicio de cinco pasos: Si no se establece esta variable, el switch intenta cargar y ejecutar el primer archivo ejecutable que puede encontrar.
- El sistema operativo IOS luego inicializa las interfaces utilizando los comandos Cisco IOS que se encuentran en el archivo de configuración de inicio. El archivo startup-config se llama **config.text** y se encuentra en flash.
- En el ejemplo, la variable de entorno BOOT se establece utilizando el comando del modo de configuración global **boot system**. Observe que el IOS se ubica en una carpeta distinta y que

S C S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin al

Comando	Definición
boot system	El comando principal
flash:	El dispositivo de almacenamiento
C2960-Lanbasek9-mz.150-2.se/	La ruta al sistema de archivos
C2960-Lanbasek9-mz.150-2.SE.bin	El nombre del archivo IOS

Configurar un switch con parámetros iniciales

Indicadores LED de un switch



LED del sistema (SYST): muestra si el sistema recibe alimentación y funciona correctamente.

LED de fuente de alimentación redundante (RPS): muestra el estado de RPS.

LED de estado del puerto (STAT): cuando está verde, indica que el modo de estado del puerto está seleccionado, que es el valor predeterminado. El estado del puerto puede ser entendido por la luz asociada a cada puerto.

LED de modo dúplex del puerto: cuando el LED es de color verde, indica que se seleccionó el modo dúplex del puerto. El dúplex de puerto se puede entender por la luz asociada a cada puerto.

LED de velocidad del puerto (SPEED): cuando está verde, indica que se ha seleccionado el modo de velocidad del puerto. La velocidad del puerto se puede entender por la luz asociada a cada puerto.

LED de alimentación a través de Ethernet (PoE): Presente si el switch es compatible con PoE. Indica el estado PoE de los puertos del switch.

Configurar un switch con parámetros iniciales

Indicadores LED de un switch (Cont.)

	Apagado	Verde	Verde intermitente	Ámbar	Ámbar intermitente	Verde y ámbar alternado: falla en el enlace.
RPS	Desactivado o/Sin RPS	Listo para RPS	RPS disponible pero no disponible	RPS en espera o falla	El PS interno falló, el RPS proporciona energía	No corresponde
PoE	No seleccionado, no hay problemas	Seleccionado	No corresponde	No corresponde	No seleccionado, problemas de puerto presentes	No corresponde

Cuando se selecciona el modo con nombre, la luz asociada a cada puerto físico indica:

ESTADO	Sin enlace o apagado	Enlace activo	Actividad	Puerto bloqueado bucle de prevención	Puerto bloqueado bucle de prevención	Falla de enlace
DUPLEX (Dúplex)	Medio dúplex	Dúplex completo	No corresponde	No corresponde	No corresponde	No corresponde
VELOCIDAD	10 Mbps	100 Mbps	1000 Mbps	No corresponde	No corresponde	No corresponde
PoE	PoE desactivado	PoE activado	No corresponde	PoE deshabilitado	PoE apagado debido a un fallo	PoE denegado (sobrepresuest

Recuperación tras un bloqueo del sistema

El cargador de arranque proporciona acceso al switch si no se puede usar el sistema operativo debido a la falta de archivos de sistema o al daño de estos. El cargador de arranque tiene una línea de comando que proporciona acceso a los archivos almacenados en la memoria flash. Se puede acceder al cargador de arranque mediante una conexión de consola con los siguientes pasos:

Paso 1. Conecte una computadora al puerto de consola del switch con un cable de consola. Configure el software de emulación de terminal para conectarse al switch.

Paso 2. Desconecte el cable de alimentación del switch.

Paso 3. Vuelva a conectar el cable de alimentación al switch, espere 15 segundos y, a continuación, presione y mantenga presionado el botón **Mode** mientras el LED del sistema sigue parpadeando con luz verde.

Paso 4. Continúe oprimiendo el botón **Mode** hasta que el LED del sistema se torne ámbar por un breve instante y luego verde, después suelte el botón **Mode**

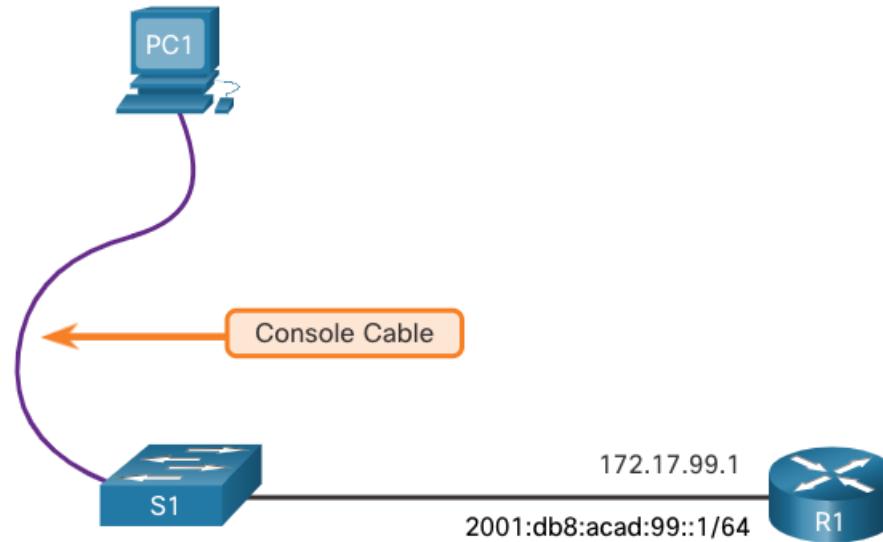
Paso 5. The boot loader **switch**: aparece en el software de emulación de terminal en la PC.

La línea de comandos de boot loader admite comandos para formatear el sistema de archivos flash, volver a instalar el software del sistema operativo y recuperar una contraseña perdida u olvidada. Por ejemplo, el comando **dir** puede usar para ver una lista de archivos dentro de un directorio específico.

Configurar el acceso a la administración de un switch

Para el acceso a la administración remota de un switch, este se debe configurar con una dirección IP y una máscara de subred.

- Para administrar el comutador desde una red remota, el router debe configurarse con una puerta de enlace predeterminada. Este es un proceso muy similar a la configuración de la información de dirección IP en los dispositivos host.
- En la ilustración, se debe asignar una dirección IP a la interfaz virtual del switch (SVI) de S1. La SVI es una interfaz virtual, no un puerto físico del switch. Se utiliza un cable de consola para conectarse a un PC de modo que el switch pueda configurarse inicialmente.



Ejemplo de configuración de SVI

De manera predeterminada, el switch está configurado para controlar su administración a través de la VLAN 1. Todos los puertos se asignan a la VLAN 1 de manera predeterminada. Por motivos de seguridad, se recomienda usar una VLAN de administración distinta de la VLAN 1.

Paso 1: Configure la interfaz de administración: Desde el modo de configuración de la interfaz VLAN, se aplica una dirección IPv4 y una máscara de subred a la SVI de administración del switch.

Nota: El SVI para VLAN 99 no aparecerá como "activo / activo" hasta que se cree VLAN 99 y haya un dispositivo conectado a un puerto de switch asociado con VLAN 99.

Nota: Es posible que el switch deba configurarse para IPv6. Por ejemplo, antes de que pueda configurar el direccionamiento IPv6 en un Cisco Catalyst 2960 con IOS versión 15.0, deberá ingresar el comando de configuración global **sdm, preferir dual-ipv4-and ipv6 default** y, a continuación, **reiniciar** el switch.

Ejemplo de configuración de SVI (Cont.)

Tarea	Comandos IOS
Ingrese al modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# interface vlan 99
Configure la dirección IPv4 de la interfaz de administración.	S1(config-if)# ip address 172.17.99.11 255.255.255.0
Configure la dirección IPv6 de la interfaz de administración	S1 (config-if) # ipv6 address 2001:db8:acad:99::1/64
Habilite la interfaz de administración.	S1(config-if)# no shutdown
Regrese al modo EXEC privilegiado.	S1(config-if)# end
Guarde la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Ejemplo de configuración de SVI (Cont.)

Paso 2: Configure el gateway predeterminado

- Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado.
- **Nota:** Debido a que recibirá la información de la puerta de enlace predeterminada de un mensaje de anuncio de router (RA), el switch no requiere una puerta de enlace predeterminada IPv6.

Tarea	Comandos IOS
Ingrese al modo de configuración global.	S1# configure terminal
Configure el gateway predeterminado para el switch.	S1(config)# ip default-gateway 172.17.99.1
Regrese al modo EXEC privilegiado.	S1(config-if)# end
Guarde la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Ejemplo de configuración de SVI (Cont.)

Paso 3: Verifique la configuración.

- Los comandos **show ip interface brief** y **show ipv6 interface brief** son útiles para determinar el estado de las interfaces físicas y virtuales. La información que se muestra confirma que la interfaz VLAN 99 se ha configurado con una dirección IPv4 e IPv6.

Nota: Una dirección IP aplicada al SVI es solo para el acceso de administración remota al switch; esto no permite que el switch enrute paquetes de Capa 3.

```
S1# show ip interface brief
Interface      IP-Address      OK? Method     Status      Protocol
Vlan99         172.17.99.11    YES manual    down       down
(output omitted)
S1# show ipv6 interface brief
Vlan99          [down/down]
FE80::C27B:BCFF:FEC4:A9C1
2001:DB8:ACAD:99::1
(output omitted)
```

1.2 - Configuración de puertos de un switch

Configurar los puertos de un switch

Comunicación en dúplex

- La comunicación en dúplex completo aumenta el ancho de banda eficaz al permitir que ambos extremos de una conexión transmitan y reciban datos simultáneamente. Esto también se conoce como comunicación bidireccional y requiere microsegmentación.
- Las LAN microsegmentadas se crean cuando un puerto de switch tiene solo un dispositivo conectado y funciona en modo dúplex completo. No hay dominio de colisión asociado con un puerto de switch que funcione en modo dúplex completo.
- A diferencia de la comunicación en dúplex completo, la comunicación en semidúplex es unidireccional. La comunicación en semidúplex genera problemas de rendimiento debido a que los datos fluyen en una sola dirección por vez, lo que a menudo provoca colisiones.
- Gigabit Ethernet y NIC de 10 Gb requieren conexiones full-duplex para funcionar. En el modo dúplex completo, el circuito de detección de colisiones de la NIC se encuentra inhabilitado. Dúplex completo ofrece el 100% de eficacia en ambas direcciones (transmisión y recepción). Esto da como resultado una duplicación del uso potencial del ancho de banda establecido.

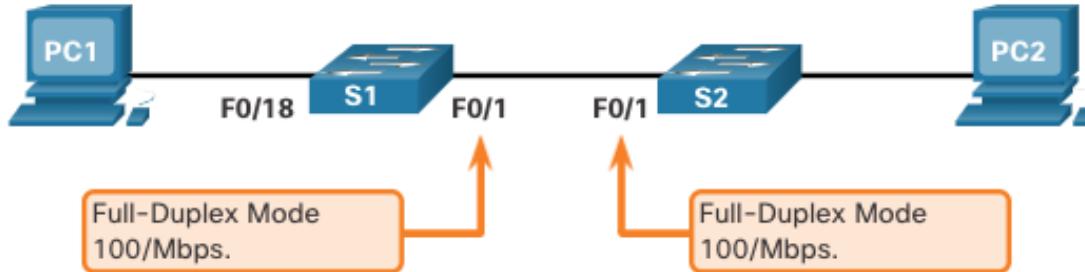
Configurar puertos de switch en la capa física

- Los puertos de switch se pueden configurar manualmente con parámetros específicos de dúplex y de velocidad. Los comandos de configuración de interfaz respectivos son **dúplex** y **velocidad**.
- La configuración predeterminada de dúplex y velocidad para los puertos de switch en los switches Cisco Catalyst 2960 y 3560 es automática. Los puertos 10/100/1000 funcionan en modo semidúplex o semidúplex cuando están configurados en 10 o 100 Mbps y operan solo en modo dúplex completo cuando está configurado en 1000 Mbps (1 Gbps).
- La negociación automática es útil cuando la configuración de velocidad y dúplex del dispositivo que se conecta al puerto es desconocida o puede cambiar. Cuando se conecta a dispositivos conocidos como servidores, estaciones de trabajo dedicadas o dispositivos de red, la mejor práctica es establecer manualmente la configuración de velocidad y dúplex.
- Al solucionar problemas de puertos del switch, es importante que se verifiquen las configuraciones de dúplex y velocidad.

Nota: si la configuración para el modo dúplex y la velocidad de puertos del switch presenta incompatibilidades, se pueden producir problemas de conectividad. Una falla de autonegociación provoca incompatibilidades en la configuración.

Todos los puertos de fibra óptica, como los puertos 1000BASE-SX, solo funcionan a una velocidad predefinida y siempre son dúplex completo.

Configurar puertos de switch en la capa física



Tarea	Comandos IOS
Ingrese al modo de configuración global.	S1# configure terminal
Ingrese el modo de configuración de interfaz.	S1(config)# interface FastEthernet 0/1
Configure el modo dúplex de la interfaz.	S1(config-if)# duplex full
Configure la velocidad de la interfaz.	S1(config-if)# speed 100
Regrese al modo EXEC privilegiado.	S1(config-if)# end
Guarde la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Configurar los puertos de un switch Auto-MDIX

- Cuando se habilita el crossover automático de interfaz dependiente del medio (auto-MDIX), la interfaz del switch detecta automáticamente el tipo de conexión de cable requerido (directo o cruzado) y configura la conexión adecuadamente.
- Al conectarse a los switches sin la función auto-MDIX, los cables directos deben utilizarse para conectar a dispositivos como servidores, estaciones de trabajo o routers. Los cables cruzados se deben utilizar para conectarse a otros switches o repetidores.
- Con la característica auto-MDIX habilitada, se puede usar cualquier tipo de cable para conectarse a otros dispositivos, y la interfaz se ajusta de manera automática para proporcionar comunicaciones satisfactorias.
- En los switches Cisco más modernos, el comando del modo de configuración de interfaz **mdix auto** habilita la característica. Cuando se usa auto-MDIX en una interfaz, la velocidad y el modo dúplex de la interfaz se deben establecer en **auto** para que la característica funcione correctamente.

Nota: la característica auto-MDIX está habilitada de manera predeterminada en los switches Catalyst 2960 y Catalyst 3560, pero no está disponible en los switches más antiguos Catalyst 2950 y Catalyst 3550.

Para examinar la configuración de auto-MDIX de una interfaz específica, use el comando **show controllers ethernet-controller** con la palabra clave **phy**. Para limitar los resultados a las líneas que se refieren a auto-MDIX, use el filtro **include Auto-MDIX**.

Configurar los puertos de un switch

Comandos de verificación del switch

Tarea	Comandos IOS
Muestra el estado y la configuración de la interfaz.	S1# show interfaces [<i>interface-id</i>]
Muestra la configuración de inicio actual.	S1# show startup-config
Muestra la configuración actual en ejecución.	S1# show running-config
Muestra información sobre el sistema de archivos flash.	S1# show flash
Muestra el estado del hardware y el software del sistema.	S1# show version
Muestra la configuración actual en ejecución.	S1# show history
Muestra información de IP de una interfaz.	S1# show ip interface [<i>interface-id</i>] O S1# show ipv6 interface [<i>interface-id</i>]
Muestra la tabla de direcciones MAC.	S1# show mac-address-table O S1# show mac address-table

Verificar la configuración de los puertos de un switch (cont.)

El comando **show running-config** se puede utilizar para verificar que el switch se ha configurado correctamente. De la salida abreviada de muestra en S1, se muestra alguna información importante en la figura:

- Interfaz Fast Ethernet 0/18 configurada con la VLAN 99 de administración
- VLAN 99 configurada con la dirección IPv4 172.17.99.11 255.255.255.0
- Gateway predeterminado establecido en 172.17.99.1

```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
(output omitted)
interface Vlan99
  ip address 172.17.99.11 255.255.255.0
  ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

Verificar la configuración de los puertos de un switch (cont.)

El comando **show interfaces** es otro comando de uso frecuente que muestra información estadística y de estado sobre las interfaces de red del switch. El comando **show interfaces** se usa habitualmente cuando se configuran y se controlan los dispositivos de red.

La primera línea de salida para el comando **show interfaces fastEthernet 0/18** indica que la interfaz FastEthernet 0/18 está activa / activa, lo que significa que está operativa. Más abajo en el resultado, se muestra que el modo dúplex es full (completo) y la velocidad es de 100 Mb/s.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
    MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

Problemas en la capa de acceso a la red

El resultado del comando **show interfaces** se puede usar para detectar problemas frecuentes de los medios. Una de las partes más importantes de esta salida es la visualización de la línea y el estado del protocolo de enlace de datos, como se muestra en el ejemplo.

El primer parámetro (FastEthernet0 /18 está activo) se refiere a la capa de hardware e indica si la interfaz está recibiendo una señal de detección de portadora. El segundo parámetro (line protocol is up) se refiere a la capa de enlace de datos e indica si se reciben los keepalives del protocolo de capa de enlace de datos. Sobre la base del resultado del comando **show interfaces**, los posibles problemas se pueden reparar de la siguiente manera:

- Si la interfaz está activa y el protocolo de línea está inactivo, hay un problema. Puede haber una incompatibilidad en el tipo de encapsulación, la interfaz en el otro extremo puede estar inhabilitada por errores o puede haber un problema de hardware.
- Si el protocolo de línea y la interfaz están inactivos, no hay un cable conectado o existe algún otro problema de interfaz. Por ejemplo, en una conexión directa, el otro extremo de la conexión puede estar administrativamente inactivo.
- Si la interfaz se encuentra administrativamente inactiva, se inhabilitó manualmente en la configuración activa (se emitió el comando **shutdown**).

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)MTU 1500 bytes, BW
100000 Kbit/sec, DLY 100 usec,
```

Problemas en la capa de acceso a la red (Cont.)

El resultado del comando **show interfaces** muestra contadores y estadísticas para la interfaz Fastethernet0/18, como se muestra a continuación:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2295197 packets input, 305539992 bytes, 0 no buffer
    Received 1925500 broadcasts (74 multicasts)
    0 runts, 0 giants, 0 throttles
    3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 74 multicast, 0 pause input
    0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
    8 output errors, 1790 collisions, 10 interface resets
    0 unknown protocol drops
    0 babbles, 235 late collision, 0 deferred
```

Problemas en la capa de acceso a la red (Cont.)

Algunos errores de los medios no son lo suficientemente graves como para hacer que el circuito falle, pero causan problemas de rendimiento de la red. La tabla explica algunos de estos errores comunes que se pueden detectar con el **show interfaces** .

Tipo de error	Descripción
Errores de entrada	Cantidad total de errores. Incluye los recuentos de fragmentos de colisión, de fragmentos gigantes, de los que no están almacenados en buffer, de CRC, de tramas, de saturación y de ignorados.
Fragmentos de colisión	Paquetes que se descartan porque son más pequeños que el tamaño mínimo de paquete para el medio. Por ejemplo, cualquier paquete Ethernet que tenga menos de 64 bytes se considera un fragmento de colisión.
Fragmentos gigantes	Paquetes que se descartan porque superan el tamaño máximo de paquete para el medio. Por ejemplo, cualquier paquete Ethernet que tenga más de 1518 bytes se considera un fragmento gigante.
CRC	Se generan errores de CRC cuando el checksum calculado no es igual al checksum recibido.
Errores de salida	La suma de todos los errores que impiden la transmisión final de los datagramas por la interfaz que se analiza.
Colisiones	Cantidad de mensajes retransmitidos debido a una colisión de Ethernet.
Colisiones tardías	Una colisión que ocurre después de que se hayan transmitido 512 bits de la trama

Errores de Entrada y Salida de la Interfaz

“Input errors” indica la suma de todos los errores en los datagramas que se recibieron en la interfaz que se analiza. Estos incluyen los recuentos de fragmentos de colisión, de fragmentos gigantes, de los que no están almacenados en buffer, de CRC, de tramas, de saturación y de ignorados. Los errores de entrada que se informan con el comando **show interfaces** incluyen lo siguiente:

- **Runt Frames** - las tramas Ethernet que son más cortas que la longitud mínima permitida de 64 bytes se llaman runts La NIC en mal funcionamiento son la causa habitual de las tramas excesivas de fragmentos de colisión, pero también pueden deberse a colisiones.
- **Giants** - Las tramas de Ethernet que son más grandes que el tamaño máximo permitido se llaman gigantes
- **CRC errors** - En las interfaces Ethernet y serie, los errores de CRC generalmente indican un error de medios o cable. Las causas más comunes incluyen interferencia eléctrica, conexiones flojas o dañadas o cableado incorrecto. Si aparecen muchos errores de CRC, hay demasiado ruido en el enlace, y se debe examinar el cable. También se deben buscar y eliminar las fuentes de ruido.

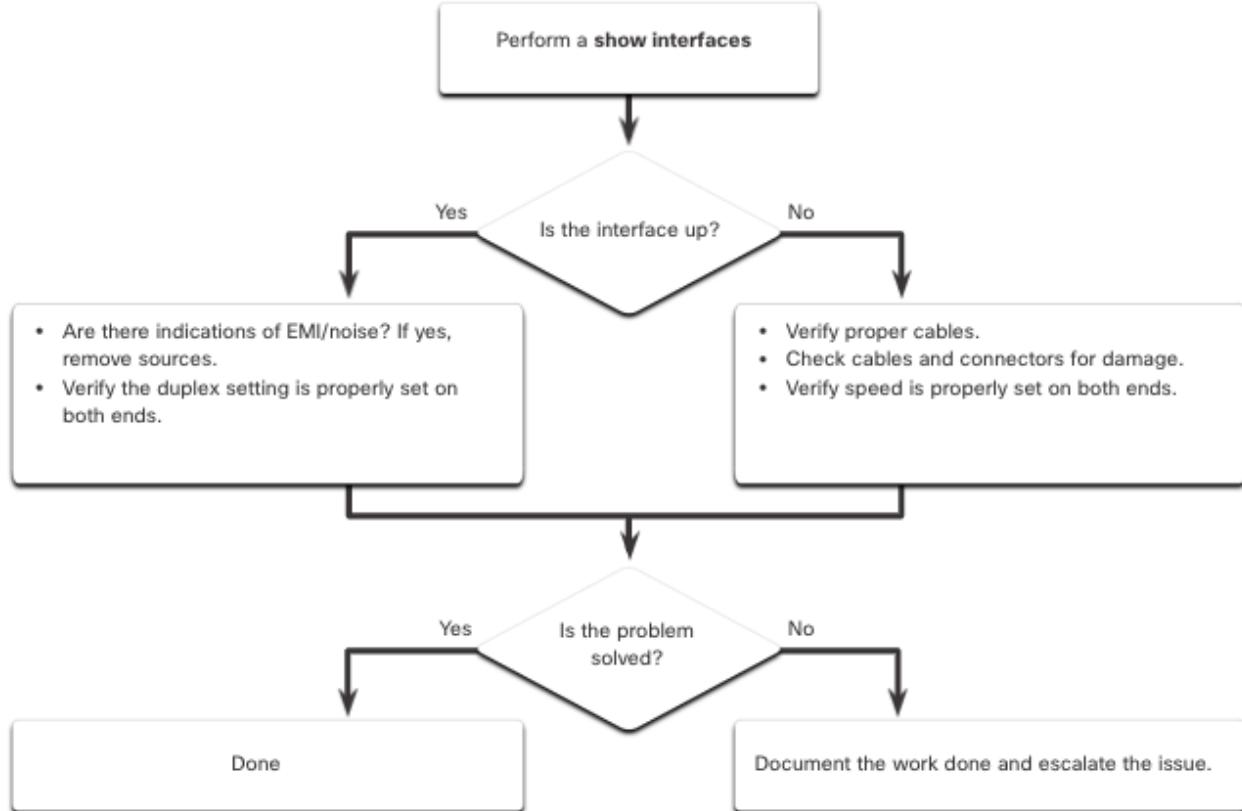
Errores de Entrada y Salida de la Interfaz (Cont.)

“Output errors” es la suma de todos los errores que impiden la transmisión final de los datagramas por la interfaz que se analiza. Los errores de salida que se informan con el comando **show interfaces** incluyen lo siguiente:

- **Colisiones** - Las colisiones en operaciones half-duplex son normales. Sin embargo, nunca debe observar colisiones en una interfaz configurada para la comunicación en dúplex completo.
- **Colisiones tardías** - Una colisión tardía se refiere a una colisión que ocurre después de que se han transmitido 512 bits de la trama. La longitud excesiva de los cables es la causa más frecuente de las colisiones tardías. Otra causa frecuente es la configuración incorrecta de dúplex.

Resolución de problemas de la capa de acceso

Para solucionar los problemas que implican que no hay conexión, o una mala conexión, entre un interruptor y otro dispositivo, siga el proceso general que se muestra en la figura.



1.3 Acceso remoto seguro

Funcionamiento de Telnet

Telnet utiliza el puerto TCP 23. Es un protocolo más antiguo que utiliza la transmisión de texto sin formato segura tanto de la autenticación de inicio de sesión (nombre de usuario y contraseña) como de los datos transmitidos entre los dispositivos de comunicación.

Un actor de amenazas puede monitorear paquetes usando Wireshark. Por ejemplo, en la figura, el actor de amenazas capturó el nombre de usuario **admin** y la contraseña **ccna** de una sesión Telnet.

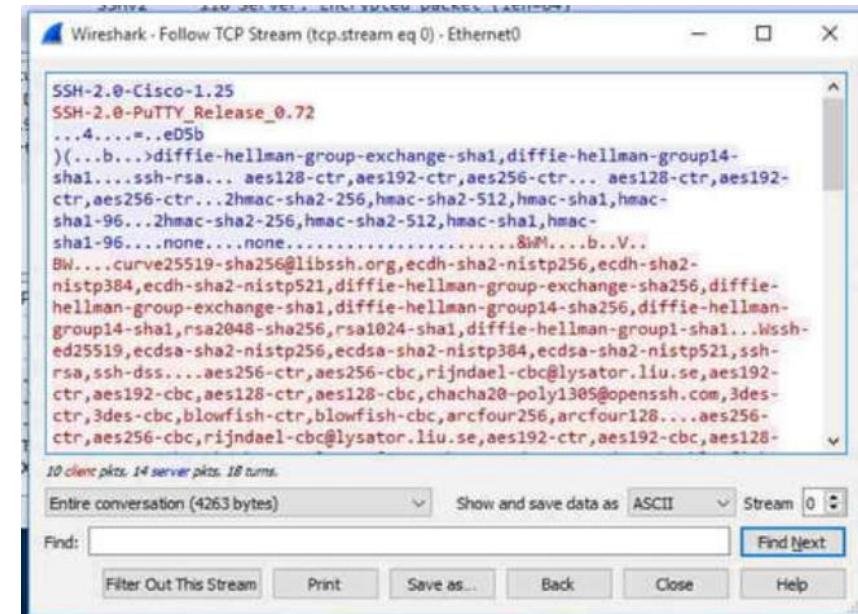


Funcionamiento de SSH

Secure Shell (SSH) es un protocolo seguro que utiliza el puerto TCP 22. Proporciona una conexión de administración segura (encriptada) a un dispositivo remoto. El SSH debe reemplazar a Telnet para las conexiones de administración.

SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro cuando se autentica un dispositivo (nombre de usuario y contraseña) y también para los datos transmitidos entre los dispositivos que se comunican.

La figura muestra una captura de Wireshark de una sesión SSH. Proporciona una conexión de administración segura (encriptada) a un dispositivo remoto. Sin embargo, a diferencia de Telnet, con SSH el nombre de usuario y la contraseña están cifrados.



Verifique que el switch admite SSH

Para habilitar SSH en un switch Catalyst 2960, el switch debe usar una versión del software IOS que incluya características y capacidades criptográficas (cifradas). Utilice el comando **show version** en el switch para ver qué IOS está ejecutando el switch. Un nombre de archivo de IOS que incluye la combinación «k9» admite características y capacidades criptográficas (cifradas).

El ejemplo muestra la salida del comando **show version** .

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE
(fcl)
```

Configuración de SSH

Antes de configurar SSH, el switch debe tener configurado, como mínimo, un nombre de host único y los parámetros correctos de conectividad de red.

Paso 1: Verifique la compatibilidad con SSH: - use el comando `show ip ssh` para verificar que el switch sea compatible con SSH. Si el switch no ejecuta un IOS que admite características criptográficas, este comando no se reconoce.

Paso 2: Configure el dominio IP: configure el nombre de dominio IP de la red mediante el comando `ip domain-name` en modo de configuración global.

Paso 3: Genere pares de claves RSA: la generación de un par de claves RSA activa automáticamente SSH. Use el comando `crypto key generate rsa` en modo de configuración global.

Nota: para eliminar el par de claves RSA, use el comando `crypto key zeroize rsa` del modo de configuración global. Despues de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

Paso 4: Configure la autenticación de usuario: el servidor SSH puede autenticar usuarios localmente o usar un servidor de autenticación. Para usar el método de autenticación local, cree un par de nombre de usuario y contraseña con el comando `username username secret password` en modo de configuración global.

Paso 5: Configure las líneas vty: habilite el protocolo SSH en las líneas vty utilizando el comando de modo de configuración `transport input ssh`. Use el comando `line vty` del modo de configuración global y, luego, el comando `login` en modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

Paso 6: Active SSH versión 2 - De manera predeterminada, SSH admite las versiones 1 y 2. Al admitir ambas versiones, esto se muestra en la salida como compatible con la versión 2. `show ip ssh` . Habilite la versión de SSH mediante el comando de configuración global `ip ssh version 2` .



Verifique que SSH esté operativo

En las computadoras se usa un cliente SSH, como PuTTY, para conectarse a un servidor SSH. Por ejemplo, suponga que se configura lo siguiente:

- SSH está habilitado en el interruptor S1
- Interfaz VLAN 99 (SVI) con la dirección IPv4 172.17.99.11 en el switch S1.
- PC1 con la dirección IPv4 172.17.99.21.

Mediante un emulador de terminal, inicie una conexión SSH a la dirección IPv4 SVI VLAN de S1 desde PC1.

Cuando está conectado, se solicita al usuario un nombre de usuario y una contraseña como se muestra en el ejemplo. Con la configuración del ejemplo anterior, se introduce el nombre de usuario **admin** y la contraseña **ccna**. Después de ingresar la combinación correcta, el usuario se conecta a través de SSH a la interfaz de línea de comando (CLI) en el switch Catalyst 2960.

```
Login as: admin
Using keyboard-interactive
Authentication.
Password:
S1> enable
Password:
S1#
```

Verifique que SSH esté operativo (Cont.)

Para mostrar los datos de la versión y de configuración de SSH en el dispositivo que configuró como servidor SSH, use el comando **show ip ssh**. En el ejemplo, se habilitó la versión 2 de SSH.

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
To check the SSH connections to the device, use the show ssh command as shown.
S1# show ssh
%No SSHv1 server connections running.

Connection Version Mode Encryption Hmac State Username
0      2.0   IN    aes256-cbc  hmac-sha1 Session started admin
0      2.0   OUT   aes256-cbc  hmac-sha1 Session started admin
S1#
```

1.4 Configuración básica de un router

Configurar los parámetros básicos de un router

Los routers y switches Cisco tienen muchas similitudes. Admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Además, los pasos de configuración inicial son similares para ambos dispositivos. Por ejemplo, las siguientes tareas de configuración siempre deben realizarse. Asigne un nombre al dispositivo para distinguirlo de otros routers y configure contraseñas, como se muestra en el ejemplo.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#

```

Configurar los parámetros básicos de un router (Cont.)

Configure un banner para proporcionar notificaciones legales de acceso no autorizado, como se muestra en el ejemplo.

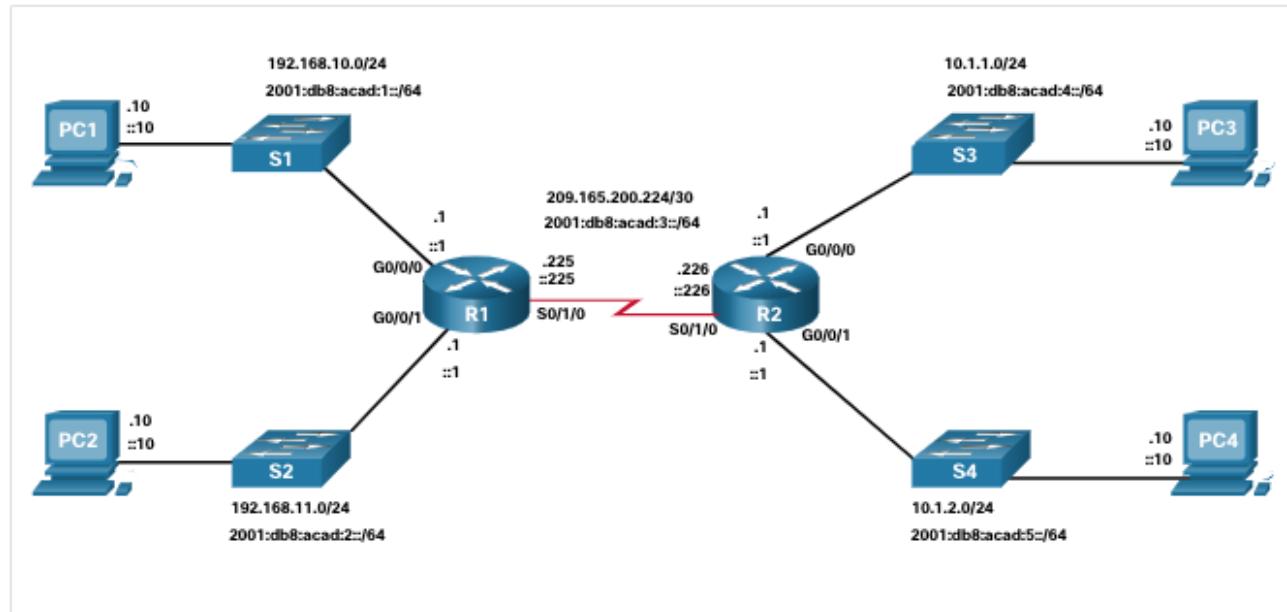
```
R1(config)# banner motd $ Authorized Access Only! $  
R1(config)#
```

Guarde los cambios en un router, como se muestra en el ejemplo.

```
R1# copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]
```

Configuración básica del router Topología Dual Stack

Una característica que distingue a los switches de los routers es el tipo de interfaces que admite cada uno. Por ejemplo, los switches de capa 2 admiten LAN; por lo tanto, tienen múltiples puertos FastEthernet o Gigabit Ethernet. La topología de pila dual de la figura se utiliza para demostrar la configuración de las interfaces IPv4 e IPv6 del router.



Configurar interfaces del router

Los routers admiten redes LAN y WAN, y pueden interconectar distintos tipos de redes; por lo tanto, admiten muchos tipos de interfaces. Por ejemplo, los ISR G2 tienen una o dos interfaces Gigabit Ethernet integradas y ranuras para tarjetas de interfaz WAN de alta velocidad (HWIC) para admitir otros tipos de interfaces de red, incluidas las interfaces seriales, DSL y de cable.

Para que una interfaz esté disponible, debe cumplir los siguientes requisitos:

- **Configurado con al menos una dirección IP** : utilice los comandos de configuración de **ip address ip-address subnet-mask** y **ipv6 address ipv6-address/prefix interface**.
- **Activar la interfaz**: - las interfaces LAN y WAN no están activadas (**shutdown**). Para habilitar una interfaz, esta se debe activar mediante el comando **no shutdown** . (Es como encender la interfaz.) La interfaz también debe estar conectada a otro dispositivo (un hub, un switch u otro router) para que la capa física se active.
- **Descripción** - Opcionalmente, la interfaz también se puede configurar con una breve descripción de hasta 240 caracteres. Es aconsejable configurar una descripción en cada interfaz. En las redes de producción, los beneficios de las descripciones de la interfaz se obtienen rápidamente, ya que son útiles para solucionar problemas e identificar una conexión de terceros y la información de contacto.

Configurar interfaces del router (Cont.)

El ejemplo muestra la configuración de las interfaces en R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:3::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#

```

Interfaces de loopback IPv4

Otra configuración común de los routers Cisco IOS es la habilitación de una interfaz loopback.

- La interfaz de bucle invertido es una interfaz lógica interna del router. No está asignado a un puerto físico y nunca se puede conectar a ningún otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado "up" (activo), siempre que el router esté en funcionamiento.
- La interfaz loopback es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, se puede usar con fines de prueba, como la prueba de procesos de routing interno, mediante la emulación de redes detrás del router.
- Las interfaces de bucle invertido también se utilizan comúnmente en entornos de laboratorio para crear interfaces adicionales. Por ejemplo, puede crear varias interfaces de bucle invertido en un router para simular más redes con fines de práctica de configuración y pruebas. La dirección IPv4 para cada interfaz loopback debe ser única y no la debe usar ninguna otra interfaz. En este plan de estudios, a menudo usamos una interfaz de bucle invertido para simular un enlace a Internet.
- El proceso de habilitación y asignación de una dirección de loopback es simple:

```
Router(config)# interface loopback number
```

```
Router(config-if)# ip address ip-address subnet-mask
```

1.5 Verificar redes conectadas directamente

Comandos de verificación de la interfaz

Existen varios comandos **show** que se pueden usar para verificar el funcionamiento y la configuración de una interfaz.

Los siguientes comandos son especialmente útiles para identificar rápidamente el estado de una interfaz:

- **show ip interface brief** y **show ipv6 interface brief** - estos muestran un resumen de todas las interfaces, incluida la dirección IPv4 o IPv6 de la interfaz y el estado operativo actual.
- **show running-config interface *interface-id*** - Esto muestra los comandos aplicados a la interfaz especificada.
- **show ip route** and **show ipv6 route** - muestra el contenido de la tabla de routing de IPv4 almacenada en la RAM. En el IOS de Cisco 15, las interfaces activas deben aparecer en la tabla de routing con dos entradas relacionadas identificadas con el código 'C' (conectada) o 'L' (Local). En versiones anteriores de IOS, solo aparece una única entrada con el código 'C' .

Verificar las redes conectadas directamente

Verifique el estado de la interfaz

La salida de los comandos **show ip interface brief** y **show ipv6 interface brief** se puede utilizar para revelar rápidamente el estado de todas las interfaces del router. Puede verificar que las interfaces están activas y operativas como se indica en el estado de «up» y el protocolo de «up», como se muestra en el ejemplo. Un resultado distinto indicaría un problema con la configuración o el cableado

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0/0 192.168.10.1   YES manual up           up
GigabitEthernet0/0/1 192.168.11.1   YES manual up           up
Serial0/1/0          209.165.200.225 YES manual up           up
Serial0/1/1          unassigned      YES unset administratively down down
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
  FE80::7279:B3FF:FE92:3130
  2001:DB8:ACAD:1::1
GigabitEthernet0/0/1 [up/up]
  FE80::7279:B3FF:FE92:3131
  2001:DB8:ACAD:2::1
Serial0/1/0          [up/up]
  FE80::7279:B3FF:FE92:3130
  2001:DB8:ACAD:3::1
Serial0/1/1          [down/down]    Unassigned
```

Verificar las redes conectadas directamente

Verificar direcciones locales y multidifusión de vínculos IPv6

El resultado del comando **show ipv6 interface brief** muestra dos direcciones IPv6 configuradas por interfaz. Una de las direcciones es la dirección de unidifusión global de IPv6 que se introdujo manualmente. La otra, que comienza con FE80, es la dirección de unidifusión link-local para la interfaz. La dirección link-local se agrega automáticamente a una interfaz cuando se asigna una dirección de unidifusión global. Las interfaces de red IPv6 deben tener una dirección link-local, pero no necesariamente una dirección de unidifusión global.

El resultado del comando **show ipv6 interface gigabitethernet 0/0/0** muestra el estado de la interfaz y todas las direcciones IPv6 que pertenecen a la interfaz. Junto con la dirección local del enlace y la dirección de unidifusión global, la salida incluye las direcciones de multidifusión asignadas a la interfaz, comenzando con el prefijo FF02, como se muestra en el ejemplo.

```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF92:3130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

Cisco y/o sus filiales. Todos los derechos reservados. Información
confidencial de Cisco



Verificar la configuración de la interfaz

El resultado del comando **show running-config interface** muestra los comandos actuales aplicados a la interfaz especificada, como se muestra.

Los dos comandos siguientes se usan para recopilar información más detallada sobre la interfaz:

- **show interfaces**- Muestra la información de la interfaz y el recuento de flujo de paquetes para todas las interfaces en el dispositivo.
- **show ip interface** y **show ipv6 interface** - Muestra la información relacionada con IPv4 e IPv6 para todas las interfaces en un router.

```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
description Link to LAN 1
ip address 192.168.10.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

Verificar las redes conectadas directamente

Verificar rutas

La salida de los comandos **show ip route** y **show ipv6 route** revelan las tres entradas de red conectadas directamente y las tres entradas de interfaz de ruta de host local, como se muestra en el ejemplo.

La ruta de host local tiene una distancia administrativa de 0. También tiene una máscara /32 para IPv4 y una máscara /128 para IPv6. La ruta del host local es para rutas en el router que posee la dirección IP. Estas se usan para permitir que el router procese los paquetes destinados a esa dirección IP.



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C  2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C  2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
C  2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/1/0, directly connected
L  2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/1/0, receive
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

Verificar redes conectadas directamente

Verificar rutas (Cont.)

Una ‘C’ junto a una ruta dentro de la tabla de enrutamiento indica que se trata de una red conectada directamente. Cuando la interfaz del router está configurada con una dirección de unidifusión global y está en el estado “up / up”, el prefijo IPv6 y la longitud del prefijo se agregan a la tabla de enrutamiento IPv6 como una ruta conectada.

La dirección de unidifusión global IPv6 aplicada a la interfaz también se instala en la tabla de enrutamiento como una ruta local. La ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente los paquetes cuyo destino es la dirección de la interfaz del router.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
Gateway of last resort is not set

 192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L   192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
 192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L   192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.224/30 is directly connected, Serial0/1/0
L   209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C  2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C  2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
C  2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/1/0, directly connected
L  2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/1/0, receive
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

Filtrar los resultados del comando show

Los comandos que generan varias pantallas de resultados se pausan al cabo de 24 líneas de manera predeterminada. Al final del resultado detenido, se muestra el texto --More--. Si presiona **Enter**, se muestra la siguiente línea, y si presiona la barra espaciadora, se muestra el siguiente grupo de líneas. Utilice el comando **terminal length** para especificar la cantidad de líneas que se muestran. Un valor 0 (cero) evita que el router haga una pausa entre las pantallas de resultados.

Otra característica muy útil que mejora la experiencia del usuario en la CLI es el filtrado de salida del comando **show**. Los comandos de filtrado se pueden utilizar para mostrar secciones específicas de los resultados. Para habilitar el comando de filtrado, introduzca una barra vertical (|) después del comando **show** y, a continuación, introduzca un parámetro de filtrado y una expresión de filtrado.

Hay cuatro parámetros de filtrado que se pueden configurar después del pipe:

- section - Muestra la sección completa que comienza con la expresión de filtrado.
- include - Incluye todas las líneas de resultados que coinciden con la expresión de filtrado.
- exclude - Excluye todas las líneas de resultados que coinciden con la expresión de filtrado.
- begin: Muestra todas las líneas de resultados desde determinado punto, comenzando por la línea que coincide con la expresión de filtrado.

Función de historial de comandos

La función de historial de comandos es útil porque almacena temporalmente la lista de comandos ejecutados para recuperar.

- Para recuperar los comandos en el búfer de historial, presione **Ctrl+P** o la tecla de **Up Arrow**. El resultado de los comandos comienza con el comando más reciente. Repita la secuencia de teclas para recuperar sucesivamente los comandos más antiguos. Para volver a los comandos más recientes en el búfer de historial, presione **Ctrl+N** o la tecla **Down Arrow**. Repita la secuencia de teclas para recuperar sucesivamente los comandos más recientes.
- De manera predeterminada, el historial de comandos está habilitado, y el sistema captura las últimas 10 líneas de comandos en el búfer de historial. Utilice el comando **show history** para mostrar el contenido del búfer.
- También es práctico aumentar la cantidad de líneas de comandos que registra el búfer de historial solamente durante la sesión de terminal actual. Utilice el comando **terminal history size** el modo EXEC del usuario para aumentar o reducir el tamaño del búfer.

Nuevos términos y comandos de configuración básica del dispositivo

- **boot system flash**
- Alimentación a través de Ethernet (PoE)
- **Desajuste**
- **Velocidad**
- auto-mdix
- **show controllers ethernet controller X**
- **phy**
- **show flash**
- **show history**
- **show ip ssh**
- **ip ssh version 2**
- Interfaz de bucle invertido
- **interface loopback x**
- **include**
- **exclude**
- **sección**
- **show history**
- **terminal history size**



Realiza tus pagos y cobros

ahorita!

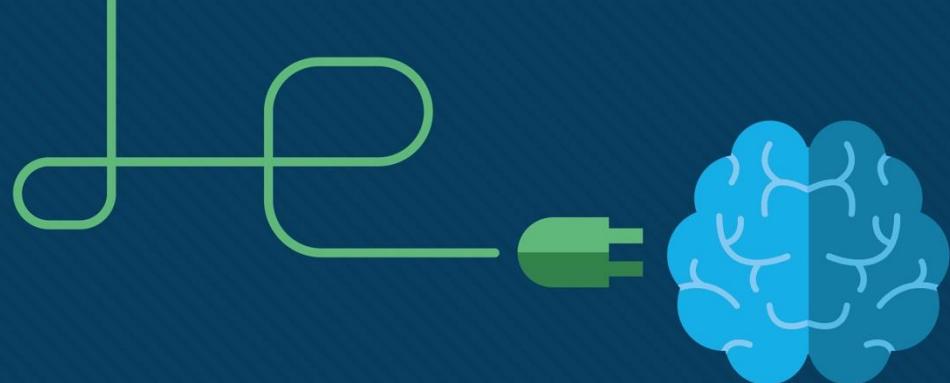


SANCHEZ GONZAGA GIANFRANCO
MICHAEL

- 1 Abre tu App Banco de Loja
- 2 Elige ahorita!
- 3 Escanea el código
- 4 Ingresa el monto y paga.

Nada
más
fácil.





Módulo 8: SLAAC y DHCPv6

Switching, Routing y Wireless
Essentials (SRWE)



Objetivos del módulo

Título del módulo: SLAAC y DHCPv6

Objetivo del módulo: configurar la asignación dinámica de direcciones en redes IPv6.

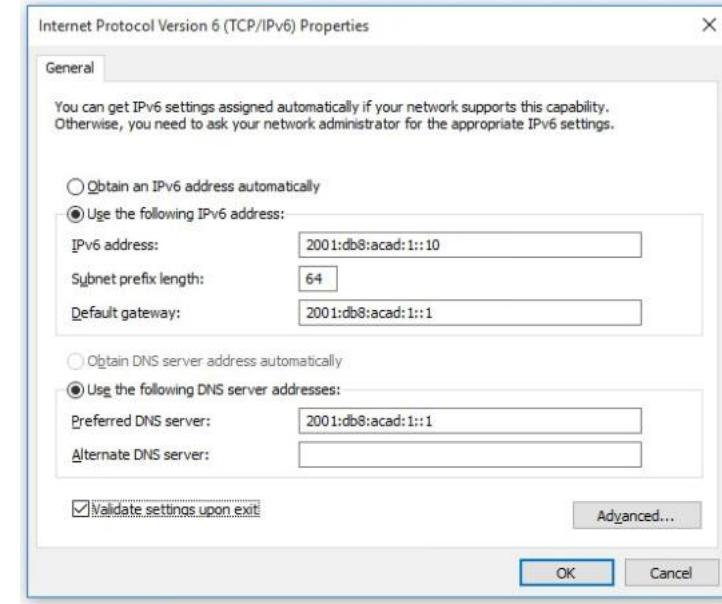
Título del tema	Objetivo del tema
Asignación de direcciones de unidifusión global IPv6	Explicar cómo un host IPv6 puede adquirir su configuración IPv6.
SLAAC	Explicar el funcionamiento de SLAAC.
DHCPv6	Explicar el funcionamiento de DHCPv6.
Configurar servidor DHCPv6	Configurar servidor DHCPv6 stateful y stateless.

8.1 Asignación de GUA IPv6

Configuración de host IPv6

En un router, una dirección global de unidifusión (GUA) **IPv6 se configura manualmente** mediante el comando de *configuración _ipv6-address__prefix-length_ interface*.

- Un host de Windows también se puede configurar manualmente con una configuración de dirección IPv6 GUA, como se muestra en la figura.
- Sin embargo, introducir manualmente una GUA IPv6 puede llevar mucho tiempo y ser algo propenso a errores.
- Por lo tanto, la mayoría de los hosts de Windows están habilitados para adquirir dinámicamente una configuración GUA IPv6.



Dirección local de enlace de host IPv6

Si se selecciona el direccionamiento IPv6 automático, el host utilizará un mensaje de anuncio de enrutador (RA) del protocolo de mensajes de control de Internet versión 6 (ICMPv6) para ayudarle a configurar automáticamente una configuración IPv6.

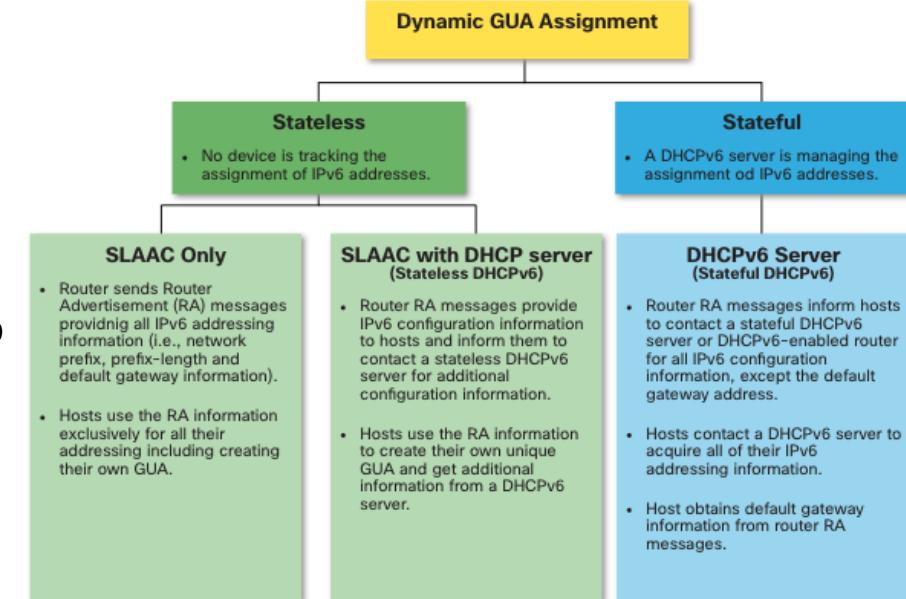
- El host crea automáticamente la dirección local del vínculo IPv6 cuando se inicia y la interfaz Ethernet está activa.
- La interfaz no creó un GUA IPv6 en la salida porque el segmento de red no tenía un enrutador para proporcionar instrucciones de configuración de red para el host.
- **Nota:** El «%» y el número al final de la dirección local del vínculo se conocen como identificador de zona o identificador de ámbito y el sistema operativo utiliza para asociar la LLA a una interfaz específica.
- **Nota:** DHCPv6 se define en RFC 3315.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . :
  IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
  Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
  IPv4 Address . . . . . : 169.254.202.140
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :
C:\>
```

Asignación de IPv6 GUA

De forma predeterminada, un enrutador habilitado para IPv6 envía periódicamente RA ICMPv6, lo que simplifica la forma en que un host puede crear o adquirir dinámicamente su configuración IPv6.

- A un host se le puede asignar dinámicamente un GUA mediante servicios sin estado y con estado.
- Todos los métodos sin estado y con estado de este módulo utilizan mensajes de RA ICMPv6 para sugerir al host cómo crear o adquirir su configuración IPv6.
- Aunque los sistemas operativos del host siguen la sugerencia de la RA, la decisión real depende en última instancia del host

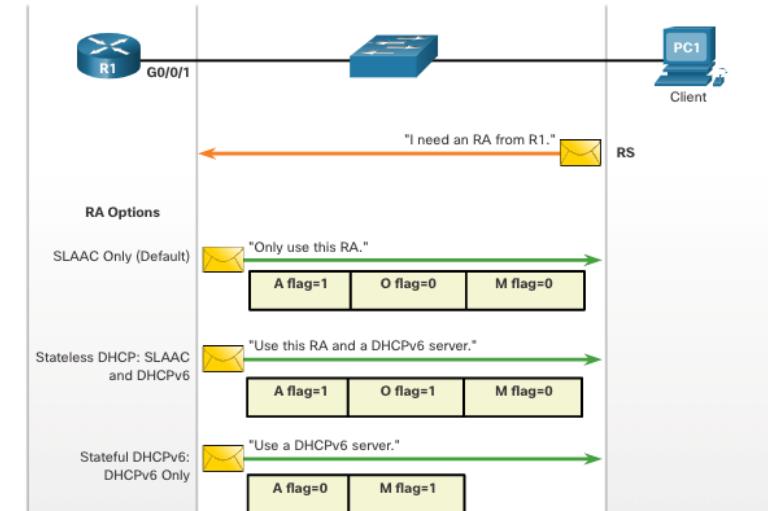


Tres indicadores de mensaje RA

La forma en que un cliente obtiene un GUA IPv6 depende de la configuración del mensaje RA.

Un mensaje de ICMPv6 RA incluye los tres indicadores siguientes:

- **Un indicador (flag):** el indicador de configuración automática de direcciones significa utilizar la configuración automática de direcciones sin estado (SLAAC) para crear un GUA de IPv6
- **El Indicador 0 (flag O)-** El otro indicador de configuración se utiliza para informarle al cliente que hay información adicional disponible de un servidor de DHCPv6 stateless.
- **Indicador M :** el indicador Configuración de dirección administrada significa usar un servidor DHCPv6 con estado para obtener una GUA IPv6.



Mediante diferentes combinaciones de los indicadores A, O y M, los mensajes RA informan al host sobre las opciones dinámicas disponibles.

8.2 SLAAC

Descripción general de SLAAC SLAAC

No todas las redes tienen acceso a un servidor DHCPv6, pero todos los dispositivos de una red IPv6 necesitan un GUA. El método SLAAC permite a los hosts crear su propia dirección única global IPv6 sin los servicios de un servidor DHCPv6.

- SLAAC es un servicio sin estado, lo que significa que no hay ningún servidor que mantenga información de direcciones de red para saber qué direcciones IPv6 se están utilizando y cuáles están disponibles.
- SLAAC envía mensajes periódicos de RA ICMPv6 (es decir, cada 200 segundos) proporcionando direcciones y otra información de configuración para que los hosts configuren automáticamente su dirección IPv6 en función de la información del RA.
- Un host también puede enviar un mensaje de solicitud de enrutador (RS) solicitando una RA.
- SLAAC sólo se puede implementar como SLAAC, o SLAAC con DHCPv6.

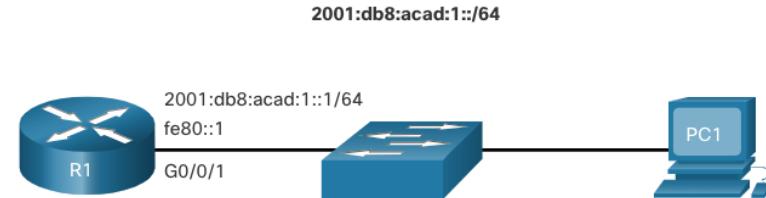
Activación de SLAAC

R1 G0/0/1 se ha configurado con la GUA IPv6 indicada y las direcciones locales de enlace.

Las direcciones IPv6 R1 G0/0/1 incluyen:

- **Link-local IPv6 address** - fe80::1
- **GUA/subred** - 2001:db8:acad:1::1, 2001:db8:acad:1::/64
- **Grupo de todos los nodos IPv6** - ff02::1

R1 está configurado para unirse al grupo de multidifusión IPv6 y comenzar a enviar mensajes RA que contienen información de configuración de direcciones a hosts que utilizan SLAAC.



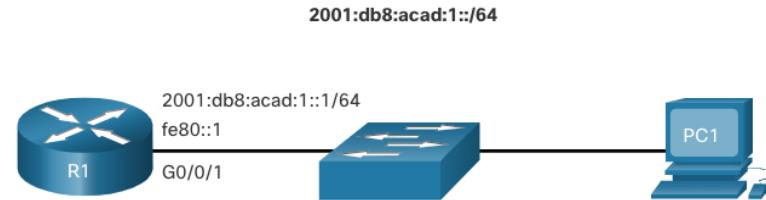
```
R1# show ipv6 interface G0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
  (output omitted)
R1#
```

```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
```

Activación de SLAAC (cont.)

El grupo de todos los routers IPv6 responde a la dirección de multidifusión IPv6 ff02 :: 2.

- El comando **show ipv6 interface** verifica que R1 se haya unido al grupo de todos los routers IPv6 (es decir, ff02::2).
- R1 comenzará ahora a enviar mensajes de RA cada 200 segundos a la dirección de multidifusión IPv6 de todos los nodos ff02::1.

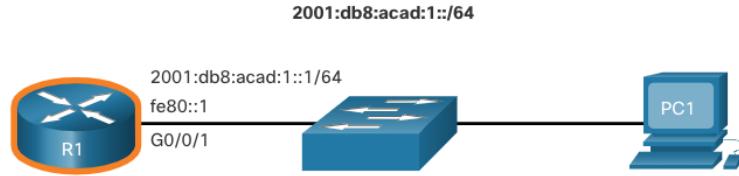


```
R1# show ipv6 interface G0/0/1 | section Joined
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
R1#
```

Método SLAAC SLAAC

Los mensajes RA de R1 tienen los siguientes indicadores establecidos:

- **A = 1**: informa al cliente que use el prefijo IPv6 GUA en la RA y cree dinámicamente su propio ID de interfaz.
- **O = 0 y M = 0**: informa al cliente que utilice también la información adicional en el mensaje RA (es decir, servidor DNS, MTU e información de puerta de enlace predeterminada).
- El comando **ipconfig** Windows confirma que PC1 ha generado un GUS IPv6 utilizando el RA R1.
- La dirección de puerta de enlace predeterminada es LLA de la interfaz R1 G0/0/1.



RA Message	
Flag	value
A	1
O	0
M	0

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
  Link-local IPv6 Address . . . . : fe80::fb:1d54:839f:f595%21
  IPv4 Address. . . . . : 169.254.202.140
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : fe80::1%6
C:\>
```

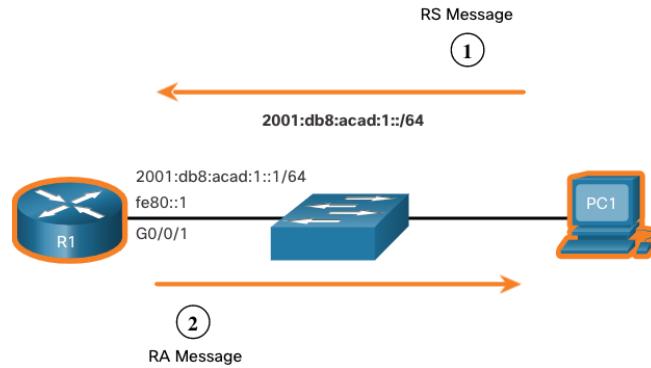
Mensajes SLAAC ICMPv6 RS

Un router envía mensajes RA cada 200 segundos o cuando recibe un mensaje RS de un host.

- Los hosts habilitados para IPv6 que deseen obtener información de direccionamiento IPv6 envían un mensaje RS a la dirección de multidifusión de IPv6 para todos los routers ff02::2.

La figura ilustra cómo un host inicia el método SLAAC.

- PC1 acaba de arrancar y envía un mensaje RS a la dirección de multidifusión IPv6 de todos los routers ff02::2 solicitando una RA.
- R1 genera un RA y, a continuación, envía el mensaje RA a la dirección de multidifusión IPv6 de todos los nodos ff02::1. PC1 utiliza esta información para crear una GUA IPv6 única.



Proceso de host SLAAC para generar ID de interfaz

Mediante SLAAC, un host adquiere la información de la subred IPv6 de 64 bits del RA del router y debe generar el identificador de interfaz (ID) de 64 bits restante mediante:

- **De generación aleatoria** - La identificación de la interfaz de 64 bits es generada aleatoriamente por el sistema operativo del cliente. Este es el método utilizado ahora por los hosts de Windows 10.
- **EUI-64** - El host crea un ID de interfaz utilizando su dirección MAC de 48 bits e inserta el valor hexadecimal de fffe en el medio de la dirección. Algunos sistemas operativos utilizan por defecto el ID de interfaz generado aleatoriamente en lugar del método EUI-64, debido a problemas de privacidad. Esto se debe a que EUI-64 utiliza la dirección MAC Ethernet del host para crear el ID de interfaz.

Nota: Windows, Linux y Mac OS permiten al usuario modificar la generación del ID de interfaz para que se genere aleatoriamente o utilice EUI-64.

Detección de direcciones duplicadas

Un host SLAAC puede utilizar el siguiente proceso de detección de direcciones duplicadas (DAD) para asegurarse de que IPv6 GUA es único.

- El host envía un mensaje ICMPv6 Neighbor Solicitation (NS) con una dirección de multidifusión de nodo solicitado especialmente construida que contiene los últimos 24 bits de dirección IPv6 del host.
- Si ningún otro dispositivo responde con un mensaje Neighbor Advertisement (NA), prácticamente se garantiza que la dirección es única y puede ser utilizada por la PC.
- Si el host recibe un NA, entonces la dirección no es única y el host debe generar un nuevo ID de interfaz para utilizarlo.

Nota: DAD realmente no es necesario porque un ID de interfaz de 64 bits proporciona 18 quintillion de posibilidades. Por lo tanto, la posibilidad de una dirección duplicada es remota. Sin embargo, Internet Engineering Task Force (IETF) recomienda que se utilice DAD. Por lo tanto, la mayoría de los sistemas operativos realizan DAD en todas las direcciones de unidifusión IPv6, independientemente de cómo se configure la dirección.

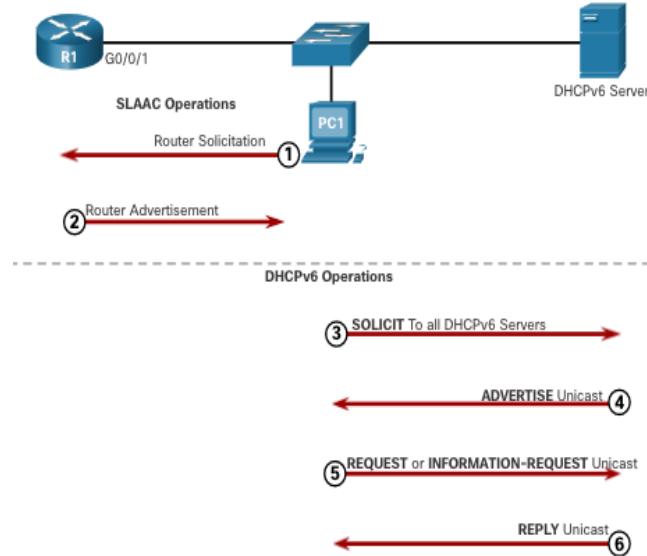
8.3 DHCPv6

Pasos de operación DHCPv6

DHCPv6 con estado no requiere SLAAC mientras que DHCPv6 sin estado lo hace.

Sin embargo, cuando un RA indica que debe usar DHCPv6 o DHCPv6 con estado:

1. El host envía un mensaje RS.
2. El router responde con un mensaje RA.
3. El host envía un mensaje DHCPv6 SOLIT.
4. El servidor DHCPv6 responde con un mensaje ADVERTISE.
5. El host responde al servidor DHCPv6.
6. El servidor DHCPv6 envía un mensaje de respuesta.



Nota: Los mensajes DHCPv6 de servidor a cliente utilizan el puerto de destino UDP 546, mientras que los mensajes DHCPv6 de cliente a servidor utilizan el puerto de destino UDP 547.

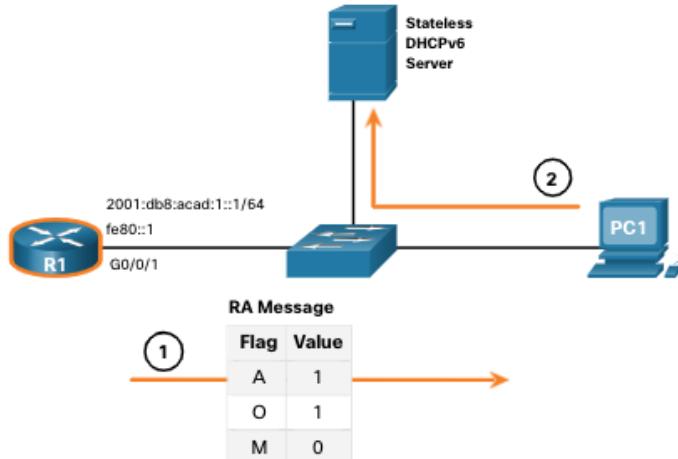
Operación DHCPv6 sin estado DHCPv6

Si un RA indica el método DHCPv6 sin estado, el host utiliza la información del mensaje RA para direccionamiento y se pone en contacto con un servidor DHCPv6 para obtener información adicional.

Nota: El servidor DHCPv6 sólo proporciona parámetros de configuración para clientes y no mantiene una lista de enlaces de direcciones IPv6 (es decir, sin estado).

Por ejemplo, PC1 recibe un mensaje de RA sin estado que contiene:

- El prefijo de red IPv6 GUA y la longitud del prefijo.
- Un indicador establecido en 1 que informa al host de usar SLAAC.
- Indicador O establecido en 1 para informar al host que busque esa información de configuración adicional de un servidor DHCPv6.
- Indicador M establecido en el valor predeterminado 0.
- PC1 envía un mensaje DHCPv6 SOLCIT buscando información adicional de un servidor DHCPv6 sin estado.



Habilitar DHCPv6 sin estado en una interfaz

DHCPv6 sin estado está habilitado mediante el comando de configuración de interfaz **ipv6 nd other-config-flag** estableciendo el indicador O en 1.

La salida resaltada confirma que el RA indicará a los hosts receptores que utilicen autoconfigure sin estado (indicador A = 1) y que se ponga en contacto con un servidor DHCPv6 para obtener otra información de configuración (indicador O = 1).

Nota: Puede utilizar el **indicador no ipv6 nd other-config-flag** para restablecer la interfaz a la opción predeterminada de sólo SLAAC (O flag = 0).

```
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Hosts use DHCP to obtain other configuration.
R1#
```

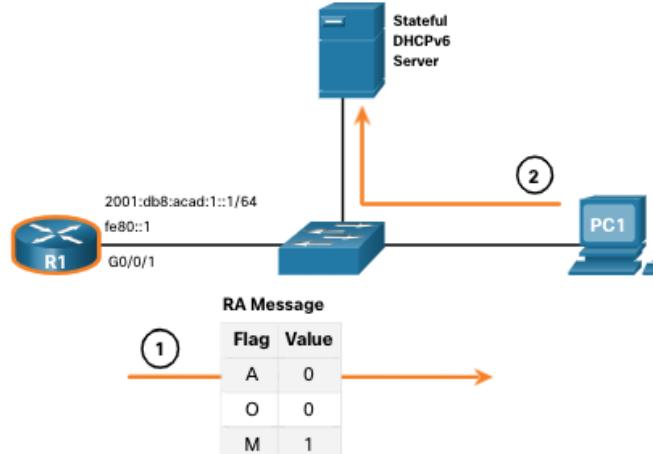
Operación DHCPv6 sin estado

Si un RA indica el método DHCPv6 con estado, el host se pone en contacto con un servidor DHCPv6 para obtener toda la información de configuración.

- **Nota:** El servidor DHCPv6 tiene estado y mantiene una lista de enlaces de direcciones IPv6.

Por ejemplo, PC1 recibe un mensaje de RA con estado que contiene:

- El prefijo de red IPv6 GUA y la longitud del prefijo.
- Indicador establecido en 0 que informa al host de ponerse en contacto con un servidor DHCPv6.
- Indicador O establecido en 0 para informar al host de ponerse en contacto con un servidor DHCPv6.
- Indicador M establecido en el valor 1.
- PC1 envía un mensaje DHCPv6 SOLCIT buscando información adicional de un servidor DHCPv6 con estado.



Habilitar DHCPv6 con estado en una interfaz

DHCPv6 con estado está habilitado mediante el comando de configuración de interfaz **ipv6 nd managed-config-flag**, estableciendo el indicador M en 1.

El resultado resaltado en el ejemplo confirma que RA indicará al host que obtenga toda la información de configuración IPv6 de un servidor DHCPv6 (indicador M = 1).

```
R1(config)# int g0/0/1
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
R1#
```

8.4 Configurar el servidor DHCPv6

Configurar las funciones de enrutador como servidor DHCPv6

Los routers IOS de Cisco son dispositivos potentes. En redes más pequeñas, no es necesario tener dispositivos separados para tener un servidor DHCPv6, un cliente o un agente de retransmisión. Se puede configurar un router Cisco para proporcionar servicios DHCPv6.

Especificamente, se puede configurar para que sea uno de los siguientes:

- **Servidor DHCPv6** - Router proporciona servicios DHCPv6 sin estado o con estado.
- **Cliente DHCPv6** : la interfaz del enrutador adquiere una configuración IP IPv6 de un servidor DHCPv6.
- **Agente de retransmisión DHCPv6** - Router proporciona servicios de reenvío DHCPv6 cuando el cliente y el servidor se encuentran en diferentes redes.

Configurar un servidor DHCPv6 sin estado

La opción de servidor DHCPv6 sin estado requiere que el enrutador anuncie la información de direccionamiento de red IPv6 en los mensajes RA.

Hay cinco pasos para configurar y verificar un enrutador como servidor DHCPv6 sin estado:

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Defina un nombre de grupo DHCPv6 mediante el comando **ipv6 dhcp pool POOL-NAME** global config.
3. Configure el grupo DHCPv6 con opciones. Las opciones comunes incluyen **dns-server X:X:X:X:X:X** y **nombre de dominio** .
4. Enlazar la interfaz al grupo mediante el comando **ipv6 dhcp server POOL-NAME** interface config.
 - El indicador O debe cambiarse de 0 a 1 mediante el comando de interfaz `ipv6 nd other-config-flag`. Los mensajes RA enviados en esta interfaz indican que hay información adicional disponible de un servidor de DHCPv6 sin estado. El indicador A es 1 de forma predeterminada, indicando a los clientes que usen SLAAC para crear su propio GUA.
5. Compruebe que los hosts han recibido información de direccionamiento IPv6 mediante el comando **ipconfig /all** .

Configurar un cliente DHCPv6 sin estado

Un enrutador también puede ser un cliente DHCPv6 y obtener una configuración IPv6 de un servidor DHCPv6, como un enrutador que funcione como servidor DHCPv6.

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Configure el enrutador cliente para crear una LLA. Una dirección local de vínculo IPv6 se crea en una interfaz de enrutador cuando se configura una dirección de unidifusión global, o sin una GUA mediante el comando de configuración de interfaz **ipv6 enable**. Cisco IOS utiliza EUI-64 para crear el ID de interfaz.
3. Configure el enrutador cliente para que utilice SLAAC mediante el comando **ipv6 address autoconfig**.
4. Compruebe que el router cliente tiene asignado un GUA mediante el comando **show ipv6 interface brief**.
5. Verifique que el enrutador cliente haya recibido otra información DHCPv6 necesaria. El comando **show ipv6 dhcp interface g0/0/1** confirma que el cliente ha recibido información de opciones DHCP, como el servidor DNS y el nombre de dominio.

Configurar un servidor DHCPv6 con estado

La opción de servidor DHCP con estado requiere que el enrutador habilitado para IPv6 indique al host que se ponga en contacto con un servidor DHCPv6 para obtener toda la información de direccionamiento de red IPv6 necesaria.

Hay cinco pasos para configurar y verificar un enrutador como un servidor DHCPv6 con estado:

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Defina un nombre de grupo DHCPv6 mediante el comando **ipv6 dhcp pool POOL-NAME** global config.
3. Configure el grupo DHCPv6 con opciones. Las opciones comunes incluyen el comando **address prefix** , el nombre de dominio, la dirección IP del servidor DHS y más.
4. Enlazar la interfaz al grupo mediante el comando **ipv6 dhcp server POOL-NAME interface config**.
 - El indicador O debe cambiarse de 0 a 1 mediante el comando de interfa **ipv6 nd other-config-flag**.
 - Cambie manualmente el indicador A de 1 a 0 mediante el comando **ipv6 nd prefix default no-autoconfig** interface para informar al cliente de que no utilice SLAAC para crear un GUA. El router responde a las solicitudes de DHCPv6 con la información incluida en el pool.
5. Compruebe que los hosts han recibido información de direccionamiento IPv6 mediante el comando **ipconfig /all** .

Configurar un cliente DHCPv6 con estado

Un router también puede ser un cliente DHCPv6. El enrutador cliente debe tener habilitado el enrutamiento **unicast-routing ipv6** y una dirección local de enlace IPv6 para enviar y recibir mensajes IPv6.

Hay cinco pasos para configurar y verificar un enrutador como cliente DHCPv6 sin estado.

1. Habilite el routing IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.
2. Configure el router cliente para crear una LLA. Una dirección local de vínculo IPv6 se crea en una interfaz de enrutador cuando se configura una dirección de unidifusión global, o sin una GUA mediante el comando de configuración de interfaz **ipv6 enable**. Cisco IOS utiliza EUI-64 para crear un ID de interfaz.
3. Configure el enrutador cliente para que utilice DHCPv6 mediante el comando **ipv6 address dhcp interface config**.
4. Compruebe que el router cliente tiene asignado un GUA mediante el comando **show ipv6 interface brief**.
5. Compruebe que el router cliente recibió otra información DHCPv6 necesaria mediante el comando **show ipv6 dhcp interface g0/0/1**.

Comandos de verificación del servidor DHCPv6

En la figura 1 el comando **show ipv6 dhcp pool** verifica el nombre del pool de DHCPv6 y sus parámetros. El comando también identifica el número de clientes activos.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:ACAD:1::/64 valid 172800 preferred 86400 (2 in use, 0
  conflicts)
    DNS server: 2001:4860:4860::8888
    Domain name: example.com
    Active clients: 2
R1#
```

Comandos de verificación del servidor DHCPv6 (cont.)

Utilice el resultado del comando **show ipv6 dhcp binding** para mostrar la dirección local del vínculo IPv6 del cliente y la dirección de unidifusión global asignada por el servidor.

- Esta información la mantiene un servidor de DHCPv6 stateful.
- Un servidor DHCPv6 sin estado no mantendría esta información.

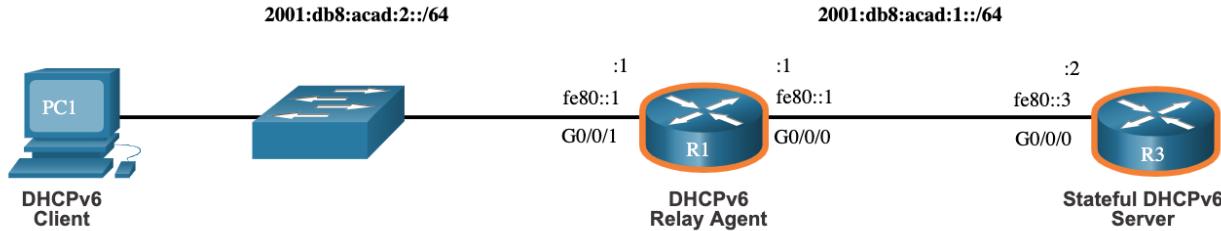
```
R1# show ipv6 dhcp binding
Client: FE80::192F:6FBC:9DB:B749
    DUID: 0001000125148183005056B327D6
    Username : unassigned
    VRF : default
    IA NA: IA ID 0x03000C29, T1 43200, T2 69120
        Address: 2001:DB8:ACAD:1:A43C:FD28:9D79:9E42
                    preferred lifetime 86400, valid lifetime 172800
                    expires at Sep 27 2019 09:10 AM (171192 seconds)
Client: FE80::2FC:BAFF:FE94:29B1
    DUID: 0003000100FCBA9429B0
    Username : unassigned
    VRF : default
    IA NA: IA ID 0x00060001, T1 43200, T2 69120
        Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C
                    preferred lifetime 86400, valid lifetime 172800
                    expires at Sep 27 2019 09:29 AM (172339 seconds)
```

R1#

Configurar un agente de retransmisión DHCPv6

Si el servidor de DHCPv6 está ubicado en una red distinta de la del cliente, el router IPv6 puede configurarse como agente de retransmisión DHCPv6.

- La configuración de un agente de retransmisión DHCPv6 es similar a la configuración de un router IPv4 como retransmisor DHCPv4.
- Este comando se configura en la interfaz que enfrenta a los clientes DHCPv6 y especifica la dirección del servidor DHCPv6 y la interfaz de salida para llegar al servidor, como se muestra en la salida. La interfaz de salida sólo es necesaria cuando la dirección de salto siguiente es una LLA.



```
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 dhcp relay destination 2001:db8:acad:1::2 G0/0/0
R1(config-if)# exit
R1(config)#
```

Verificar el agente de retransmisión DHCPv6

Compruebe que el agente de retransmisión DHCPv6 esté operativo con los comandos **show ipv6 dhcp interface** y **show ipv6 dhcp binding**.

```
R1# show ipv6 dhcp interface
GigabitEthernet0/0/1 is in relay mode
Relay destinations:
  2001:DB8:ACAD:1::2
  2001:DB8:ACAD:1::2 via GigabitEthernet0/0/0
R1#
```

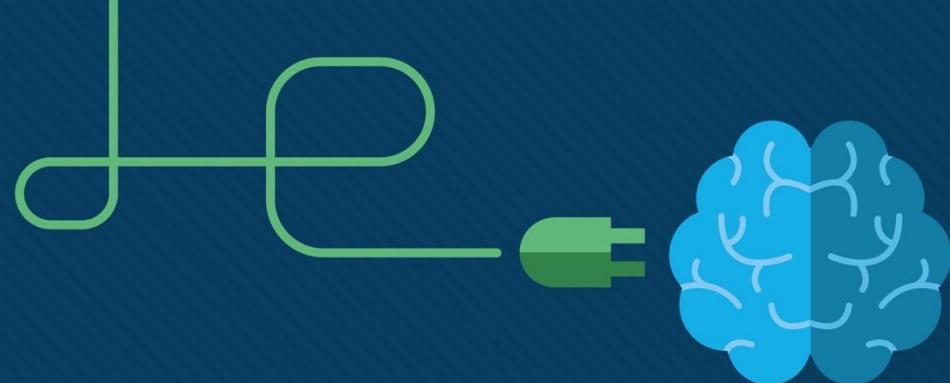
```
R3# show ipv6 dhcp binding
Client: FE80::5C43:EE7C:2959:DA68
DUID: 0001000124F5CEA2005056B3636D
Username : unassigned
VRF : default
IA NA: IA ID 0x03000C29, T1 43200, T2 69120
Address: 2001:DB8:ACAD:2:9C3C:64DE:AADA:7857
        preferred lifetime 86400, valid lifetime 172800
        expires at Sep 29 2019 08:26 PM (172710 seconds)
R3#
```

Compruebe que los hosts de Windows hayan recibido información de direccionamiento IPv6 con el comando **ipconfig /all**.

New Terms and Commands

- | | |
|---|--|
| <ul style="list-style-type: none">• Stateless Address Autoconfiguration (SLAAC)• Global Unicast Address (GUA)• Link Local Address (LLA)• Zone ID• Scope ID• Address Autoconfiguration Flag• Other Configuration Flag• Managed Address Configuration Flag• Router Solicitation (RS)• Router Advertisement (RA)• ipv6 unicast-routing• EUI-64• Duplicate Address Detection (DAD)• Neighbor Solicitation (NS)• Neighbor Advertisement (NA)• DHCPv6 SOLICIT• DHCPv6 ADVERTISE• DHCPv6 REPLY | <ul style="list-style-type: none">• Stateless DHCPv6 Client• Stateful DHCPv6 Client• ipv6 nd other-config-flag• ipv6 nd managed-config-flag• DHCPv6 Relay Agent• ipv6 dhcp pool pool-name• ipv6 dhcp server pool-name• ipv6 enable• ipv6 address autoconfig• show ipv6 dhcp interface• address prefix X:X:X:X:X:X:X:YY• dns-server X:X:X:X:X:X:X:X• domain-name name• ipv6 nd prefix default no-autoconfig• ipv6 address dhcp• show ipv6 dhcp pool• show ipv6 dhcp binding• ipv6 dhcp relay destination ipv6-address [interface-type interface-number] |
|---|--|





Módulo 7: DHCPv4

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



Objetivos del módulo

Título del módulo: DHCPv4

Objetivo del módulo: Implemente DHCPv4 para operar en varias LAN.

Título del tema	Objetivo del tema
Conceptos DHCP4	Explicar la forma en la que funciona DHCPv4 en la red de una pequeña o mediana empresa.
Configurar un servidor DHCP4 del IOS de Cisco	Configurar un router como servidor DHCPv4.
Configurar un cliente DHCP4	Configurar un router como cliente DHCPv4.

7.1 Conceptos DHCPv4

Conceptos DHCPv4

Servidor y cliente

- Dynamic Host Configuration Protocol v4 (DHCPv4) asigna direcciones IPv4 y otra información de configuración de red dinámicamente. Dado que los clientes de escritorio suelen componer gran parte de los nodos de red, DHCPv4 es una herramienta extremadamente útil para los administradores de red y que ahorra mucho tiempo.
- Un servidor de DHCPv4 dedicado es escalable y relativamente fácil de administrar. Sin embargo, en una sucursal pequeña o ubicación SOHO, se puede configurar un router Cisco para proporcionar servicios DHCPv4 sin necesidad de un servidor dedicado. El software Cisco IOS admite un servidor DHCPv4 con funciones completas opcional.

Servidor y cliente (Cont.)

- El servidor DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.
- Los clientes arriendan la información del servidor durante un período definido administrativamente. Los administradores configuran los servidores de DHCPv4 para establecer los arrendamientos, a fin de que caduquen a distintos intervalos. El arrendamiento típicamente dura de 24 horas a una semana o más. Cuando caduca el arrendamiento, el cliente debe solicitar otra dirección, aunque generalmente se le vuelve a asignar la misma.

Conceptos DHCPv4

OperaciónDHCPv4

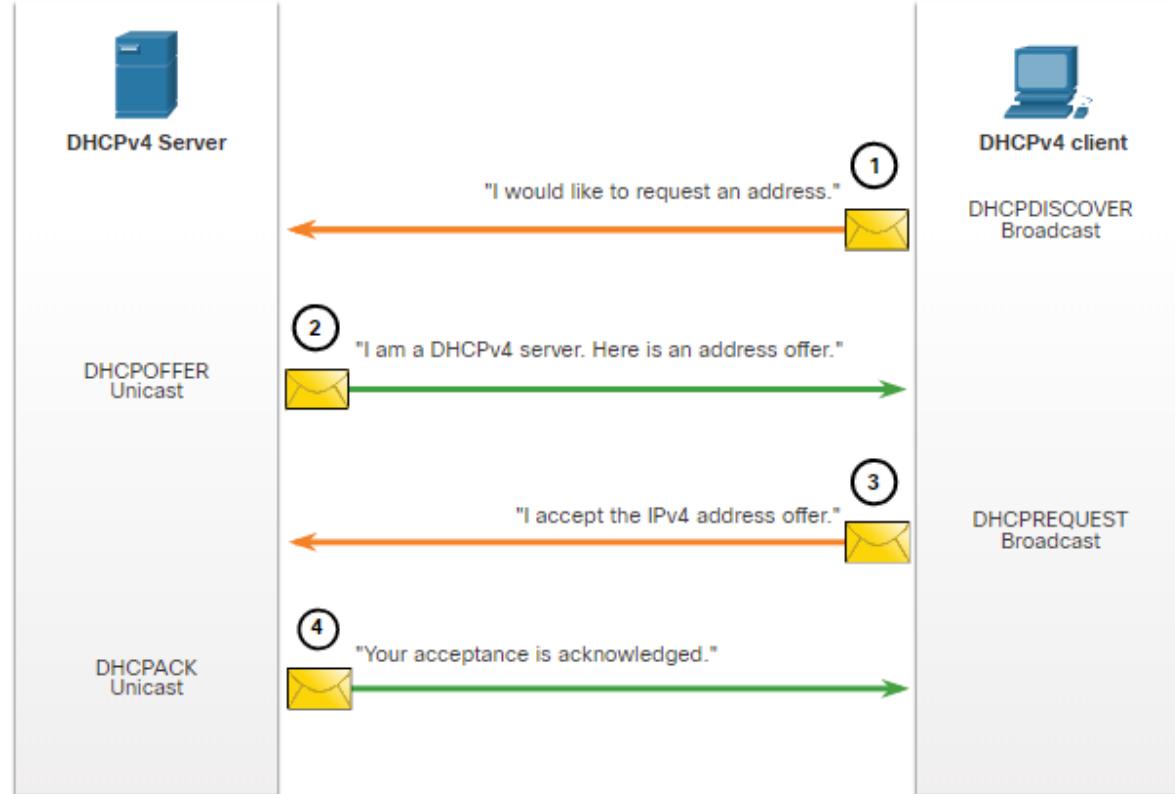
DHCPv4 funciona en un modo cliente/servidor. Cuando un cliente se comunica con un servidor de DHCPv4, el servidor asigna o arrienda una dirección IPv4 a ese cliente.

- El cliente se conecta a la red con esa dirección IPv4 arrendada hasta que caduque el arrendamiento. El cliente debe ponerse en contacto con el servidor de DHCP periódicamente para extender el arrendamiento.
- Este mecanismo de arrendamiento asegura que los clientes que se trasladan o se desconectan no mantengan las direcciones que ya no necesitan.
- Cuando caduca un arrendamiento, el servidor de DHCP devuelve la dirección al conjunto, donde se puede volver a asignar según sea necesario.

Pasos para obtener una concesión

Cuando el cliente arranca (o quiere unirse a una red), comienza un proceso de cuatro pasos para obtener un arrendamiento:

- 1. Detección de DHCP (DHCPDISCOVER)**
- 2. Oferta de DHCP (DHCPOFFER)**
- 3. Solicitud de DHCP (DHCPREQUEST)**
- 4. Acuse de recibo de DHCP (DHCPACK)**



Pasos para renovar una concesión

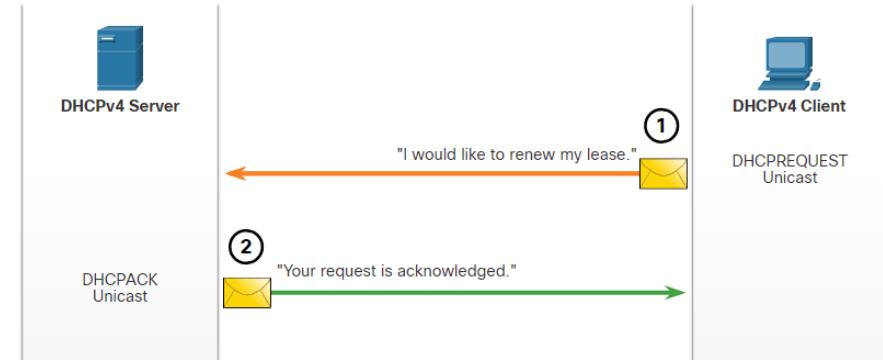
Antes de la expiración de la concesión, el cliente inicia un proceso de dos pasos para renovar la concesión con el servidor DHCPv4, como se muestra en la figura:

1. Solicitud de DHCP (DHCPREQUEST)

Antes de que caduque el arrendamiento, el cliente envía un mensaje DHCPREQUEST directamente al servidor de DHCPv4 que ofreció la dirección IPv4 en primera instancia. Si no se recibe un mensaje DHCPACK dentro de una cantidad de tiempo especificada, el cliente transmite otro mensaje DHCPREQUEST de modo que uno de los otros servidores de DHCPv4 pueda extender el arrendamiento.

2. Acuse de recepción de DHCP (DHCPACK)

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento al devolver un DHCPACK.



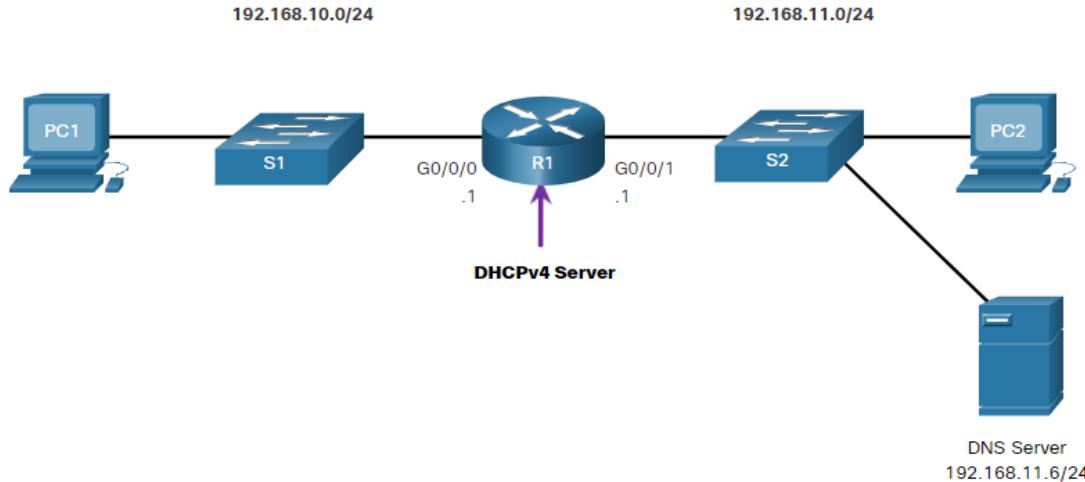
Nota: Estos mensajes (principalmente DHCPOFFER y DHCPACK) se pueden enviar como unidifusión o difusión según la IETF RFC 2131.

7.2 Configurar un servidor DHCPv4 del IOS de Cisco

Configurar un servidor DHCPv4 del IOS de Cisco

Servidor DHCPv4

Ahora usted tiene una comprensión básica de cómo funciona DHCPv4 y cómo puede hacer su trabajo un poco más fácil. Un router Cisco que ejecuta el software IOS de Cisco puede configurarse para que funcione como servidor de DHCPv4. El servidor de DHCPv4 que utiliza IOS de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4.



Pasos para configurar un servidor DHCPv4 de Cisco IOS

Utilice los siguientes pasos para configurar un servidor DHCPv4 del IOS de Cisco:

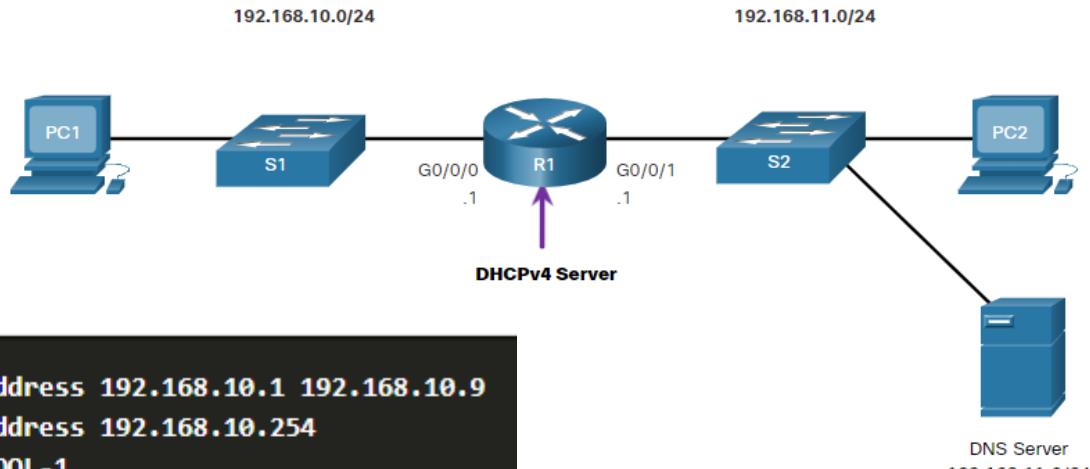
- **Paso 1.** Excluir direcciones IPv4 Se puede excluir una única dirección o un rango de direcciones especificando la *dirección más baja* y la *dirección más alta* del rango. Las direcciones excluidas deben incluir las direcciones asignadas a los routers, a los servidores, a las impresoras y a los demás dispositivos que se configuraron o se configurarán manualmente. También puede introducir el comando varias veces. El comando es **ip dhcp excluded-address *low-address [high-address]***
- **Paso 2.** Defina un nombre de grupo DHCPv4. El comando **ip dhcp pool *pool-name*** crea un conjunto con el nombre especificado y coloca al router en el modo de configuración de DHCPv4, que se identifica con el indicador **Router(dhcp-config)#[**.

Pasos para configurar un servidor DHCPv4 de Cisco IOS (Cont.)

- Paso 3.** Configure el grupo DHCPv4. El conjunto de direcciones y el router de gateway predeterminado deben estar configurados. Utilice la instrucción **network** para definir el rango de direcciones disponibles. Utilice el comando **default-router** para definir el router de gateway predeterminado. Estos comandos y otros comandos opcionales se muestran en la tabla.

Tarea	Comando de IOS
Definir el conjunto de direcciones.	<code>network network-number [mask /prefix-length]</code>
Definir el router o gateway predeterminado.	<code>default-router address [address2...address8]</code>
Definir un servidor DNS.	<code>dns-server address [address2...address8]</code>
Definir el nombre de dominio.	<code>domain-name domain</code>
Definir la duración de la concesión DHCP.	<code>lease {days [hours [minutes]] infinite}</code>
Definir el servidor WINS con NetBIOS.	<code>netbios-name-server address [address2...address8]</code>

Ejemplo de configuración de servidor DHCPv4 de Cisco IOS



```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

DNS Server
192.168.11.6/24

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique que DHCPv4 esté activo

Utilice los comandos de la tabla para verificar que el servidor DHCPv4 del IOS de Cisco esté operativo.

Comando	Descripción
show running-config section dhcp	Muestra los comandos DHCPv4 configurados en el router.
show ip dhcp binding	Muestra una lista de todos los enlaces de dirección IPv4 a dirección MAC proporcionadas por el servicio de DHCPv4.
show ip dhcp server statistics	Muestra información relacionada al numero de mensajes DHCPv4 que han sido mandados y recibidos.

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique la configuración DHCPv4

Como se muestra en el ejemplo, la salida del comando **show running-config | section dhcp** muestra los comandos DHCPv4 configurados en R1. El parámetro **| section** muestra solamente los comandos asociados a la configuración de DHCPv4.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 192.168.11.5
  domain-name example.com
```

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique los enlaces DHCPv4

Como se muestra en el ejemplo, el funcionamiento de DHCPv4 se puede verificar utilizando el comando **show ip dhcp binding**. Este comando muestra una lista de todas las vinculaciones de la dirección IPv4 con la dirección MAC que fueron proporcionadas por el servicio DHCPv4.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration        Type      State       Interface
                  Hardware address/
                  User name
192.168.10.10   0100.5056.b3ed.d8    Sep 15 2019 8:42 AM  Automatic  Active
GigabitEthernet0/0/0
```

Configurar un servidor DHCPv4 del IOS de Cisco

Verifique las estadísticas de DHCPv4

La salida de **show ip dhcp server statistics** es utilizada para verificar que los mensajes están siendo recibidos o enviados por el router. Este comando muestra información de conteo con respecto a la cantidad de mensajes DHCPv4 que se enviaron y recibieron.

```
R1# show ip dhcp server statistics
Memory usage          19465
Address pools          1
Database agents         0
Automatic bindings      2
Manual bindings         0
Expired bindings        0
Malformed messages      0
Secure arp entries      0
Renew messages          0
Workspace timeouts       0
Static routes           0
Relay bindings           0
Relay bindings active     0
Relay bindings terminated   0
Relay bindings selecting    0
Message                Received
BOOTREQUEST              0
DHCPDISCOVER               4
DHCPREQUEST                 2
DHCPDECLINE                  0
DHCPRELEASE                  0
DHCPINFORM                   0
```

Configurar un servidor DHCPv4 del IOS de Cisco

Verificar el direccionamiento IPv4 recibido del cliente DHCPv4

El comando ipconfig /all, cuando se emite en PC1, muestra los parámetros TCP/IP, como se muestra en el ejemplo. Dado que la PC1 se conectó al segmento de red 192.168.10.0/24, recibió automáticamente un sufijo DNS, una dirección IPv4, una máscara de subred, un gateway predeterminado y una dirección del servidor DNS de ese pool. No se requiere ninguna configuración de interfaz del router específica de DHCP. Si una computadora está conectada a un segmento de red que tiene un pool de DHCPv4 disponible, la computadora puede obtener una dirección IPv4 del pool adecuado de manera automática.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration
  Host Name . . . . . : ciscolab
  Primary Dns Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No
  Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . : example.com
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : 00-05-9A-3C-7A-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained . . . . . : Saturday, September 14, 2019 8:42:22AM
    Lease Expires . . . . . : Sunday, September 15, 2019 8:42:22AM
    Default Gateway . . . . . : 192.168.10.1
    DHCP Server . . . . . : 192.168.10.1
    DNS Servers . . . . . : 192.168.11.5
```



Configurar un servidor DHCPv4 del IOS de Cisco

Desactivar el servidor DHCPv4

El servicio DHCPv4 está habilitado de manera predeterminada. Para deshabilitar el servicio, use el comando **no service dhcp** global configuration mode. Utilice el comando del modo de configuración del global **service dhcp** para volver a activar el proceso del servidor de DHCPv4. Si los parámetros no se configuran, active el servicio no tiene ningún efecto.

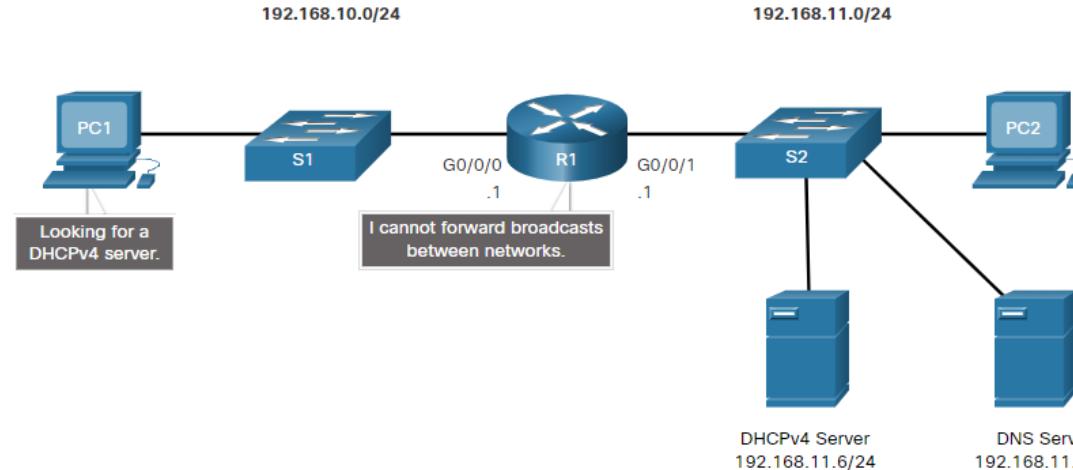
Nota: Si se borra los enlaces DHCP o se detiene y reinicia el servicio DHCP, se pueden asignar direcciones IP duplicadas en la red.

```
R1(config)# no service dhcp  
R1(config)# service dhcp  
R1(config)#{
```

Configurar un servidor DHCPv4 del IOS de Cisco

Relay DHCPv4

- En una red jerárquica compleja, los servidores empresariales suelen estar ubicados en una central. Estos servidores pueden proporcionar servicios DHCP, DNS, TFTP y FTP para la red. Generalmente, los clientes de red no se encuentran en la misma subred que esos servidores. Para ubicar los servidores y recibir servicios, los clientes con frecuencia utilizan mensajes de difusión.
- En la figura, la PC1 intenta adquirir una dirección IPv4 de un servidor de DHCPv4 mediante un mensaje de difusión. En esta situación, el router R1 no está configurado como servidor de DHCPv4 y no reenvía el mensaje de difusión. Dado que el servidor de DHCPv4 está ubicado en una red diferente, la PC1 no puede recibir una dirección IP mediante DHCP. R1 debe configurarse para retransmitir mensajes DHCPv4 al servidor DHCPv4.



Configurar un servidor DHCPv4 del IOS de Cisco Relay DHCPv4

- Configure R1 con el comando de configuración **ip helper-address address interface**. Esto hará que R1 retransmita transmisiones DHCPv4 al servidor DHCPv4. Como se muestra en el ejemplo, la interfaz en R1 que recibe la difusión desde PC1 está configurada para retransmitir la dirección DHCPv4 al servidor DHCPv4 en 192.168.11.6.
- Cuando se configura el R1 como agente de retransmisión DHCPv4, acepta solicitudes de difusión para el servicio DHCPv4 y, a continuación, reenvía dichas solicitudes en forma de unidifusión a la dirección IPv4 192.168.11.6. El administrador de red puede utilizar el comando **show ip interface** para verificar la configuración.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
  (output omitted)
```

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```



Otras transmisiones de servicio retransmitidas

DHCPv4 no es el único servicio que puede configurarse para que retransmita el router. De manera predeterminada, el comando **ip helper-address** reenvía los siguientes ocho siguientes servicios UDP:

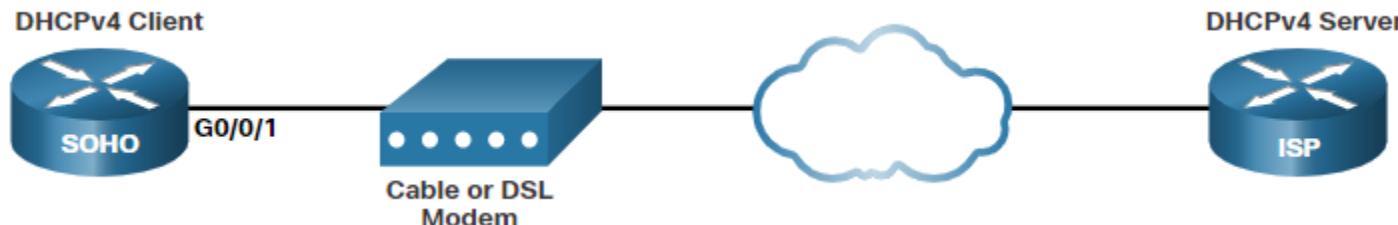
- **Puerto 37:** Tiempo
- **Puerto 49:** TACACS
- **Puerto 53:** DNS
- **Puerto 67:** servidor de DHCP/BOOTP
- **Puerto 68:** cliente DHCP/BOOTP
- **Puerto 69:** TFTP
- **Puerto 137:** servicio de nombres NetBIOS
- **Puerto 138:** servicio de datagrama NetBIOS

7.3 Configurar un cliente DHCPv4

Router Cisco como cliente DHCPv4.

Hay escenarios en los que puede tener acceso a un servidor DHCP a través de su ISP. En estos casos, puede configurar un router Cisco IOS como cliente DHCPv4.

- En ocasiones, los routers Cisco en oficinas pequeñas y oficinas domésticas (SOHO) y en los sitios de sucursales deben configurarse como clientes DHCPv4 de manera similar a los equipos cliente. El método específico utilizado depende del ISP. Sin embargo, en su configuración más simple, se utiliza la interfaz Ethernet para conectarse a un cable módem o a un módem DSL.
- Para configurar una interfaz Ethernet como cliente DHCP, utilice el comando del modo de configuración de interfaz **ip address dhcp**.
- En la figura, suponga que un ISP ha sido configurado para proporcionar a clientes seleccionados direcciones IP del rango de red 209.165.201.0/27 después de que la interfaz G0/0/1 es configurada con el comando **ip address dhcp**.



Ejemplo de Configuración de Cliente DHCPv4

- Para configurar una interfaz Ethernet como cliente DHCP, utilice comando del modo de configuración de interfaz **ip address dhcp** como se muestra en el ejemplo. Esta configuración supone que el ISP se ha configurado para proporcionar a los clientes seleccionados información de direcciones IPv4.
- El comando **show ip interface g0/1** confirma que la interfaz está activa y que la dirección fue asignada por un servidor DHCPv4.

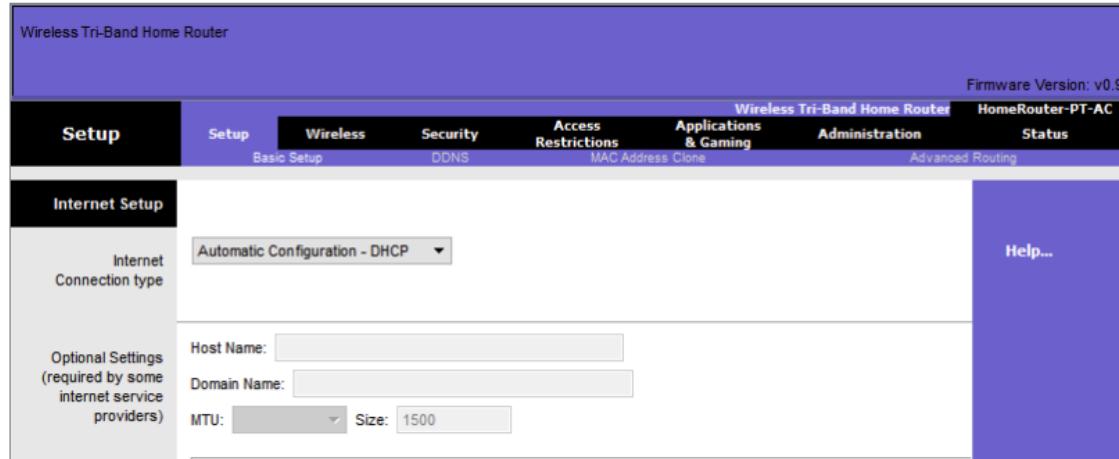
```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address
209.165.201.12, mask 255.255.255.224, hostname SOHO
```

```
SOHO# show ip interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  (output omitted)
```

Router Cisco como cliente DHCPv4.

Los routers de los hogares se configuran para recibir información de asignación de dirección IPv4 automáticamente desde el ISP. Esto es para que los clientes puedan configurar fácilmente el enrutador y conectarse a Internet.

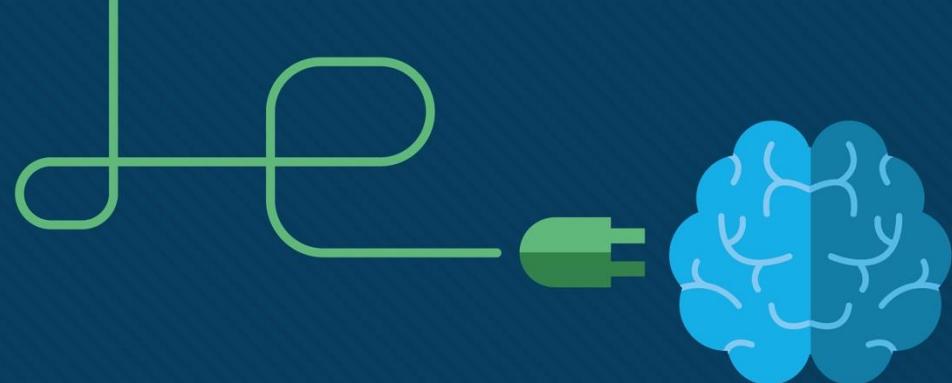
- Por ejemplo, en la ilustración se muestra la página de configuración de WAN predeterminada para un router inalámbrico de Packet Tracer. Notice that the internet connection type is set to **Automatic Configuration - DHCP**. Se utiliza esta selección cuando el router se conecta a un cable módem o DSL y actúa como cliente DHCPv4 y solicita una dirección IPv4 del ISP.
- Varios fabricantes de enrutadores domésticos tendrán una configuración similar.



Nuevos términos y comandos

- Dynamic Host Configuration Protocol (DHCP)
- DHCP Discover (DHCPDISCOVER)
- DHCP Offer (DHCPOFFER)
- DHCP Request (DHCPREQUEST)
- DHCP Acknowledgment (DHCPACK)
- **ip dhcp excluded-address low-address [high-address]**
- **ip dhcp pool name**
- **network network-number [mask | /prefix-length]**
- **default-router address [address2 ... address8]**
- **dns-server address [address2 ... address8]**
- **domain-name domain**
- **lease {days [hours [minutes]] | infinite}**
- **netbios-name-server address [address2 ... address8]**
- **show running-config | section dhcp**
- **show ip dhcp binding**
- **show ip dhcp server statistics**
- **[no] service dhcp**
- **ip helper-address address**
- **ip address dhcp**





Módulo 6: EtherChannel

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



Objetivos del módulo

Título del módulo: EtherChannel

Objetivo del módulo: TResuelva problemas de EtherChannel en enlaces de switches.

Título del tema	Objetivo del tema
Funcionamiento de EtherChannel	Describa la tecnología EtherChannel.
Configuración de EtherChannel	Configure EtherChannel.
Verificación y solución de problemas de EtherChannel	Solucionar problemas de EtherChannel.

6.1 – Funcionamiento de EtherChannel

Funcionamiento de EtherChannel

Etherchannel

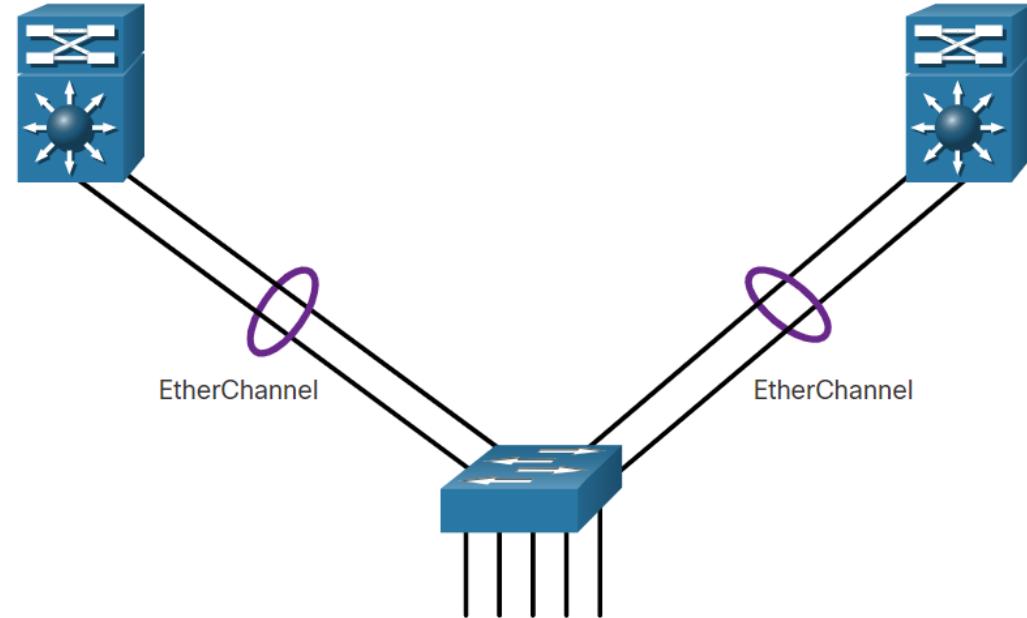
- Hay escenarios en los que se necesita más ancho de banda o redundancia entre dispositivos que lo que puede proporcionar un único enlace. Se pueden conectar varios enlaces entre dispositivos para aumentar el ancho de banda. Sin embargo, el protocolo de árbol de expansión (STP), que está habilitado en dispositivos de capa 2 como switches Cisco de forma predeterminada, bloqueará enlaces redundantes para evitar bucles de conmutación.
- Se necesita una tecnología de agregación de enlaces que permita vínculos redundantes entre dispositivos que no serán bloqueados por STP. Esa tecnología se conoce como EtherChannel.
- EtherChannel es una tecnología de agregación de enlaces que agrupa varios enlaces físicos Ethernet en un único enlace lógico. Se utiliza para proporcionar tolerancia a fallos, uso compartido de carga, mayor ancho de banda y redundancia entre switches, routers y servidores.
- La tecnología de EtherChannel hace posible combinar la cantidad de enlaces físicos entre los switches para aumentar la velocidad general de la comunicación switch a switch.

Funcionamiento de EtherChannel

EtherChannel

En los inicios, Cisco desarrolló la tecnología EtherChannel como una técnica switch a switch LAN para agrupar varios puertos Fast Ethernet o gigabit Ethernet en un único canal lógico.

Cuando se configura un EtherChannel, la interfaz virtual resultante se denomina “canal de puertos”. Las interfaces físicas se agrupan en una interfaz de canal de puertos, como se muestra en la figura.



Ventajas de la operación EtherChannel

La tecnología EtherChannel tiene muchas ventajas, incluidas las siguientes:

- La mayoría de las tareas de configuración se pueden realizar en la interfaz EtherChannel en lugar de en cada puerto individual, lo que asegura la coherencia de configuración en todos los enlaces.
- EtherChannel depende de los puertos de switch existentes. No es necesario actualizar el enlace a una conexión más rápida y más costosa para tener más ancho de banda.
- El equilibrio de carga ocurre entre los enlaces que forman parte del mismo EtherChannel.
- EtherChannel crea una agregación que se ve como un único enlace lógico. Cuando existen varios grupos EtherChannel entre dos switches, STP puede bloquear uno de los grupos para evitar los bucles de switching. Cuando STP bloquea uno de los enlaces redundantes, bloquea el EtherChannel completo. Esto bloquea todos los puertos que pertenecen a ese enlace EtherChannel. Donde solo existe un único enlace EtherChannel, todos los enlaces físicos en el EtherChannel están activos, ya que STP solo ve un único enlace (lógico).
- EtherChannel proporciona redundancia, ya que el enlace general se ve como una única conexión lógica. Además, la pérdida de un enlace físico dentro del canal no crea ningún cambio en la topología.

Funcionamiento de EtherChannel

Restricciones de implementación

EtherChannel tiene ciertas restricciones de implementación, entre las que se incluyen las siguientes:

- No pueden mezclarse los tipos de interfaz. Por ejemplo, Fast Ethernet y Gigabit Ethernet no se pueden mezclar dentro de un único EtherChannel.
- En la actualidad, cada EtherChannel puede constar de hasta ocho puertos Ethernet configurados de manera compatible. El EtherChannel proporciona un ancho de banda full-duplex de hasta 800 Mbps (Fast EtherChannel) u 8 Gbps (Gigabit EtherChannel) entre un switch y otro switch o host.
- El switch Cisco Catalyst 2960 Layer 2 soporta actualmente hasta seis EtherChannels.
- La configuración de los puertos individuales que forman parte del grupo EtherChannel debe ser coherente en ambos dispositivos. Si los puertos físicos de un lado se configuran como enlaces troncales, los puertos físicos del otro lado también se deben configurar como enlaces troncales dentro de la misma VLAN nativa. Además, todos los puertos en cada enlace EtherChannel se deben configurar como puertos de capa 2.
- Cada EtherChannel tiene una interfaz de canal de puertos lógica. La configuración aplicada a la interfaz de canal de puertos afecta a todas las interfaces físicas que se asignan a esa interfaz.

Protocolos de negociación automática

Los EtherChannels se pueden formar por medio de una negociación con uno de dos protocolos: Port Aggregation Protocol (PAgP) o Link Aggregation Control Protocol (LACP). Estos protocolos permiten que los puertos con características similares formen un canal mediante una negociación dinámica con los switches adyacentes.

Nota: también es posible configurar un EtherChannel estático o incondicional sin PAgP o LACP.

Funcionamiento de EtherChannel

Funcionamiento PAgP

PAgP (pronunciado “Pag - P”) es un protocolo patentado por Cisco que ayuda en la creación automática de enlaces EtherChannel. Cuando se configura un enlace EtherChannel mediante PAgP, se envían paquetes PAgP entre los puertos aptos para EtherChannel para negociar la formación de un canal. Cuando PAgP identifica enlaces Ethernet compatibles, agrupa los enlaces en un EtherChannel. El EtherChannel después se agrega al árbol de expansión como un único puerto.

Cuando se habilita, PAgP también administra el EtherChannel. Los paquetes PAgP se envían cada 30 segundos. PAgP revisa la coherencia de la configuración y administra los enlaces que se agregan, así como las fallas entre dos switches. Cuando se crea un EtherChannel, asegura que todos los puertos tengan el mismo tipo de configuración.

Nota: en EtherChannel, es obligatorio que todos los puertos tengan la misma velocidad, la misma configuración de dúplex y la misma información de VLAN. Cualquier modificación de los puertos después de la creación del canal también modifica a los demás puertos del canal.

Operación de EtherChannel PAgP (Cont.)

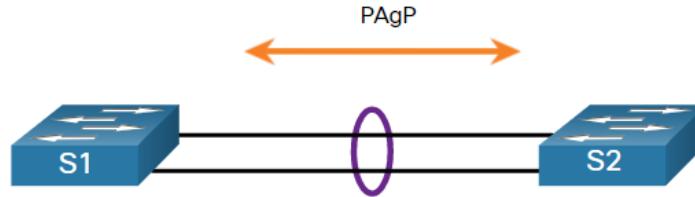
PAgP ayuda a crear el enlace EtherChannel al detectar la configuración de cada lado y asegurarse de que los enlaces sean compatibles, de modo que se pueda habilitar el enlace EtherChannel cuando sea necesario. Los modos de PAgP de la siguiente manera:

- **Encendido:** este modo obliga a la interfaz a proporcionar un canal sin PAgP. Las interfaces configuradas en el modo encendido no intercambian paquetes PAgP.
- **PAgP deseable** - Este modo PAgP coloca una interfaz en un estado de negociación activa en el que la interfaz inicia negociaciones con otras interfaces al enviar paquetes PAgP.
- **PAgP auto** - este modo PAgP coloca una interfaz en un estado de negociación pasiva en el que la interfaz responde a los paquetes PAgP que recibe, pero no inicia la negociación PAgP.

Los modos deben ser compatibles en cada lado. Si se configura un lado en modo automático, se coloca en estado pasivo, a la espera de que el otro lado inicie la negociación del EtherChannel. Si el otro lado se establece en modo automático, la negociación nunca se inicia y no se forma el canal EtherChannel. Si se deshabilitan todos los modos mediante el comando **no** o si no se configura ningún modo, entonces se deshabilita el EtherChannel. El modo encendido coloca manualmente la interfaz en un EtherChannel, sin ninguna negociación. Funciona solo si el otro lado también se establece en modo encendido. Si el otro lado se establece para negociar los parámetros a través de PAgP, no se forma ningún EtherChannel, ya que el lado que se establece en modo encendido no negocia. El hecho de que no haya negociación entre los dos switches significa que no hay un control para asegurarse de que todos los enlaces en el EtherChannel terminen del otro lado o de que haya compatibilidad con PAgP en el otro switch.

Operación de EtherChannel

Ejemplo de configuración del modo PAgP



La tabla muestra las diversas combinaciones de modos PAgP en S1 y S2 y el resultado resultante del establecimiento de canales.

S1	S2	Establecimiento del canal
On	On	Sí
On	Desirable/Auto	No
Desirable	Desirable	Sí
Desirable	Auto	Sí
Auto	Desirable	Sí
Auto	Auto	No

Funcionamiento de EtherChannel

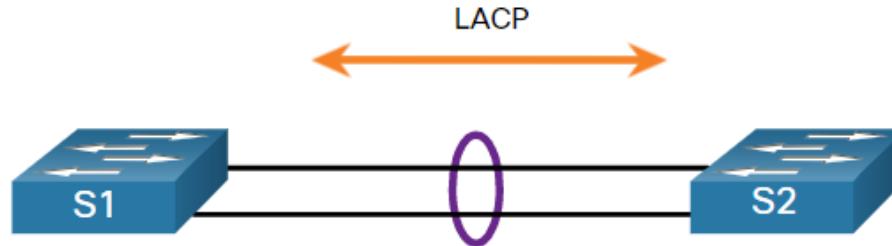
Funcionamiento LACP

LACP forma parte de una especificación IEEE (802.3ad) que permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al otro switch. Realiza una función similar a PAgP con EtherChannel de Cisco. Debido a que LACP es un estándar IEEE, se puede usar para facilitar los EtherChannels en entornos de varios proveedores. En los dispositivos de Cisco, se admiten ambos protocolos.

LACP proporciona los mismos beneficios de negociación que PAgP. LACP ayuda a crear el enlace EtherChannel al detectar la configuración de cada lado y al asegurarse de que sean compatibles, de modo que se pueda habilitar el enlace EtherChannel cuando sea necesario. Los modos para LACP son los siguientes:

- **On** - Este modo obliga a la interfaz a proporcionar un canal sin LACP. Las interfaces configuradas en el modo encendido no intercambian paquetes LACP.
- **LACP active** - Este modo de LACP coloca un puerto en estado de negociación activa. En este estado, el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP.
- **LACP passive** - Este modo de LACP coloca un puerto en estado de negociación pasiva. En este estado, el puerto responde a los paquetes LACP que recibe, pero no inicia la negociación de paquetes LACP.

Ejemplo de configuración del modo LACP



La tabla muestra las diversas combinaciones de modos LACP en S1 y S2 y el resultado resultante del establecimiento de canales.

S1	S2	Establecimiento del canal
On	On	Sí
On	Active/Passive	No
Active	Active	Sí
Active	Passive	Sí
Passive	Active	Sí
Passive	Passive	No

6.2 Configuración de EtherChannel

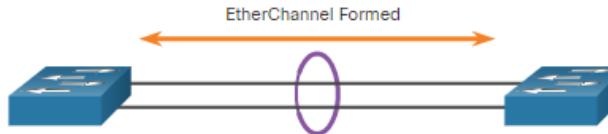
Pautas para la configuración

Las siguientes pautas y restricciones son útiles para configurar EtherChannel:

- **EtherChannel support** - Todas las interfaces Ethernet deben admitir EtherChannel, sin necesidad de que las interfaces sean físicamente contiguas
- **Speed and duplex** - Configure todas las interfaces en un EtherChannel para que funcionen a la misma velocidad y en el mismo modo dúplex.
- **VLAN match** - Todas las interfaces en el grupo EtherChannel se deben asignar a la misma VLAN o se deben configurar como enlace troncal (mostrado en la figura).
- Rango de VLAN: un EtherChannel admite el mismo rango permitido de VLAN en todas las interfaces de un EtherChannel de enlace troncal. Si el rango permitido de VLAN no es el mismo, las interfaces no forman un EtherChannel, incluso si se establecen en modo auto **o desirable** .

Pautas para la configuración (cont.)

- La figura muestra una configuración que permitiría que se forme un EtherChannel entre el S1 y el S2.
- Si se deben modificar estos parámetros, configúrelos en el modo de configuración de interfaz de canal de puertos. Cualquier configuración que se aplique a la interfaz de canal de puertos también afectará a las interfaces individuales. Sin embargo, las configuraciones que se aplican a las interfaces individuales no afectan a la interfaz de canal de puertos. Por ello, realizar cambios de configuración a una interfaz que forma parte de un enlace EtherChannel puede causar problemas de compatibilidad de interfaces.
- El canal de puertos se puede configurar en modo de acceso, modo de enlace troncal (más frecuente) o en un puerto enrutado.



S1 Port Configurations

Speed	1 Gbps
Duplex	Full
VLAN	10

S2 Port Configurations

Speed	1 Gbps
Duplex	Full
VLAN	10

Configuración de EtherChannel

Ejemplo de LACP

La configuración de EtherChannel con LACP requiere tres pasos:

- **Paso 1.** Especifique las interfaces que conforman el grupo EtherChannel mediante el comando **interface range interface** en modo de configuración global. La palabra clave **range** le permite seleccionar varias interfaces y configurarlas a la vez.
- **Paso 2.** Cree la interfaz de canal de puerto con el comando **channel-group identifier mode active** en el modo de configuración de rango de interfaz. El identificador especifica el número del grupo del canal. Las palabras clave **mode active** identifican a esta configuración como EtherChannel LACP.
- **Paso 3.** Para cambiar la configuración de capa 2 en la interfaz de canal de puertos, ingrese al modo de configuración de interfaz de canal de puertos mediante el comando **interface port-channel** seguido del identificador de la interfaz. En el ejemplo, S1 está configurado con un EtherChannel LACP. El canal de puertos está configurado como interfaz de enlace troncal con VLAN permitidas específicas.

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config-if)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```



6.3 – Verificación y solución de problemas de EtherChannel

Verificación y solución de problemas de EtherChannel

Como siempre, al configurar dispositivos en su red, debe verificar su configuración. Si hay problemas, también deberá poder solucionarlos y solucionarlos. Existe una variedad de comandos para verificar una configuración EtherChannel.

- Primero, el comando **show interfaces port-channel** muestra el estado general de la interfaz de canal de puertos.
- El comando **show etherchannel summary** muestra una línea de información por canal de puerto.
- Use el comando **show etherchannel port-channel** para mostrar la información sobre una interfaz de canal de puertos específica.
- Utilice el comando **show interfaces etherchannel** para proporcionar información sobre el rol de la interfaz en EtherChannel.

Verificación y solución de problemas de EtherChannel

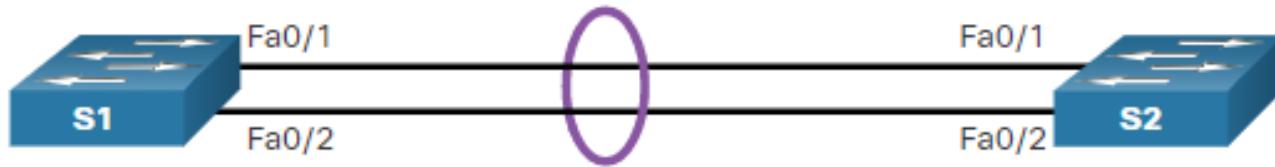
Solución de problemas de EtherChannel

Todas las interfaces dentro de un EtherChannel deben tener la misma configuración de velocidad y modo dúplex, de VLAN nativas y permitidas en los enlaces troncales, y de VLAN de acceso en los puertos de acceso. Garantizar estas configuraciones reducirá significativamente los problemas de red relacionados con EtherChannel. Entre los problemas comunes de EtherChannel se incluyen los siguientes:

- Los puertos asignados en el EtherChannel no son parte de la misma VLAN ni son configurados como enlace troncal. Los puertos con VLAN nativas diferentes no pueden formar un EtherChannel.
- La conexión troncal se configuró en algunos de los puertos que componen el EtherChannel, pero no en todos ellos. No se recomienda que configure el modo de enlace troncal en los puertos individuales que conforman el EtherChannel. Al configurar un enlace troncal en un EtherChannel, compruebe el modo de enlace troncal en EtherChannel.
- Si el rango permitido de VLAN no es el mismo, los puertos no forman un EtherChannel incluso cuando PAgP está configurado en modo **auto** o **desirable** .
- Las opciones de negociación dinámica para PAgP y LACP no se encuentran configuradas de manera compatible en ambos extremos del EtherChannel.

Solución de problemas de EtherChannel (Cont.)

En la figura, las interfaces F0/1 y F0/2 en los switches S1 y S2 se conectan con un EtherChannel. Sin embargo, el EtherChannel no está operativo.



Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

Paso 1. Ver la información de resumen de EtherChannel: la salida del comando show etherchannel summary indica que EtherChannel está inactivado.

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3      L - Layer2
      U - in use      N - not in use, no aggregation
      f - failed to allocate aggregator
      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
      A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group  Port-channel  Protocol    Ports
-----+-----+-----+
 1     Po1(SD)        -       Fa0/1(D)   Fa0/2(D)
```

Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

Paso 2. Ver configuración del canal de puerto: En el **show run | begin interface puerto** salida canal, salida más detallada indica que hay modos PAgP incompatibles configurados en S1 y S2.

```
S1# show run | begin interface port-channel
interface Port-channel1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/2
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode on
=====
S2# show run | begin interface port-channel
interface Port-channel1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/2
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode desirable
```

Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

Paso 3: Corrija la configuración incorrecta: Para corregir el problema, el modo PAgP en el EtherChannel se cambia a deseable.

Nota: EtherChannel y STP deben interoperar. Por este motivo, el orden en el que se introducen los comandos relacionados con EtherChannel es importante, y por ello se puede ver que se quitó el canal de puertos de interfaz1 y después se volvió a agregar con el comando **channel-group** en vez de cambiarse directamente. Si se intenta cambiar la configuración directamente, los errores STP hacen que los puertos asociados entren en estado de bloqueo o errdisabled.

```
S1(config)# no interface port-channel 1
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Verificación y solución de problemas de EtherChannel

Solución de problemas de EtherChannel (Cont.)

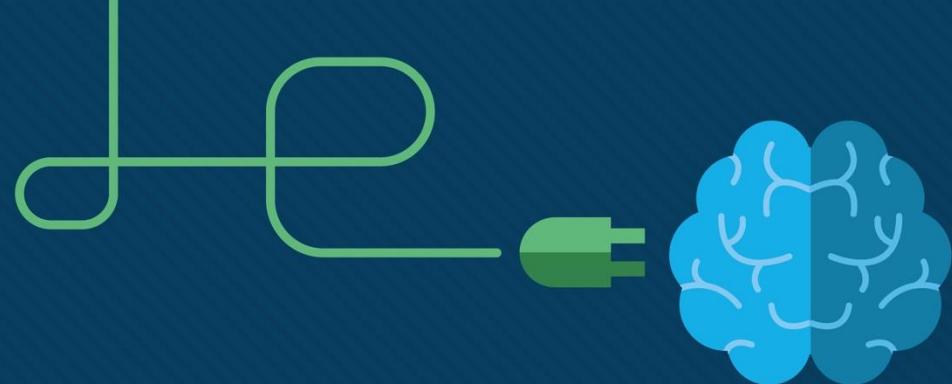
Paso 4. Verifique que EtherChannel esté operativo: el EtherChannel está activo como se ha verificado mediante la salida del comando show etherchannel summary.

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3      S - Layer2
      U - in use       N - not in use, no aggregation
      f - failed to allocate aggregator
      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
      A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1(SU)        PAgP        Fa0/1(P)   Fa0/2(P)
```

Nuevos términos y comandos

- Link Aggregation
- EtherChannel
- Port Channel
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- PAgP desirable
- PAgP auto
- LACP active
- LACP passive
- **channel-group X mode [desirable | auto | active | passive]**
- **interface port-channel X**
- **show interfaces port-channel**
- **show etherchannel summary**
- **show etherchannel port-channel**
- **show interfaces etherchannel**





Módulo 5: Conceptos STP

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



Objetivos del módulo

Título del módulo: Conceptos STP

Objetivo del módulo: Explicar cómo STP permite la redundancia en una red de capa 2.

Título del tema	Objetivo del tema
Propósito del STP	Explique los problemas comunes en una red commutada redundante L2.
Funcionamientos del STP	Explicar cómo opera STP en una red commutada simple.
Evolución del STP	Explique la forma en que funciona PVST+ rápido.

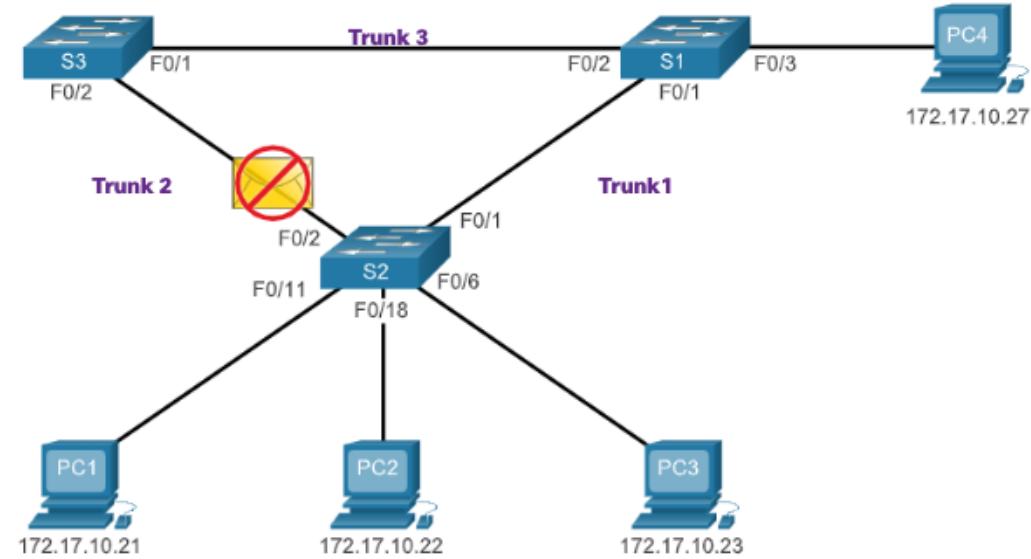
5.1 Propósito de STP

Redundancia en redes conmutadas de capa 2

- En este tema se tratan las causas de los bucles en una red de capa 2 y se explica brevemente cómo funciona el protocolo de árbol de expansión. La redundancia es una parte importante del diseño jerárquico para eliminar puntos únicos de falla y prevenir la interrupción de los servicios de red para los usuarios. Las redes redundantes requieren la adición de rutas físicas, pero la redundancia lógica también debe formar parte del diseño. Tener rutas físicas alternativas para que los datos atraviesen la red permite que los usuarios accedan a los recursos de red, a pesar de las interrupciones de la ruta. Sin embargo, las rutas redundantes en una red Ethernet conmutada pueden causar bucles físicos y lógicos en la capa 2.
- Las LAN Ethernet requieren una topología sin bucles con una única ruta entre dos dispositivos. Un bucle en una LAN Ethernet puede provocar una propagación continua de tramas Ethernet hasta que un enlace se interrumpe y interrumpa el bucle.

Protocolo de árbol de expansión (Spanning Tree Protocol, STP)

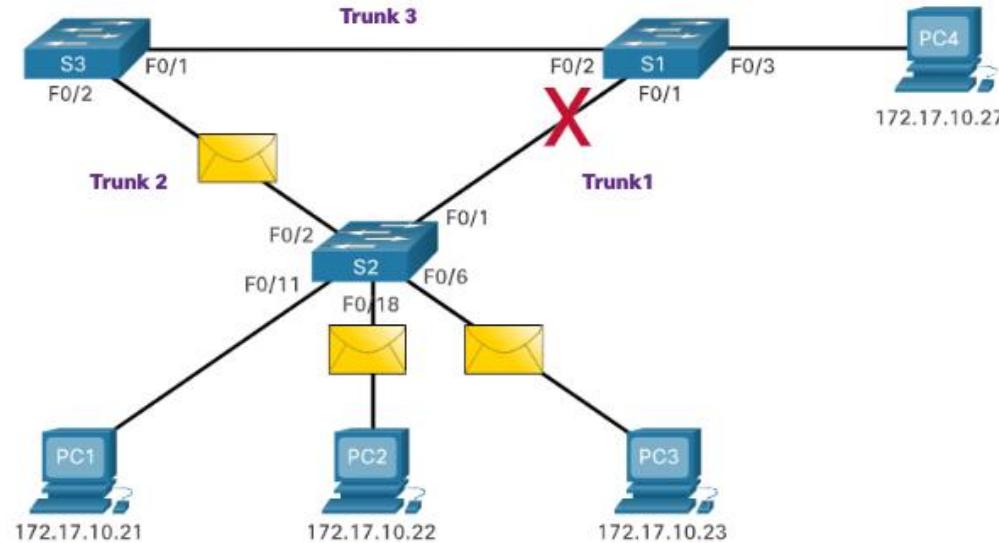
- El protocolo de árbol de expansión (STP) es un protocolo de red de prevención de bucles que permite redundancia mientras crea una topología de capa 2 sin bucles.
- STP bloquea lógicamente los bucles físicos en una red de Capa 2, evitando que las tramas circulen por la red para siempre.



S2 drops the frame because it received it on a blocked port.

Propósito del STP Recálculo STP

STP compensa un error en la red al volver a calcular y abrir los puertos previamente bloqueados.



Problemas con vínculos de switches redundantes

- La redundancia de ruta proporciona múltiples servicios de red al eliminar la posibilidad de un solo punto de falla. Cuando existen múltiples rutas entre dos dispositivos en una red Ethernet, y no hay implementación de árbol de expansión en los switches, se produce un bucle de capa 2. Un bucle de capa 2 puede provocar inestabilidad en la tabla de direcciones MAC, saturación de enlaces y alta utilización de CPU en switch y dispositivos finales, lo que hace que la red se vuelva inutilizable.
- La capa 2 Ethernet no incluye un mecanismo para reconocer y eliminar tramas de bucle sin fin. Tanto IPv4 como IPv6 incluyen un mecanismo que limita la cantidad de veces que un dispositivo de red de Capa 3 puede retransmitir un paquete. Un router disminuirá el TTL (Tiempo de vida) en cada paquete IPv4 y el campo Límite de saltos en cada paquete IPv6. Cuando estos campos se reducen a 0, un router dejará caer el paquete. Los switches Ethernet y Ethernet no tienen un mecanismo comparable para limitar el número de veces que un switch retransmite una trama de Capa 2. STP fue desarrollado específicamente como un mecanismo de prevención de bucles para Ethernet de Capa 2.

Bucles de Capa 2

- Sin STP habilitado, se pueden formar bucles de capa 2, lo que hace que las tramas de difusión, multidifusión y unidifusión desconocidos se reproduzcan sin fin. Esto puede derribar una red rápidamente.
- Cuando se produce un bucle, la tabla de direcciones MAC en un switch cambiará constantemente con las actualizaciones de las tramas de difusión, lo que resulta en la inestabilidad de la base de datos MAC. Esto puede causar una alta utilización de la CPU, lo que hace que el switch no pueda reenviar tramas.
- Una trama de unidifusión desconocida se produce cuando el switch no tiene la dirección MAC de destino en la tabla de direcciones MAC y debe reenviar la trama a todos los puertos, excepto el puerto de ingreso.

Tormenta de difusión (Broadcast Storm)

- Una tormenta de difusión es un número anormalmente alto de emisiones que abruman la red durante un período específico de tiempo. Las tormentas de difusión pueden deshabilitar una red en cuestión de segundos al abrumar los switch y los dispositivos finales. Las tormentas de difusión pueden deberse a un problema de hardware como una NIC defectuosa o a un bucle de capa 2 en la red.
- Las emisiones de capa 2 en una red, como las solicitudes ARP, son muy comunes. Las multidifusión de capa 2 normalmente se reenvían de la misma manera que una difusión por el switch. Los paquetes IPv6 nunca se reenvían como una difusión de Capa 2, ICMPv6 Neighbor Discovery utiliza multidifusión de Capa 2.
- Un host atrapado en un bucle de capa 2 no está accesible para otros hosts en la red. Además, debido a los constantes cambios en su tabla de direcciones MAC, el switch no sabe desde qué puerto reenviar las tramas de unidifusión.
- Para evitar que ocurran estos problemas en una red redundante, se debe habilitar algún tipo de árbol de expansión en los switch. De manera predeterminada, el árbol de expansión está habilitado en los switch Cisco para prevenir que ocurran bucles en la capa 2.

El algoritmo de árbol de expansión (Spanning Tree)

- STP se basa en un algoritmo inventado por Radia Perlman mientras trabajaba para Digital Equipment Corporation, y publicado en el artículo de 1985 "Un algoritmo para la computación distribuida de un árbol de expansión en una LAN extendida". Su algoritmo de árbol de expansión (STA) crea una topología sin bucles al seleccionar un único puente raíz donde todos los demás switch determinan una única ruta de menor costo.
- STP evita que ocurran bucles mediante la configuración de una ruta sin bucles a través de la red, con puertos “en estado de bloqueo” ubicados estratégicamente. Los switch que ejecutan STP pueden compensar las fallas mediante el desbloqueo dinámico de los puertos bloqueados anteriormente y el permiso para que el tráfico se transmita por las rutas alternativas.

El algoritmo de árbol de expansión (cont.)

¿Cómo crea STA una topología sin bucles?

- **Selección de un puente raíz:** Este puente (switch) es el punto de referencia para que toda la red cree un árbol de expansión alrededor.
- **Bloquear rutas redundantes:** STP garantiza que solo haya una ruta lógica entre todos los destinos de la red al bloquear intencionalmente las rutas redundantes que podrían causar un bucle. Cuando se bloquea un puerto, se impide que los datos del usuario entren o salgan de ese puerto.
- **Crear una topología sin bucle:** un puerto bloqueado tiene el efecto de convertir ese vínculo en un vínculo no reenvío entre los dos switch. Esto crea una topología en la que cada switch tiene una única ruta al puente raíz, similar a las ramas de un árbol que se conectan a la raíz del árbol.
- **Vuelva a calcular en caso de falla de enlace:** las rutas físicas todavía existen para proporcionar redundancia, pero estas rutas están deshabilitadas para evitar que ocurran los bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active. Los recálculos STP también pueden ocurrir cada vez que se agrega un nuevo switch o un nuevo vínculo entre switches a la red.

5.2 Operaciones STP

Pasos para una topología sin bucles

Usando STA, STP crea una topología sin bucles en un proceso de cuatro pasos:

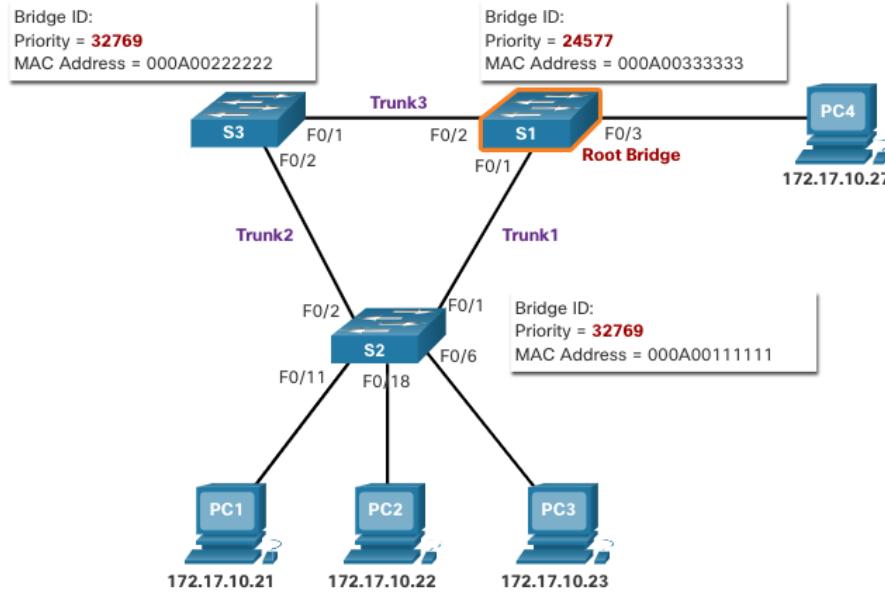
1. Elige el puente raíz.
 2. Seleccione los puertos raíz.
 3. Elegir puertos designados.
 4. Seleccione puertos alternativos (bloqueados).
- Durante las funciones STA y STP, los switch utilizan unidades de datos de protocolo de puente (BPDU) para compartir información sobre sí mismos y sus conexiones. Las BPDU se utilizan para elegir el puente raíz, los puertos raíz, los puertos designados y los puertos alternativos.
 - Cada BPDU contiene una ID de puente (BID) que identifica qué switch envió la BPDU. El BID participa en la toma de muchas de las decisiones STA, incluidos los roles de puente raíz y puerto.
 - El BID contiene un valor de prioridad, la dirección MAC del switch y un ID de sistema extendido. El valor de BID más bajo lo determina la combinación de estos tres campos.

Pasos para una topología sin bucles(cont.)

- **Prioridad de puente:** el valor de prioridad predeterminado para todos los switch Cisco es el valor decimal 32768 El rango va de 0 a 61440 y aumenta de a 4096. Es preferible una prioridad de puente más baja. La prioridad de puente 0 prevalece sobre el resto de las prioridades de puente.
- **ID del sistema extendido:** el valor de ID del sistema extendido es un valor decimal agregado al valor de prioridad del puente en el BID para identificar la VLAN para esta BPDU.
- **Dirección MAC:** cuando dos switch se configuran con la misma prioridad y tienen la misma ID de sistema extendida, el switch que tiene la dirección MAC con el valor más bajo, expresado en hexadecimal, tendrá el BID más bajo.

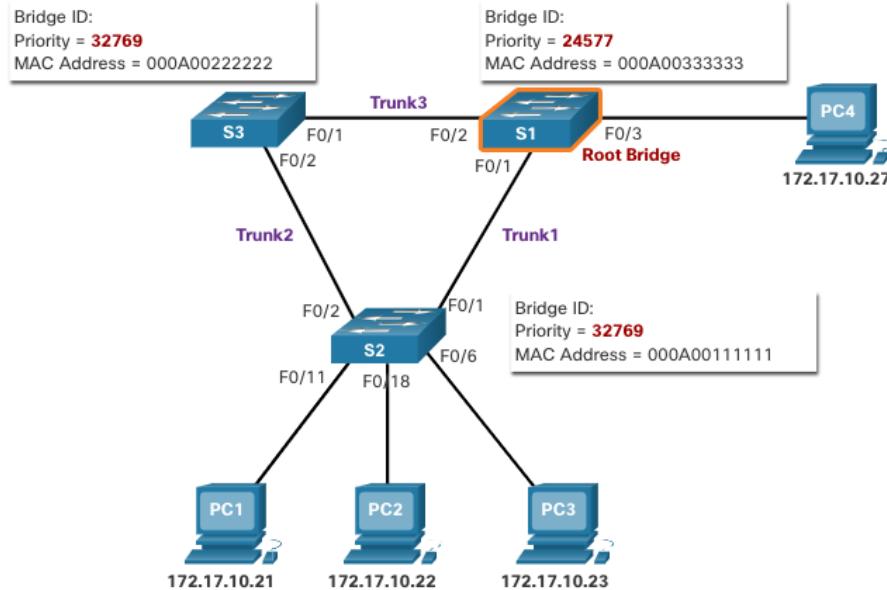
1. Elige el puente raíz

- El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. Los switch intercambian BPDU para crear la topología sin bucles comenzando con la selección del puente raíz.
- Todos los switch del dominio de difusión participan del proceso de elección. Una vez que el switch arranca, comienza a enviar tramas BPDU cada dos segundos. Estas tramas BPDU contienen el BID del switch de envío y el BID del puente raíz, conocido como ID raíz.
- El switch que tiene el BID más bajo se convierte en el puente raíz. Al principio, todos los switch se declaran a sí mismos como el puente raíz con su propio BID establecido como ID raíz. Eventualmente, los switch aprenden a través del intercambio de BPDU qué switch tiene el BID más bajo y acordarán un puente raíz.



Operaciones STP Impacto del BID predeterminado

- Dado que el BID predeterminado es 32768, es posible que dos o más switches tengan la misma prioridad. En este escenario, donde las prioridades son las mismas, el switch con la dirección MAC más baja se convertirá en el puente raíz. El administrador debe configurar el switch de puente raíz deseado con una prioridad inferior.
- En la figura, todos los switch están configurados con la misma prioridad de 32769. Aquí la dirección MAC se convierte en el factor decisivo en cuanto a qué interruptor se convierte en el puente raíz. El switch con el valor de dirección MAC hexadecimal más bajo es el puente raíz preferido. En este ejemplo, S2 tiene el valor más bajo para su dirección MAC y se elige como el puente raíz para esa instancia de árbol de expansión.
- Nota:** La prioridad de todos los switch es 32769. El valor se basa en la prioridad de puente predeterminada 32768 y la ID del sistema extendida (asignación de VLAN 1) asociada con cada switch ($32768 + 1$).



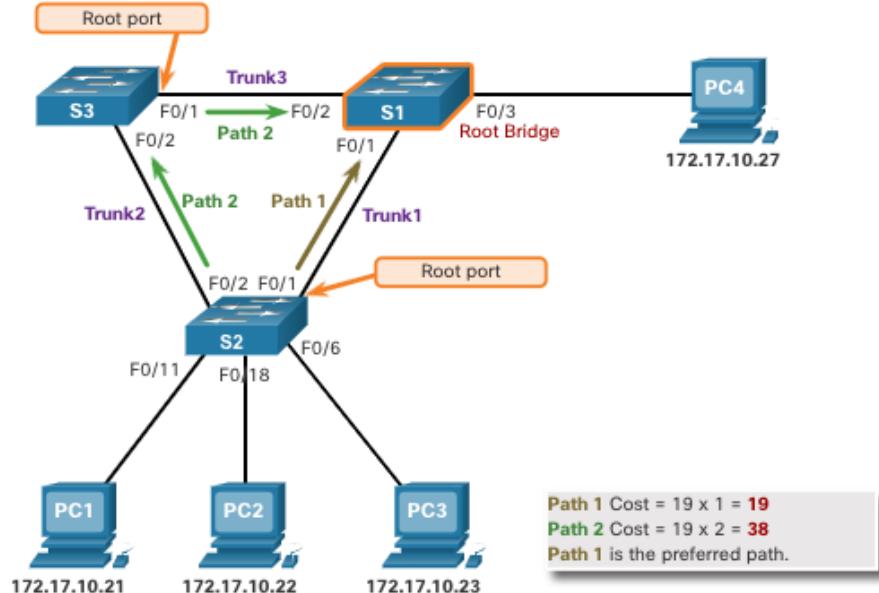
Determinar el costo de la ruta raíz

- Cuando se ha elegido el puente raíz para una instancia de árbol de expansión dado, el STA comienza a determinar las mejores rutas al puente raíz desde todos los destinos en el dominio de difusión. La información de la ruta, conocida como el costo interno de la ruta raíz, está determinada por la suma de todos los costos de los puertos individuales a lo largo de la ruta desde el switch hasta el puente raíz.
- Cuando un switch recibe la BPDU, agrega el costo del puerto de ingreso del segmento para determinar el costo interno de la ruta hacia la raíz.
- Los costos de los puertos predeterminados se definen por la velocidad a la que funcionan los mismos. La tabla muestra los costos de puerto predeterminados sugeridos por IEEE. Los switch Cisco utilizan de forma predeterminada los valores definidos por el estándar IEEE 802.1D, también conocido como costo de ruta corta, tanto para STP como para RSTP.
- Pese a que los puertos de switch cuentan con un costo de puerto predeterminado asociado a los mismos, tal costo puede configurarse. La capacidad de configurar costos de puerto individuales le da al administrador la flexibilidad para controlar de forma manual las rutas de árbol de expansión hacia el puente raíz.

Velocidad de enlace	STP Cost: IEEE 802.1D-1998	Costo de RSTP: IEEE 802.1w-2004
10 Gbps	2	2000
1 Gbps	4	20 000
100 Mbps	19	200 000
10 Mbps	100	2 000 000

2. Elegir los puertos raíz

- Después de determinar el puente raíz, se utiliza el algoritmo STA para seleccionar el puerto raíz. Cada switch que no sea root seleccionará un puerto raíz. El puerto raíz es el puerto más cercano al puente raíz en términos de costo general para el puente raíz. Este costo general se conoce como costo de ruta raíz interna.
- El costo interno de la ruta raíz es igual a la suma de todos los costos del puerto a lo largo de la ruta al puente raíz, como se muestra en la figura. Las rutas con el costo más bajo se convierten en las preferidas, y el resto de las rutas redundantes se bloquean. En el ejemplo, el costo de la ruta raíz interna desde S2 hasta el puente raíz S1 sobre la ruta 1 es 19, mientras que el costo de la ruta raíz interna sobre la ruta 2 es 38. Debido a que la ruta 1 tiene un costo de ruta general más bajo para el puente raíz, es la ruta preferida y F0 / 1 se convierte en el puerto raíz en S2.



Elegir un puerto raíz a partir de múltiples rutas de igual costo

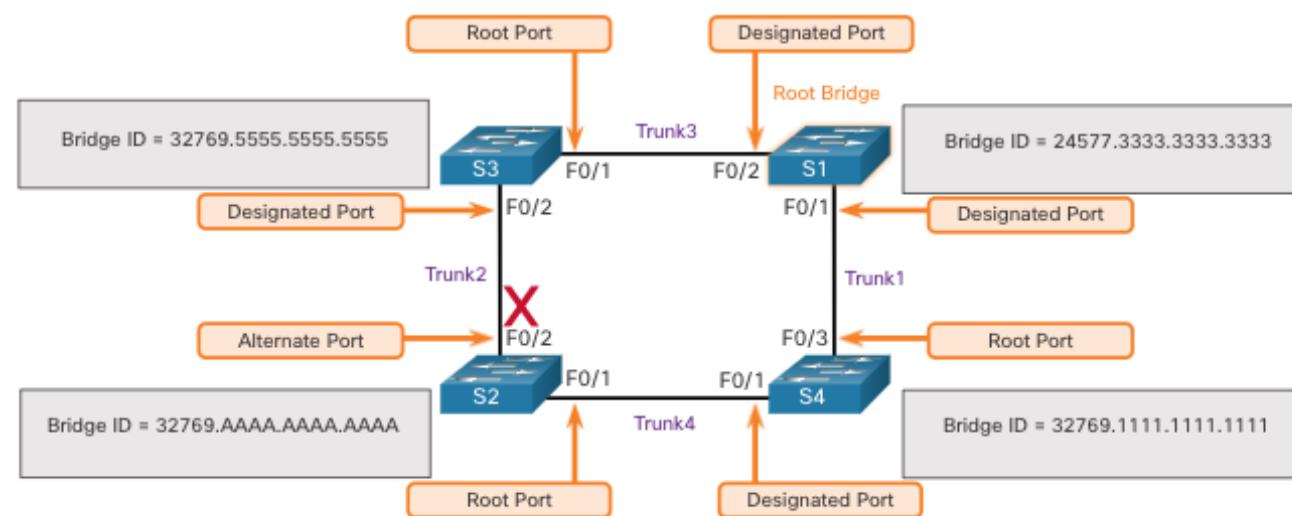
Cuando un switch tiene varias rutas de igual costo al puente raíz, el switch determinará un puerto utilizando los siguientes criterios:

- Oferta de remitente más baja
- Prioridad de puerto del remitente más baja
- ID de puerto del remitente más bajo

Elegir un puerto raíz a partir de varias rutas de igual costo (Cont.)

Oferta más baja del remitente: esta topología tiene cuatro switch con el switch S1 como puente raíz. El puerto F0/1 en el switch S3 y el puerto F0/3 en el switch S4 se han seleccionado como puertos raíz porque tienen el costo de la ruta raíz al puente raíz para sus respectivos switch.

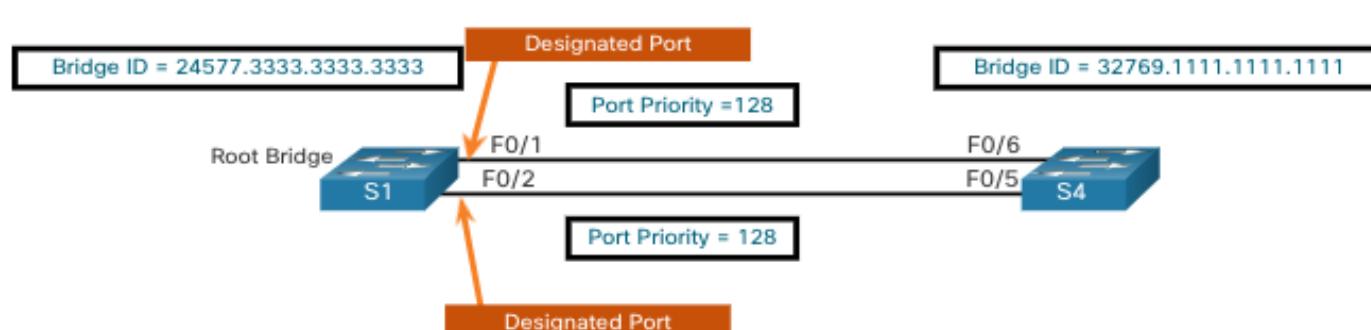
S2 tiene dos puertos, F0/1 y F0/2 con rutas de igual costo al puente raíz. Las ID de puente de S3 y S4 se utilizarán para romper el empate. Esto se conoce como BID del emisor. S3 tiene un BID de 32769.5555.5555.5555 y S4 tiene un BID de 32769.1111.1111.1111. Como S4 tiene un BID más bajo, el puerto F0/1 de S2, que es el puerto conectado a S4, será el puerto raíz.



Elegir un puerto raíz a partir de varias rutas de igual costo (Cont.)

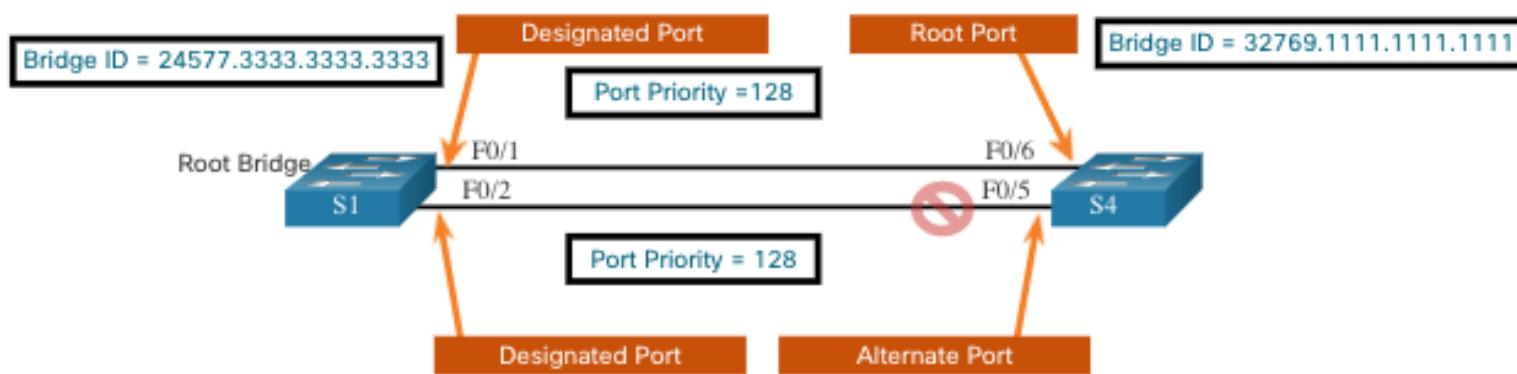
Prioridad de puerto de remitente más baja: Esta topología tiene dos switch que están conectados con dos rutas de igual costo entre ellos. S1 es el puente raíz, por lo que ambos puertos son puertos designados.

- S4 tiene dos puertos con rutas de igual costo al puente raíz. Dado que ambos puertos están conectados al mismo switch, el BID (S1) del remitente es igual. Entonces el primer paso es un empate.
- A continuación, es la prioridad del puerto del remitente (S1). La prioridad de puerto predeterminada es 128, por lo que ambos puertos de S1 tienen la misma prioridad de puerto. Esto también es un empate. Sin embargo, si cualquiera de los puertos de S1 se configuraba con una prioridad de puerto más baja, S4 pondría su puerto adyacente en estado de reenvío. El otro puerto en S4 sería un estado de bloqueo.



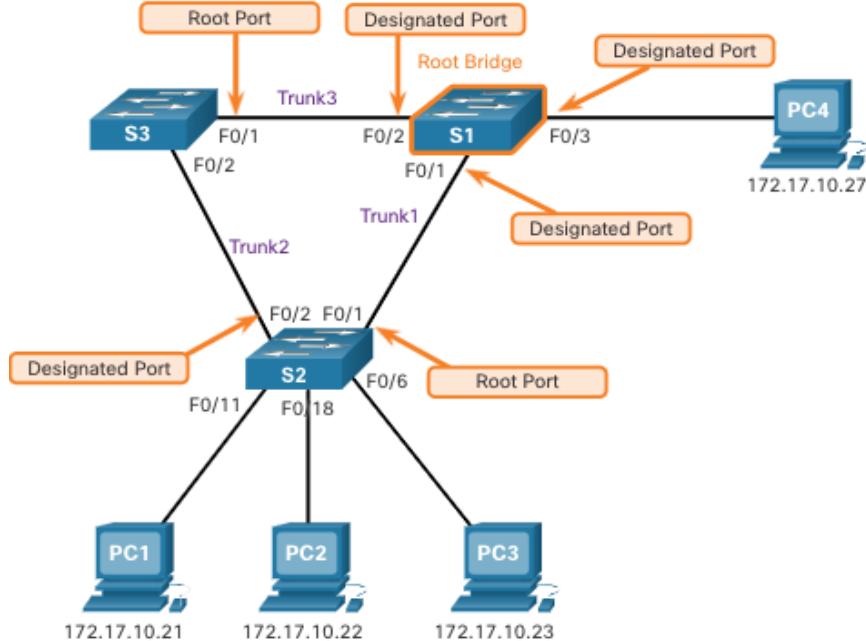
Elegir un puerto raíz a partir de varias rutas de igual coste (Cont.)

- **Id. de puerto del remitente más bajo:** el último desempate es el Id. de puerto del remitente más bajo. El switch S4 ha recibido BPDU desde el puerto F0/1 y el puerto F0/2 en S1. La decisión se basa en el ID del puerto del remitente, no en el ID del puerto del receptor. Dado que el Id. de puerto de F0/1 en S1 es menor que el puerto F0/2, el puerto F0/6 en el switch S4 será el puerto raíz. Este es el puerto de S4 que está conectado al puerto F0/1 de S1.
- El puerto F0/5 en S4 se convertirá en un puerto alternativo y se colocará en el estado de bloqueo.



3. Seleccionar puertos designados

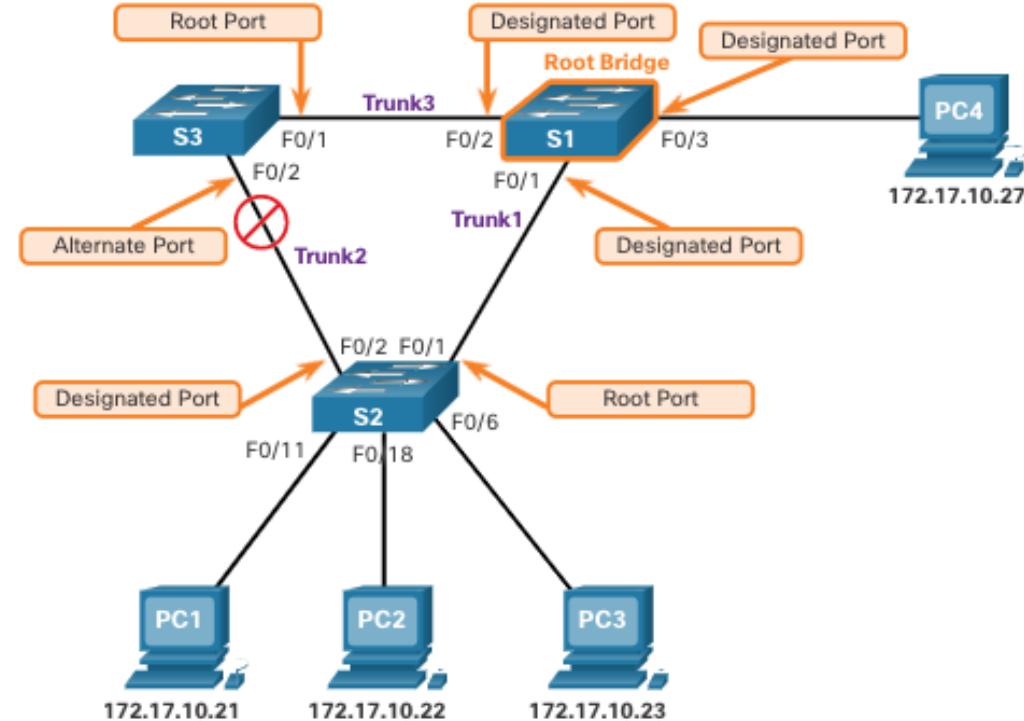
- Cada segmento entre dos switch tendrá un puerto designado. El puerto designado es un puerto en el segmento que tiene el costo de ruta raíz interna para el puente raíz. En otras palabras, el puerto designado tiene la mejor ruta para recibir el tráfico que conduce al puente raíz.
- Lo que no es un puerto raíz o un puerto designado se convierte en un puerto alternativo o bloqueado.
- Todos los puertos en el puente raíz son puertos designados.
- Si un extremo de un segmento es un puerto raíz, el otro extremo es un puerto designado.
- Todos los puertos conectados a los dispositivos finales son puertos designados.
- En segmentos entre dos switch donde ninguno de los switch es el puente raíz, el puerto del switch con la ruta de menor costo al puente raíz es un puerto designado.



4. Seleccionar puertos alternativos (bloqueados)

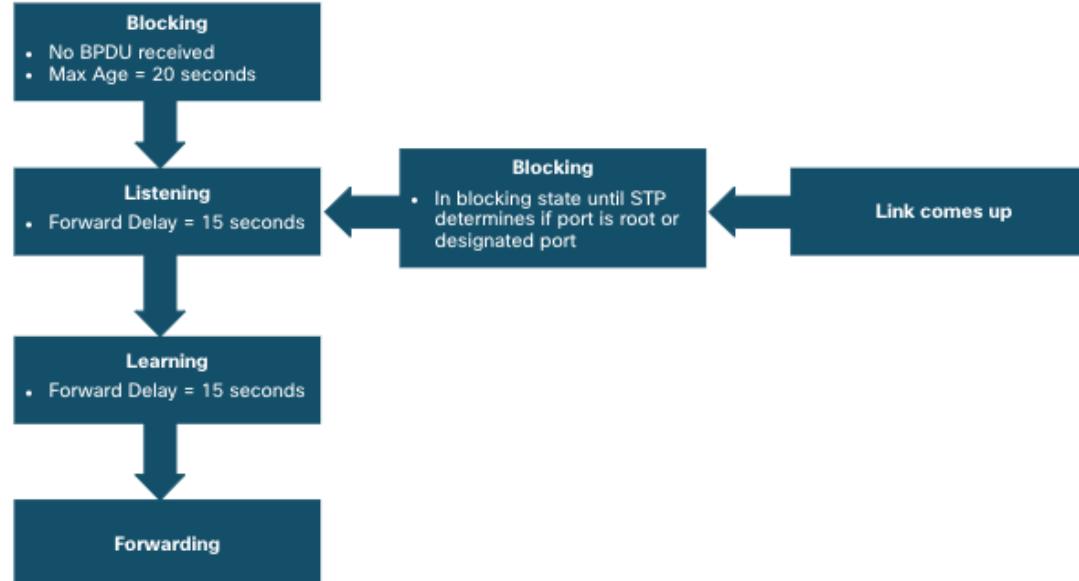
Si un puerto no es un puerto raíz o un puerto designado, se convierte en un puerto alternativo (o de copia de seguridad). Los puertos alternativos están en estado de descarte o bloqueo para evitar bucles.

En la figura, la STA ha configurado el puerto F0/2 en S3 en el rol alternativo. El puerto F0/2 en S3 está en estado de bloqueo y no reenviará tramas Ethernet. Todos los demás puertos entre switch están en estado de reenvío. Esta es la parte de prevención de bucles de STP.



Detalles operativos de cada estado de puerto (cont.)

STP facilita la ruta lógica sin bucles en todo el dominio de difusión. El árbol de expansión se determina a través de la información obtenida en el intercambio de tramas de BPDU entre los switch interconectados. Si un puerto de switch pasa directamente del estado de bloqueo al de reenvío sin información acerca de la topología completa durante la transición, el puerto puede crear un bucle de datos temporal. Por esta razón, STP tiene cinco estados de puertos, cuatro de los cuales son estados de puertos operativos, como se muestra en la figura. El estado deshabilitado se considera no operativo.



Detalles operativos de cada estado de puerto

La tabla resume los detalles operativos de cada estado del puerto

Estado del puerto	BPDU	Tabla de direcciones MAC	Reenvío de tramas de datos
Bloqueo	Recibir solo	No hay actualización	No
Escucha	Recibir y enviar	No hay actualización	No
Aprendizaje	Recibir y enviar	Actualización de la tabla	No
Reenvío	Recibir y enviar	Actualización de la tabla	Sí
Deshabilitado	No se ha enviado ni recibido	No hay actualización	No

Temporizadores STP

La convergencia STP requiere tres temporizadores, como sigue:

- **Hello Timer** - el tiempo de saludo es el intervalo entre BPDU. El valor predeterminado es 2 segundos, pero se puede modificar entre 1 y 10 segundos.
- **Temporizador de demora directa**: la demora directa es el tiempo que se pasa en el estado de escucha y aprendizaje. El valor predeterminado es 15 segundos, pero se puede modificar a entre 4 y 30 segundos.
- **Temporizador de edad máxima**: la antigüedad máxima es la duración máxima de tiempo que un switch espera antes de intentar cambiar la topología STP. El valor predeterminado es 20 segundos, pero se puede modificar entre 6 y 40 segundos.

Nota: Los tiempos predeterminados se pueden cambiar en el puente raíz, que dicta el valor de estos temporizadores para el dominio STP.

Árbol de expansión por VLAN

STP se puede configurar para operar en un entorno con varias VLAN. En el árbol de expansión por VLAN (PVST) versión para STP, hay un puente raíz ha elegir por cada instancia de árbol de expansión.

Esto hace posible tener diferentes puentes raíz para diferentes conjuntos de VLAN. STP opera una instancia independiente de STP para cada VLAN individual. Si todos los puertos de todos los switch pertenecen a la VLAN 1, solo se da una instancia de árbol de expansión.

5.3 Evolución del STP

Diferentes versiones de STP

- Muchos profesionales usan genéricamente árbol de expansión (spanning tree) y STP para referirse a las diversas implementaciones de árbol de expansión, como Rapid Spanning Tree Protocol (RSTP) y Multiple Spanning Tree Protocol (MSTP). Para comunicar los conceptos del árbol de expansión correctamente, es importante hacer referencia a la implementación o al estándar del árbol de expansión en contexto.
- El documento más reciente del IEEE acerca del árbol de expansión (IEEE-802-1D-2004) establece que “STP se reemplazó con el protocolo de árbol de expansión rápido (RSTP)”. El IEEE utiliza “STP” para referirse a la implementación original del árbol de expansión y “RSTP” para describir la versión del árbol de expansión especificada en IEEE-802.1D-2004.
- Debido a que los dos protocolos comparten gran parte de la misma terminología y métodos para la ruta sin bucles, el enfoque principal estará en el estándar actual y las implementaciones propietarias de Cisco de STP y RSTP.
- Los switch de Cisco con IOS 15.0 o posterior ejecutan PVST+ de manera predeterminada. Esta versión incluye muchas de las especificaciones IEEE 802.1D-2004, como puertos alternativos en lugar de los puertos no designados anteriores. Los switch deben configurarse explícitamente para el modo de árbol de expansión rápida para ejecutar el protocolo de árbol de expansión rápida.

Evolución de STP

Diferentes versiones de STP (cont.)

Variedad STP	Descripción
STP	Esta es la versión original IEEE 802.1D (802.1D-1998 y anteriores) que proporciona una topología sin bucles en una red con enlaces redundantes. También llamado Common Spanning Tree (CST), asume una instancia de árbol de expansión para toda la red puenteada, independientemente de la cantidad de VLAN.
PVST+	El árbol de expansión por VLAN (PVST +) es una mejora de Cisco de STP que proporciona una instancia de árbol de expansión 802.1D separada para cada VLAN configurada en la red. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
802.1D-2004	Esta es una versión actualizada del estándar STP, que incorpora IEEE 802.1w.
RSTP	Rapid Spanning Tree Protocol (RSTP) o IEEE 802.1w es una evolución de STP que proporciona una convergencia más rápida que STP.
PVST+ rápido	Esta es una mejora de Cisco de RSTP que utiliza PVST + y proporciona una instancia independiente de 802.1w por VLAN. Cada instancia aparte admite PortFast, protección de BPDU, filtro de BPDU, protección de raíz y protección de bucle.
MSTP	El Protocolo de árbol de expansión múltiple (MSTP) es un estándar IEEE inspirado en la implementación anterior de STP de instancia múltiple (MISTP) de Cisco. MSTP asigna varias VLAN en la misma instancia de árbol de expansión.
Instancia	Multiple Spanning Tree (MST) es la implementación de Cisco de MSTP, que proporciona hasta 16 instancias de RSTP y combina muchas VLAN con la misma topología física y lógica en una instancia RSTP común. Cada instancia admite PortFast, protección BPDU, filtro BPDU, protección de raíz y protección de bucle.

Conceptos de RSTP

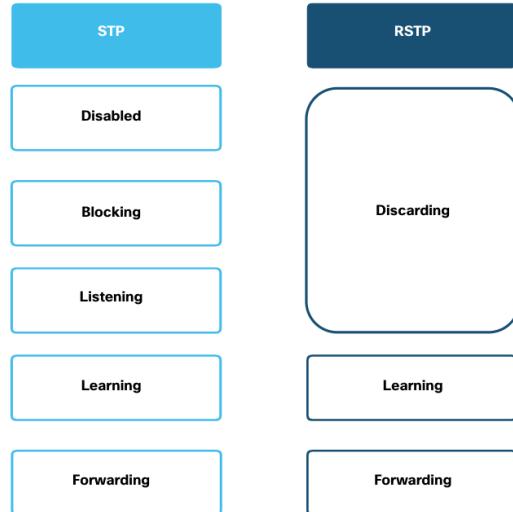
- RSTP (IEEE 802.1w) reemplaza al 802.1D original mientras conserva la compatibilidad con versiones anteriores. La terminología de STP 802.1w sigue siendo fundamentalmente la misma que la de STP IEEE 802.1D original. La mayoría de los parámetros se han dejado sin cambios. Los usuarios que estén familiarizados con el estándar STP original pueden configurar fácilmente RSTP. El mismo algoritmo de árbol de expansión se utiliza tanto para STP como para RSTP para determinar los roles de puerto y la topología.
- RSTP aumenta la velocidad del recálculo del árbol de expansión cuando cambia la topología de la red de Capa 2. RSTP puede lograr una convergencia mucho más rápida en una red configurada en forma adecuada, a veces sólo en unos pocos cientos de milisegundos. Si un puerto está configurado para ser un puerto alternativo, puede cambiar inmediatamente a un estado de reenvío sin esperar a que la red converja.

Nota: Rapid PVST + es la implementación de Cisco de RSTP por VLAN. Con Rapid PVST + se ejecuta una instancia independiente de RSTP para cada VLAN.

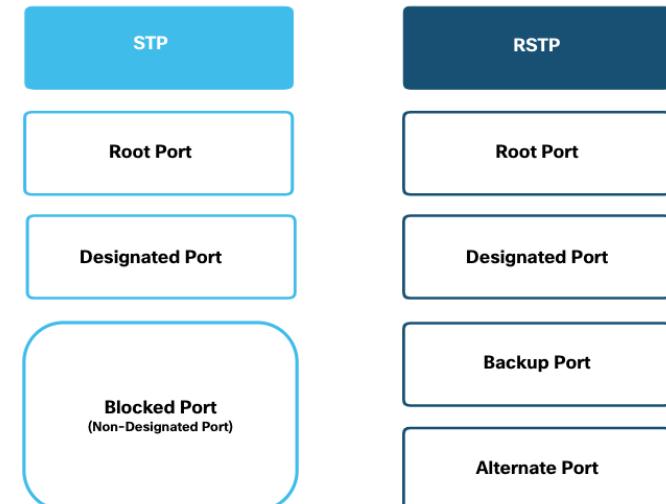
Estados del puerto RSTP y las funciones del puerto

Solo hay tres estados de puerto en RSTP que corresponden a los tres estados operativos posibles en STP.

Los estados de desactivación, bloqueo y escucha 802.1D se fusionan en un único estado de descarte 802.1w.

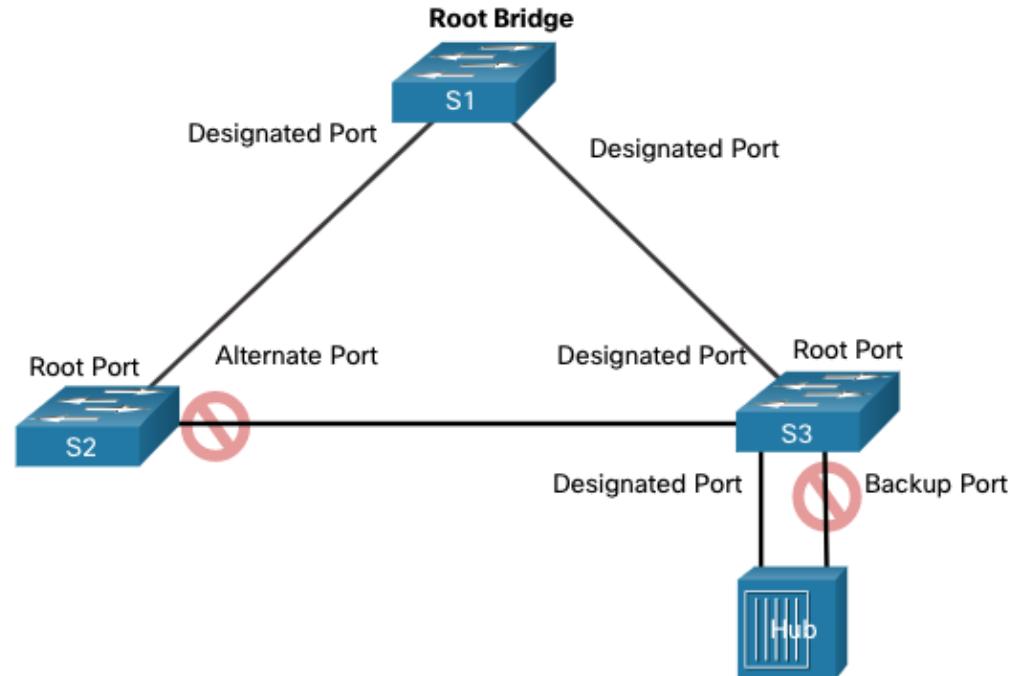


Los puertos raíz y los puertos designados son los mismos para STP y RSTP. Sin embargo, hay dos roles de puerto RSTP que corresponden al estado de bloqueo de STP. En STP, un puerto bloqueado se define como no ser el puerto designado o raíz. RSTP tiene dos funciones de puerto para este propósito.



Estados de puerto RSTP y las funciones de puerto (cont.)

El puerto alternativo tiene una ruta alternativa al puente raíz. El puerto de copia de seguridad es una copia de seguridad en un medio compartido, como un concentrador. Un puerto de copia de seguridad es menos común porque ahora los concentradores se consideran dispositivos heredados.



PortFast y BPDU Guard

- Cuando un dispositivo está conectado a un puerto del switch o cuando un switch se enciende, el puerto del switch pasa por los estados de escucha y aprendizaje, esperando cada vez que expire el temporizador de retardo de reenvío. Este retraso es de 15 segundos para cada estado durante un total de 30 segundos. Esto puede presentar un problema para los clientes DHCP que intentan detectar un servidor DHCP porque el proceso DHCP puede agotarse. El resultado es que un cliente IPv4 no recibirá una dirección IPv4 válida.
- Cuando un puerto de switch está configurado con PortFast, ese puerto pasa de un estado de bloqueo al de reenvío inmediatamente, evitando el retraso de 30 segundos. Puede utilizar PortFast en los puertos de acceso para permitir que los dispositivos conectados a estos puertos accedan a la red inmediatamente. PortFast sólo debe utilizarse en puertos de acceso. Si habilita PortFast en un puerto que se conecta a otro switch, corre el riesgo de crear un bucle de árbol de expansión.
- Un puerto de switch habilitado para PortFast nunca debería recibir BPDU porque eso indicaría que el switch está conectado al puerto, lo que podría causar un bucle de árbol de expansión. Los switch Cisco admiten una característica denominada “protección BPDU”. Cuando está habilitado, inmediatamente pone el puerto del switch en un estado errdisabled (error-disabled) al recibir cualquier BPDU. Esto protege contra posibles bucles al apagar eficazmente el puerto. El administrador debe volver a poner manualmente la interfaz en servicio.

Alternativas a STP

- A lo largo de los años, las organizaciones requerían una mayor resiliencia y disponibilidad en la LAN. Las LAN Ethernet pasaron de unos pocos switch interconectados conectados a un único enrutador, a un sofisticado diseño de red jerárquica que incluía switch de acceso, distribución y capa central.
- Dependiendo de la implementación, la capa 2 puede incluir no solo la capa de acceso, sino también la distribución o incluso las capas principales. Estos diseños pueden incluir cientos de switch, con cientos o incluso miles de VLAN. STP se ha adaptado a la redundancia y complejidad añadida con mejoras, como parte de RSTP y MSTP.
- Un aspecto importante del diseño de red es la convergencia rápida y predecible cuando se produce un error o un cambio en la topología. El árbol de expansión no ofrece las mismas eficiencias y predictibilidades proporcionadas por los protocolos de enrutamiento en la Capa 3.
- El enrutamiento de capa 3 permite rutas y bucles redundantes en la topología, sin bloquear puertos. Por esta razón, algunos entornos están en transición a la capa 3 en todas partes, excepto donde los dispositivos se conectan al switch de capa de acceso. En otras palabras, las conexiones entre los switch de capa de acceso y los switch de distribución serían Capa 3 en lugar de Capa 2.

Nuevos términos y comandos

- Spanning Tree Protocol (STP)
- Spanning Tree Algorithm (STA)
- IEEE 802.1D
- IEEE 802.1w
- Broadcast Storm
- Root Bridge
- Root Port
- Designated Port
- Alternate (Blocked) Port
- Learning
- Listening
- Bridge ID (BID)
- Root ID
- Bridge Protocol Data Unit (BPDU)
- Bridge Priority
- Extended System ID
- short path cost
- long path cost
- root path cost
- Rapid STP (RSTP)
- port priority
- Hello timer
- Max Age timer
- Forward Delay timers
- Blocking
- Forwarding
- Discarding
- Per-VLAN Spanning Tree (PVST)
- PVST+
- Rapid PVST+
- Multiple Spanning Tree Protocol (MSTP)
- Multiple Spanning Tree (MST)
- PortFast
- BPDU Guard

