INSTITUTO SUPERIOR TECNOLÓGICO "HUAQUILLAS"

Arquitectura de Redes

Tecnología
▪ **Redes y Telecomunicaciones**

Autor(a):

Ing. Jorge David Herrera Sarango

Huaquillas – Ecuador

2024

Misión del Instituto

Formar profesionales competentes, creativos, investigadores e innovadores con altos valores éticos y espíritu emprendedor, que generen soluciones a los problemas y necesidades del sector fronterizo sur.

Visión del Instituto

Formar profesionales competentes, creativos, investigadores e innovadores con altos valores éticos y espíritu emprendedor, que generen soluciones a los problemas y necesidades del sector fronterizo sur.

Índice de contenido

ÍNDICE DE FIGURAS

Prólogo

Los estudiantes de la carrera de Tecnología Superior en Redes y Telecomunicaciones deben conocer a profundidad el área de arquitectura de redes, debido a que su carrera depende mucho de ella, siendo muy fundamentales al momento de diseñar una red.

En este manual técnico se pretende abarcar los temas más importantes y útiles en el campo de la arquitectura de redes, con la finalidad de enseñar progresivamente cada tema relacionado al área y como se debe ser implementadas las herramientas requeridas para este tipo de actividades.

Asimismo, el presente documento busca que el lector entienda adecuadamente la importancia de la electrónica en el ámbito diario, además le ayudara a resolver posibles problemas generados en el área.

Introducción

En el presente manual se pretende enseñar a los estudiantes sobre conceptos básicos de la arquitectura de redes, con la finalidad de que ellos puedan realizar actividades referentes a esta área, por ejemplo, diseñar una red, usando aplicaciones de estructuras como AutoCAD.

En la primera parte del documento, se observan los objetivos propuestos por el docente para este semestre. Asimismo, en la segunda parte, se conceptualizan los siguientes temas básicos:

- **Unidad 1. –** Conceptos básicos de la electrónica como los conceptos básicos de switching VLANS y enrutamiento entre redes VLAN.
- **Unidad 2. –** Redes redundantes; redes disponibles y confiables.
- **Unidad 3.-** Seguridad de L2 y WLAN y conceptos de enrutamiento y configuración.
- **Unidad 4.** – Conceptos básicos de RIPV1 y RIPV2.
- **Unidad 5.** – Conceptos básicos de FTTH y XPON.
- **Unidad 6.** – Norma técnica de diseño y construcción en edificios y urbanizaciones de acuerdo a CNT..

De la misma manera en esta sección, se puede visualizar una práctica y una autoevaluación, que ayudara a los estudiantes reforzar lo aprendido. Por otro lado, en la tercera parte del manual, se detalla la información del autor. Mientras que, en la cuarta parte, se coloca un pequeño glosario.

En la quinta parte del documento, se anexan las pruebas que se van a realizar en este ciclo con los estudiantes, y por último, en la sexta parte, se referencia los sitios web, libros y revistas que se usaron como fuente de información.

Saludo a los estudiantes

Estimad@s estudiantes reciban un cordial saludo en este nuevo ciclo, esperando que el estudio de esta materia como es la de **Arquitectura de redes** y los nuevos conocimientos adquiridos sean fructíferos para el cumplimiento de sus objetivos como futuros profesionales.

3.1. Objetivo general

Promover el conocimiento de los estudiantes sobre los conceptos básicos, estructuras y servicios, definiendo los requerimientos para su correcta implementación y de esta manera puedan resolver problemas en infraestructuras de redes y servicios de internet.

3.2. Objetivos específicos

- Explicar los principios generales que rigen las arquitecturas de redes y ordenadores.
- Aplicar los principios de arquitecturas a nivel de una red.
- Estudiar los protocolos de enrutamiento, los cuales hacen posible la comunicación a larga distancia.
- Estudiar las características y arquitecturas de redes.
- Explicar los protocolos y servicios a través de las redes de datos.

4. Contenido Técnico

En este apartado, se podrá observar los temas que se van a abarcar en el manual con respecto a la arquitectura de redes.

4.1. Conceptos básicos de switching VLANS y enrutamiento entre redes VLAN

Esta unidad ayudará a los estudiantes a identificar la configuración básica de dispositivos y VLAN, verificar como se conectan directamente las redes, identificar el switching en la red y su método de reenvió.

4.1.1. Configuración de parámetros iniciales de un switch.

- ***Secuencia de arranque de un switch***.

Antes de poder configurar un switch, debe encenderlo y permitirle pasar por la secuencia de arranque de cinco pasos. En este tema se tratan los conceptos básicos de la configuración de un switch e incluye un laboratorio al final.

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 autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Esta 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 cargador de arranque lleva a cabo la inicialización de la 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 inicia el sistema de archivos flash en la placa del sistema.

Paso 5: Por último, el cargador de arranque localiza y carga una imagen de software del sistema operativo de IOS en la memoria y delega el control del switch a 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. En los switches de la serie Catalyst 2960, el archivo de imagen generalmente se encuentra en un directorio que tiene el mismo nombre que el archivo de imagen (excepto la extensión de archivo .bin).

El sistema operativo IOS luego inicializa las interfaces utilizando los comandos Cisco IOS que se encuentran en el archivo de configuración de inicio. Se llama al archivo startup-config config.text y se encuentra en flash.

En el ejemplo, la variable de entorno BOOT se establece mediante el boot system comando del modo de configuración global. Observe que el IOS se ubica en una carpeta distinta y que se especifica la ruta de la carpeta. Use el comando show boot para ver en qué está configurado el archivo de arranque IOS actual.

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

La tabla define cada parte del comando boot system.

Tabla 1

Comando Boot system

Comando	Definición
boot system	El comando principal
flash:	The storage device
c2960-lanbasek9-mz.150-2.SE/	La ruta al sistema de archivos
c2960-lanbasek9-mz.150-2.SE.bin	El nombre del archivo IOS

Nota. Describen la sintanxis del comando boot system.

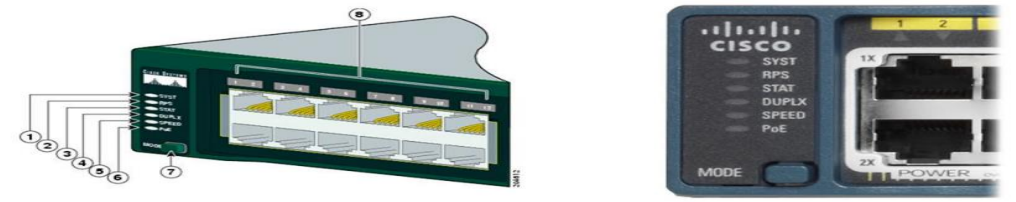
- ***Indicadores LED del swtich.***

Los switches Cisco Catalyst tienen varios indicadores luminosos LED de estado. Puede usar los LED del switch para controlar rápidamente la actividad y el rendimiento del switch. Los diferentes modelos y conjuntos de características de los switches tienen diferentes LED, y la ubicación de estos en el panel frontal del switch también puede variar.

En la ilustración, se muestran los LED y el botón Mode de un switch Cisco Catalyst 2960.

Figura 1.

Switch Cisco Catalyst 2960



Nota. Leds del switch Cisco Catalyst 2960.

El botón Modo (7 en la figura) se usa para alternar entre el estado del puerto, el dúplex del puerto, la velocidad del puerto y, si es compatible, el estado de la alimentación a través de Ethernet (PoE) de los LED del puerto (8 en la figura).

Botón Led del sistema (1): Muestra si el sistema está recibiendo energía y funciona correctamente. Si el LED está apagado, significa que el sistema no está encendido. Si

el LED es de color verde, el sistema funciona normalmente. Si el LED es de color ámbar, el sistema recibe alimentación, pero no funciona correctamente.

Botón Led del sistema de alimentación redundante (2): Muestra el estado de RPS. Si el LED está apagado, el RPS está apagado o no está conectado correctamente. Si el LED es de color verde, el RPS está conectado y listo para proporcionar alimentación de respaldo. Si el LED parpadea y es de color verde, el RPS está conectado, pero no está disponible porque está proporcionando alimentación a otro dispositivo. Si el LED es de color ámbar, el RPS está en modo de reserva o presenta una falla. Si el LED parpadea y es de color ámbar, la fuente de alimentación interna del switch presenta una falla, y el RPS está proporcionando alimentación.

Botón Led del estado de puerto (3): Indica que el modo de estado del puerto está seleccionado cuando el LED está verde. Este es el modo predeterminado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, no hay enlace, o el puerto estaba administrativamente inactivo. Si el LED es de color verde, hay un enlace presente. Si el LED parpadea y es de color verde, hay actividad, y el puerto está enviando o recibiendo datos. Si el LED alterna entre verde y ámbar, hay una falla en el enlace. Si el LED es de color ámbar, el puerto está bloqueado para asegurar que no haya un bucle en el dominio de reenvío y no reenvía datos (normalmente, los puertos permanecen en este estado durante los primeros 30 segundos posteriores a su activación). Si el LED parpadea y es de color ámbar, el puerto está bloqueado para evitar un posible bucle en el dominio de reenvío.

Botón LED de modo dúplex del puerto (4): Indica que el modo dúplex del puerto está seleccionado cuando el LED está verde. Al seleccionarlo, los LED del puerto que

están apagados están en modo semidúplex. Si el LED del puerto es de color verde, el puerto está en modo dúplex completo.

Botón led de velocidad del puerto (5): Indica que el modo de velocidad del puerto está seleccionado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, el puerto está funcionando a 10 Mbps. Si el LED es verde, el puerto está funcionando a 100 Mbps. Si el LED parpadea en verde, el puerto está funcionando a 1000 Mbps.

Botón led de modo de alimentación por Ethernet (6): Si se admite PoE, estará presente un LED de modo PoE. Si el LED está apagado, indica que no se seleccionó el modo de alimentación por Ethernet, que a ninguno de los puertos se le negó el suministro de alimentación y ninguno presenta fallas. Si el LED está parpadeando en ámbar, el modo PoE no está seleccionado, pero al menos uno de los puertos ha sido denegado o tiene una falla PoE. Si el LED es de color verde, indica que se seleccionó el modo de alimentación por Ethernet, y los LED del puerto muestran colores con diferentes significados. Si el LED del puerto está apagado, la alimentación por Ethernet está desactivada. Si el LED del puerto es de color verde, la alimentación por Ethernet está activada. Si el LED del puerto alterna entre verde y ámbar, se niega la alimentación por Ethernet, ya que, si se suministra energía al dispositivo alimentado, se excede la capacidad de alimentación del switch. Si el LED parpadea en ámbar, PoE está apagado debido a una falla. Si el LED es de color ámbar, se inhabilitó la alimentación por Ethernet para el puerto.

- ***Recuperarse de 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 comandos 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 interruptor y, en 15 segundos, presione y mantenga presionado el botón Mode mientras el LED del sistema todavía parpadea en verde.

Paso 4. Continúe presionando el botón Mode hasta que el LED del sistema se vuelva brevemente ámbar y luego verde sólido; luego suelte el botón Mode.

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

Escriba **help** o **?** en el símbolo del gestor de arranque para ver una lista de comandos disponibles.

De manera predeterminada, el switch intenta iniciarse automáticamente mediante el uso de información en la variable de entorno BOOT. Para ver la ruta de acceso de la variable de entorno BOOT del switch, escriba el comando **set.** A continuación, inicialice el sistema de archivos flash utilizando el comando **flash_init** para ver los archivos actuales en flash, como se muestra en la salida.

```
switch: set
BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin
(output omitted)
switch: flash_init
Initializing Flash...
flashfs[0]: 2 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11838464
flashfs[0]: Bytes available: 20675584
flashfs[0]: flashfs fsck took 10 seconds.
```

Después de que flash haya terminado de inicializar, puede ingresar el dir flash: comando para ver los directorios y archivos en flash, como se muestra en la salida.

```
switch: dir flash:
Directory of flash:/
   2  -rwx  11834846              c2960-lanbasek9-mz.150-2.SE8.bin
   3  -rwx  2072                  multiple-f
```

Introduzca el BOOT=flash comando para cambiar la ruta de la variable de entorno BOOT que utiliza el switch para cargar el nuevo IOS en flash. Para verificar la nueva ruta de la variable de entorno BOOT, vuelva a set ejecutar el comando. Finalmente, para cargar el nuevo IOS escriba el boot comando sin ningún argumento, como se muestra en la salida.

```
switch: BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
switch: set
BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
(output omitted)
switch: boot
```

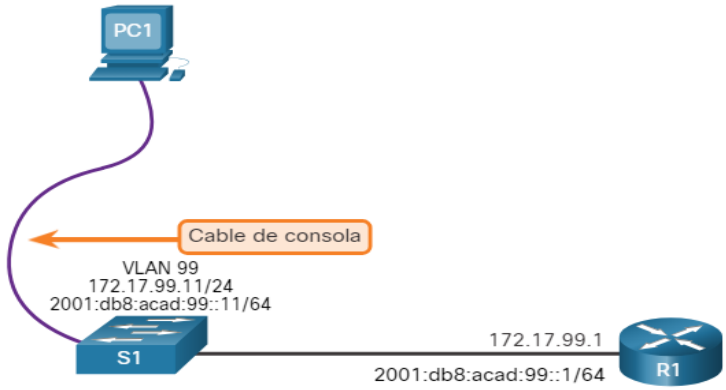
Los comandos del gestor de arranque admiten la inicialización de flash, el formateo de flash, la instalación de un nuevo IOS, el cambio de la variable de entorno BOOT y la recuperación de contraseñas pérdidas u olvidadas.

- ***Acceso a administración de switches***

Para el acceso a la administración remota de un switch, este se debe configurar con una dirección IP y una máscara de subred. Tenga en cuenta que para administrar el switch desde una red remota, el switch 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 acceder a una PC de modo que el switch puede configurar específicamente.

Figura 2.

Acceso a administracion de switches



Nota. Conexión desde el switch hasta la PC.

- ***Ejemplo de configuración de Switch 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 considera una práctica recomendada utilizar una VLAN distinta de la VLAN 1 para la VLAN de administración, como la VLAN 99 en el ejemplo.

Paso 1. Configuración de 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 debata configurar para IPv6. Por ejemplo, antes de que pueda configurar el direccionamiento IPv6 en un Cisco Catalyst 2960 que ejecute IOS versión 15.0, deberá ingresar el comando de configuración global sdm prefer dual-ipv4-and-ipv6 default y, a continuación, reload el switch.

Tabla 2.

Configuracion del switch

Tarea	Comando 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 inetrfaz de administración.	S1(config-if)# no shutdown
Vuelva al modo EXEC privilegiado.	S1(config-if)# end
Guarde la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Nota. Sintaxis de configuración del switch.

Paso 2. Configuración del 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: Dado 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.

Tabla 3.

Configuración del gateway predeterminado.

Tarea	Comando 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
Vuelva al modo EXEC privilegiado.	S1(config-if)# end

Guarde la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Nota. Sintaxis de configuración del gateway en el switch.

Paso 3. Verificar la configuración

Los show ip interface brief comandos show ipv6 interface brief y 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 SÍ manual hacia abajo
(resultado omitido)
S1# show ipv6 interface brief
Vlan99 [abajo/abajo]
    FE80: :C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99: :1
(resultado omitido)
```

- **Práctica de laboratorio: configuración básica de un switch.**

Tendrá la oportunidad de practicar las siguientes habilidades:

Part 1: Tender el cableado de red y verificar la configuración predeterminada del switch

Part 2: Configurar los parámetros básicos de los dispositivos de red

Part 3: Verificar y probar la conectividad de red

Podrá practicar estas habilidades usando Packet Tracer o equipo de laboratorio, de estar disponible.

Figura 3.

Configuración básica del conmutador.

Topología

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP / Prefijo
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:1: :10 /64

Nota. Topología y tabla de asignación del ejercicio.

4.1.2. Configuración básica de un router

- ***Configuración de parámetros básicos del router***

Hasta ahora, este módulo solo ha cubierto switches. Si desea que los dispositivos puedan enviar y recibir datos fuera de su red, deberá configurar routeres. En este tema se enseña la configuración básica del router y se proporcionan dos Comprobadores de sintaxis y una actividad de Rastreador de paquetes para que pueda practicar estas habilidades.

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 routeres 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)#
```

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

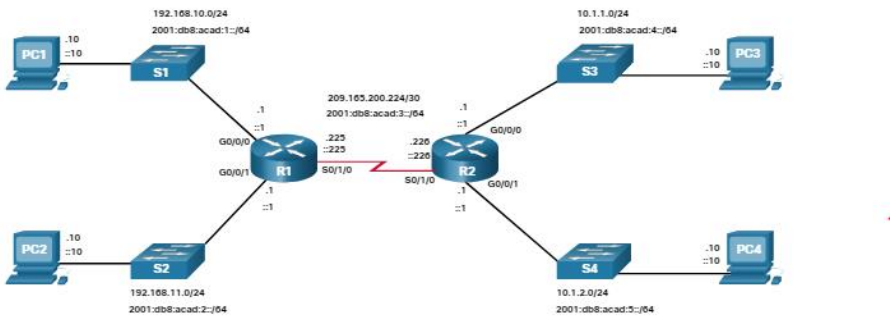
```
R1(config)# banner motd #Authorized Access Only!#
R1(config)#
Guarde los cambios en un router, como se muestra en el ejemplo.
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
1.4.2
```

- ***Topología de doble pila***

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.

Figura 4.

Topología pila dual



Nota. Topología de red de doble pila que consta de múltiples hosts, switches y routeres con interfaces configuradas.

- ***Configurar interfaces de routers***

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.

Activado: - Las interfaces LAN y WAN no están activadas de manera predeterminada (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.

El siguiente 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
```

- ***Interfaces de bucle invertido 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. 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
```

Se pueden habilitar varias interfaces loopback en un router. La dirección IPv4 para cada interfaz de bucle invertido debe ser única y no debe ser utilizada por ninguna otra interfaz, como se muestra en la configuración de ejemplo de la interfaz de bucle invertido 0 en R1.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

- ***Packet Tracer- Configurar Interfaces de Router***

En esta actividad Packet Tracer, configurará routeres con direccionamiento IPv4 e IPv6.

Figura 5.

Tabla de asignación

Dispositivo	Interfaz	Dirección/prefijo IP	Gateway predeterminado
R1	G0/0	172.16.20.1 /25	N/D
	G0/1	172.16.20.129 /25	N/D
	S0/0/0	209.165.200.225 /30	N/D
PC1	NIC	172.16.20.10 /25	172.16.20.1
PC2	NIC	172.16.20.138 /25	172.16.20.129
R2	G0/0	2001:db8:c0de:12: :1/64	N/D
	G0/1	2001:db8:c0de:13: :1/64	N/D
	S0/0/1	2001:db8:c0de:11: :1/64	N/D
		fe80::2	No corresponde
PC3	NIC	2001:db8:c0de:12: :a/64	fe80::2
PC4	NIC	2001:db8:c0de:13: :a/64	fe80::2

Nota. Direcciones ipv4 e ipv6.

4.1.3. Verificar redes conectadas directamente.

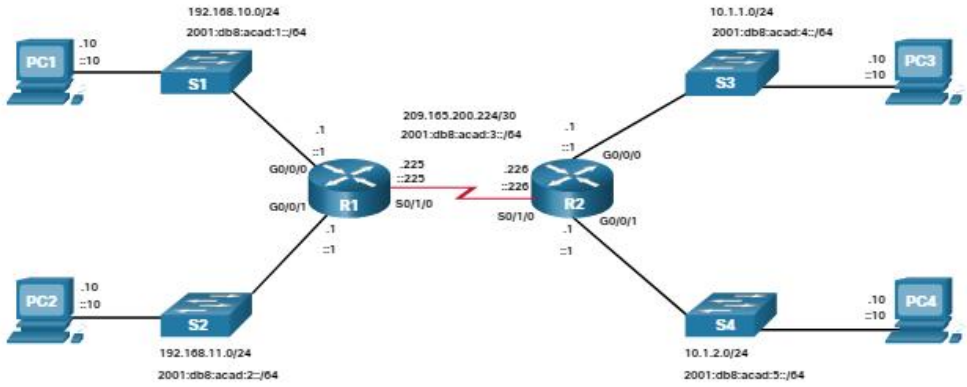
- ***Comandos de verificación de interfaz.***

No tiene sentido configurar el router a menos que verifique la configuración y la conectividad. En este tema se describen los comandos que se van a utilizar para comprobar las redes conectadas directamente. Incluye dos verificadores de sintaxis y un trazador de paquetes.

Hay varios comandos show que se pueden usar para verificar el funcionamiento y la configuración de una interfaz. La topología de la figura se utiliza para demostrar la verificación de la configuración de la interfaz del router.

Figura 6.

Topología



Nota. Configuración de la interfaz del router.

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 y show ipv6 route - Este muestra el contenido de la tabla IPv4 o IPv6 almacenada en la memoria RAM. En Cisco IOS 15, las interfaces activas deben aparecer en la tabla de ruteo con dos entradas relacionadas identificadas con el código 'C' (Conectado) o 'L' (Local). En versiones anteriores de IOS, solo aparece una entrada con el código 'C'.

- ***Verificación del estado de una interfaz***

La salida de los comandos show ip interface brief y show ipv6 interface brief y se puede usar para revelar rápidamente el estado de todas las interfaces en el 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 direcciones locales y multidifusión de vínculos IPV6***

El resultado del comando show ipv6 interface brief show ipv6 interface brief 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 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
  ICMP redirects are enabled
  ICMP unreachables are sent
  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
```

- ***Verificar la configuración de la interfaz***

Junto con la dirección local del enlace y la dirección de unidifusión global, show running-config interface la salida incluye las direcciones de multidifusión asignadas a la interfaz, comenzando con el prefijo FF02, como se muestra en el ejemplo.

```
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#
```

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 and show ipv6 interface -Muestra la información relacionada con IPv4 e IPv6 para todas las interfaces en un router.

- ***Verificar Rutas***

La salida de los **show ip route** comandos **show ipv6 route** y muestra 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, Serial0/1/0
```

```
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#
```

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 "arriba / arriba", 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.

El **ping** comando para IPv6 es idéntico al comando usado con IPv4, excepto que se usa una dirección IPv6. Como se muestra en el ejemplo, el **ping** comando se usa para verificar la conectividad de Capa 3 entre R1 y PC1.

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- ***Filtrado de 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--. Al presionar Enter se muestra la siguiente línea y al presionar la barra espaciadora se muestra el siguiente conjunto de líneas. Use el terminal length comando para especificar el número de líneas que se mostrarán. 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 show filtrado de salida. Los comandos de filtrado se pueden utilizar para mostrar secciones específicas de los resultados. Para habilitar el comando de filtrado, ingrese una barra vertical partida (|) después del show comando y luego ingrese un parámetro de filtrado y una expresión de filtrado.

Hay cuatro parámetros de filtrado que se pueden configurar después de la tubería.

Section. - Muestra la sección completa que comienza con la expresión de filtrado, como se muestra en el ejemplo.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 110A1016141D
 login
 transport input all
```

Include. - Incluye todas las líneas de salida que coinciden con la expresión de filtrado, como se muestra en el ejemplo.

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0 / 0/0 192.168.10.1 SÍ manual arriba
GigabiteThernet0/0/1 192.168.11.1 SÍ manual arriba
Serie0 / 1/0 209.165.200.225 SÍ manual arriba
Serial0/1/1 unassigned NO unset down down
R1#
R1# show ip interface brief | include up
GigabitEthernet0 / 0/0 192.168.10.1 SÍ manual arriba
GigabiteThernet0/0/1 192.168.11.1 SÍ manual arriba
Serie0 / 1/0 209.165.200.225 SÍ manual arriba
```

Exclude. - Excluye todas las líneas de salida que coinciden con la expresión de filtrado, como se muestra en el ejemplo.

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0 / 0/0 192.168.10.1 SÍ manual arriba
GigabiteThernet0/0/1 192.168.11.1 SÍ manual arriba
Serie0 / 1/0 209.165.200.225 SÍ manual arriba
Serial0/1/1 unassigned NO unset down down
R1#
R1# show ip interface brief | exclude unassigned
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0 / 0/0 192.168.10.1 SÍ manual arriba
GigabiteThernet0/0/1 192.168.11.1 SÍ manual arriba
Serie0 / 1/0 209.165.200.225 SÍ manual arriba
```

Begin. - Muestra todas las líneas de salida desde un punto determinado, comenzando con la línea que coincide con la expresión de filtrado, como se muestra en el ejemplo.

```
R1# show ip route | begin Gateway
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 está directamente conectado, GigabitEthernet0/0/0
L 192.168.10.1/32está directamente conectado, GigabitEthernet0/0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 está directamente conectado, GigabitEthernet0/0/0
L 192.168.10.1/32está directamente conectado, GigabitEthernet0/0/0
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30está directamente conectado, Serial0/1/0
L 209.165.200.225/32 está conectado directamente, Serie0 / 1/0
```

- ***Historial de comandos***

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

Para recuperar comandos en el búfer de historial, presione Ctrl+P o la Up Arrow tecla. 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 Down Arrow tecla. 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 show history comando EXEC privilegiado 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. Use el terminal history size comando EXEC del usuario para aumentar o disminuir el tamaño del búfer.

Un ejemplo de los comandos terminal history size y show history se muestra en la figura.

```
R1# terminal history size 200
R1# show history
  show ip int brief
  show interface g0/0/0
  show ip route
  show running-config
  show history
  terminal history size 200
```

4.1.4. Autoevaluación

a) ¿Cuál es la definición del comando Boot System?

- Nombre del archivo de IOS.
- Comando principal.
- Restauración del sistema.

b) ¿Cuál es la función del comando flash_init?

- Muestra los archivos actuales en flash.
- Muestra los directorios almacenados en la BIOS.
- Muestra el estado de la IOS.

c) ¿Qué comando te permite ingresar a la configuración global del router?

- Configure global
- Enable
- Configure terminal

d) ¿Una dirección ip aplicado al SVI permite que el switch enrute paquetes de capa 3?

- Verdadero
- Falso

e) ¿Qué comando te permite asignar o cambiar el nombre de un dispositivo?

- Hostname
- Renable
- Name

4.1.5. Actividad Propuesta: Configurar los ajustes básicos en un router para enrutar entre dos redes conectadas directamente, utilizando CLI

Figura 7.

Tabla de asignación IP.

Dispositivo	Interfaz	Dirección IP / Prefijo	Gateway predeterminado
R1	G0/0/0	172.16.20.1/25	N/D
	G0/0/1	172.16.20.129/25	N/D
	S0/1/0	209.165.200.225/30	N/D
PC1	NIC	172.16.20.10/25	172.16.20.1
PC2	NIC	172.16.20.138/25	172.16.20.129
R2	G0/0/0	2001:db8:c0de:12: :1/64	N/D
	G0/0/1	2001:db8:c0de:13: :1/64	N/D
	/1/1	2001:db8:c0de:11: :1/64	N/D
		fe80::2	No corresponde
PC3	NIC	2001:db8:c0de:12: :a/64	fe80::2
PC4	NIC	2001:db8:c0de:13: :a/64	fe80::2

Nota. Direccionamiento ip de la red.

Objetivos

- Verifique las redes IPv4 conectadas directamente
- Verifique las redes IPv6 conectadas directamente

- Troubleshoot connectivity issues.

Aspectos básicos

Los routers R1 y R2 tienen dos LAN cada uno. Su tarea es verificar el direccionamiento en cada dispositivo y verificar la conectividad entre las LAN.

Nota: la contraseña de EXEC del usuario es cisco. La contraseña de EXEC privilegiado es class.

Instrucciones

Parte 1: Verifique las redes IPv4 conectadas directamente

Paso 1: Verifique las direcciones IPv4 y el estado del puerto en R1.

a. Compruebe el estado de las interfaces configuradas filtrando la salida**.**

```
R1# show ip interface brief | exclude unassigned
```

b. En función de la salida, corrija cualquier problema de estado de puerto que vea.

c. Consulte la Tabla de direcciones y verifique las direcciones IP configuradas en R1. Realice cualquier corrección en el tratamiento si es necesario.

d. Muestra la tabla de enrutamiento filtrando para iniciar la salida en la palabra Gateway.

Nota: Los términos que se utilizan para filtrar la salida se pueden acortar para que coincida con el texto siempre que la coincidencia sea única. Por ejemplo, Gateway, Gate y Ga tendrán el mismo efecto. G no lo hará. El filtrado distingue entre mayúsculas y minúsculas

```
R1# show ip route | begin Gate
```

¿Cuál es el Gateway of last resort address?

e. Muestra la información de la interfaz y el filtro para Descripción o conectado.

Nota: Al utilizar incluir o excluir varias búsquedas se pueden realizar separando las cadenas de búsqueda con un símbolo de tubería (|)

```
R1# show interface | include Desc|conn
```

¿Cuál es el ID de circuito que se muestra en la salida?

f. Mostrar información específica de la interfaz para G0/0/0 filtrando para dúplex.

¿Cuál es la configuración dúplex, la velocidad y el tipo de medio?

Paso 2: Verificar la conectividad

PC1 and PC2 deberían poder hacer ping entre sí y al servidor de doble pila. Si no es así, verifique el estado de las interfaces y las asignaciones de direcciones IP.

Parte 2: Verifique las redes IPv6 conectadas directamente

Paso 1: Verifique las direcciones IPv6 y el estado del puerto en R2.

a. Verifique el estado de las interfaces configuradas.

```
R2# show ipv6 int brief
```

¿Cuál es el estado de las interfaces configuradas?

b. Consulte la Tabla de direcciones y realice las correcciones necesarias en la dirección según sea necesario.

Nota: Al cambiar una dirección IPv6, es necesario eliminar la dirección incorrecta, ya que una interfaz es capaz de admitir varias redes IPv6.

```
R2 (config) # int g0/0/1
R2 (config-if) # no ipv6 address 2001:db8:c0de:14: :1/64
```

Configure la dirección correcta en la interfaz.

c. Mostrar la tabla de routing IPv6.

Nota: Los comandos de filtrado no funcionan actualmente con los comandos IPv6.

d. Mostrar todas las direcciones IPv6 configuradas en las interfaces filtrando la salida de running-config.

Filtrar la salida en R2 para ipv6 o interfaz.

```
R2# sh run | incluye ipv6|interface
```

¿Cuántas direcciones están configuradas en cada interfaz Gigabit?

Paso 2: Verificar la conectividad

PC3 and PC4 deberían poder hacer ping entre sí y al servidor de doble pila. Si no es así, compruebe el estado de la interfaz y las asignaciones de direcciones IPv6.

4.2. Redes redundantes y redes disponibles y confiables.

Esta unidad explicará a los estudiantes cómo STP permite la redundancia en una red de capa 2.y cómo los FHRP proporcionan servicios de gateway predeterminados en una red redundante.

4.1.1. Propósito del 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.

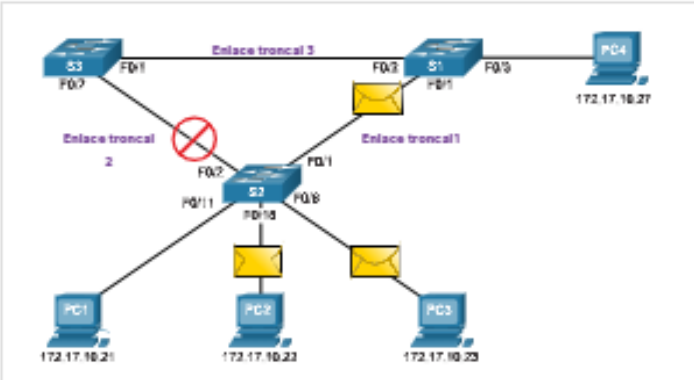
Las LAN Ethernet requieren una topología sin bucles con una única ruta entre dos dispositivos. Un bucle en una LAN Ethernet puede provocar una propagación continua de tramas Ethernet hasta que un enlace se interrumpe y interrumpa el bucle.

- ***Protocolo de árbol de extensión***

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. IEEE 802.1D es el estándar original IEEE MAC Bridging para STP.

Figura 8.

Protocolo STP.

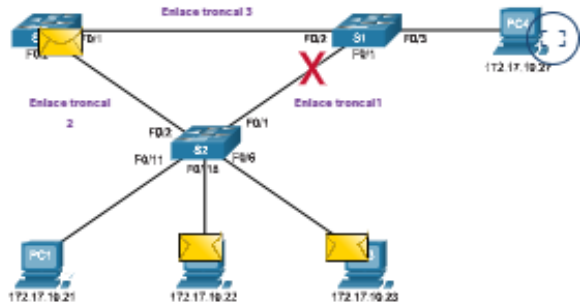


Nota. Operación Normal STP.

- ***Recalcular STP***

Figura 9.

Recálculo de STP



Nota. Operación Normal STP.

- ***Problemas con los vínculos de switch 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 conmutadores, 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 conmutadores y dispositivos finales, lo que hace que la red se vuelva inutilizable.

A diferencia de los protocolos de Capa 3, IPv4 e IPv6, Layer 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 switches retransmite una trama de Capa 2. STP fue desarrollado específicamente como un mecanismo de prevención de bucles para Ethernet de Capa 2.

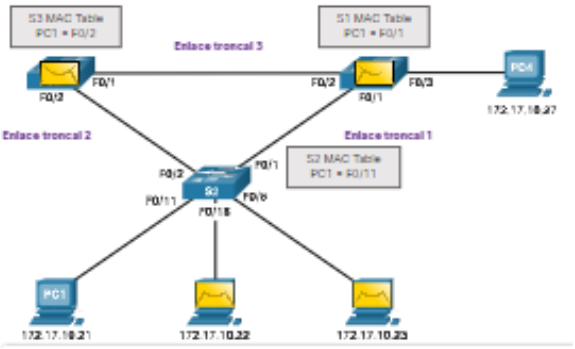
- ***Bucles de la capa 2***

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 en un período de tiempo muy corto, a veces en pocos segundos. Por ejemplo, las tramas de difusión, como una solicitud ARP, se reenvían a todos los puertos del conmutador, excepto el puerto de entrada original. Esto asegura que todos los dispositivos en un dominio de difusión reciban la trama. Si hay más de una ruta para reenviar la trama, se puede formar un bucle infinito. Cuando se produce un bucle, la tabla de direcciones MAC en un conmutador 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.

Las tramas de difusión no son el único tipo de tramas que son afectadas por los bucles. Si se envían tramas de unidifusión desconocidas a una red con bucles, se puede producir la llegada de tramas duplicadas al dispositivo de destino. 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.

Figura 10.

Bucles de capa 2.



Nota. Operación de un bucle de la capa 2.

- ***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 conmutadores 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. Es probable que un bucle de capa 2 tenga consecuencias inmediatas y de desactivación en la red. Las multidifusión de capa 2 normalmente se reenvían de la misma manera que una difusión por el conmutador. Por lo tanto, aunque los paquetes IPv6 nunca se reenvían como una difusión de Capa 2, ICMPv6 Neighbor Discovery utiliza multidifusión de Capa 2.

Figura 11.

Tormenta de difusión.

Nota. Operación Normal STP.

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 conmutador no sabe desde qué puerto reenviar las tramas de unidifusión. En la animación anterior, los conmutadores tendrán los puertos incorrectos listados para PC1. Cualquier trama de unidifusión con destino a la PC1 se repite en bucle por la red, como

lo hacen las tramas de difusión. Cuando se repiten en bucle cada vez más tramas, se termina creando una tormenta de difusión.

Para evitar que ocurran estos problemas en una red redundante, se debe habilitar algún tipo de árbol de expansión en los switches. De manera predeterminada, el árbol de expansión está habilitado en los switches Cisco para prevenir que ocurran bucles en la capa 2.

- ***El algoritmo de árbol de expansión***

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 conmutadores determinan una única ruta de menor costo.

Sin el protocolo de prevención de bucles, se producirían bucles que harían inoperable una red de conmutadores redundantes.

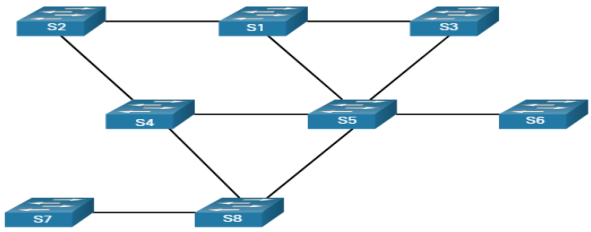
STP evita que ocurran bucles mediante la configuración de una ruta sin bucles a través de la red, con puertos “en estado de bloqueo” ubicados estratégicamente. Los switches que ejecutan STP pueden compensar las fallas mediante el desbloqueo dinámico de los puertos bloqueados anteriormente y el permiso para que el tráfico se transmita por las rutas alternativas.

Topología de la situación

Este escenario STA utiliza una LAN Ethernet con conexiones redundantes entre varios conmutadores.

Figura 12.

Conexiones redundantes



Nota. Varios conmutadores conectados.

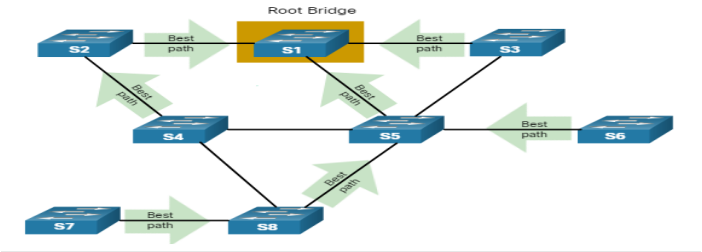
Seleccionar el Root Bridge

El algoritmo de árbol de expansión comienza seleccionando un único puente raíz. La figura muestra que el switch S1 se ha seleccionado como puente raíz. En esta topología, todos los enlaces tienen el mismo costo (mismo ancho de banda). Cada switch determinará una única ruta de menor costo desde sí mismo hasta el puente raíz.

Nota: STA y STP se refieren a conmutadores como puentes. Esto se debe a que en los primeros días de Ethernet, los switches se denominaban puentes.

Figura 13.

STA y STP



Nota. Los switches sirven como puentes.

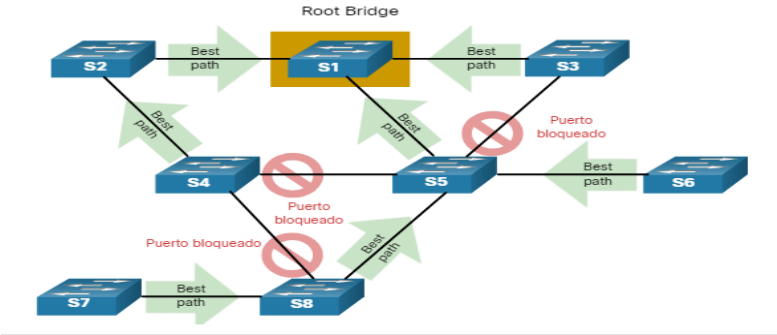
Bloquear rutas redundantes

STP asegura que solo haya una ruta lógica entre todos los destinos en la red al bloquear intencionalmente las rutas redundantes que podrían causar un bucle, como se muestra en la figura. Cuando se bloquea un puerto, se impide que los datos del usuario

entren o salgan de ese puerto. El bloqueo de las rutas redundantes es fundamental para evitar bucles en la red.

Figura 14.

Bloqueo de rutas.



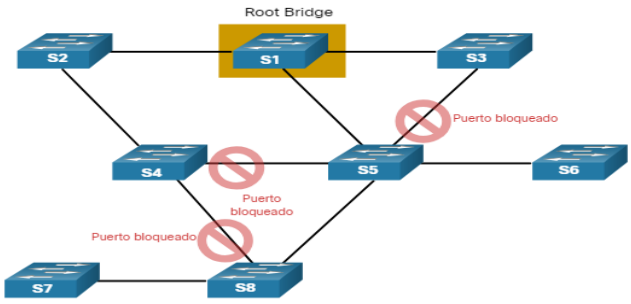
Nota. Los conmutadores S4, S5 y S8 han bloqueado rutas redundantes al puente raíz.

Topología sin bucle

Un puerto bloqueado tiene el efecto de convertir ese enlace en un vínculo no reenvío entre los dos switches, como se muestra en la figura. Observe que esto crea una topología en la que cada conmutador tiene una única ruta al puente raíz, similar a las ramas de un árbol que se conectan a la raíz del árbol.

Figura 15.

Topología sin bucle.



Nota. Cada conmutador tiene ahora sólo una ruta de reenvío al puente raíz.

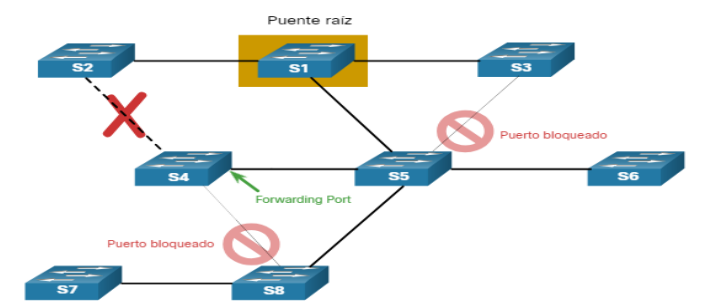
Fallos de enlace causan recálculo

Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen 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 conmutador o un nuevo vínculo entre switches a la red.

La figura muestra un error de enlace entre los conmutadores S2 y S4 que hace que STP se vuelva a calcular. Observe que el vínculo anteriormente redundante entre S4 y S5 se está reenviando para compensar este error. Todavía hay solo una ruta entre cada switch y el puente raíz.

Figura 16.

Fallo de enlace



Nota. El error de enlace provoca el recalculo de STP.

4.2.2. Evolución del STP

- ***Diferentes versiones de STP***

En este tema se detallan las diferentes versiones de STP y otras opciones para evitar bucles en la red.

Hasta ahora, hemos utilizado el término Protocolo Spanning Tree y el acrónimo STP, que puede ser engañoso. La mayoría de los profesionales suele utilizar estas

denominaciones para referirse a las diversas implementaciones del árbol de expansión, como el protocolo de árbol de expansión rápido (RSTP) y el protocolo de árbol de expansión múltiple (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 último estándar para árbol de expansión está contenido en IEEE-802-1D-2004, el estándar IEEE para redes de área local y metropolitana:puentes de control de acceso a medios (MAC). Esta versión del estándar indica que los conmutadores y puentes que cumplen con el estándar utilizarán Rapid Spanning Tree Protocol (RSTP) en lugar del protocolo STP anterior especificado en el estándar 802.1d original. En este currículo, cuando se analiza el protocolo de árbol de expansión original, se utiliza la frase “árbol de expansión 802.1D original” para evitar confusiones. 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.

Desde el lanzamiento del estándar IEEE 802.1D original, surgió una gran variedad de protocolos de árbol de expansión.

STP.- Esta es la versión original de IEEE 802.1D (802.1D-1998 y versiones 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 provides a separate 802.1D spanning tree instance for each VLAN Configure la red

PVST+ soporta PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, y loop guard.

802.1D-2004. - Esta es una versión actualizada del estándar STP, que incorpora IEEE 802.1w.

RSTP. - Protocolo de Árbol de Expansión Rápido (RSTP), o IEEE 802.1w, es una evolución de STP que proporciona una convergencia más veloz de STP. Proporciona una convergencia más rápida de STP.

PVST+ rápido. - Esta es una mejora de Cisco de RSTP que utiliza PVST + y proporciona una instancia separada de 802.1w por VLAN. Cada instancia independiente admite PortFast, BPDU guard, BPDU filter, root guard, y loop guard.

MSTP. - El Protocolo de árbol de expansión múltiple (MSTP) es un estándar IEEE inspirado en el STP de instancia múltiple (MISTP) anterior propietario de Cisco de Cisco. MSTP asigna varias VLAN en la misma instancia de árbol de expansión. VRF.

Instancia. - Múltiple Spanning Tree (MST) es la implementación de MSTP de Cisco, que proporciona hasta 16 instancias de RSTP y combina muchas VLAN con el misma topología física y lógica en una instancia RSTP común. Cada instancia aparte admite PortFast, protección de BPDU, filtro de BPDU, protección de raíz y protección de bucle. loop guard.

Es posible que un profesional de red, cuyas tareas incluyen la administración de los switches, deba decidir cuál es el tipo de protocolo de árbol de expansión que se debe implementar.

Los switches 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 conmutadores deben configurarse explícitamente para el modo de árbol de expansión rápida para ejecutar el protocolo de árbol de expansión rápida.

- ***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 como puerto alternativo o de respaldo, puede cambiar automáticamente al estado de reenvío sin esperar a que converja la red.

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

- ***Estados de puertos RSTP y roles de puerto***

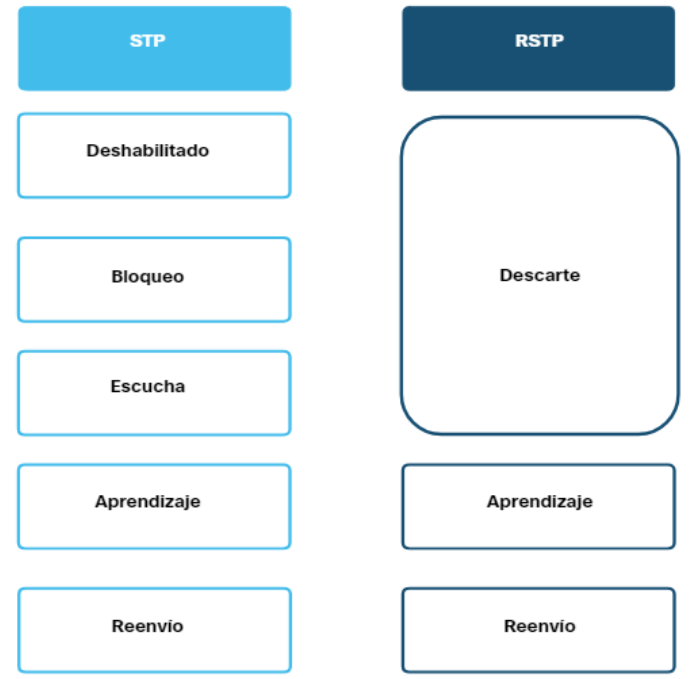
Los estados de puerto y las funciones de puerto entre STP y RSTP son similares.

Estados de puertos STP y RSTP

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.

Figura 17.

STP y RSTP



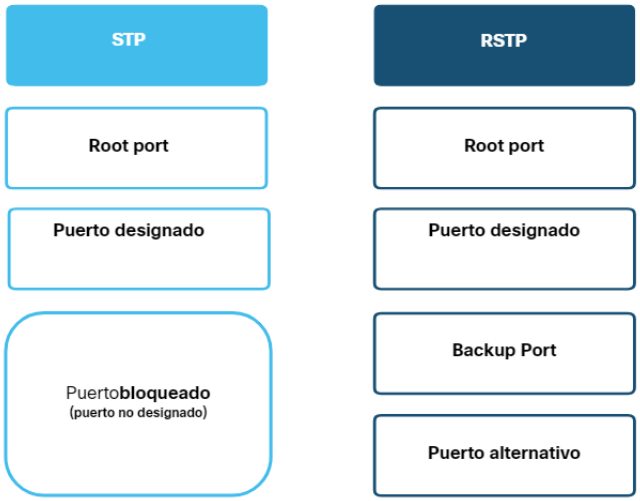
Nota. Estados de STP y RSTP.

Estados de puertos STP y RSTP

Como se muestra en la figura, 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.

Figura 18.

Estados de puertos STP y RSTP



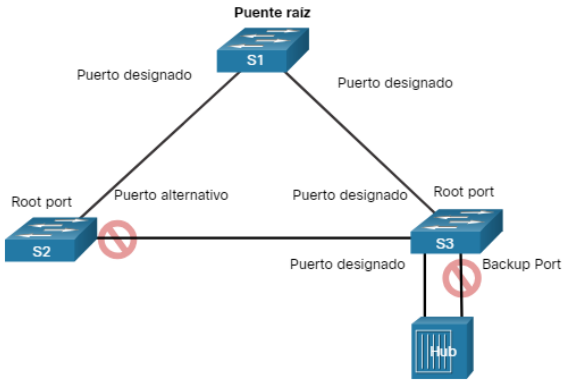
Nota. Los puertos raíz y puertos designados son para ambos .

Puertos RSTP alternativos y de copia de seguridad

Como se muestra en la figura, 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.

Figura 19.

Puertos RSTP



Nota. Cada puerto RSTP tiene su función en la red.

- ***PorFast y protección BPDU***

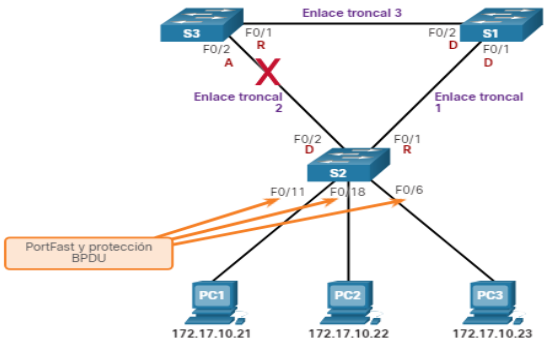
Cuando un dispositivo está conectado a un puerto del conmutador o cuando un conmutador se enciende, el puerto del conmutador pasa por los estados de escucha y aprendizaje, esperando cada vez que expire el temporizador de retardo de reenvío. Este retraso es de 15 segundos para cada estado, escuchando y aprendiendo, para un total de 30 segundos. Este retraso puede presentar un problema para los clientes DHCP que intentan detectar un servidor DHCP. Los mensajes DHCP del host conectado no se reenviarán durante los 30 segundos de temporizadores de retardo de reenvío y el proceso DHCP puede agotarse. El resultado es que un cliente IPv4 no recibirá una dirección IPv4 válida.

Note: Aunque esto puede ocurrir con clientes que envían mensajes de solicitud de enrutador ICMPv6, el enrutador continuará enviando mensajes de anuncio de enrutador ICMPv6 para que el dispositivo sepa cómo obtener su información de dirección.

Cuando un puerto de conmutador se configura con PortFast, ese puerto pasa del bloqueo al estado de reenvío inmediatamente, omitiendo los estados de escucha y aprendizaje STP y evitando un retraso de 30 segundos. Use PortFast en los puertos de acceso para permitir que los dispositivos conectados a estos puertos, como los clientes DHCP, accedan a la red de inmediato, en lugar de esperar a que STP converja en cada VLAN. Debido a que el propósito de PortFast es minimizar el tiempo que los puertos de acceso deben esperar a que el árbol de expansión converja, solo debe usarse en los 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. PortFast solo se puede usar en puertos conmutadores que se conectan a dispositivos finales.

Figura 20.

PortFast y protección BPDU.



Nota. El BPDU indica la existencia de otro puente o switch conectado.

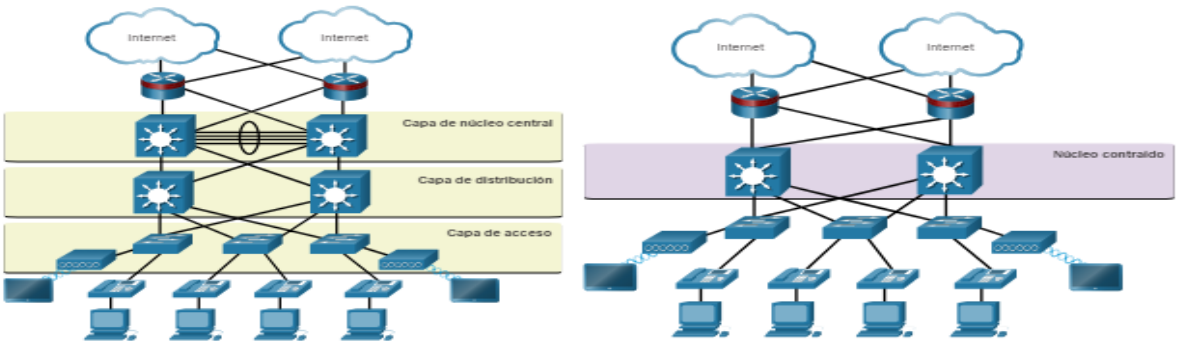
En una configuración de PortFast válida, nunca se deben recibir BPDU, ya que esto indicaría que hay otro puente o switch conectado al puerto, lo que podría causar un bucle de árbol de expansión. Esto potencialmente causa un bucle de árbol de expansión. Para evitar que se produzca este tipo de escenario, los switches Cisco admiten una función llamada guardia BPDU. Cuando está habilitado, inmediatamente pone el puerto del conmutador en un estado errdisabled (error-disabled) al recibir cualquier BPDU. Esto protege contra posibles bucles al apagar eficazmente el puerto. La característica de protección BPDU proporciona una respuesta segura a la configuración no válida, ya que se debe volver a activar la interfaz de forma manual.

- ***Alternativas a STP***

STP era y sigue siendo un protocolo de prevención de bucles Ethernet. A lo largo de los años, las organizaciones requerían una mayor resiliencia y disponibilidad en la LAN. Las LAN Ethernet pasaron de unos pocos conmutadores interconectados conectados a un único enrutador, a un sofisticado diseño de red jerárquica que incluye conmutadores de acceso, distribución y capa central, como se muestra en la figura.

Figura 21.

Distribución y capa central.



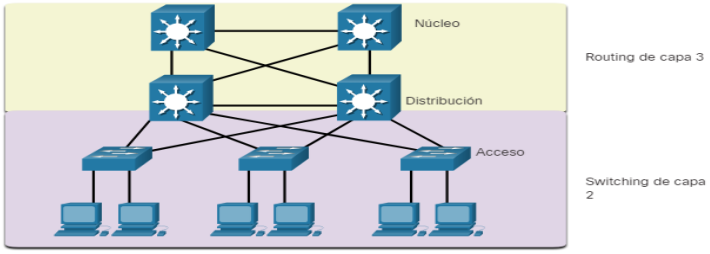
Nota. Se pueden incluir otras capas en la capa 2.

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 switches, 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 predecibilidades proporcionadas por los protocolos de enrutamiento en la Capa 3. La figura muestra un diseño de red jerárquica tradicional con los conmutadores multicapa de distribución y núcleo que realizan enrutamiento.

Figura 22.

Red jerárquica tradicional



Nota. Distribución de la red jerárquica.

Aunque es muy probable que STP siga utilizándose como mecanismo de prevención de bucles en la empresa, en los conmutadores de capa de acceso también se están utilizando otras tecnologías, incluidas las siguientes:

Agregación de enlaces de

- Múltiples sistemas (MLAG)
- Puente de ruta más corta (SPB)
- Interconexión transparente de muchos enlaces. (TRILL)
- Note: Estas tecnologías están fuera del alcance de este curso.

4.2.3. Conceptos de DHCPv4

- ***Servidor y cliente DHCPv4***

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.

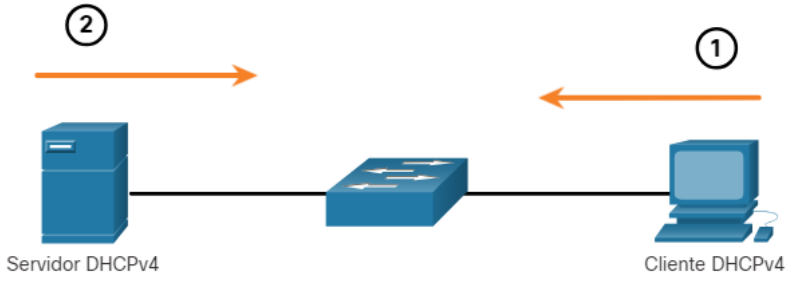
El servidor DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.

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.

Figura 23.

Servidor y Cliente DHCPv4.



Nota. Comunicación entre servidor y cliente.

- ***Funcionamiento de DHCPv4***

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 un arrendamiento***

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). -** El cliente inicia el proceso con un mensaje de difusión DHCPDISCOVER con su propia dirección MAC para detectar los servidores de DHCPv4 disponibles. Dado que el cliente no tiene información de IPv4 válida durante el arranque, utiliza direcciones de difusión de capa 2 y de capa 3 para comunicarse con el servidor. El propósito del mensaje DHCPDISCOVER es encontrar los servidores de DHCPv4 en la red.
2. **Oferta de DHCP (DHCPOFFER).-** Cuando el servidor de DHCPv4 recibe un mensaje DHCPDISCOVER, reserva una dirección IPv4 disponible para arrendar al cliente. El servidor también crea una entrada ARP que consta de la dirección MAC del cliente que realiza la solicitud y la dirección IPv4 arrendada del cliente. El servidor de DHCPv4 envía el mensaje DHCPOFFER asignado al cliente que realiza la solicitud.
3. **Solicitud de DHCP (DHCPREQUEST). -** Cuando el cliente recibe el mensaje DHCPOFFER proveniente del servidor, envía un mensaje DHCPREQUEST. Este mensaje se utiliza tanto para el origen como para la renovación del arrendamiento. Cuando se utiliza para el origen del arrendamiento, el mensaje DHCPREQUEST sirve como notificación de aceptación vinculante al servidor seleccionado para los parámetros que ofreció y como un rechazo implícito a cualquier otro servidor que pudiera haber proporcionado una oferta vinculante al cliente.

   Muchas redes empresariales utilizan varios servidores de DHCPv4. El mensaje DHCPREQUEST se envía en forma de difusión para informarle a este servidor de DHCPv4 y a cualquier otro servidor de DHCPv4 acerca de la oferta aceptada.
4. **Acuse de recibo de DHCP (DHCPACK). -** Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento con un ping ICMP a esa dirección para asegurarse de que no esté en uso, crea una nueva entrada ARP para el arrendamiento del cliente y responde con un mensaje DHCPACK. El mensaje

DHCPACK es un duplicado del mensaje DHCPOFFER, a excepción de un cambio en el campo de tipo de mensaje. Cuando el cliente recibe el mensaje DHCPACK, registra la información de configuración y realiza una búsqueda de ARP para la dirección asignada. Si no hay respuesta al ARP, el cliente sabe que la dirección IPv4 es válida y comienza a utilizarla como propia.

- ***Pasos para renovar un contrato de arrendamiento***

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. Detección 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.

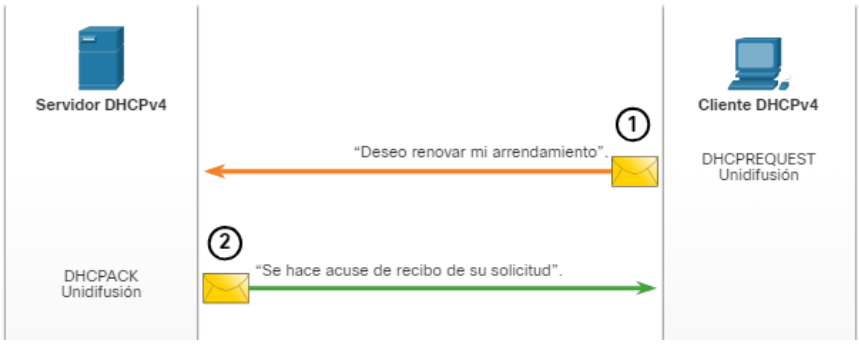
2. Ofrecimiento de DHCP (DHCPACK)

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.

Figura 24.

Arrendamiento DHCPv4



Nota. Proceso de arrendamiento DHCPv4 del cliente al servidor.

4.2.3. Asignación de direcciones de unidifusión global IPV6

- ***Configuración de host con IPV6***

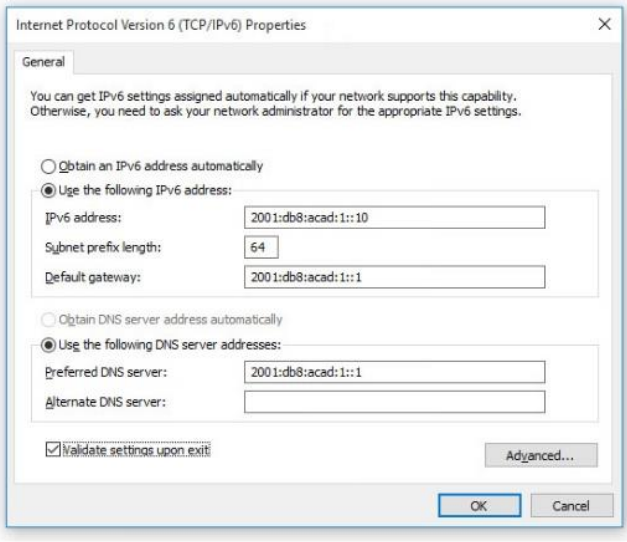
En primer lugar, lo más importante. Para utilizar la configuración automática de direcciones stateless (SLAAC) o DHCPv6, debe revisar las direcciones globales de unidifusión (GUA) y las direcciones link-local (LLAs). Este tema abarca ambas cosas.

En un router, una dirección global de unidifusión (GUA) IPv6 se configura manualmente mediante el comando de configuración ipv6 address 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.

Figura 25.

IPV6

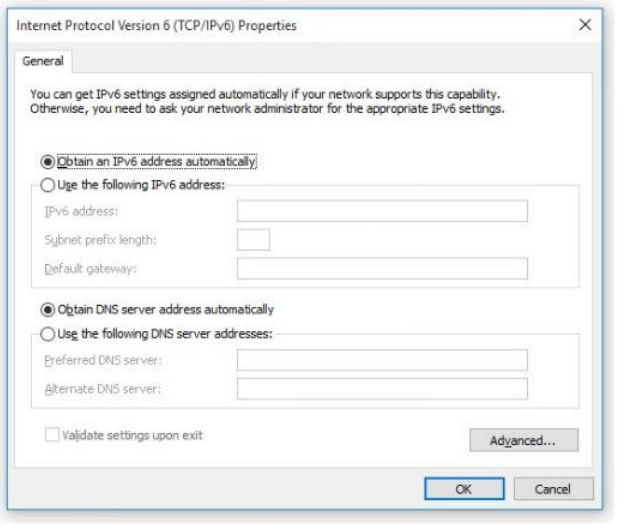


Nota. Cuadro de propiedades del protocolo IPVP6..

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, como se muestra en la figura.

Figura 26.

IPV6 Dinamico.



Nota. Se pueden incluir otras capas en la capa 2.

- ***IPV6 Host Link-Local Address***

Cuando se selecciona el direccionamiento IPv6 automático, el host intentará obtener y configurar automáticamente la información de direcciones IPv6 en la interfaz. El host utilizará uno de los tres métodos definidos por el Internet Control Message Protocol version 6 (ICMPv6) mensaje Router Advertisement (RA) recibidos en la interfaz. Un router IPv6 que está en el mismo vínculo que el host envía mensajes de RA que sugieren a los hosts cómo obtener su información de direccionamiento IPv6. El host crea automáticamente la dirección local del vínculo IPv6 cuando se inicia y la interfaz Ethernet está activa. El ipconfig resultado de ejemplo muestra una dirección link-local (LLA) generada automáticamente en una interfaz.

En la figura, observe que la interfaz no creó una GUA IPv6. La razón se debe a que, en este ejemplo, el segmento de red no tiene un router que proporcione instrucciones de configuración de red para el host.

Nota: A veces, los sistemas operativoshost mostrarán una dirección link-local anexada con un "%" y un número. Esto se conoce como Id. de zona o Id. de ámbito. Es utilizado por el sistema operativo para asociar el LLA con una interfaz específica.

```
      Nota: DHCPv6 se define en RFC 3315.
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . :
   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:\PC1>
```

- ***IPV6 GUA Asignment***

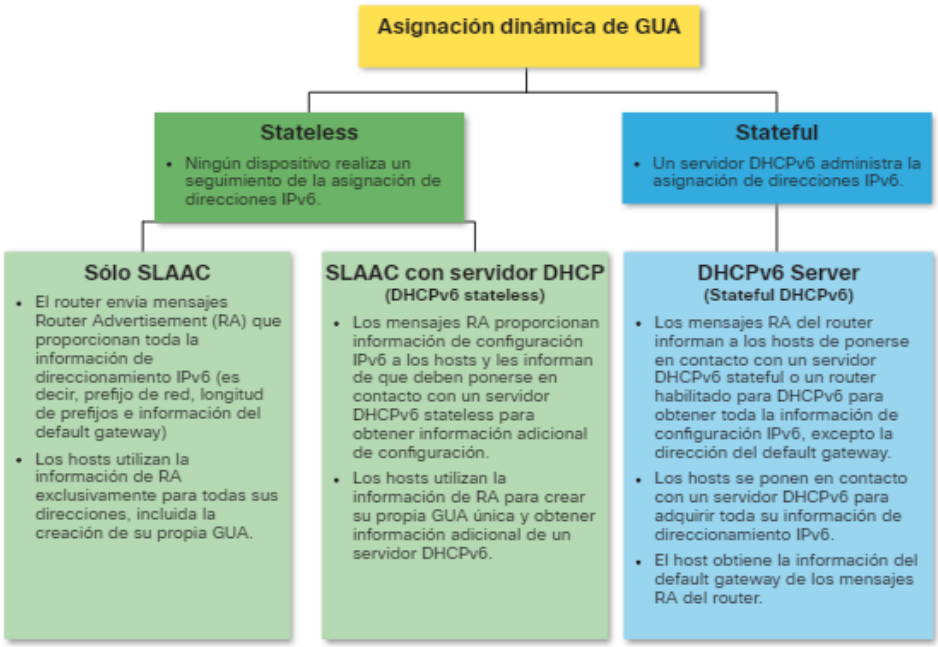
Pv6 fue diseñado para simplificar la forma en que un host puede adquirir su configuración IPv6. De forma predeterminada, un router habilitado para IPv6 anuncia su información IPv6. Esto permite a un host crear o adquirir dinámicamente su configuración IPv6.

IPv6 GUA se puede asignar dinámicamente utilizando servicios stateless y stateful, como se muestra en la figura.

Todos los métodos stateless y stateful 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 del RA, la decisión real depende en última instancia del host.

Figura 27.

Asignación dinámica de GUA.



Nota. Métodos Stateless y Stateful.

- ***Tres Flags de mensajes RA***

La decisión de cómo un cliente obtendrá un GUA IPv6 depende de la configuración dentro del mensaje RA. Un mensaje de RA ICMPv6 incluye tres flags para identificar las opciones dinámicas disponibles para un host, como se indica a continuación:

Un flag - Este es el indicador de configuración automática de direcciones. Usa Stateless Address Autoconfiguration (SLAAC) para crear un GUA de IPv6.

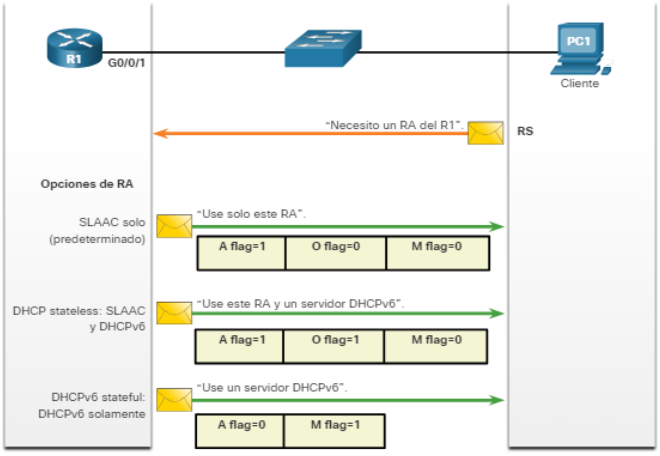
O flag - Este es otro indicador de configuración (Other) Otra información está disponible desde un servidor DHCPv6 stateless.

M flag - Este es es indicador Managed Address. Utilice un servidor DHCPv6 stateful para obtener una GUA IPv6.

Mediante diferentes combinaciones de los flags A, O y M, los mensajes RA informan al host sobre las opciones dinámicas disponibles. La figura ilustra estos tres métodos

Figura 28.

Combinaciones de los Flags.



Nota. Funcionamientos de los métodos.

4.2.6. SLAAC

- ***Descripción general de 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 stateless. Esto 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 utiliza mensajes ICMPv6 RA para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor DHCP Un host configura su dirección IPv6 en función de la información que se envía en la RA. Los mensajes RA son enviados por un router IPv6 cada 200 segundos.

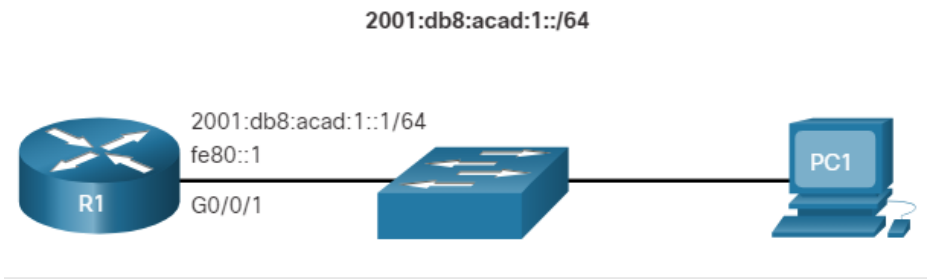
Un host también puede enviar un mensaje Router Solicitation (RS) solicitando que un router habilitado para IPv6 envíe al host un RA. SLAAC se puede implementar como SLAAC solamente, o SLAAC con DHCPv6.

- ***Activación de SLAAC***

Consulte la topología siguiente para ver cómo está habilitado SLAAC para proporcionar asignación GUA dinámica stateless.

Figura 29.

Asignación GUA dinámica stateless



Nota. Habilitación de SLAAC para la asignación.

Suponga que R1 GigabitEthernet 0/0/1 se ha configurado con la GUA IPv6 indicada y direcciones link-local. Haga clic en cada botón para obtener una explicación de cómo R1 está habilitado para SLAAC.

Verificar direcciones IPV6

El resultado del show ipv6 interface comando muestra la configuración actual en la interfaz G0/0/1.

Como se destaca, a R1 se le han asignado las siguientes direcciones IPv6:

- Link-local IPv6 address - fe80::1
- GUA and subnet - 2001:db8:acad:1: :1 y 2001:db8:acad:1: :/64
- IPv6 all-nodes group - ff02::1

```
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
  Unido a la direccion grupal(es):
    FF02::1
    FF02::1:FF00:1
(output omitted)
R1#
```

Habilitar enrutamiento IPV6

Aunque la interfaz del router tiene una configuración IPv6, todavía no está habilitada para enviar RA que contengan información de configuración de direcciones a hosts que utilicen SLAAC.

Para habilitar el envío de mensajes RA, un router debe unirse al grupo de todos los routers IPv6 mediante el comando ipv6 unicast-routing global config, como se muestra en el ejemplo.

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

Verificar que SLAAC este habilitado

El grupo de todos los routers IPv6 responde a la dirección de multidifusión IPv6 ff02 :: 2. Puede utilizar el show ipv6 interface comando para verificar si un router está habilitado como se muestra, en el ejemplo.

Un router Cisco habilitado para IPv6 envía mensajes RA a la dirección de multidifusión de todos los nodos IPv6 ff02: :1 cada 200 segundos.

```
R1# show ipv6 interface G0/0/1 | section Joined
  Unido a la direccion grupal(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
R1#
```

- ***Método Sólo SLAAC***

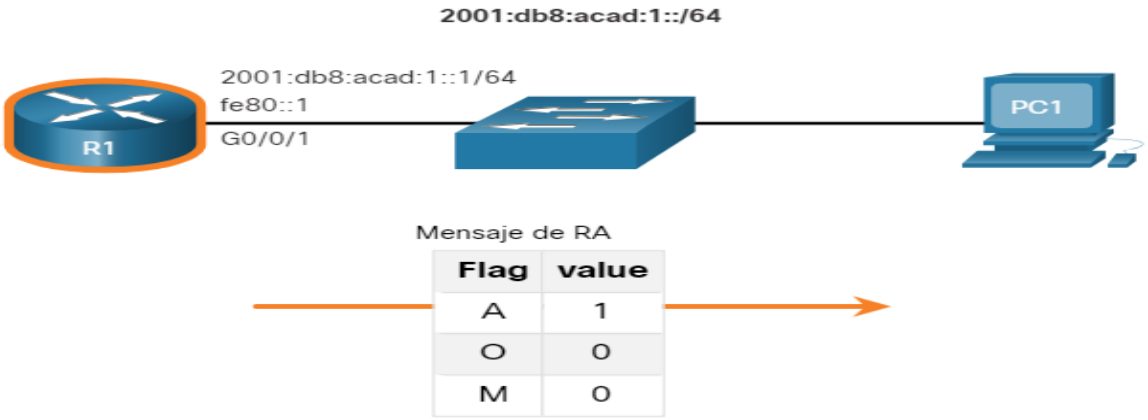
El método sólo SLAAC está habilitado de forma predeterminada cuando se configura el ipv6 unicast-routing comando. Todas las interfaces Ethernet habilitadas con un GUA IPv6 configurado comenzarán a enviar mensajes RA con el flag A establecido en 1 y los flags O y M establecidos en 0, como se muestra en la figura.

El A = 1 flag sugiere al cliente que cree su propio IPv6 GUA usando el prefijo anunciado en la RA. El cliente puede crear su propio ID de interfaz utilizando el método Extended Unique Identifier (EUI-64) o hacer que se genere aleatoriamente.

Los flags O =0 y M=0 le indican al cliente que use la información del mensaje RA exclusivamente. Esto incluye información del prefijo, de la longitud de prefijo, del servidor DNS, de la MTU y del default gateway. No se encuentra disponible ninguna otra información de un servidor de DHCPv6

Figura 30.

Estado de Flag



Nota. Valor de los métodos flag en la asignación..

En el ejemplo, PC1 esta habilitada para obtener su información de direccion de IPv6 de forma automática. Debido a la configuración de los flags A, O y M, PC1 sólo realiza SLAAC, utilizando la información contenida en el mensaje RA enviado por R1.

La dirección del default gateway es la dirección IPv6 de origen del mensaje RA, que es la LLA para R1. El default gateway solo se puede obtener de forma automática mediante un mensaje RA. Un servidor DHCPv6 no proporciona esta información.

```
C:\PC1> 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%21
C:\PC1>
```

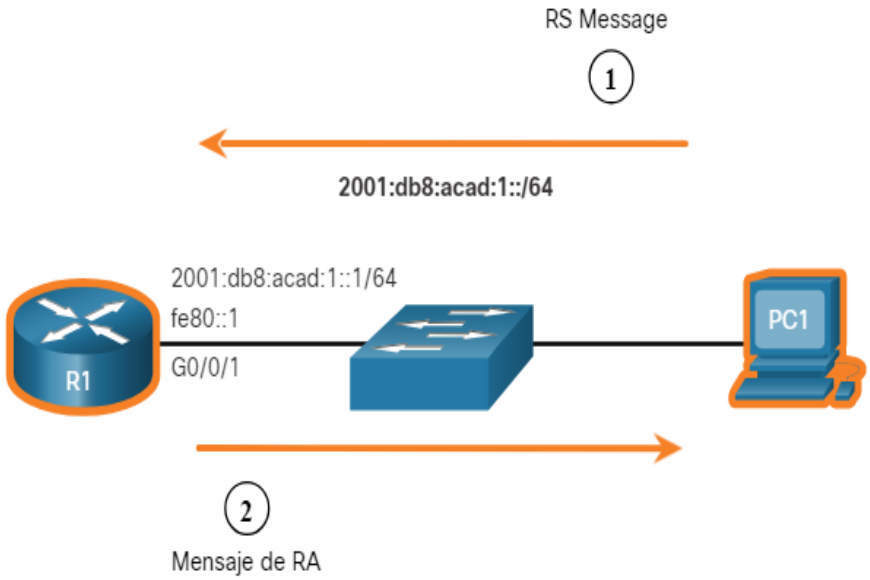
- ***ICMPV6 RS Messages***

Un router envía mensajes de RA cada 200 segundos. Sin embargo, también enviará un mensaje RA si recibe un mensaje RS de un host.

Cuando un cliente está configurado para obtener su información de direccionamiento automáticamente, envía un mensaje RS a la dirección de multidifusión IPv6 de ff02: :2.

Figura 31.

Multidifusión IPV6



Nota. Ilustración de como un host inicia el método SLAAC.

- ***Proceso de host para generar ID de interfaz***

Mediante SLAAC, un host suele adquirir su información de subred IPv6 de 64 bits del RA del router. Sin embargo, debe generar el resto del identificador de interfaz (ID) de 64 bits utilizando uno de estos dos métodos:

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.

Por ejemplo, en el siguiente ipconfig resultado, el host PC1 de Windows 10 utilizó la información de subred IPv6 contenida en el R1 RA y generó aleatoriamente un ID de interfaz de 64 bits como se destaca en el ejemplo.

```
C:\PC1> 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:\PC1>
```

- ***Detección de direcciones duplicadas***

El proceso permite al host crear una dirección IPv6. Sin embargo, no hay garantía de que la dirección sea única en la red.

Ya que SLAAC es stateless; por lo tanto, un host tiene la opción de verificar que una dirección IPv6 recién creada sea única antes de que pueda usarse Un host utiliza el proceso de detección de direcciones duplicadas (DAD) para asegurarse de que IPv6 GUA es único.

DAD se implementa usando ICMPv6. Para realizar DAD, el host envía un mensaje ICMPv6 NS con una dirección de multidifusión especialmente construida, llamada dirección de multidifusión de nodo solicitado. Esta dirección duplica los últimos 24 bits de dirección IPv6 del host.

Si ningún otro dispositivo responde con un mensaje NA, prácticamente se garantiza que la dirección es única y puede ser utilizada por la PC1. Si un mensaje NA es recibido

por el host, la dirección no es única, y el sistema operativo debe determinar una nueva ID de interfaz para utilizar.

Internet Engineering Task Force (IETF) recomienda que DAD se utilice en todas las direcciones de unidifusión IPv6 independientemente de si se crea con SLAAC sólo, se obtiene con DHCPv6 stateful, o se configura manualmente. DAD no es obligatorio porque un ID de interfaz de 64 bits proporciona 18 quintillion de posibilidades y la posibilidad de que haya una duplicación es remota. Sin embargo, la mayoría de los sistemas operativos realizan DAD en todas las direcciones de unidifusión IPv6, independientemente de cómo se configure la dirección.

4.2.6. Protocolos de Redundancia de primer salto

- ***Limitaciones del Gateway Predeterminado***

Si falla un router o una interfaz del router (que funciona como gateway predeterminado), los hosts configurados con ese gateway predeterminado quedan aislados de las redes externas. Se necesita un mecanismo para proporcionar gateways predeterminados alternativos en las redes conmutadas donde hay dos o más routers conectados a las mismas VLAN. Este mecanismo es proporcionado por los protocolos de redundancia de primer salto (FHRP).

En una red conmutada, cada cliente recibe solo un gateway predeterminado. No hay forma de usar un gateway secundario, incluso si existe una segunda ruta que transporte paquetes fuera del segmento local.

En la figura, el R1 es el responsable de enrutar los paquetes de la PC1. Si el R1 deja de estar disponible, los protocolos de routing pueden converger de forma dinámica.

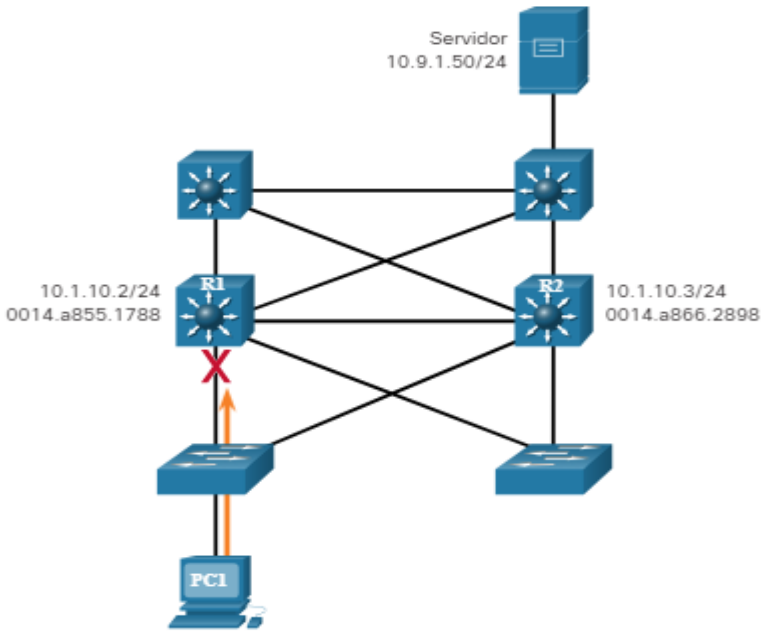
Ahora, el R2 enruta paquetes de redes externas que habrían pasado por el R1. Sin embargo, el tráfico de la red interna asociado al R1, incluido el tráfico de las estaciones de trabajo, de los servidores y de las impresoras que se configuraron con el R1 como gateway predeterminado, aún se envía al R1 y se descarta.

Nota: Nota: Para los efectos del análisis de la redundancia de los routers, no hay diferencia funcional entre un switch capa 3 y un router en la capa de distribución. En la práctica, es común que un switch capa 3 funcione como gateway predeterminado para cada VLAN en una red conmutada. Esta discusión se centra en la funcionalidad del enrutamiento, independientemente del dispositivo físico utilizado.

La topología de red física muestra dos switches, un router, un PC y un servidor (server). Las PC, PC1, está enviando un paquete a través de la red. El gráfico muestra el paquete que se está descartando en la interfaz de R1.

Figura 32.

Topología de 2 switches.



Nota. PC1 no puede alcanzar la puerta de enlace predeterminada.

Por lo general, los dispositivos finales o terminales se configuran con una única dirección IPv4 para un gateway predeterminado. Esta dirección no se modifica cuando cambia la topología de la red. Si no se puede llegar a esa dirección IPv4 de gateway predeterminado, el dispositivo local no puede enviar paquetes fuera del segmento de red local, lo que lo desconecta completamente de las demás redes. Aunque exista un router redundante que sirva como puerta de enlace predeterminada para ese segmento, no hay un método dinámico para que estos dispositivos puedan determinar la dirección de una nueva puerta de enlace predeterminada.

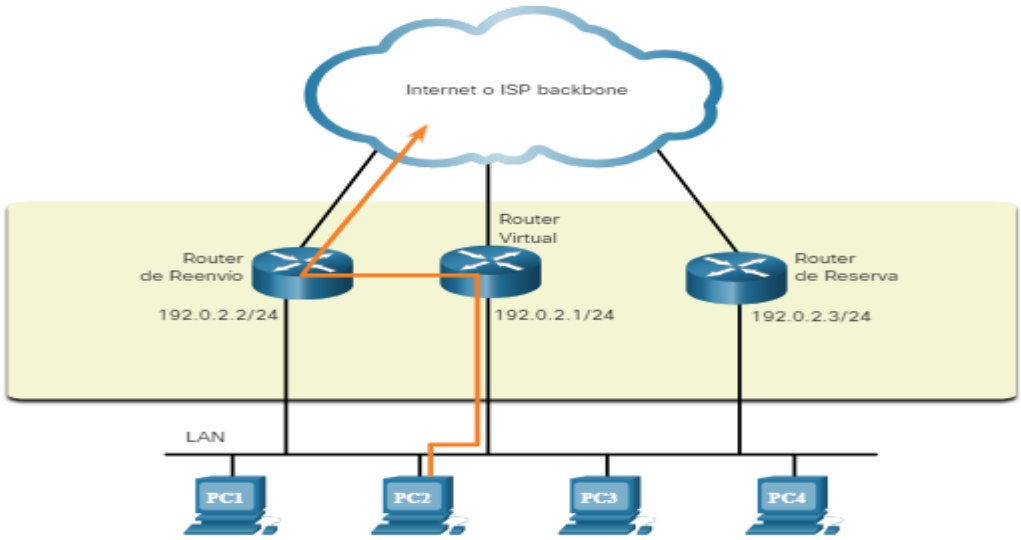
Nota: Los dispositivos IPv6 reciben dinámicamente su dirección de puerta de enlace predeterminada del anuncio de router ICMPv6. Sin embargo, los dispositivos IPv6 se benefician con una conmutación por error más rápida a la nueva puerta de enlace predeterminada cuando se utiliza FHRP

- ***Redundancia del router***

Una forma de evitar un único punto de falla en el gateway predeterminado es implementar un router virtual. Como se muestra en la figura, para implementar este tipo de redundancia de router, se configuran varios routers para que funcionen juntos y así dar la sensación de que hay un único router a los hosts en la LAN. Al compartir una dirección IP y una dirección MAC, dos o más routers pueden funcionar como un único router virtual.

Figura 33.

Red LAN



Nota. Red Lan con enlaces troncales.

La dirección IPv4 del router virtual se configura como la puerta de enlace predeterminada para las estaciones de trabajo de un segmento específico de IPv4. Cuando se envían tramas desde los dispositivos host hacia el gateway predeterminado, los hosts utilizan ARP para resolver la dirección MAC asociada a la dirección IPv4 del gateway predeterminado. La resolución de ARP devuelve la dirección MAC del router virtual. El router actualmente activo dentro del grupo de routers virtuales puede procesar físicamente las tramas que se envían a la dirección MAC del router virtual. Los protocolos se utilizan para identificar dos o más routers como los dispositivos responsables de procesar tramas que se envían a la dirección MAC o IP de un único router virtual. Los dispositivos host envían el tráfico a la dirección del router virtual. El router físico que reenvía este tráfico es transparente para los dispositivos host.

Un protocolo de redundancia proporciona el mecanismo para determinar qué router debe cumplir la función activa en el reenvío de tráfico. Además, determina cuándo un router de reserva debe asumir la función de reenvío. La transición entre los routers de reenvío es transparente para los dispositivos finales.

La capacidad que tiene una red para recuperarse dinámicamente de la falla de un dispositivo que funciona como gateway predeterminado se conoce como “redundancia de primer salto”.

- ***Pasos para la conmutación por falla del router***

Cuando falla el router activo, el protocolo de redundancia hace que el router de reserva asuma el nuevo rol de router activo, como se muestra en la figura. Estos son los pasos que se llevan a cabo cuando falla el router activo:

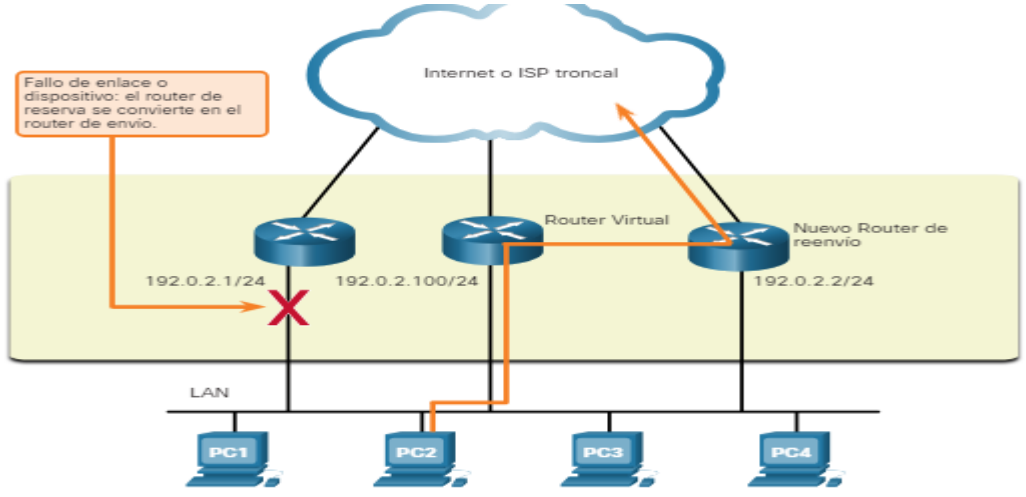
El router de reserva deja de recibir los mensajes de saludo del router de reenvío.

El router de reserva asume la función del router de reenvío.

Debido a que el nuevo router de reenvío asume tanto la dirección IPv4 como la dirección MAC del router virtual, los dispositivos host no perciben ninguna interrupción en el servicio.

Figura 34.

Internet o ISP troncal



Nota. Por la existencia de un fallo, el router de reserva se convierte en el router de envio.

- ***Opciones de FHRP***

La FHRP utilizada en un entorno de producción depende en gran medida del equipo y las necesidades de la red.

Protocolo de Router de Reserva Directa (HSRP, Hot Standby Router Protocol)

HRSP es una FHRP propietaria de Cisco que está diseñada para permitir conmutación por error (failover) transparente de un dispositivo IPv4 de primer salto. HSRP proporciona alta disponibilidad de red al proporcionar redundancia de enrutamiento de primer salto para IPv4 hosts en redes configuradas con una dirección de puerta de enlace predeterminada IPv4. HSRP se utiliza en un grupo de routers para seleccionar un dispositivo activo y un dispositivo de espera. En un grupo de interfaces de dispositivo, el dispositivo activo es el dispositivo que se utiliza para enrutar los paquetes; el dispositivo de espera es el dispositivo que se hace cargo cuando el dispositivo activo falla o cuando se preconfigura se cumplen las condiciones. La función del router de espera HSRP es supervisar el estado operativo del grupo HSRP y asumir rápidamente responsabilidad de reenvío de paquetes si falla el router activo.

HSRP para IPv6

Esta es una FHRP propietaria de Cisco que proporciona la misma funcionalidad de HSRP, pero en un entorno IPv6. Un grupo IPv6 HSRP tiene un MAC virtual derivada del número de grupo HSRP y un vínculo IPv6 virtual local derivada de la dirección MAC virtual HSRP. Router Periódico se envían anuncios (RA) para el enlace IPv6 virtual HSRP local cuando el grupo HSRP está activo. Cuando el grupo se vuelve inactivo, estos RAs se detienen después de enviar una RA final.

Virtual Router Redundancy Protocol version 2 (VRRPv2)

Este es un protocolo electoral no propietario que asigna dinámicamente responsabilidad de uno o más routeres virtuales a los routeres VRRP en una LAN IPv4. Esto permite que varios routers en un enlace multiacceso utilicen la misma dirección IPv4 virtual. Un router VRRP está configurado para ejecutar el protocolo VRRP junto con uno o más routeres conectados a una LAN. En una configuración VRRP, se elige un router como el virtual router master, con los otros routers actuando como copias de seguridad, en caso de que el virtual router master falle

VRRPv3

Proporciona la capacidad de admitir direcciones IPv4 e IPv6. VRRPv3 Funciona en entornos de varios proveedores y es más escalable que VRRPv2.

Protocolo de Equilibrio de Carga del Gateway (Load Balancing Protocol, GLBP)

Este es un FHRP propiedad de Cisco que protege el tráfico de datos de un router o circuito fallido, como HSRP y VRRP, mientras que también permite la carga equilibrada (también llamado uso compartido de carga) entre un grupo de routers.

GLBP para IPv6

Esta es una FHRP propietaria de Cisco que proporciona la misma funcionalidad de GLBP, pero en un entorno IPv6. GLBP para IPv6 proporciona automáticamente un respaldo de router para los hosts IPv6 configurados con un único gateway predeterminado en una LAN. Múltiples routers de primer salto en la LAN se combinan para ofrecer un único router IPv6 virtual de primer salto mientras comparte el reenvío de paquetes IPv6 carga.

Protocolo de detección del router ICMP (IRDP, ICMP Router Discovery Protocol)

Especificado en RFC 1256, IRDP es una solución FHRP heredada. IRDP permite IPv4 hosts ubiquen routers que proporcionan conectividad IPv4 a otras redes IP (no locales).

4.2.7. Autoevaluación

a) ¿Qué puerto funciona para RSTP y STP?

- Puerto raíz
- Puerto salida
- Puerto bloqueado

b) ¿Qué protocolo fue diseñado para lograr una convergencia más rápida a STP?

- PortFast
- RSTP
- PVST

c) ¿Qué función de puerto de STP adopta un puerto de switch si no hay ningún otro puerto con un costo menor al puente raíz?

- Puerto salida
- Puerto raíz
- Puerto bloqueado

d) ¿Qué mensaje envia un cliente DHCPV4 para iniciar el proceso de obtención de concesión?

- DHCPDISCOVER
- DHCPOFFER
- DHCPACK

e) ¿Qué método describe mejor DHCP Stateless

- Solo SLAAC
- SLAAC con servidor DHCPV6 stateless
- Servidor DHCPV5 stateful

4.2.8. Actividad Propuesta

Figura 35.

Topología y Tabla de asignación

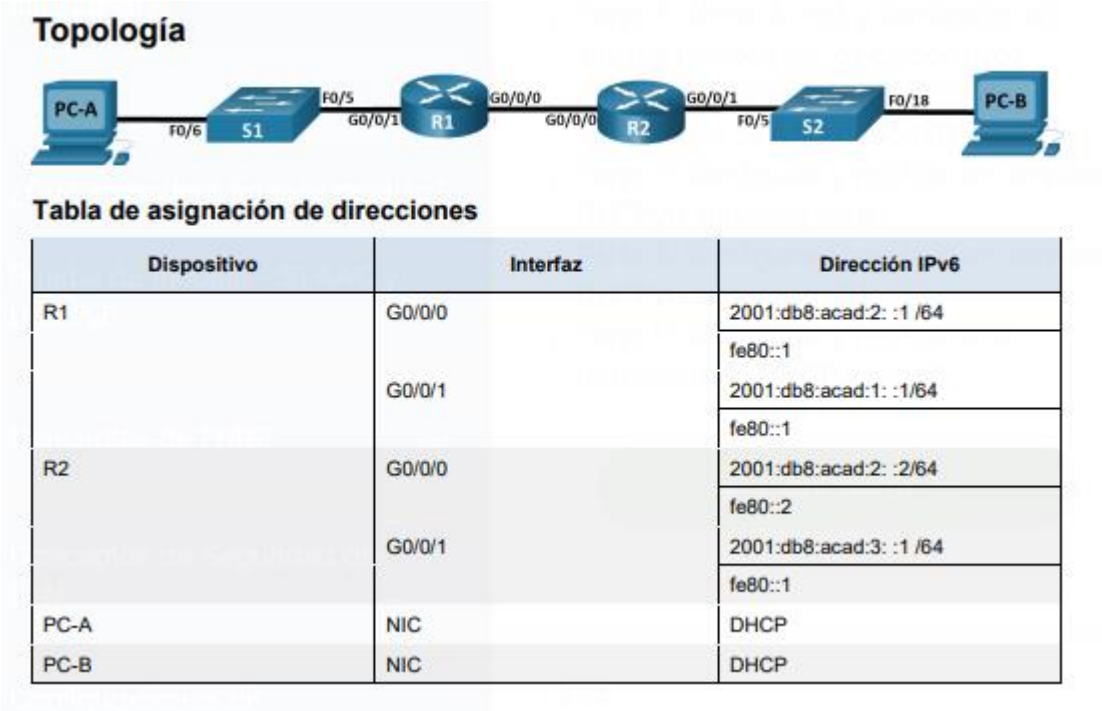


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv6
R1	G0/0/0	2001:db8:acad:2: :1 /64
		fe80::1
	G0/0/1	2001:db8:acad:1: :1/64
		fe80::1
R2	G0/0/0	2001:db8:acad:2: :2/64
		fe80::2
	G0/0/1	2001:db8:acad:3: :1 /64
		fe80::1
PC-A	NIC	DHCP
PC-B	NIC	DHCP

Objetivos

- Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Verificar la asignación de direcciones SLAAC desde R1
- Parte 3: Configurar y verificar un servidor DHCPv6 sin estado en R1 Parte 4: Configurar y verificar un servidor DHCPv6 con estado en R1 Parte 5: Configurar y verificar un relé DHCPv6 en R2

Antecedentes/Escenario

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Configuración automática de direcciones independiente del estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Cuando se utiliza SLACC para asignar direcciones IPv6 a hosts, no se utiliza un servidor DHCPv6. Dado que no se utiliza un servidor DHCPv6 al implementar SLACC, los hosts no pueden recibir información adicional de red crítica, incluida una dirección de servidor de nombres de dominio (DNS) y un nombre de dominio.

Cuando se utiliza DHCPv6 sin estado para asignar direcciones IPv6 al host, se utiliza un servidor DHCPv6 para asignar la información de red crítica adicional, sin embargo, la dirección IPv6 se asigna mediante SLACC.

Cuando se implementa DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar

el router R2 para asignar direcciones IPv6 en dos subredes diferentes conectadas al router R1.

Nota:Los routers utilizados con los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.4 (universalk9 image). Los switches utilizados en los laboratorios son Cisco Catalyst 2960s con Cisco IOS Release 15.2 (2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

• 2 Router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.3 o comparable)

• 2 switches (Cisco 2960 con Cisco IOS versión 15.2(2), imagen lanbasek9 o comparable)- Opcional

• 2 PC (Windows con un programa de emulación de terminal, como Tera Term)

• Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola

• Cables Ethernet, como se muestra en la topología

Instrucciones

Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

Paso 1: Realizar el cableado de red como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realizar el cableado necesario.

Paso 2: Configurar los parámetros básicos para cada switch (Opcional)

a. Asigne un nombre de dispositivo al switch.

b. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

c. Asigne class como la contraseña cifrada del modo EXEC privilegiado.

d. Asigne cisco como la contraseña de la consola y habilite el inicio de sesión.

e. Asigne cisco como la contraseña de VTY y habilite el inicio de sesión.

f. Cifre las contraseñas de texto sin formato.

g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

h. Apagar todos los puertos sin usar

i. Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 3: Configure los parámetros básicos para cada router.

a. Asigne un nombre de dispositivo al router.

b. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

c. Asigne class como la contraseña cifrada del modo EXEC privilegiado.

d. Asigne cisco como la contraseña de la consola y habilite el inicio de sesión.

e. Asigne cisco como la contraseña de VTY y habilite el inicio de sesión.

f. Cifre las contraseñas de texto sin formato.

g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

h. Habilitar el routing IPv6

i. Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 4: Configure las interfaces y el enrutamiento para ambos routers.

a. Configure las interfaces G0/0/0 y G0/0/1 en R1 y R2 con las direcciones IPv6 especificadas en la tabla anterior.

b. Configure una ruta predeterminada en cada enrutador que apunte a la dirección IP de G0/0/0 en el otro enrutador.

c. Verifique que el enrutamiento funcione haciendo ping a la dirección G0/0/1 de R2 desde R1

d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2: Verifique la asignación de direcciones SLAAC desde R1

En la Parte 2, comprobará que el host PC-A recibe una dirección IPv6 mediante el método SLAAC. Encienda el PC-A y asegúrese de que la NIC está configurada para la configuración automática IPv6.

Después de unos momentos, los resultados del comando ipconfig deberían mostrar que PC-A se ha asignado una dirección de la red 2001:db 8:1: :/64.

¿De dónde vino la porción de ID de host de la dirección?

Parte 3: Configurar y verificar un servidor DHCPv6 en R1

En la Parte 3, configurará y verificará un servidor DHCP sin estado en R1. El objetivo es proporcionar a PC-A información de servidor DNS y dominio.

Paso 1: Examine la configuración de PC-A con más detalle.

a. Ejecute el comando ipconfig /all en PC-A y eche un vistazo a la salida.

b. Observe que no hay sufijo DNS principal. Tenga en cuenta también que las direcciones del servidor DNS proporcionadas son direcciones de «transmisión local del sitio», y no direcciones de unidifusión, como cabría esperar.

Paso 2: Configure R1 para proporcionar DHCPv6 sin estado para PC-A.

a. Cree un grupo DHCP IPv6 en R1 denominado R1-ASTAPT. Como parte de ese grupo, asigne la dirección del servidor DNS como 2001:db8:acad: :1 y el nombre del dominio como stateless.com.

b. Configure la interfaz G0/0/1 en R1 para proporcionar el indicador de configuración Other a la LAN R1 y especifique el grupo DHCP que acaba de crear como recurso DHCP para esta interfaz.

c. Guarde la configuración en ejecución en el archivo de configuración de inicio.

d. Reinicie PC-A.

e. Examine la salida de ipconfig /all y observe los cambios.

f. Pruebe la conectividad haciendo ping a la dirección IP de la interfaz G0/0/1 de R2.

Parte 4: Configurar un servidor DHCPv6 con estado en R1

En la Parte 4, configurará R1 para que responda a las solicitudes DHCPv6 desde la LAN en R2.

a. Cree un grupo DHCPv6 en R1 para la red 2001:db8:acad:3:aaaa: :/80. Esto proporcionará direcciones a la LAN conectada a la interfaz G0/0/1 en R2. Como parte del grupo, establezca el servidor DNS en 2001:db8:acad: :254 y establezca el nombre de dominio en Stateful.com.

b. Asigne el grupo DHCPv6 que acaba de crear a la interfaz g0/0/0 en R1.

Parte 5: Configure y verifique la retransmisión DHCPv6 en R2.

En la Parte 5, configurará y verificará la retransmisión DHCPv6 en R2, permitiendo que PC-B reciba una dirección IPv6.

Paso 1: Encienda el PC-B y examine la dirección SLAAC que genera.

Observe en la salida que el prefijo utilizado es 2001:db8:acad:3::

Paso 2: Configure R2 como un agente de retransmisión DHCP para la LAN en G0/0/1.

a. Configure el comando ipv6 dhcp relay en la interfaz R2 G0/0/1, especificando la dirección de destino de la interfaz G0/0/0 en R1. Configure también el comando managed-config-flag .

b. Guarde su configuración.

Paso 3: Intentar adquirir una dirección IPv6 de DHCPv6 en PC-B.

a. Reinicie PC-B.

b. Abra un símbolo del sistema en PC-B y ejecute el comando ipconfig /all y examine la salida para ver los resultados de la operación de retransmisión DHCPv6.

c. Pruebe la conectividad haciendo ping a la dirección IP de la interfaz G0/0/1 de R1.

4.3. Seguridad de L2 y WLAN y conceptos de enrutamiento y configuración

Esta unidad permitirá a los estudiantes, conocer e identificar como las vulnerabilidades ponen en riesgo la seguridad de LAN, además, les ayudara a identificar como los routers utilizan la información en los paquetes para tomar decisiones de reenvió.

4.3.1. Seguridad de punto terminal

- ***Ataques de red actuales***

Normalmente, los medios de comunicación cubren los ataques de red externos a redes empresariales. Sencillamente busque en el internet por "Los ataques más recientes de red" y encontrará información actualizada de ataques actuales. Muy posiblemente, estos ataques envuelven una o más de las siguientes:

Negación de Servicio Distribuido(DDoS) – Esto es un ataque coordinado desde muchos dispositivos, llamados zombies, con la intención de degradar o detener acceso publico al sitio web y los recursos de una organización.

Filtración de Datos – Este es un ataque en el que los servidores de datos o los hosts de una organización han sido comprometidos con el fin de robar información confidencial.

Malware – Este es un ataque en el que los hosts de una organización son infectados con software malicioso que causa una serie de problemas. Por ejemplo, ransomware como WannaCry, mostrado en la figura, encripta los datos en un host y bloquea el acceso hasta que se le pague un rescate.

- ***Dispositivos de seguridad de red***

Se necesitan diversos dispositivos de seguridad para proteger el perímetro de la red del acceso exterior. Estos dispositivos podrían incluir un router habilitado con una Red Privada Virtual (VPN), un Firewall de Siguiente Generación (NGFW), y un Dispositivo de Acceso a la Red (NAC)

Router habilitado con VPN. - Red Privada Virtual (VPN) proporciona una conexión segura para que usuarios remotos se conecten a la red empresarial a través de una red pública. Los servicios VPN pueden ser integrados en el firewall.

NGFW. - Firewall de Siguiente Generación (NGFW) - proporciona inspección de paquetes con estado, visibilidad y control de aplicaciones, un Sistema de Prevención de Intrusos de Próxima Generación (NGIPS), Protección Avanzada contra Malware (AMP) y filtrado de URL.

NAC. - Un dispositivo NAC incluye autenticación, autorización y registro (AAA) En empresas más grandes, estos servicios podrían incorporarse en un dispositivo que pueda administrar políticas de acceso en una amplia variedad de usuarios y tipos de dispositivos. El Cisco Identity Services Engine (ISE) en un ejemplo de dispositivo NAC.

- ***Protección de terminales***

Los dispositivos LAN como los switches, los Controladores de LAN Inalámbricos (WLCs), y otros puntos de acceso (AP) interconectan puntos terminales. La mayoría de estos dispositivos son susceptibles a los ataques LAN que se cubren en este módulo.

Sin embargo, muchos ataques se originan dentro de la red. Si un atacante se infiltra en un host interno, este puede ser el punto de partida para que obtenga acceso a dispositivos esenciales del sistema, como servidores e información confidencial.

Los puntos terminales son hosts que generalmente consisten en computadoras portátiles, computadoras de escritorio, servidores y teléfonos IP, así como dispositivos propiedad de los empleados (BYOD). Los puntos terminales son particularmente susceptibles a ataques relacionados con malware que se originan a través del correo electrónico o la navegación web. Estos puntos finales suelen utilizar características de seguridad tradicionales basadas en host, como antivirus/antimalware, firewalls basados en host y sistemas de prevención de intrusiones (HIPS) basados en host. Sin embargo, actualmente los puntos finales están más protegidos por una combinación de NAC, software AMP basado en host, un Dispositivo de Seguridad de Correo Electrónico (ESA) y un Dispositivo de Seguridad Web (WSA). Los productos de Protección Avanzado de Malware (AMP) incluyen soluciones de dispositivos finales como Cisco AMP.

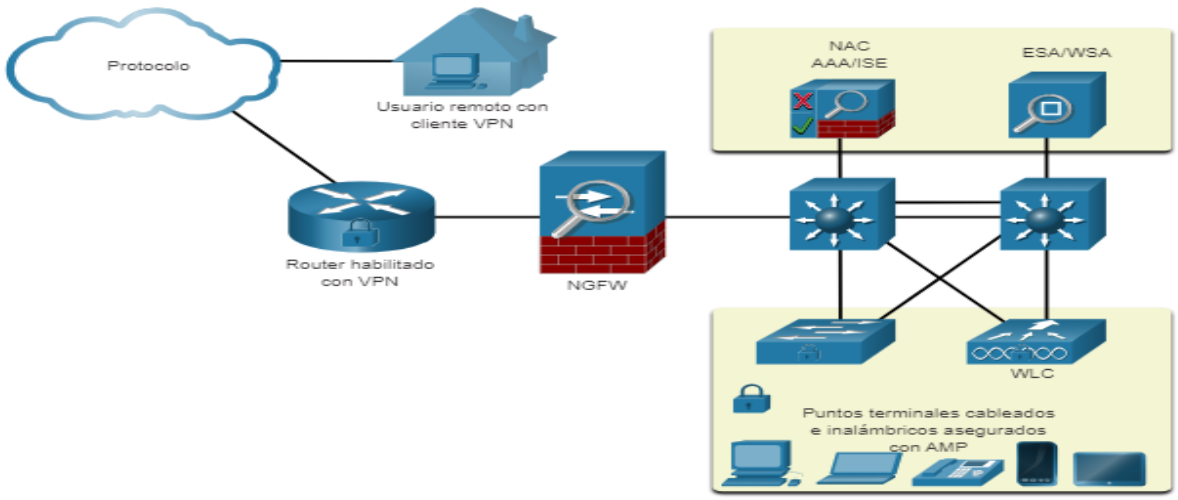
La figura es una topología simple que representa todos los dispositivos de seguridad de red y soluciones de dispositivos finales discutidas en este módulo.

La figura es una topologia de red mostrando dispositivos de seguridad de red y soluciones de dispositivos finales. La nube de internet esta en la parte superior izquierda. Adjunto a la nube en Internet está un usuario remoto con un cliente de VPN. Conectado a la nube en la red interna hay un router habilitado para VPN que está conectado a un

NGFW. El NGFW está conectado a un switch multicapa que tiene dos conexiones a otro switch multicapa. Conectado al primer switch esta un dispositivo NAC AAA/ISE. Conectado al segundo switch esta un dispositivo ESA/WSA. Los dos switches multicapa están conectados a un switch LAN seguro y a un WLC. También se muestran varios dispositivos finales cableados e inalámbricos protegidos con AMP, que incluyen una computadora de escritorio, una computadora portátil, un teléfono IP y un teléfono inteligente.

Figura 36.

Topología de red



Nota. Seguridad en la red con una topología simple

.

- ***Dispositivo de seguridad de correo electrónico cisco (ESA)***

Los dispositivos de seguridad de contenido incluyen un control detallado sobre el correo electrónico y la navegación web para los usuarios de una organización.

Según el Talos Intelligence Group de Cisco, en junio de 2019, el 85% de todos los correos electrónicos enviados eran spam. Los ataques de suplantación de identidad son una forma de correo electronico no deseado paticularmente virulento. Recuerde que un ataque de phishing lleva al usuario a hacer clic en un enlace o abrir un archivo adjunto. Spear phishing selecciona como objetivo a empleados o ejecutivos de alto perfil que pueden tener credenciales de inicio de sesión elevadas. Esto es particularmente crucial en el ambiente actual, donde, de acuerdo al instituto SANS, 95% de todos los ataques en redes empresariales son del resultado de un spear phishing exitoso.

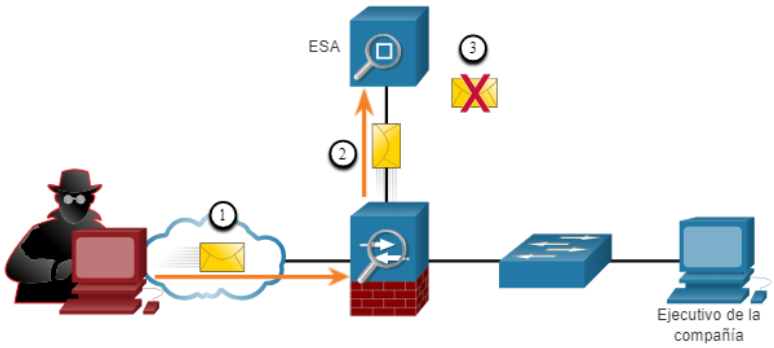
El dispositivo Cisco ESA está diseñado para monitorear el Protocolo Simple de Transferencia de Correo (SMTP). Cisco ESA se actualiza en tiempo real de Cisco Talos, quien detecta y correlaciona las amenazas con un sistema de monitoreo que utiliza una base de datos mundial. Cisco ESA extrae estos datos de inteligencia de amenazas cada tres o cinco minutos. Estas son algunas funciones de Cisco ESA:

- Bloquear las amenazas
- Remediar contra el malware invisible que evade la detección inicial
- Descartar correos con enlaces malos (como se muestra en la figura).
- Bloquear el acceso a sitios recién infectados
- Encriptar el contenido de los correos salientes para prevenir perdida de datos.

En la figura Cisco ESA descarta el correo con enlaces malos.

Figura 37.

Correos no deseados



Nota. El atacante envía un ataque de suplantación a un importante host en la red.

- ***Dispositivo de seguridad de la red de cisco (WSA)***

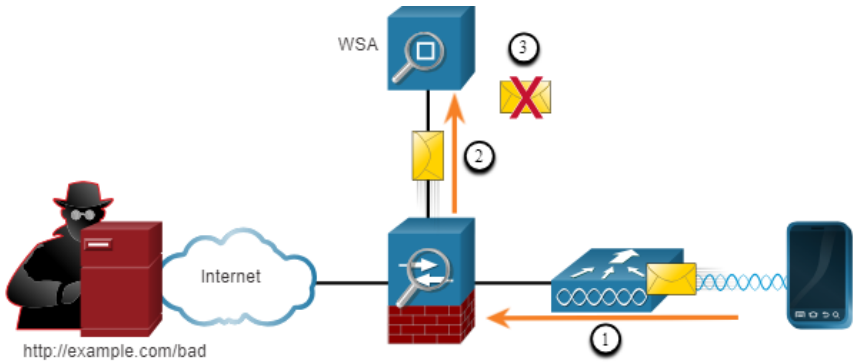
Cisco Web Security Appliance (WSA) es una tecnología de mitigación para amenazas basadas en la web. Ayuda a las organizaciones a abordar los desafíos de asegurar y controlar el tráfico web. Cisco WSA combina protección avanzada contra malware, visibilidad y control de aplicaciones, controles de políticas de uso aceptable e informes.

Cisco WSA proporciona un control completo sobre cómo los usuarios acceden a Internet. Ciertas funciones y aplicaciones, como chat, mensajería, video y audio, pueden permitirse, restringirse con límites de tiempo y ancho de banda, o bloquearse, de acuerdo con los requisitos de la organización. La WSA puede realizar listas negras de URL, filtrado de URL, escaneo de malware, categorización de URL, filtrado de aplicaciones web y cifrado y descifrado del tráfico web.

En la figura, un usuario corporativo intenta conectarse a un sitio marcado en la lista negra.

Figura 38.

Usuario conectado.



Nota. La WSA evalúa la url y determina si es un sitio marcado en la lista negra.

4.3.2. Amenazas a la seguridad de Capa 2

- ***Capa 2 Vulnerabilidades***

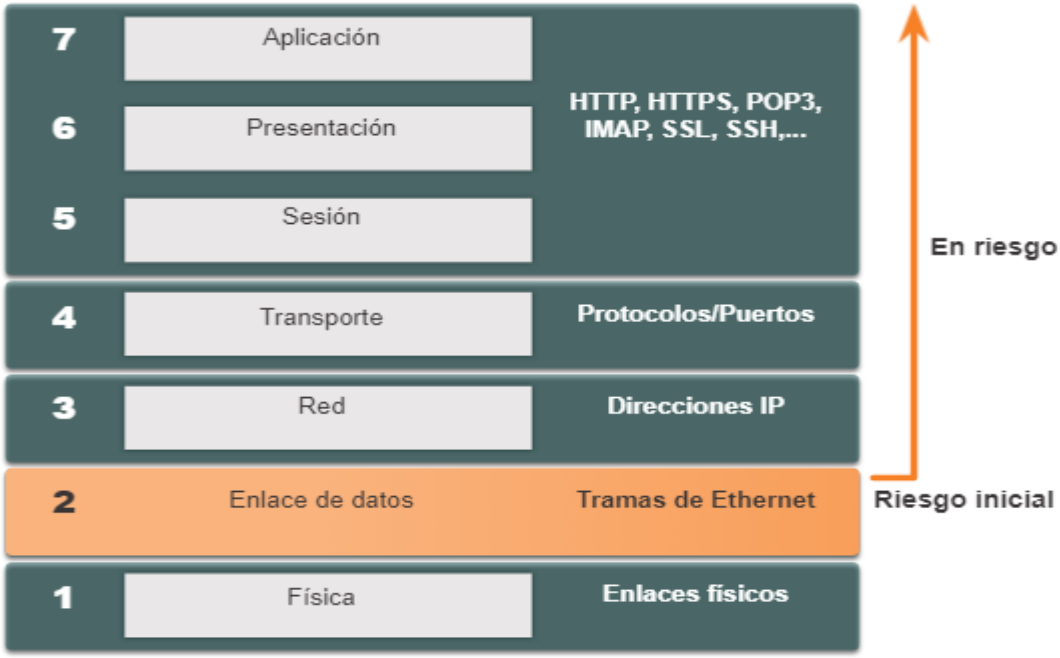
Los dos temas anteriores discutieron seguridad en puntos terminales. En este tema, usted va a seguir aprendiendo sobre formas de asegurar una LAN, enfocándose en las tramas de la Capa de Enlace (Capa 2) y el switch.

Recuerde que el modelo de referencia OSI está dividido en siete capas, las cuales trabajan de manera independiente una de otra. La figura muestra la función de cada capa y los principales componentes que pueden ser explotados.

Los administradores de red regularmente implementan soluciones de seguridad para proteger los componentes en la Capa 3 y hasta la Capa 7. Ellos usan VPNs, firewalls, y dispositivos IPS para proteger estos elementos. Si la Capa 2 se ve comprometida, todas las capas superiores también se ven afectadas. Por ejemplo, si un atacante con acceso a la red interna captura los marcos de la Capa 2, entonces toda la seguridad implementada en las capas anteriores sería inútil. El atacante podría causar mucho daño en la infraestructura de red LAN de Capa 2

Figura 39.

Capas de red



Nota. Amenaza de seguridad desde la capa 2.

- ***Categorías de ataques a switches***

La seguridad es solamente tan sólida como el enlace más débil en el sistema, y la Capa 2 es considerada el enlace más débil. Esto se debe a que las LAN estaban tradicionalmente bajo el control administrativo de una sola organización. Nosotros confiábamos inherentemente en todas las personas y dispositivos conectados a nuestra LAN. Hoy, con BYOD y ataques más sofisticados, nuestras LAN se han vuelto más vulnerables a la penetración. Además de proteger de la Capa 3 a la Capa 7, los profesionales de seguridad de red también deben mitigar los ataques a la infraestructura LAN de la Capa 2.

El primer paso para mitigar los ataques a la infraestructura de Capa 2 es comprender el funcionamiento de la Capa 2 y las amenazas de la infraestructura de Capa 2.

Ataques a la tabla MAC. - Incluye ataques de saturación de direcciones MAC.

Ataques de VLAN. - Incluye ataques VLAN Hopping y VLAN Double-Tagging Esto también incluye ataques entre dispositivos en una misma VLAN.

Ataques de DHCP. - Incluye ataques de agotamiento y suplantación DHCP

Ataques ARP. - Incluye la suplantación de ARP y los ataques de envenenamiento de ARP.

Ataques de suplantación de direcciones. - Incluye los ataques de suplantación de direcciones MAC e IP.

Ataques de STP. - Incluye ataques de manipulación al Protocolo de Árbol de Extensión

- ***Técnicas de mitigación en el switch***

Seguridad de puertos. - Previene muchos tipos de ataques incluyendo ataques MAC address flooding Ataque por agotamiento del DHCP

DHCP Snooping. - Previene ataques de suplantación de identidad y de agotamiento de DHCP

Inspección ARP dinámica (DAI). - Previene la suplantación de ARP y los ataques de envenenamiento de ARP.

Protección de IP de origen (IPSG). - Impide los ataques de suplantación de direcciones MAC e IP.

Estas soluciones de Capa 2 no serán efectivas si los protocolos de administración no son seguros. Por ejemplo, los protocolos administrativos Syslog, Protocolo Simple de Administración de Red (SNMP), Protocolo Trivial de Transferencia de Archivos (TFTP),

Telnet, Protocolo de Transferencia de Archivos (FTP) y la mayoría de otros protocolos comunes son inseguros, por lo tanto, se recomiendan las siguientes estrategias.

- Utilice siempre variantes seguras de protocolos de administración como SSH, Protocolo de Copia Segura (SCP), FTP Seguro (SFTP) y Seguridad de capa de sockets seguros / capa de transporte (SSL / TLS).
- Considere usar una red de administración fuera de banda para administrar dispositivos.
- Usar una VLAN de administración dedicada que solo aloje el tráfico de administración.
- Use ACL para filtrar el acceso no deseado.

4.3.3. Ataques a la LAN

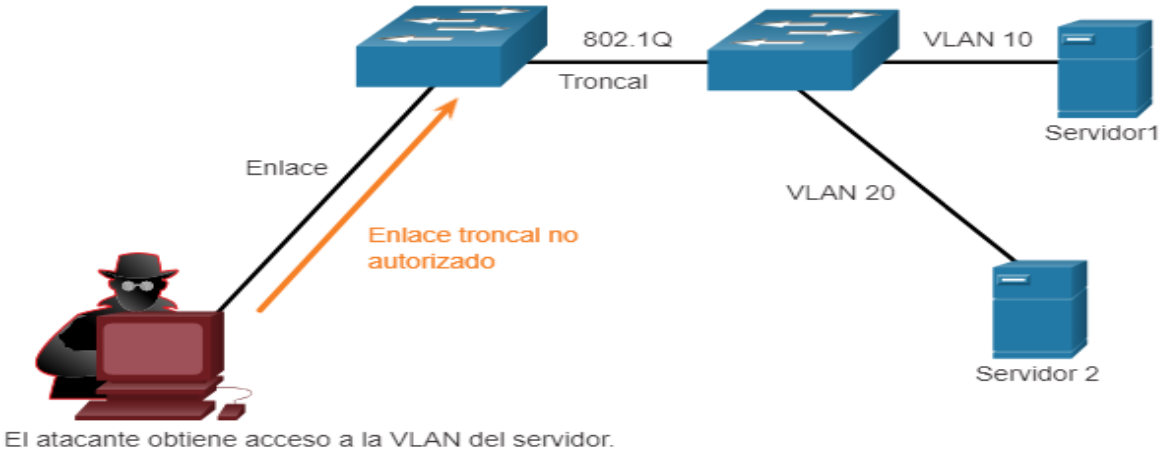
- ***Ataque de VLAN Hopping***

El VLAN Hopping permite que una VLAN pueda ver el tráfico de otra VLAN sin cruzar primero un router. En un ataque de VLAN Hopping básico, el atacante configura un host para que actúe como un switch para aprovechar la función de entroncamiento automático habilitada de forma predeterminada en la mayoría de los puertos del switch.

El atacante configura el host para falsificar la señalización 802.1Q y la señalización del Protocolo de enlace dinámico (DTP), propiedad de Cisco, hacia el enlace troncal con el switch de conexión. Si es exitoso, el switch establece un enlace troncal con el host, como se muestra en la figura. Ahora el atacante puede acceder todas las VLANS en el switch..

Figura 40.

Ataque de VLAN hopping



Nota. El atacante puede enviar y recibir tráfico en cualquier VLAN, saltando efectivamente entre las VLAN.

- ***Ataque de VLAN Double-Tagging***

Un atacante, en situaciones específicas, podrían insertar una etiqueta 802.1Q oculta dentro de la trama que ya tiene una etiqueta 802.1Q. Esta etiqueta permite que la trama se envíe a una VLAN que la etiqueta 802.1Q externa no especificó.

Un ataque de VLAN Double-tagging es unicast, y funciona unidireccional, y funciona cuando el atacante está conectado a un puerto que reside en la misma VLAN que la VLAN nativa del puerto troncal. La idea es que el doble etiquetado permite al atacante enviar datos a hosts o servidores en una VLAN que de otro modo se bloquearía por algún tipo de configuración de control de acceso. Presumiblemente, también se permitirá el tráfico de retorno, lo que le dará al atacante la capacidad de comunicarse con los dispositivos en la VLAN normalmente bloqueada.

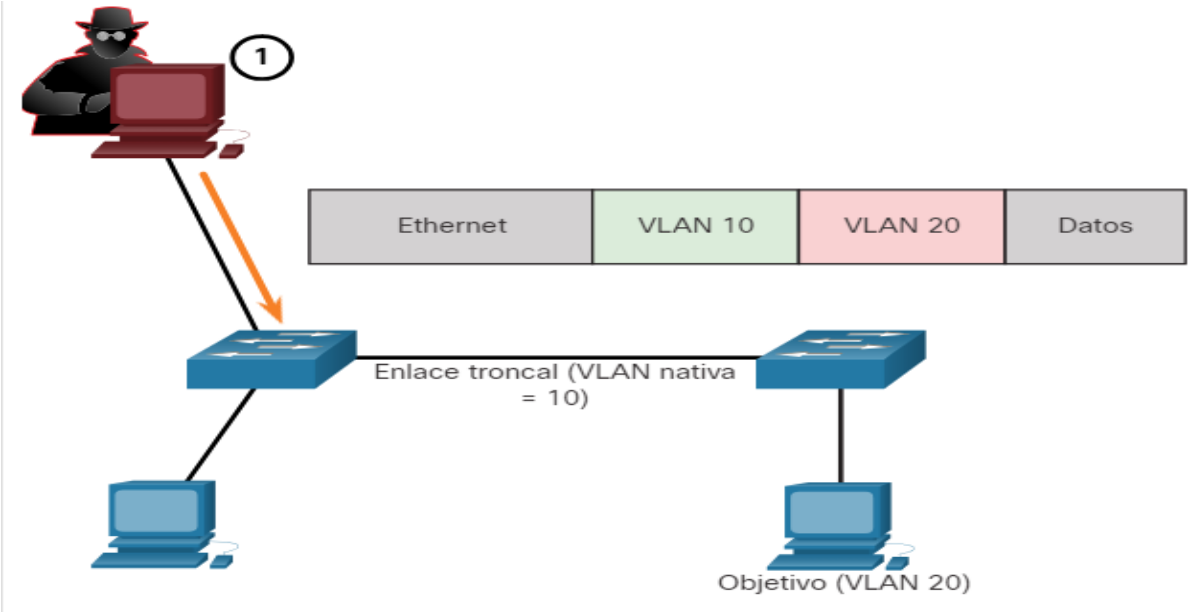
Paso 1

El atacante envía una trama 802.1Q con doble etiqueta (double tag) al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN

nativa del puerto de enlace troncal. Para fines de este ejemplo, supongamos que es la VLAN 10. La etiqueta interna es la VLAN víctima; en este caso, la VLAN 20.

Figura 41.

Ataque con trama



Nota. El objetivo del ataque es la VLAN 20.

Paso 2

El frame llega al primer switch, que mira la primera etiqueta 802.1Q de 4 bytes. El switch ve que la trama está destinada para la VLAN 10, la cual es una VLAN nativa. El switch reenvía el paquete a todos los puertos de VLAN 10, después de quitar la etiqueta de VLAN 10. La trama no es re-etiquetada porque es parte de la VLAN nativa. En este punto, la etiqueta de VLAN 20 todavía está intacta y no ha sido inspeccionada por el primer switch.

Paso 3

La trama llega al segundo switch, que no tiene conocimiento de que debía ser para la VLAN 10. El switch emisor no etiqueta el tráfico de la VLAN nativa, como se especifica en la especificación 802.1Q. El segundo switch observa solo la etiqueta interna 802.1Q,

que el atacante insertó, y ve que la trama está destinada a la VLAN 20 (la VLAN víctima). El segundo switch envía el paquete al puerto víctima o lo satura, dependiendo de si existe una entrada en la tabla de MAC para la host víctima.

Mitigación de Ataques a VLAN

Los ataques de VLAN hopping y VLAN Double-Tagging se pueden evitar mediante la implementación de las siguientes pautas de seguridad troncal, como se discutió previamente en este modulo:

- Deshabilitar troncal en todos los puertos de acceso.
- Deshabilitar entroncamiento automático en enlaces troncales para poder habilitarlos de manera manual.
- Asegúrese de que la VLAN nativa sólo se usa para los enlaces troncales.
- ***Mensaje DHCP***

Los servidores DHCP, de manera dinámica, proporcionan información de configuración de IP a los clientes, como la dirección IP, la máscara de subred, el gateway predeterminado, los servidores DNS y más. Una revisión de la secuencia típica de un intercambio de mensajes DHCP entre el cliente y el servidor es mostrada en la figura.

Figura 42.

Mensajes DHCP

Nota. Proceso de envió de mensajes DHCP.

- ***Ataques de DHCP***

Los dos tipos de ataques DHCP son agotamiento y suplantación de identidad. Ambos ataques pueden ser mitigados implementando DHCP snooping.

Ataque por Agotamiento DHCP

El objetivo de un ataque de agotamiento DHCP es crear un DoS para la conexión de clientes. Los ataques de agotamiento de DHCP requieren una herramienta de ataque, como Gobbler.

Gobbler tiene la capacidad de ver todo el alcance de las direcciones IP alquilables e intenta alquilarlas todas. Específicamente, este crea un mensaje DHCP DISCOVER con una dirección MAC falsa.

Ataque de Suplantación DHCP

Un ataque de suplantación DHCP se produce cuando un servidor DHCP, no autorizado, se conecta a la red y brinda parámetros de configuración IP falsos a los

clientes legítimos. Un servidor no autorizado puede proporcionar una variedad de información engañosa:

- ***Puerta de enlace predeterminada incorrecta -*** el atacante proporciona una puerta de enlace no válida o la dirección IP de su host para crear un ataque de MITM. Esto puede pasar totalmente inadvertido, ya que el intruso intercepta el flujo de datos por la red.
- ***Servidor DNS incorrecto*** el atacante proporciona una dirección del servidor DNS incorrecta que dirige al usuario a un sitio web malicioso.
- ***Dirección IP incorrecta -*** El servidor no autorizado proporciona una dirección IP no válida que crea efectivamente un ataque DoS en el cliente DHCP

Paso 1: El atacante se conecta a un servidor DHCP dudoso

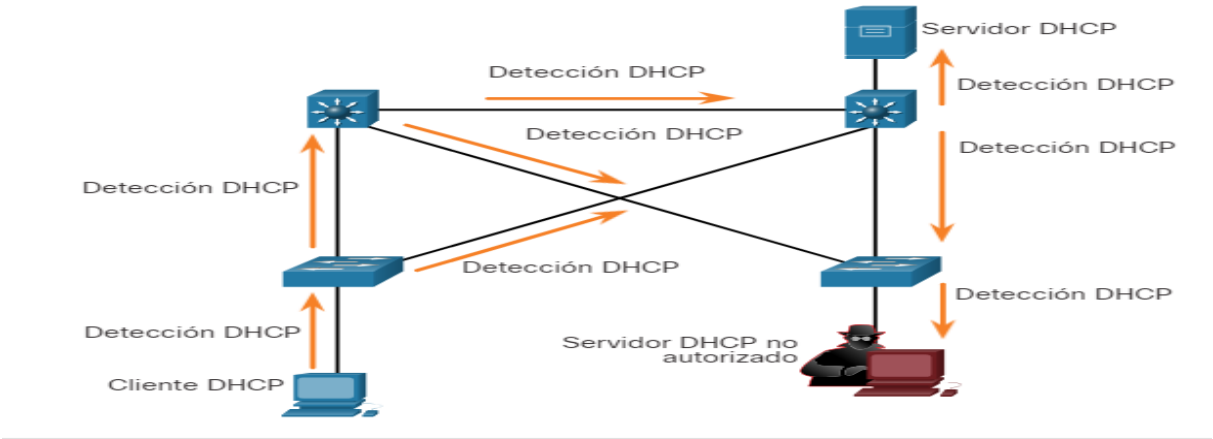
Supongamos que un atacante conecta con éxito un servidor DHCP no autorizado a un puerto de switch en la misma subred que los clientes. El objetivo del servidor no autorizado es proporcionar a los clientes información de configuración de IP falsa.

Paso 2: El cliente transmite mensajes DHCP DISCOVER, tipo broadcast

Un cliente legítimo se conecta a la red y requiere parámetros de configuración de IP. Por lo tanto, el cliente emite un DHCP DISCOVER, tipo broadcast, en búsqueda de una respuesta de un servidor DHCP. Ambos servidores recibirán el mensaje y responden.

Figura 43.

Envió de mensajes en la red



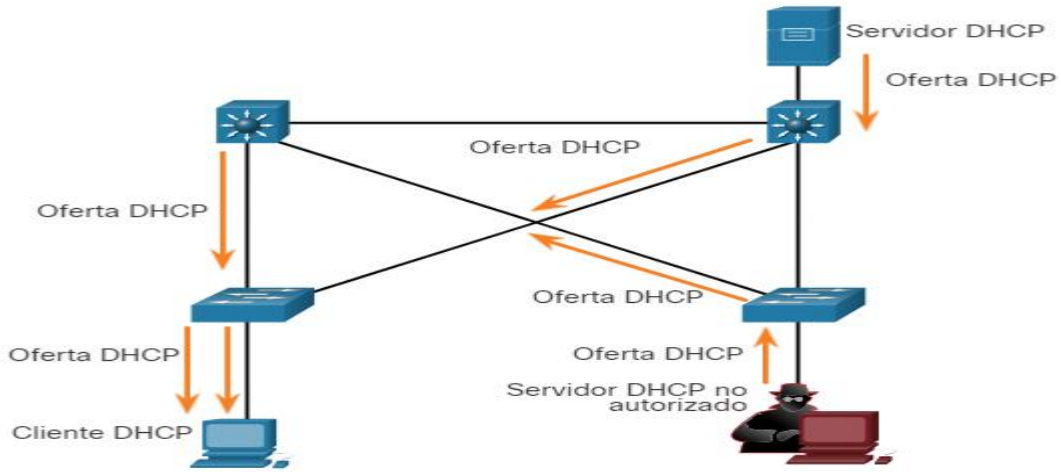
Nota. Conexión de cliente legitimo.

Paso 3: Respuesta DHCP legítima y no autorizada

El servidor DHCP legitimo responde con parámetros de configuración de IP válidos. Sin embargo, el servidor no autorizado también responde con una oferta DHCP, la cual contiene parámetros de configuración IP definidos por el atacante. El cliente responderá a la primera oferta recibida.

Figura 44.

Respuestas DHCP



Nota. Respuesta del servidor DHCP legitima y dudosa.

Paso 4: El cliente acepta la oferta del servidor DHCP no autorizado

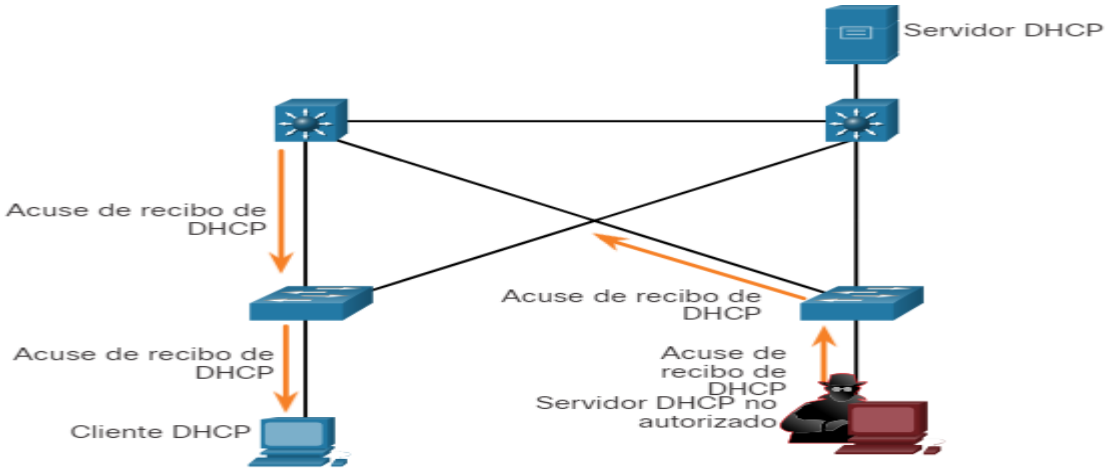
La oferta maliciosa fue recibida primero, y por lo tanto, el cliente hace envía un DHCP REQUEST, tipo broadcast, aceptando los parámetros IP definidos por el atacante. El servidor legítimo y el dudoso recibirán la solicitud.

Paso 5: El servidor malicioso confirma que recibió la solicitud

Solamente el servidor no autorizado emite una respuesta individual al cliente para acusar recibo de su solicitud. El servidor legítimo dejará de comunicarse con el cliente.

Figura 45.

Acuse de recibo DHCP



Nota. Intervención del servidor DHCP no autorizado con el cliente legitimo.

- ***Ataques ARP***

Recuerde que los hosts transmiten una solicitud de ARP a otros hosts del segmento para determinar la dirección MAC de un host con una dirección IP específica. Esto es típicamente hecho para descubrir la dirección MAC de una puerta de enlace predeterminada. Todos los hosts de la subred reciben y procesan la solicitud de ARP. El host con la dirección IP que coincide con la de la solicitud de ARP envía una respuesta de ARP.

Según ARP RFC, cualquier cliente puede enviar una respuesta de ARP no solicitada llamada “ARP gratuito” Cuando un host envía un ARP gratuito, otros hosts en la subred almacenan en sus tablas de ARP la dirección MAC y la dirección IP que contiene dicho ARP.

El problema es que un atacante puede enviar un mensaje ARP gratuito al switch y el switch podría actualizar su tabla MAC de acuerdo a esto. Por lo tanto, cualquier host puede reclamar ser el dueño de cualquier combinación de direccion IP Y MAC que ellos elijan. En un ataque típico el atacante puede enviar respuestas ARP, no solicitadas, a otros hosts en la subred con la dirección MAC del atacante y la dirección IP de la puerta de enlace predeterminada.

Hay muchas herramientas disponibles en Internet para crear ataques de MITM de ARP, como dsniff, Cain & Abel, ettercap y Yersinia. IPv6 utiliza el protocolo de descubrimiento de vecinos ICMPv6 para la resolución de direcciones de Capa 2. IPv6 utiliza el protocolo de descubrimiento de vecinos ICMPv6 para la resolución de direcciones de capa 2.

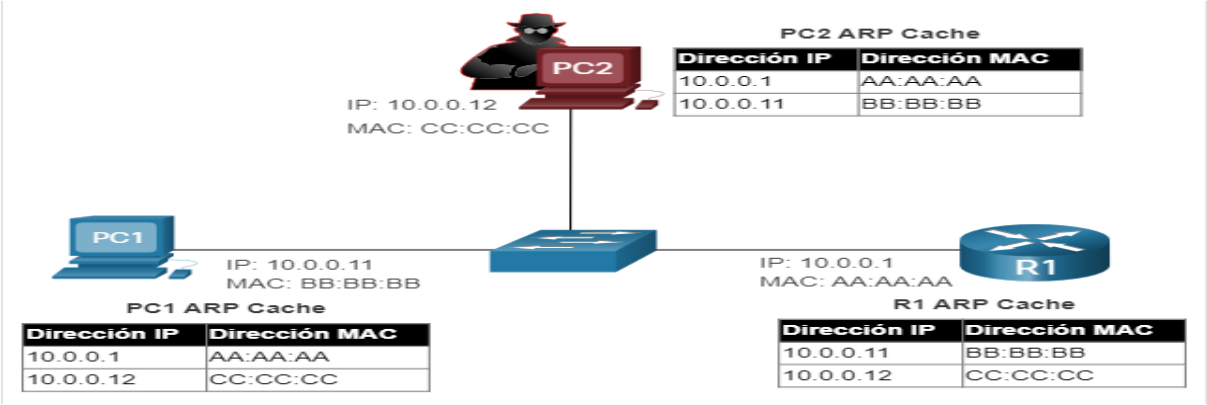
La suplantación de identidad ARP y el envenenamiento ARP son mitigados implementando DAI.

Paso 1: Estado normal con una tabla MAC convergida.

Cada dispositivo tiene una tabla MAC actualizada con la dirección IP y MAC correctas de cada dispositivo en la red.

Figura 46.

Tabla MAC convergida



Nota. Cada dispositivo de la red tiene su propia MAC.

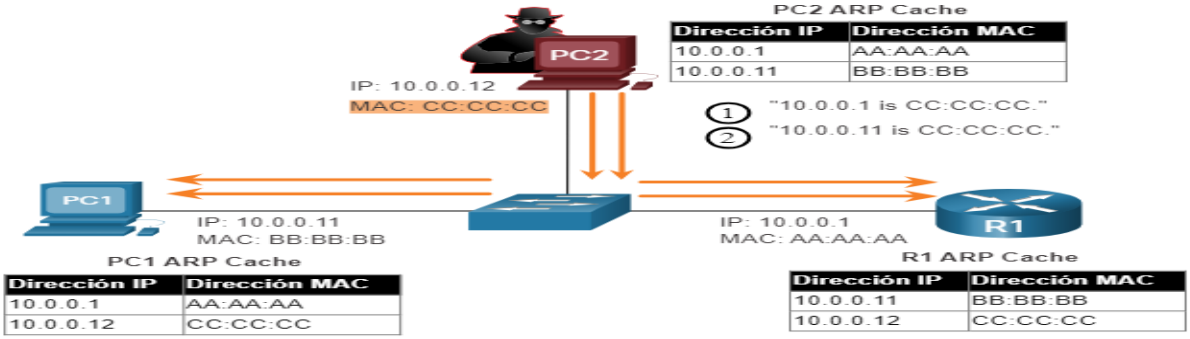
Paso 2: Ataque por Suplantación de ARP

El atacante envía dos respuestas gratuitas falsas en un intento de reemplazar R1 como la puerta de enlace predeterminada.

1. En el primero ARP informa todos los dispositivos en la LAN que la direccion MAC del atacante (CC:CC:CC) está mapeado a la direccion IP de la PC1, 10.0.0.11.
2. EL segundo le informa a todos los dispositivos en la LAN que la direccion MAC del atacante (CC:CC:CC) está mapeado a la direccion IP de la PC1, 10.0.0.11.

Figura 47

Ataque por suplantación de ARP.



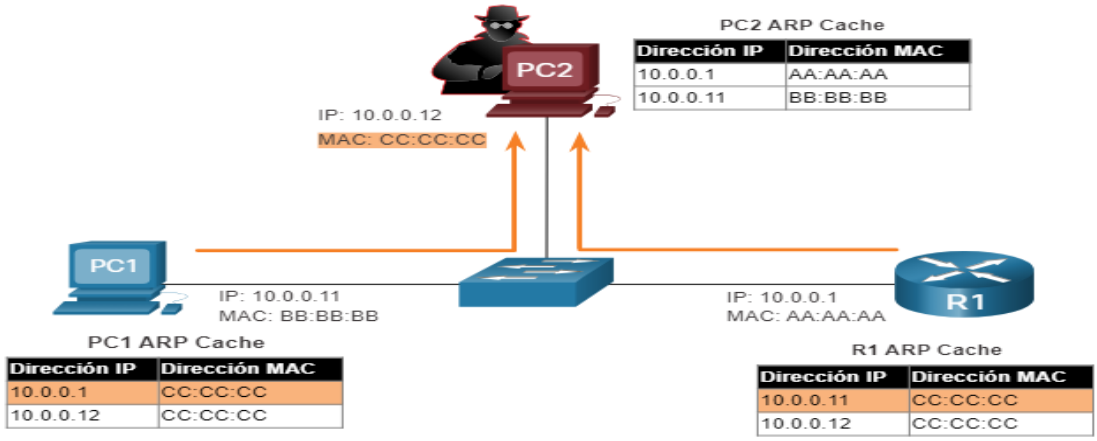
Nota. Mapeado de red.

Paso 3: Ataque de envenenamiento ARP con ataque MITM.

R1 y PC1 remueven la entrada correcta de la dirección MAC de cada uno y la reemplaza con la dirección MAC de PC2. El atacante ha logrado envenenar la caché ARP de todos los dispositivos en la subred. El envenenamiento ARP lleva a varios ataques MITM, posando una seria amenaza de seguridad en la red.

Figura 48.

Ataque MITM



Nota. Los ataques MITM son una gran amenaza para la red.

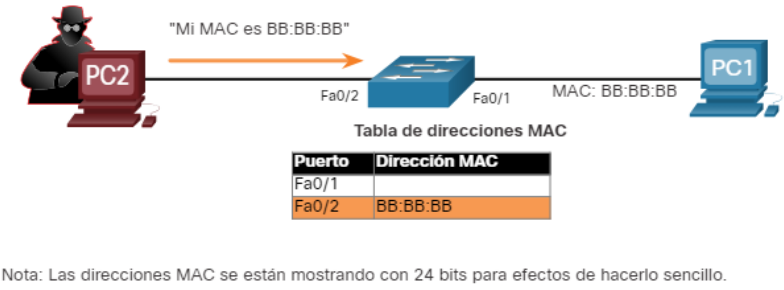
- ***Ataque de suplantación de dirección***

Las direcciones IP y las direcciones MAC pueden ser suplantadas por una cantidad de razones. El ataque de suplantación de identidad se da cuando un atacante secuestra una dirección IP valida de otro dispositivo en la subred o usa una dirección IP al azar. La suplantación de direcciones IP es difícil de mitigar, especialmente cuando se usa dentro de una subred a la que pertenece la IP.

Los atacantes cambian la dirección MAC de su host para que coincida con la dirección MAC conocida de un otro host objetivo. Luego, el host atacante envía una trama a través de la red con la dirección MAC recién configurada. Cuando el switch recibe la trama, examina la dirección MAC de origen. El switch sobrescribe la entrada actual en la tabla MAC y asigna la dirección MAC al nuevo puerto, como se ve en la figura. Luego, sin darse cuenta, reenvía las tramas host atacante.

Figura 49.

Ataque de suplantación



Nota. Esta acción provoca que el swtich reescriba las direcciones MAC

Cuando el host de destino envía tráfico, el switch corregirá el error, re-alineando la dirección MAC al puerto original. Para evitar que el switch corrija la asignación del puerto a su estado correcto, el atacante puede crear un programa o script que constantemente enviará tramas al switch, para que el switch mantenga la información incorrecta o falsificada. No hay un mecanismo de seguridad en la Capa 2 que permita a un switch verificar la fuente de las direcciones MAC, lo que lo hace tan vulnerable a la suplantación de identidad.

La suplantación de identidad de direcciones IP y direcciones MAC puede ser mitigada implementado IPSG.

- ***Ataque de STP***

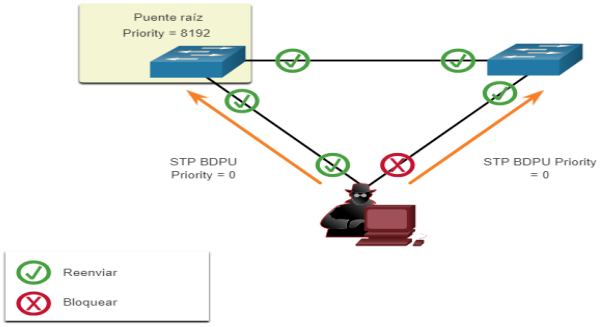
Los atacantes de red pueden manipular el Protocolo de Árbol de Expansión (STP) para realizar un ataque falsificando el root bridge y cambiando la topología de una red. Los atacantes hacen que su host parezca ser un root bridge; por lo tanto, capturan todo el tráfico para el dominio del Switch inmediato.

Para realizar un ataque de manipulación de STP, el host atacante transmite Unidades de Datos de Protocolo de Puente STP (BPDU), que contienen cambios de configuración y topología que forzarán los re-cálculos de Árbol de Expansión, como se

muestra en la figura. Las BPDU enviadas por el host atacante anuncian una prioridad de puente (bridge) inferior, en un intento de ser elegidas como root bridge.

Figura 50.

Ataques STP

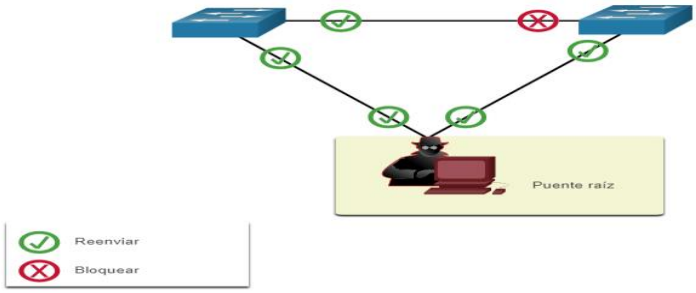


Nota. Las BPDU pueden ser seleccionadas como un root bridge*,*

Si tiene éxito, el host atacante se convierte en el puente raíz, como se muestra en la figura, y ahora puede capturar una variedad de frames, que de otro modo no serían accesibles.

Figura 51.

Captura de frames



Nota. El atacante se convierte en el puente raíz*.*

4.3.4. Implementación de seguridad de puertos

- ***Asegurar los puertos sin utilizar***

Los dispositivos de Capa 2 se consideran el eslabón más débil en la infraestructura de seguridad de una compañía. Los ataques de Capa 2 son de los más sencillos de

desplegar para los hackers, pero estas amenazas también pueden ser mitigadas con algunas soluciones comunes de capa 2.

Se deben proteger todos los puertos del switch (interfaces) antes de implementar el switch para su uso en producción. Como un puerto es protegido depende de su función.

Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Por ejemplo, si un switch Catalyst 2960 tiene 24 puertos y hay tres conexiones Fast Ethernet en uso, es aconsejable inhabilitar los 21 puertos que no se utilizan. Navegue a cada puerto no utilizado y emita el comando shutdown de Cisco IOS. Si un puerto debe reactivarse más tarde, se puede habilitar con el comando no shutdown.

Para configurar un rango de puertos, use el comando interface range.

```
Switch(config)# interface range type module/first-number – last-number
```

Por ejemplo, para apagar los puertos for Fa0/8 hasta Fa0/24 en S1, usted debe ingresar el siguiente comando.

```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
(output omitted)
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#
```

- ***Mitigación de ataques por saturación de tabla de direcciones MAC***

El método más simple y eficaz para evitar ataques por saturación de la tabla de direcciones MAC es habilitar la sport security.

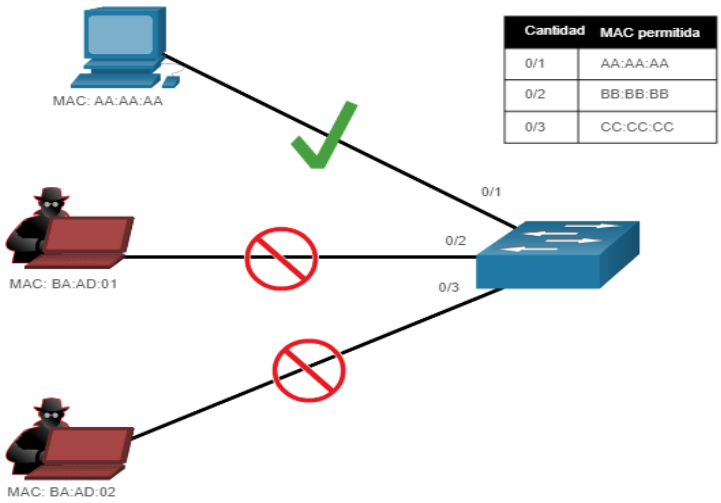
La seguridad de puertos limita la cantidad de direcciones MAC válidas permitidas en el puerto. Permite a un administrador configurar manualmente las direcciones MAC para un puerto o permitir que el switch aprenda dinámicamente un número limitado de direcciones MAC. Cuando un puerto configurado con port security recibe un frame, la

dirección MAC de origen del frame se compara con la lista de direcciones MAC de origen seguro que se configuraron manualmente o se aprendieron dinámicamente en el puerto.

Al limitar a uno la cantidad de direcciones MAC permitidas en un puerto, la seguridad de puertos se puede usar para controlar la expansión no autorizada de la red, como se muestra en la figura.

Figura 52.

Saturación de MAC



Nota. Se pueden mitigar los ataques a través de la saturación del direccionamiento MAC.

- ***Habilitar la seguridad del puerto***

Observe en el ejemplo, el comando switchport port-security fue rechazado. Esto se debe a que port security solo se puede configurar en puertos de acceso o trunks configurados manualmente Los puertos capa 2 del switch están definidos como dynamic auto (troncal encendido), de manera predeterminada. Por lo tanto, en el ejemplo, el puerto se configura con el comando switchport mode access de configuración de la interfaz.

Note: La seguridad del puerto troncal está más allá del alcance de este curso.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
```

```
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Use el comando show port-security interface para mostrar la configuración de seguridad del puerto actual para FastEthernet 0/1, como se muestra en el ejemplo. Note que port security este habilitado, el modo de violación esta apagado, y que el número máximo de direcciones MAC permitidas es 1. Si un dispositivo esta conectado al puerto, el switch automáticamente agregara la direccion MAC de este dispositivo como una direccion MAC segura. En este ejemplo, no existe ningún dispositivo conectado al puerto.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Note: Si un puerto activo está configurado con el comando switchport port-security y hay más de un dispositivo conectado a ese puerto, el puerto pasará al estado de error desactivado. Esta condición se discute más adelante en este capitulo

Una vez que se activa port security, se pueden configurar otras funciones específicas de port security, como se muestra en el ejemplo.

```
S1(config-if)# switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
S1(config-if)# switchport port-security
```

- ***Limitar y Aprender MAC addresses***

Para poner el número máximo de direcciones MAC permitidas en un puerto, utilice el siguiente comando

```
Switch(config-if)# switchport port-security maximum value
```

El valor predeterminado de port security es 1. EL número maximo de direcciones MAC seguras que se puede configurar depende del switch y el IOS. En este ejemplo, el maximo es 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

El switch se puede configurar para aprender direcciones MAC en un puerto seguro de tres maneras:

1. Configurado Manualmente

El administrador configura manualmente una(s) direccion MAC estatica usando el siguiente comando para cada direccion MAC en el puerto:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

2. Aprendido automáticamente

Cuando se ingresa el comando switchport port-security, la fuente MAC actual para el dispositivo conectado al puerto se asegura automáticamente pero no se agrega a la configuración de inicio. Si el switch es reiniciado, el puerto tendrá que re-aprender la dirección MAC del dispositivo.

3. Aprendido automáticamente – Sticky

El administrador puede configurar al switch para que aprenda la direccion MAC automáticamente a la "pegue" a la configuración en ejecución usando el siguiente comando:

```
Switch(config-if)# switchport port-security mac-address sticky
```

Al guardar la configuración en ejecución la direccion MAC aprendida automáticamente se quedará en NVRAM.

EL siguiente ejemplo muestra una configuración completa de port security en la interfaz FastEthernet 0/1. El administrador especifica una cantidad máxima de 4 direcciones MAC, configura una direccion MAC segura, y luego configura el puerto para que aprenda más direcciones MAC de manera automática hasta un máximo de 4 direcciones MAC. Use los comandos show port-security interface y show port-security address para verificar la configuración.

```
*Mar  1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1# show port-security address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                       (mins)
----    -----------       ----                          -----   -------------
1    a41f.7272.676a    SecureSticky                Fa0/1       -
1    aaaa.bbbb.1234    SecureConfigured            Fa0/1       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
```

```
Max  Addresses limit in System (excluding one mac per port) : 8192
S1#
```

El resultado del comando show port-security interface verifica que la seguridad del puerto esté habilitada, que haya un host conectado al puerto (es decir, Secure-up), se permitirá un total de 2 direcciones MAC y que S1 tenga aprendió una dirección MAC estáticamente y una dirección MAC dinámicamente (es decir, fija).

El resultado del comando show port-security Address enumera las dos direcciones MAC aprendidas.

- ***Vencimiento de la seguridad del puerto***

EL vencimiento de la seguridad del puerto puede usarse para poner el tiempo de vencimiento de las direcciones seguras estáticas y dinámicas en un puerto. Hay dos tipos de envejecimiento por puerto:

Absoluto - Las direcciones seguras en el puerto se eliminan después del tiempo de caducidad especificado.

Inactivo - Las direcciones seguras en el puerto se eliminan solo si están inactivas durante el tiempo de caducidad especificado.

Utilice el vencimiento para remover las direcciones MAC seguras en un puerto seguro sin necesidad de eliminar manualmente las direcciones MAC existentes. Los tiempos límite de vencimiento pueden ser incrementados para asegurarse que las direcciones MAC pasadas se queden, aun cuando se agregan nuevas direcciones MAC. El vencimiento de direcciones seguras configuradas estáticamente puede ser habilitado o des-habilitado por puerto.

Use el comando switchport port-security aging para habilitar o deshabilitar el envejecimiento estático para el puerto seguro, o para establecer el tiempo o el tipo de envejecimiento.

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

Los parámetros para el comando son los siguientes:

***Static.* -** Habilite el vencimiento para las direcciones seguras estaticamente configuradas en este puerto.

***Time time.* -** Especifique el tiempo de vencimiento de este puerto. El rango es de 0 a 1440 minutos. Sin embargo, si el tiempo es 0, el vencimiento esta des-habilitado en este puerto.

***Type absolute.* -** Ponga el tiempo absoluto de vencimiento. Todas las direcciones seguras en este puerto se vencen exactamente después del tiempo (in minutes) especificado y son removidas de la lista de direcciones seguras.

***Type inactivity.* -** Defina el tipo de inactividad de vencimiento. Las direcciones seguras en este puerto se vencen solo si no hay tráfico desde la dirección segura de origen por un periodo de tiempo especificado.

Note: Las direcciones MAC se están mostrando con 24 bits para efectos de hacerlo sencillo.

El ejemplo muestra a un administrador configurando el tipo de envejecimiento a 10 minutos de inactividad y utilizando el comando show port-security interface para verificar la configuración.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
```

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

- ***Seguridad de puertos: modos de violación de seguridad***

Si la dirección MAC de un dispositivo conectado al puerto difiere de la lista de direcciones seguras, entonces ocurre una violación de puerto. El puerto entra en el estado de error-disabled de manera predeterminada.

Para poner el modo de violación de seguridad de puerto, use el siguiente comando:

```
Switch(config-if)# switchport port-security violation { protect | restrict | shutdown}
```

Figura 53.

Descripción de modo de violación de seguridad

del router	Descripción
shutdown (predeterminados)	El puerto transiciona al estado de error-disabled inmediatamente, apaga el LED del puerto, y envía un mensaje syslog. Aumenta el contador de violaciones Contador. Cuando un puerto seguro esta en estado error-disabled un administrador debe re-habilitarlo ingresando los comandos **shutdown** y **no shutdown** .
restrict	El puerto bota los paquetes con direcciones MAC de origen desconocidas hasta que usted remueva un numero suficiente de direcciones MAC seguras para llegar debajo del maximo valor o incremente el máximo valor Este modo causa que el contador de violación de seguridad incremente y genere un mensaje syslog.
protect	Este modo es el menos seguro de los modos de violaciones de seguridad. No se realiza el tráfico de puertos los paquetes con direcciones MAC de origen desconocidas hasta que usted remueva un numero suficiente de direcciones MAC seguras para llegar debajo del valor máximo o o incremente el máximo valor No se envía ningún mensaje syslog.

Nota. La reacción del switch basado en la configuración de modo de violación.

Figura 54.

Comparación de los modos de violación de seguridad

Violation Mode	Discards Offending Traffic	Envía mensaje de syslog	Incrementa el contador de violaciones	Desactiva el puerto
Protect	Sí	No	No	No
Restrict	Sí	Sí	Sí	No
Apagado	Sí	Sí	Sí	Sí

Nota. Los modos de violación de seguridad están destinados a diferentes actividades.

El siguiente ejemplo muestra un administrador cambiando la violación de seguridad a "restringir". La salida delshow port-security interface comando confirma que se ha realizado el cambio.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

- ***Puertos en estado error – disabled***

Cuando un puerto esta apagado y puesto en modo error-desabilitado, no se envía ni se recibe tráfico a través de ese puerto. En la consola, se muestra una serie de mensajes relacionados con la seguridad del puerto.

```
S1(config)# int fa0/1
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# end
S1#
*Mar  1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
```

```
*Mar  1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1#
*Mar  1 00:24:32.829: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state
*Mar  1 00:24:32.838: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.
*Mar  1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
S1#
```

Note: The port protocol and link status are changed to down and the port LED is turned off.

In the example, the show interface command identifies the port status as err-disabled. La salida del show port-security interface comando ahora muestra el estado del puerto como secure-shutdown. El contador de violación incrementa en uno.

```
S1# show interface fa0/1 | include down
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 1
S1#
```

El administrador debe determinar que causo la violación de seguridad, si un dispositivo no autorizado está conectado a un puerto seguro,la amenazas de seguridad es eliminada antes de restablecer el puerto.

Para volver a habilitar el puerto, primero use el shutdown comando, luego use el no shutdown comando para que el puerto sea operativo, como se muestra en el ejemplo.

```
S1(config)# interface fa0/1
S1(config-if)# shutdown
S1(config-if)#
*Mar  1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
S1(config-if)# no shutdown
S1(config-if)#
*Mar  1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1(config-if)#
```

- ***Verificar la seguridad del puerto***

Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

Seguridad de puertos para todas las interfaces.

Para mostrar la configuración de seguridad del puerto para el conmutador, show port-security use el comando. El ejemplo indica que todas las 24 interfaces están configuradas con el comando switchport port-security porque el máximo permitido es 1 y el modo de violación está en shutdown. No hay dispositivos conectados, Por lo tanto, el contandor CurrentAddr (Count) es 0 para cada interfaz.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
             (Count)       (Count)         (Count)
---------------------------------------------------------------------------
     Fa0/1            2           2                0        Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Seguridad de puertos para una Interfaz Específica

Use el show port-security interface comando para ver los detalles de una interfaz específica, como se muestra anteriormente y en este ejemplo.

```
S1# show port-security interface fastethernet 0/1
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 10 mins
Aging Type                   : Inactivity
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 2
Total MAC Addresses          : 2
Configured MAC Addresses     : 1
Sticky MAC Addresses         : 1
Last Source Address:Vlan     : a41f.7273.018c:1
Security Violation Count     : 0
S1#
```

Verificar las direcciones MAC aprendidas

Para verificar que las direcciones MAC están "pegadas" a la configuración, use el show run comando como se muestra en el ejemplo de FastEthernet 0/19.

```
S1# show run interface fa0/1
Building configuration...

Current configuration : 365 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky a41f.7272.676a
 switchport port-security mac-address aaaa.bbbb.1234
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 switchport port-security
end

S1#
```

Verificar las Direcciones MAC Seguras

Para mostrar todas las direcciones MAC seguras que se configuran manualmente o se aprenden dinámicamente en todas las interfaces de conmutador, use el comando show port-security address como se muestra en el ejemplo.

```
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports   Remaining Age
                                                (mins)
----    -----------       ----                  -----   -------------
   1    a41f.7272.676a    SecureSticky          Fa0/1       -
   1    aaaa.bbbb.1234    SecureConfigured      Fa0/1       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

4.3.5. Mitigación de ataques de DHCP

- ***Revisión de ataques DHCP***

El objetivo de un ataque de inanición de DHCP es crear una denegación de servicio (DoS) para la conexión de los clientes. Los ataques de agotación de DHCP requieren

una herramienta de ataque, como Gobbler. Recuerde que los ataques de inanición de DHCP pueden ser efectivamente mitigados usando seguridad de puertos porque Gobbler usa una dirección MAC de origen única para cada solicitud DHCP enviada.

Sin embargo, mitigar ataques DHCP de suplantación de identidad requiere más protección. Gobbler podría configurarse para usar la dirección MAC de la interfaz real como la dirección Ethernet de origen, pero especifique una dirección Ethernet diferente en la carga útil de DHCP. Esto haría que la seguridad del puerto sea ineficaz porque la dirección MAC de origen sería legítima.

Los ataques de suplantación de DHCP se pueden mitigar mediante el uso de detección DHCP en puertos confiables.

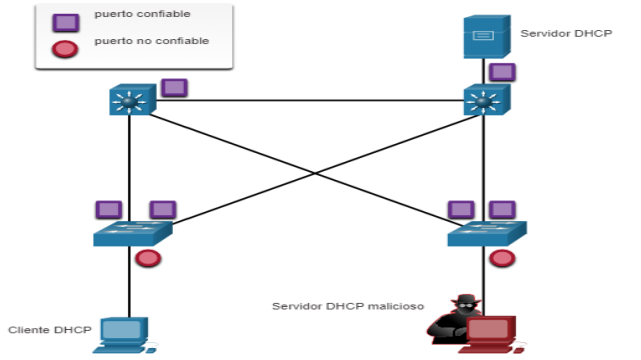
- ***Indagación de DHCP***

La inspección de DHCP no depende de las direcciones MAC de origen. En cambio, la inspección de DHCP determina si los mensajes de DHCP vienen de una fuente configurada administrativamente como confiable o no confiable. Luego filtra los mensajes de DHCP y limita la velocidad del tráfico DHCP viniendo desde fuentes no confiables.

Dispositivos que están bajo su control administrativo como Switches, enrutadores y servidores, son fuentes confiables. Cualquier dispositivo más allá del cortafuegos fuera de su red son fuentes no confiables. Además, todos los puertos de acceso son tratados generalmente como fuentes no confiables. La figura muestra un ejemplo de puertos confiables y no confiables.

Figura 55.

Indagación DHCP



Nota. Puertos confiables y no confiables.

Tenga en cuenta que el servidor DHCP dudoso podría estar en un puerto no confiable después de habilitar DHCP snooping. Todas las interfaces son tratadas por defecto como no confiables. Típicamente las interfaces confiables son enlaces troncales y puertos conectados directamente a un servidor DHCP legítimo. Estas interfaces deben ser configuradas explícitamente como confiables.

Se crea una tabla DHCP que incluye la dirección MAC de origen de un dispositivo en un puerto no confiable y la dirección IP asignada por el servidor DHCP a ese dispositivo. La dirección MAC y la dirección IP están unidas. Por lo tanto, esta tabla se denomina tabla de enlace DHCP snooping.

- ***Pasos para implementar DHCP snooping***

Utilice los siguientes pasos para habilitar la vigilancia DHCP

Paso 1 . Habilite la inspección DHCP mediante el comando ip dhcp snooping de configuración global.

Paso 2 . En puertos de confianza, utilice el comando de configuración de la interfaz ip dhcp snooping trust .

Paso 3 : Limite la cantidad de mensajes de descubrimiento de DHCP que puede recibir por segundo en puertos no confiables mediante el comando de configuración de la interfaz ip dhcp snooping limit rate .

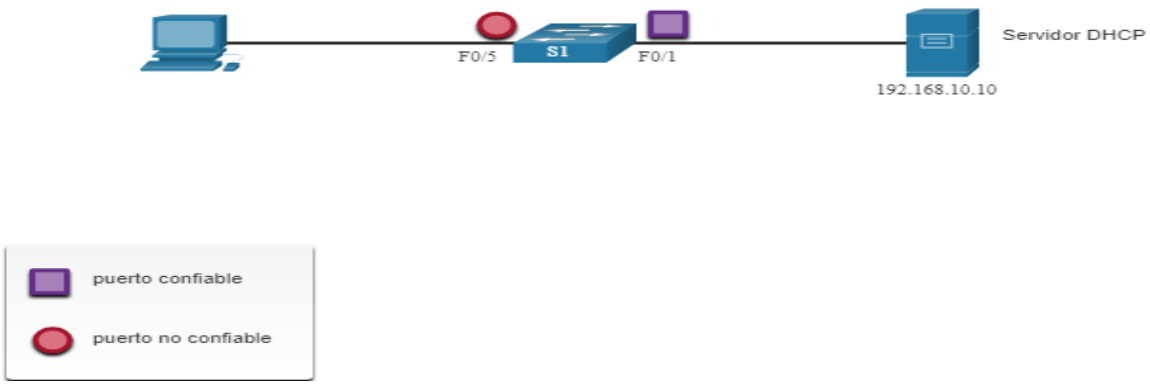
Paso 4 . Habilite la inspección DHCP por VLAN, o por un rango de VLAN, utilizando el comando ip dhcp snooping vlan de la configuración global.

- ***Un ejemplo de configuración de detección de DHCP***

La topología de referencia para este ejemplo de DHCP snooping se muestra en la figura. Tenga en cuenta que F0/5 es un puerto no confiable porque este se conecta con una computadora. F0/1 es un puerto confiable porque se conecta con el servidor DHCP

Figura 56.

Puertos confiables y no confiables



Nota. Configuración DHCP snooping.

El siguiente es un ejemplo de cómo configurar DHCP snooping en S1. Tenga en cuenta que el espionaje DHCP se activa primero. La interfaz ascendente al servidor DHCP es explícitamente confiable. Luego, el rango de puertos FastEthernet de F0/5 a F0/24 no son confiables de manera predeterminada, de manera que se establece un límite de transferencia de seis paquetes por segundo. Finalmente, la inspección DHCP está habilitada en VLANS 5, 10, 50, 51 y 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Utilice el comando show ip dhcp snooping EXEC privilegiado para verificar la inspección DHCP show ip dhcp snooping vinculante y para ver los clientes que han recibido información DHCP, como se muestra en el ejemplo.

Nota : La inspección dinámica de ARP (DAI) también requiere de la inspección DHCP, que es el siguiente tema

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
FastEthernet0/1          yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5          no         no              6
  Custom circuit-ids:
FastEthernet0/6          no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec) Type         VLAN Interface
----------------- --------------- ---------- ------------ ---- --------------------
00:03:47:B5:9F:AD  192.168.10.11   193185     dhcp-snooping 5    FastEthernet0/5
```

4.3.6. WLAN seguras

- ***Encubrimiento SSID y filtrado de direcciones MAC***

Las señales inalámbricas pueden viajar a través de materiales sólidos como techos, pisos, paredes, fuera de casa o del espacio de la oficina. Sin medidas de seguridad estrictas, la instalación de una WLAN puede ser equivalente a colocar puertos Ethernet en todas partes, incluso en el exterior.

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

Encubrimiento SSID

Los AP y algunos enrutadores inalámbricos permiten deshabilitar la trama de baliza SSID, como se muestra en la figura. Los clientes inalámbricos deben configurarse manualmente con el SSID para conectarse a la red.

Figura 57.

Encubrimiento SSID

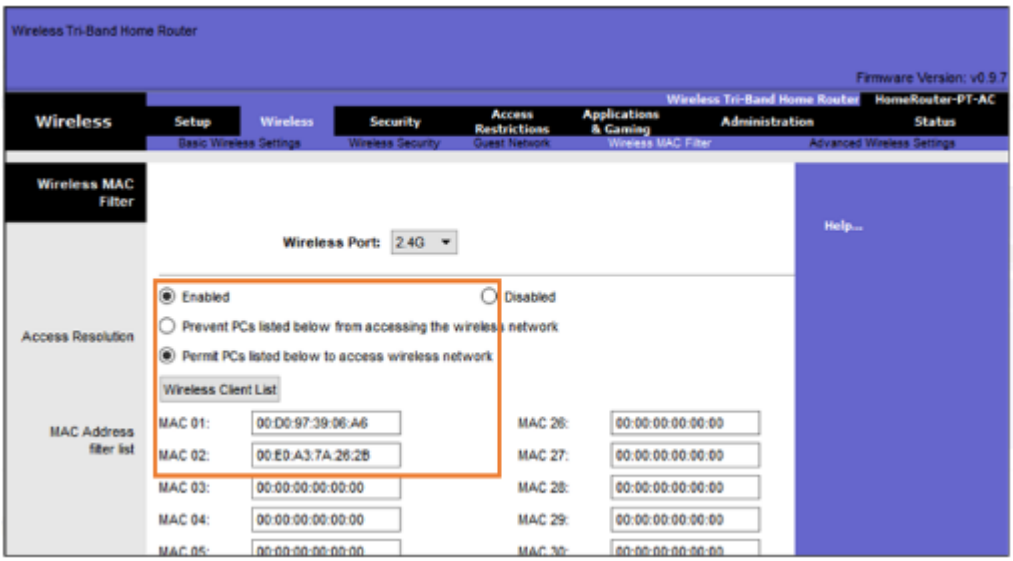
Nota. La GUI del enrutador inalámbrico que muestra la transmisión SSID se ha deshabilitado dentro de la configuración inalámbrica básica

Filtrado de direcciones MAC

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

Figura 58.

Filtrado de direcciones MAC



Nota. La GUI del enrutador inalámbrico muestra que la resolución de acceso se ha habilitado desde la configuración del filtro MAC inalámbrico, lo que permite que solo las PC coincidan con dos direcciones MAC.

- ***802.11 Métodos de autenticación originales***

Aunque estas dos características disuadirían a la mayoría de los usuarios, la realidad es que ni el ocultamiento de SSID ni el filtrado de direcciones MAC disuadirían a un intruso astuto. Los SSID se descubren fácilmente incluso si los AP no los transmiten y las direcciones MAC pueden ser falsificadas. La mejor manera de proteger una red inalámbrica es utilizar sistemas de autenticación y cifrado.

Se introdujeron dos tipos de autenticación con el estándar 802.11 original

Sistema de autenticación abierto - Cualquier cliente inalámbrico debería poder conectarse fácilmente y solo debería usarse en situaciones en las que la seguridad no

sea una preocupación, como las que proporcionan acceso gratuito a Internet, como cafeterías, hoteles y áreas remotas. El cliente inalámbrico es responsable de proporcionar seguridad, como el uso de una red privada virtual (VPN) para conectarse de forma segura. Los VPN proporcionan servicios de autenticación y cifrado. Las VPN están más allá del alcance de este tema.

Autenticación de llave compartida: proporciona mecanismos, como WEP, WPA, WPA2 y WPA3 para autenticar y cifrar datos entre un cliente inalámbrico y AP. Sin embargo, la contraseña debe ser precompartida entre las dos partes para conectarse.

- ***Métodos de autenticación de clave compartida***

Actualmente hay cuatro técnicas de autenticación de clave compartida disponibles, como se muestra en la tabla. Hasta que la disponibilidad de dispositivos WPA3 vuelva a ser omnipresente, las redes inalámbricas deben usar el estándar WPA2.

Figura 59.

Métodos de autenticación

Método de autenticación	Descripción
Privacidad equivalente al cableado (WEP)	La especificación original 802.11 designada para proteger los datos usando el método de cifrado Rivest Cipher 4 (RC4) con una llave estática. Sin embargo, La llave nunca cambia cuando se intercambian paquetes. Esto lo hace fácil de hackear. WEP ya no se recomienda y nunca debe usarse.
Acceso Wi-Fi protegido (WPA)	Un estándar de alianza Wi-Fi que usa WEP, pero asegura los datos con un cifrado más sólido que el Protocolo de integridad de clave temporal (TKIP). generación de hash. El TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de hackear
WPA2	WPA2 es un estándar de la industria para proteger las redes inalámbricas. Suele Utilizar el Estándar de cifrado avanzado (AES) para el cifrado. AES es actualmente se considera el protocolo de cifrado más sólido.
WPA3	La próxima generación de seguridad Wi-Fi. Todos los dispositivos habilitados para WPA3 utilizan los últimos métodos de seguridad, no permiten protocolos heredados obsoletos y requieren el uso de Tramas de administración protegidas (PMF). Sin embargo, los dispositivos con WPA3 no están disponibles fácilmente.

Nota. Descripción de los diferentes modos de autenticación.

- ***Autenticando a un usuario doméstico***

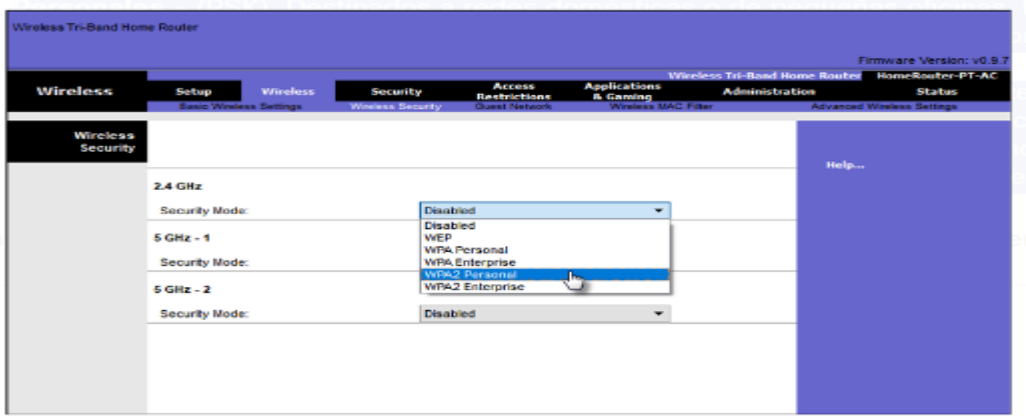
Los enrutadores domésticos suelen tener dos opciones de autenticación: WPA y WPA2 WPA2 es el más fuerte de los dos La figura muestra la opción para seleccionar uno de los dos métodos de autenticación WPA2:

Personales - (PSK). Destinados a redes domésticas o de pequeñas oficinas, los usuarios se autentican utilizando una clave precompartida (PSK). Los clientes inalámbricos se autentican con el enrutador inalámbrico utilizando una contraseña previamente compartida. no requiere un servidor de autenticación especial.

empresa - destinada a redes empresariales, pero requiere un servidor de autenticación de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). Aunque requiere una configuración más complicada, proporciona seguridad adicional. El servidor RADIUS debe autenticar el dispositivo y luego los usuarios deben autenticarse utilizando el estándar 802.1X, que utiliza el Protocolo de autenticación extensible (EAP) para la autenticación.

Figura 60.

Autenticación de usuario doméstico



Nota. el administrador está configurando el enrutador inalámbrico con autenticación personal WPA2 en la banda 2.4 GHz.

- ***Método de encriptación***

El cifrado suele utilizarse para proteger datos. Si un intruso ha capturado datos cifrados, no podrá descifrarlos en un período de tiempo razonable.

Los estándares WPA y WPA2 utilizan los siguientes métodos de cifrado:

Protocolo de integridad de clave temporal (TKIP) : TKIP es el método de encriptación utilizado por WPA. Proporciona soporte para equipos WLAN heredados al abordar las fallas originales asociadas con el método de encriptación WEP 802.11. Utiliza WEP, pero encripta la carga útil de la Capa 2 usando TKIP y realiza una Verificación de integridad de mensajes (MIC) en el paquete encriptado para garantizar que el mensaje no haya sido alterado.

Estándar de cifrado avanzado (AES) - AES es el método de encriptación utilizado por WPA2. este es el método de cifrado preferido porque es un método mucho más fuerte. Utilice el modo de contador de cifrado con el protocolo de código de autenticación de mensajes de bloqueo de cadena (CCMP) que permite a los hosts de destino reconocer si se han alterado los bits cifrados y no cifrados.

Figura 61.

Métodos de encriptación

Nota. El administrador está configurando el enrutador inalámbrico para usar WPA2 con cifrado AES en la banda 2.4 GHz.

- ***Autenticación en la empresa***

En redes que tienen requisitos de seguridad estrictos, se requiere una autenticación adicional o inicio de sesión para garantizar al cliente el acceso inalámbrico. La elección del modo de seguridad empresarial requiere un servidor RADIUS de autenticación, autorización y contabilidad (AAA).

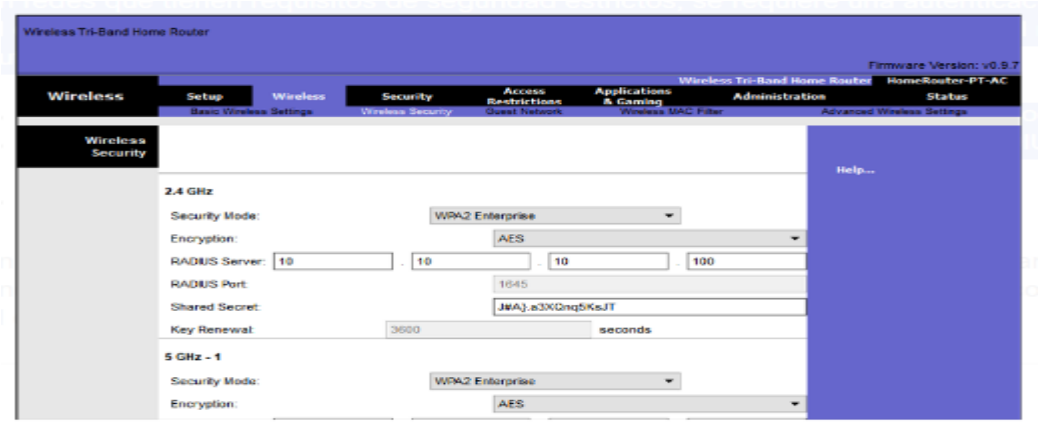
Dirección IP del servidor RADIUS - Esta es la dirección accesible del servidor RADIUS.

Números de puerto UDP - Los puertos UDP 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS, pero también pueden funcionar utilizando los puertos UDP 1645 y 1646.

Llave compartida : se utiliza para autenticar el AP con el servidor RADIUS.

Figura 62.

Autenticación en la empresa



Nota. el administrador está configurando el enrutador inalámbrico para usar autenticación WPA2 Enterprise con encriptación AES. La dirección IPv4 del servidor RADIUS también se configura con una contraseña segura que se utilizará entre el enrutador inalámbrico y el servidor RADIUS.

La llave compartida no es un parámetro que debe ser configurado en un cliente inalámbrico. Solo se requiere en el AP para autenticarse con el servidor RADIUS. Nota: La autenticación y autorización del usuario se maneja mediante el estándar 802.1X, que proporciona una autenticación centralizada basada en el servidor de los usuarios finales.

El proceso de inicio de sesión 802.1X utiliza EAP para comunicarse con el servidor AP y RADIUS. EAP es un marco para autenticar el acceso a la red. Puede proporcionar un mecanismo de autenticación segura y negociar una clave privada segura que luego puede usarse para una sesión de encriptación inalámbrica usando encriptación TKIP o AES.

- ***WAP3***

En el momento de este escrito, los dispositivos que soportan la autenticación WPA3 no están fácilmente disponibles. Sin embargo, WPA2 ya no se considera seguro WPA3, si está disponible, es el método de autenticación 802.11 recomendado. WPA3 incluye cuatro características;

WPA3-personal

En WPA2-Personal, los actores de amenazas pueden escuchar el "handshake" entre un cliente inalámbrico y el AP y utilizar un ataque de fuerza bruta para intentar adivinar el PSK. WPA3-Personal frustra este ataque utilizando la Autenticación Simultánea (SAE), una característica especificada en el IEEE 802.11-2016. El PSK nunca es expuesto, haciendo imposible de adivinar para el atacante.

WPA3-empresa

WPA3 - Empresa: Utiliza la autenticación 802.1X / EAP. Sin embargo, requiere el uso de una suite criptográfica de 192 bits y eliminar la combinación de protocolos de seguridad para los estándares 802.11 anteriores. WPA3-Enterprise se adhiere a la Suite de Algoritmo de Seguridad Nacional Comercial (CNSA) que se usa combinada en redes Wi-Fi de alta seguridad.

Redes abiertas

Las redes abiertas en WPA2 envían tráfico de usuarios en texto claro no autenticado. En WPA3, las redes Wi-Fi abiertas o públicas aún no utilizan ninguna autenticación. Sin embargo, utilice el cifrado inalámbrico oportunista (OWE) para cifrar todo el tráfico inalámbrico.

Integración IOT

Aunque WPA2 incluyó la Configuración protegida de Wi-Fi (WPS) para incorporar rápidamente dispositivos sin configurarlos primero, WPS es vulnerable a una variedad de ataques y no se recomienda. Además, los dispositivos IoT generalmente no tienen cabeza, lo que significa que no tienen una interfaz gráfica de usuario incorporada para la configuración, y necesitan una forma fácil de conectarse a la red inalámbrica. El Protocolo de aprovisionamiento de dispositivos (DPP) se diseñó para abordar esta necesidad. Cada dispositivo sin cabeza tiene una clave pública codificada. La clave suele estar impresa en el exterior del dispositivo o en su embalaje como un código de Respuesta rápida (QR). El administrador de red puede escanear el código QR y rápidamente a bordo del dispositivo. Aunque no es estrictamente parte del estándar WPA3, DPP reemplazará a WPS con el tiempo.

4.3.7. Determinación de ruta

- ***Dos funciones del router***

Antes de que un router reenvíe un paquete a cualquier lugar, tiene que determinar la mejor ruta para que el paquete tome. En este tema se explica cómo los enrutadores realizan esta determinación.

Los switches Ethernet se utilizan para conectar dispositivos finales y otros dispositivos intermediarios, como otros conmutadores Ethernet, a la misma red. Un

router conecta varias redes, lo que significa que posee varias interfaces, cada una de las cuales pertenece una red IP diferente.

Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz debe usar para reenviar el paquete hacia el destino. Esto se conoce como enrutamiento. La interfaz que usa el router para reenviar el paquete puede ser el destino final o una red conectada a otro router que se usa para llegar a la red de destino. Generalmente, cada red a la que se conecta un router requiere una interfaz separada, pero puede que este no siempre el caso.

Las funciones principales de un router son determinar la mejor ruta para reenviar paquetes basándose en la información de su tabla de enrutamiento, y reenviar paquetes hacia su destino.

- ***Ejemplos de funciones del router***

El router usa su tabla de routing para encontrar la mejor ruta para reenviar un paquete. Haga clic en Reproducir en la animación de la ilustración, para seguir un paquete desde la computadora de origen hasta la computadora de destino. Observe cómo tanto R1 como R2 utilizan sus respectivas tablas de enrutamiento IP para determinar primero la mejor ruta y, a continuación, reenviar el paquete.

Figura 63.

Mejor Ruta

Nota. Redes LAN con host conectados por dos routers.

- ***Mejor ruta es igual a la coincidencia más larga***

¿Qué significa que el router deba encontrar la mejor coincidencia en la tabla de routing? La mejor ruta de la tabla de enrutamiento también se conoce como la coincidencia más larga. La coincidencia más larga es un proceso que el router utiliza para encontrar una coincidencia entre la dirección IP de destino del paquete y una entrada de enrutamiento en la tabla de enrutamiento.

La tabla de enrutamiento contiene entradas de ruta que consisten en un prefijo (dirección de red) y una longitud de prefijo. Para que haya una coincidencia entre la dirección IPv4 de destino de un paquete y una ruta en la tabla de routing, una cantidad mínima de los bits del extremo izquierdo deben coincidir entre la dirección IPv4 del paquete y la ruta en la tabla de routing. La máscara de subred de la ruta en la tabla de routing se utiliza para determinar la cantidad mínima de bits del extremo izquierdo que deben coincidir. Recuerde que un paquete IP sólo contiene la dirección IP de destino y no la longitud del prefijo.

La mejor coincidencia es la ruta de la tabla de routing que contiene la mayor cantidad de bits del extremo izquierdo coincidentes con la dirección IPv4 de destino del paquete. La ruta con la mayor cantidad de bits del extremo izquierdo equivalentes, o la coincidencia más larga, es siempre la ruta preferida.

Nota: El término longitud del prefijo se utilizará para hacer referencia a la parte de red de direcciones IPv4 e IPv6.

- ***Ejemplo de coincidencia más larga de direcciones IPV4***

En la tabla, un paquete IPv4 tiene la dirección IPv4 de destino 172.16.0.10. El router tiene tres rutas posibles que coinciden con este paquete: 172.16.0.0/12, 172.16.0.0/18 y 172.16.0.0/26. De las tres rutas, 172.16.0.0/26 tiene la coincidencia más larga y se elige para reenviar el paquete. Recuerde que para que cualquiera de estas rutas se considere

una coincidencia debe tener al menos la cantidad de bits coincidentes que se indica en la máscara de subred de la ruta.

Figura 64.

Ruta IPV4

Dirección IPv4 de destino		Dirección de host en formato binario
172.16.0.10		**10101100.00010000.00000000.00**001010
Entradas de ruta	**Longitud del prefijo/prefijo**	**Dirección de host en formato binario**
1	172.16.0.0/**12**	**10101100.0001**0000.000000001010
2	172.16.0.0/**18**	**10101100.00010000.00**000000.00001010
3	172.16.0.0/**26**	**10101100.00010000.00000000.00**001010

Nota. Tablas de rutas de direccionamiento IPV4.

- ***Ejemplo de coincidencia más larga de direcciones IPV6***

En la tabla, un paquete IPv6 tiene la dirección IPv6 de destino 2001:db8:c000: :99. En este ejemplo se muestran tres entradas de ruta, pero sólo dos de ellas son una coincidencia válida, siendo una de ellas la coincidencia más larga. Las dos primeras entradas de ruta tienen longitudes de prefijo que tienen el número requerido de bits coincidentes como indica la longitud del prefijo. La primera entrada de ruta con una longitud de prefijo de /40 coincide con los 40 bits del extremo izquierdo de la dirección IPv6. La segunda entrada de ruta tiene una longitud de prefijo de /48 y con los 48 bits que coinciden con la dirección IPv6 de destino, y es la coincidencia más larga. La tercera entrada de ruta no coincide porque su prefijo /64 requiere 64 bits coincidentes. Para que el prefijo 2001:db8:c 000:5555: :/64 sea una coincidencia, los primeros 64 bits deben ser la dirección IPv6 de destino del paquete. Solo coinciden los primeros 48 bits, por lo que esta entrada de ruta no se considera una coincidencia.

Para el paquete IPv6 de destino con la dirección 2001:db8:c000: :99, considere las tres entradas de ruta siguientes:

Figura 65.

Ruta IPV6

Entradas de ruta	Longitud del prefijo/prefijo	¿Coincide?
1	**2001:db8:c000::/40**	Partido de 40 bits
2	**2001:db8:c000::/48**	Partido de 48 bits (partido más largo)
3	**2001:db8:c000:5555**:: /64	No coincide con 64 bits

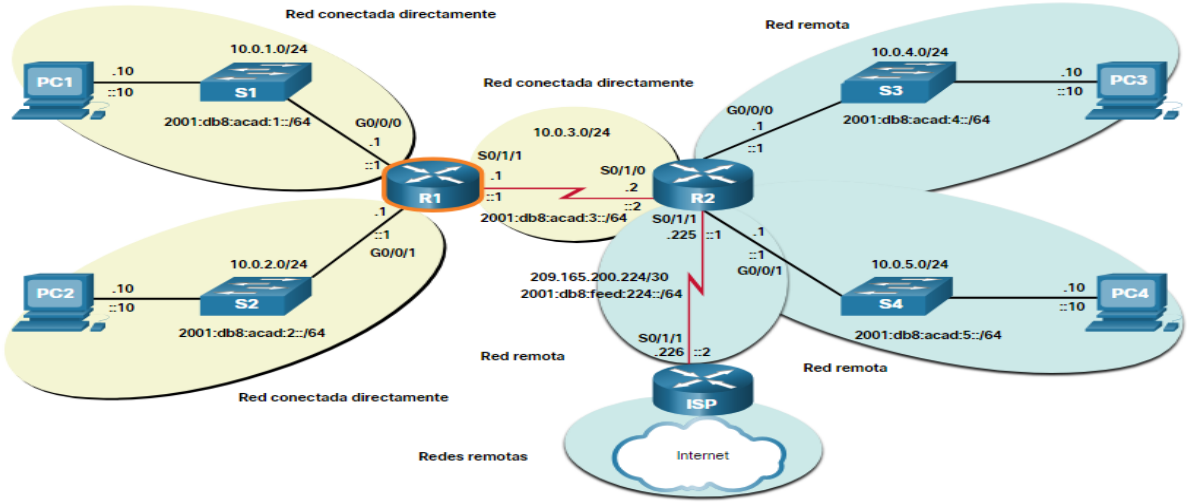
Nota. Tablas de rutas de direccionamiento IPV6.

- ***Creación de la tabla de enrutamiento***

Una tabla de enrutamiento consta de prefijos y sus longitudes de prefijo. Pero, ¿cómo aprende el router sobre estas redes? ¿Cómo rellena R1 en la figura su tabla de enrutamiento?

Figura 66.

Redes desde la perspectiva R1



Nota. Las redes IPV4 e IPV6 resaltadas en amarillas están conectadas directamente, mientras que las que resaltan en azul, son redes remotas.

Redes conectadas directamente

Las redes conectadas directamente son redes que están configuradas en las interfaces activas de un router. Una red conectada directamente se agrega a la tabla de enrutamiento cuando una interfaz se configura con una dirección IP y una máscara de subred (longitud de prefijo) y está activa (arriba y arriba)

Redes remotas

Las redes remotas son redes que no están conectadas directamente al router. Un router descubre redes remotas de dos maneras:

Rutas estáticas : se agrega a la tabla de enrutamiento cuando se configura manualmente una ruta. Protocolos de enrutamiento **dinámico** : se han añadido a la tabla de enrutamiento cuando los protocolos de enrutamiento aprenden dinámicamente acerca de la red remota. Estos protocolos incluyen el protocolo de información de routing versión 2 (RIPv2), abrir primero la ruta más corta (OSPF) y el protocolo de routing de gateway interior mejorado (EIGRP).

Ruta predeterminada

Una ruta predeterminada específica un router de salto siguiente que se utilizará cuando la tabla de enrutamiento no contiene una ruta específica que coincida con la dirección IP de destino. La ruta predeterminada puede configurarse manualmente como ruta estática o puede introducirla el protocolo de routing.

Una ruta predeterminada sobre IPv4 tiene una entrada de ruta de 0.0.0.0/0 y una ruta predeterminada sobre IPv6 tiene una entrada de ruta de: :/0. La longitud del prefijo /0 indica que cero bits o ningún bit deben coincidir con la dirección IP de destino para que se utilice esta entrada de ruta. Si no hay rutas con una coincidencia más larga, más de 0 bits, entonces la ruta predeterminada se utiliza para reenviar el paquete. A veces, la ruta predeterminada se conoce como una puerta de enlace de último recurso.

4.3.8. Configuración básica de un router

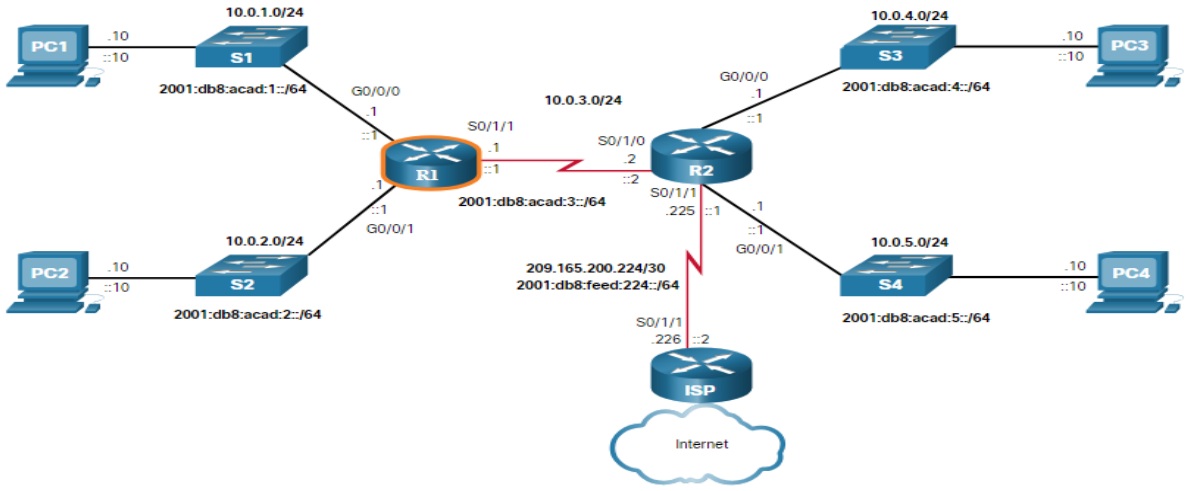
- ***Topología***

Un router utiliza una tabla de enrutamiento para determinar a dónde enviar los paquetes. Pero antes de sumergirse en los detalles de la tabla de enrutamiento IP, este tema revisa las tareas básicas de configuración y verificación del enrutador. También completarás una actividad de Rastreador de paquetes para actualizar tus habilidades.

La topología de la figura se utilizará para los ejemplos de configuración y verificación. También se usará en el siguiente tema para discutir la tabla de enrutamiento IP.

Figura 67.

Diagrama de Topología



Nota. Diagrama de tres routers conectados a 4 switches.

- ***Comandos de configuración***

Los siguientes ejemplos muestran la configuración completa de R1.

```
Router> enable
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)# logging synchronous
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)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
#
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1:a link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1:b link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.3.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1:c link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

- ***Comandos de verificación***

Algunos comandos de verificación comunes incluyen los siguientes:

show ip interface brief

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabiteThernet0/0/0 10.0.1.1 Sí manual arriba
GigabiteThernet0/0/1 10.0.2.1 Sí manual arriba
Serial0/1/0 unassigned YES unset administratively down down
```

```
Serial0/1/1 10.0.3.1 SÍ manual arriba
GigabitEthernet0 unassigned YES unset down down
R1#
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80: :1:A
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1 [up/up]
    FE80: :1:B
    2001:DB8:ACAD:2::1
Serial0/1/0 [administratively down/down]
    no asignado
Serial0/1/1 [up/up]
    FE80: :1:C
    2001:DB8:ACAD:3: :1
GigabiteThernet0 [abajo/abajo]
    no asignado
R1#
```

show running-config interface interface-type number

```
R1# show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 189 bytes
!
interfaz GigabiteThernet0/0/0
 description Link to LAN 1
 ip address 10.0.1.1 255.255.255.0
 automatización de negociación
 dirección ipv6 FE80: :1:Un enlace local
 ipv6 address 2001:DB8:ACAD:1::1/64
finalizar
R1#
```

show interfaces

```
R1# show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  El hardware es ISR4321-2x1GE, la dirección es a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Internet address is 10.0.1.1/24
  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 not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

```
  5 minute input rate 2000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     57793 packets input, 10528767 bytes, 0 no buffer
     Received 19711 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 36766 multicast, 0 pause input
     10350 packets output, 1280030 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R1#
```

show ip interface

```
R1# show ip interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 10.0.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound access list is not set
  El ARP del proxy está habilitado
  El Proxy local ARP esta desabilitado
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  Vector turbo IP nulo
  Topologías de enrutamiento de unidifusión asociadas:
       Topología «base», estado de operación es UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Las respuestas de nombre de proxy de sondeo están deshabilitadas
  Policy routing is disabled
```

```
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Características de entrada: MCI Check
  IPv4 WCCP Redirect outbound is disabled
  IPv4 WCCP Redirect inbound is disabled
  IPv4 WCCP Redirect exclude is disabled
R1#
```

```
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::1:A
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1: :1, la subred es 2001:DB8:ACAD:1: :/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:1
    FF02: :1:FF01:A
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  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.
R1#
```

show ip route

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(Output omitted)
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C 10.0.1.0/24 está conectado directamente, GigabiteThernet0/0/0
L 10.0.1.1/32 está conectado directamente, GigabiteThernet0/0/0
C 10.0.2.0/24 está conectado directamente, GigabiteThernet0/0/1
L 10.0.2.1/32 está conectado directamente, GigabiteThernet0/0/1
C 10.0.3.0/24 está conectado directamente, Serial0/1/1
L 10.0.3.1/32 está conectado directamente, Serial0/1/1
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(Output omitted)
```

```
C 2001:DB8:ACAD:1::/64 [0/0]
     a través de GigabiteThernet0/0/0, conectado directamente
L 2001:DB8:ACAD:1::1/128 [0/0]
     a través de GigabiteThernet0/0/0, recibir
C 2001:DB8:ACAD:2::/64 [0/0]
     a través de GigabiteThernet0/0/1, conectado directamente
L 2001:DB8:ACAD:2::1/128 [0/0]
     a través de GigabiteThernet0/0/1, reciba
C 2001:DB8:ACAD:3: :/64 [0/0]
     via Serial0/1/1, directly connected
L 2001:DB8:ACAD:3: :1/128 [0/0]
     via Serial0/1/1, receive
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

ping

```
R1# ping 10.0.3.2
Escriba la secuencia de escape para interrumpir la acción.
Sending 5, 100-byte ICMP Echos to 10.0.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms
R1# ping 2001:db8:acad:3::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:3::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms
R1#
```

En cada caso, ip reemplace ipv6 por la versión IPv6 del comando. .

- ***Salida del comando de filtro***

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

Los parámetros de filtrado que se pueden configurar después de la barra vertical incluyen lo siguiente:

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 filtra

Nota: Los filtros de salida se pueden usar en combinación con cualquier comando show.

Estos ejemplos demuestran algunos de los usos más comunes de los parámetros de filtrado.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 121A0C0411044C
 login
 transport input telnet ssh
R1#
R1# show ipv6 interface brief | include up
GigabitEthernet0/0/0   [up/up]
GigabitEthernet0/0/1   [up/up]
Serial0/1/1            [up/up]
R1#
R1# show ip interface brief | exclude unassigned
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
Serial0/1/1            209.165.200.225 YES manual up                    up
R1#
R1# show ip route | begin Gateway
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, Serial0/1/1
L        209.165.200.225/32 is directly connected, Serial0/1/1
R1#
```

4.3.9. Enrutamiento estático y dinámico

- ***¿Estático o dinámico?***

En el tema anterior se discutieron las formas en que un router crea su tabla de enrutamiento. Por lo tanto, ahora sabe que el enrutamiento, como el direccionamiento IP, puede ser estático o dinámico. ¿Debería usar enrutamiento estático o dinámico? ¡La respuesta es ambas cosas! El routing estático y el routing dinámico no son mutuamente excluyentes. En cambio, la mayoría de las redes utilizan una combinación de protocolos de routing dinámico y rutas estáticas.

Rutas Estáticas

Las rutas estáticas se utilizan comúnmente en los siguientes escenarios:

Como ruta predeterminada de reenvío de paquetes a un proveedor de servicios

Para rutas fuera del dominio de enrutamiento y no aprendidas por el protocolo de enrutamiento dinámico

Cuando el administrador de red desea definir explícitamente la ruta de acceso para una red específica

Para el enrutamiento entre redes de código auxiliar

Las rutas estáticas son útiles para redes más pequeñas con solo una ruta hacia una red externa. También proporcionan seguridad en una red más grande para ciertos tipos de tráfico o enlaces a otras redes que necesitan más control.

Protocolos de enrutamiento dinámico

Los protocolos de enrutamiento dinámico ayudan al administrador de red a administrar el proceso riguroso y lento de configuración y mantenimiento de rutas estáticas. Los protocolos de enrutamiento dinámico se implementan en cualquier tipo de red que consta de más de unos pocos enrutadores. Los protocolos de enrutamiento dinámico son escalables y determinan automáticamente las mejores rutas si se produce un cambio en la topología.

- Los protocolos de enrutamiento dinámico se utilizan comúnmente en los siguientes escenarios.
- En redes que consisten en más de unos pocos routers
- Cuando un cambio en la topología de red requiere que la red determine automáticamente otra ruta
- Escalabilidad A medida que la red crece, el protocolo de enrutamiento dinámico aprende automáticamente sobre cualquier red nueva.

La tabla muestra una comparación de algunas de las diferencias entre el enrutamiento dinámico y estático.

Figura 68.

Enrutamiento dinámico y estático

Característica	Routing dinámico	Routing estático
Complejidad de la configuración	Independiente del tamaño de la red	Aumentos en el tamaño de la red
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere intervención del administrador
Escalabilidad	Adecuado para topologías complejas	Adecuado para topologías simples
Seguridad	La seguridad debe estar configurada	La seguridad es inherente
Uso de recursos	Usa CPU, memoria, ancho de banda de enlaces	No se necesitan recursos adicionales
Predictibilidad de Ruta	La ruta depende de la topología y el protocolo de enrutamiento utilizados	Definido explícitamente por el administrador

Nota. Características de los tipos de enrutamiento

- ***Evolución de protocolo de routing dinámico***

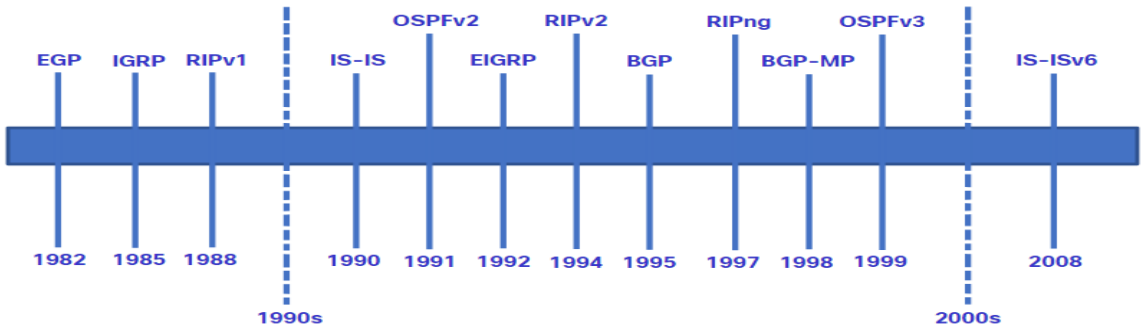
Los protocolos de enrutamiento dinámico se utilizan en el ámbito de las redes desde finales de la década de los ochenta. Uno de los primeros protocolos de enrutamiento fue RIP. RIPv1 se lanzó en 1988, pero ya en 1969 se utilizaban algunos de los algoritmos básicos en dicho protocolo en la Advanced Research Projects Agency Network (ARPANET).

A medida que las redes evolucionaron y se volvieron más complejas, surgieron nuevos protocolos de enrutamiento. El protocolo RIP se actualizó a RIPv2 para hacer lugar al crecimiento en el entorno de red. Sin embargo, RIPv2 aún no se escala a las implementaciones de red de mayor tamaño de la actualidad. Con el objetivo de satisfacer las necesidades de las redes más grandes, se desarrollaron dos protocolos de enrutamiento: el protocolo OSPF (abrir primero la ruta más corta) y sistema intermedio a sistema intermedio (IS-IS). Cisco desarrolló el protocolo de enrutamiento de gateway interior (IGRP) e IGRP mejorado (EIGRP), que también tiene buena escalabilidad en implementaciones de redes más grandes.

Asimismo, surgió la necesidad de conectar distintos dominios de enrutamiento de diferentes organizacions y proporcionar enrutamiento entre ellas. En la actualidad, se utiliza el protocolo de gateway fronterizo (BGP) entre proveedores de servicios de Internet (ISP). El protocolo BGP también se utiliza entre los ISP y sus clientes privados más grandes para intercambiar información de enrutamiento.

Figura 69

Línea cronológica de protocolos.



Nota. A fin de admitir la comunicación basada en IPv6, se desarrollaron versiones más nuevas de los protocolos de routing IP.

La tabla clasifica los protocolos de enrutamiento actuales. Los protocolos de puerta de enlace interior (IGP) son protocolos de enrutamiento utilizados para intercambiar información de enrutamiento dentro de un dominio de enrutamiento administrado por una sola organización. Sólo hay un EGP y es BGP. BGP se utiliza para intercambiar información de enrutamiento entre diferentes organizaciones, conocidos como sistemas autónomos (AS). Los ISP utilizan BGP para enrutar paquetes a través de Internet. Los protocolos de enrutamiento vectorial de distancia, estado de vínculo y vector de ruta se refieren al tipo de algoritmo de enrutamiento utilizado para determinar la mejor ruta.

Figura 70

Protocolos de Gateway.

	Protocolos de gateway interior				Protocolos de gateway exterior
	Vector distancia		Estado de enlace		Vector ruta
IPv4	RIPv2	EIGRP	OSPFv2	Sistema intermedio a sistema intermedio (IS-IS)	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

Nota. Protocolos de enrutamiento de vector distancia, ruta y estado de enlace en el Gateway.

- ***Conceptos de protocolos de routing dinámico***

Un protocolo de routing es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de routing y completar la tabla de routing con la elección de los mejores caminos que realiza el protocolo. El objetivo de los protocolos de routing dinámico incluye lo siguiente:

- Detectar redes remotas
- Mantener la información de routing actualizada
- Elección de la mejor ruta hacia las redes de destino
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible

Los componentes principales de los protocolos de routing dinámico incluyen los siguientes:

Estructuras de datos - por lo general, los protocolos de routing utilizan tablas o bases de datos para sus operaciones. Esta información se guarda en la RAM.

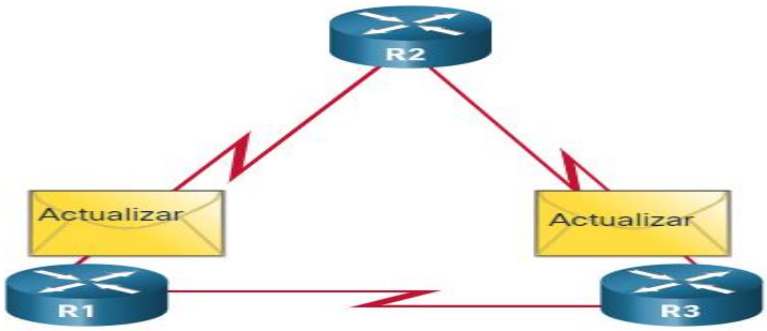
Mensajes del protocolo de routing - los protocolos de routing usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de routing y realizar otras tareas para descubrir la red y conservar información precisa acerca de ella.

Algoritmo - un algoritmo es una lista finita de pasos que se usan para llevar a cabo una tarea. Los protocolos de routing usan algoritmos para facilitar información de routing y para determinar el mejor camino.

Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y ofrecer esta información automáticamente en sus propias tablas de routing.

Figura 71

Protocolos de enrutamiento dinámico



Nota. Funcionamiento de los protocolos de enrutamiento en una red.

Los protocolos de routing determinan la mejor ruta hacia cada red y, a continuación, esa ruta se ofrece a la tabla de routing. La ruta se instalará en la tabla de routing si no hay otro origen de routing con una distancia administrativa menor. Uno de los beneficios principales de los protocolos de routing dinámico es que los routers intercambian información de routing cuando se produce un cambio en la topología. Este intercambio permite a los routers obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual.

- ***El mejor camino***

Antes de ofrecer una ruta a una red remota a la tabla de enrutamiento, el protocolo de enrutamiento dinámico debe determinar la mejor ruta a esa red. La determinación de la mejor ruta implica la evaluación de varias rutas hacia la misma red de destino y la selección de la ruta óptima o la más corta para llegar a esa red. Cuando existen varias rutas hacia la misma red, cada ruta utiliza una interfaz de salida diferente en el router para llegar a esa red.

El mejor camino es elegido por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Una métrica es un

valor cuantitativo que se utiliza para medir la distancia que existe hasta una red determinada. El mejor camino a una red es la ruta con la métrica más baja.

Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico.

Figura 72

Protocolos dinámicos comunes.

Protocolo de enrutamiento	Métrica
Protocolo de información de enrutamiento (RIP, Routing Information Protocol)	• La métrica es «recuento de saltos». • Cada router a lo largo de una ruta agrega un salto al recuento de saltos. • Se permite un máximo de 15 saltos.
Abrir primero la ruta más corta (OSPF)	• La métrica es «costo», que es la basada en la Basado en el ancho de banda acumulado de origen a destino • A los enlaces más rápidos se les asignan costos más bajos en comparación con los más lentos (mayor costo).
Protocolo de routing de gateway interno mejorado (EIGRP)	• Calcula una métrica basada en el ancho de banda más lento y el retardo anormales. • También podría incluir carga y fiabilidad en la métrica cálculo.

Nota. Métricas de protocolos de enrutamiento dinámicos más usados.

- ***Balance de carga***

¿Qué sucede si una tabla de routing tiene dos o más rutas con métricas idénticas hacia la misma red de destino?

Cuando un router tiene dos o más rutas hacia un destino con métrica del mismo costo, el router reenvía los paquetes usando ambas rutas por igual. Esto se denomina “balanceo de carga de mismo costo”. La tabla de routing contiene la única red de destino pero tiene varias interfaces de salida, una para cada ruta de mismo costo. El router reenvía los paquetes utilizando las distintas interfaces de salida que se indican en la tabla de routing.

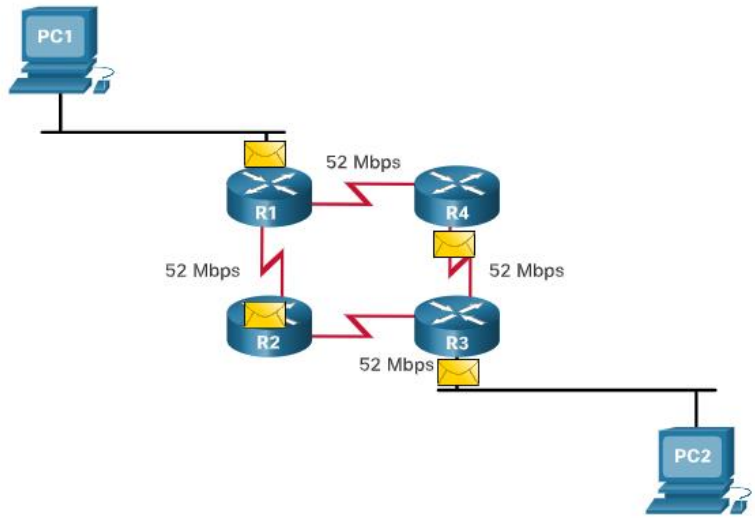
Si está configurado correctamente, el balanceo de carga puede aumentar la efectividad y el rendimiento de la red.

Equilibrio de carga de igual costo se implementa automáticamente mediante protocolos de enrutamiento dinámico. Se habilita con rutas estáticas cuando hay varias rutas estáticas a la misma red de destino utilizando diferentes enrutadores de siguiente salto.

Nota: Solo EIGRP admite el balanceo de carga con distinto costo.

Figura 73

Balanceo de carga.



Nota. Balanceo de carga de un mismo costo en una red.

4.3.10. Configuración de rutas estáticas IP

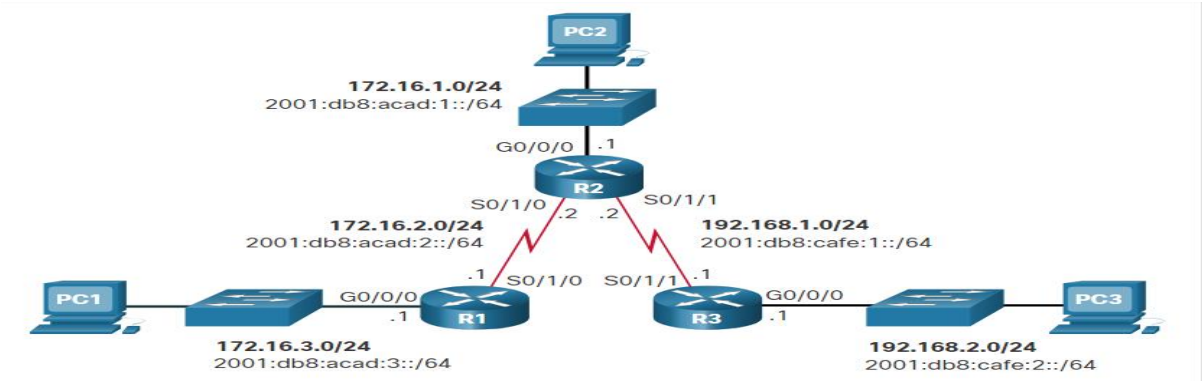
- ***Ruta estática IPV4 de siguiente salto***

Los comandos para configurar rutas estáticas estándar varían ligeramente entre IPv4 e IPv6. En este tema se muestra cómo configurar rutas estáticas estándar de siguiente salto, conectadas directamente y completas especificadas para IPv4 e IPv6

En una ruta estática de siguiente salto, solo se especifica la dirección IP del siguiente salto. La interfaz de salida se deriva del próximo salto. Por ejemplo, se configuran tres rutas estáticas de siguiente salto en el R1 con la dirección IP del siguiente salto, el R2.

Figura 74

Rutas estáticas de siguiente salto.



Nota. Configuración de protocolos de siguiente salto en la red con tres routers.

Los comandos para configurar R1 con las rutas estáticas IPv4 a las tres redes remotas son los siguientes:

```
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

La tabla de enrutamiento para R1 ahora tiene rutas a las tres redes IPv4 remotas.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.2.2
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.1/32 is directly connected, Serial0/1/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
```

```
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 [1/0] via 172.16.2.2
S     192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

- ***Ruta estática IPV6 de siguiente salto***

Los comandos para configurar R1 con las rutas estáticas IPv6 a las tres redes remotas son los siguientes:

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 route 2001:db8:acad:1::/64 2001:db8:acad:2::2
R1(config)# ipv6 route 2001:db8:cafe:1::/64 2001:db8:acad:2::2
R1(config)# ipv6 route 2001:db8:cafe:2::/64 2001:db8:acad:2::2
```

La tabla de enrutamiento para R1 ahora tiene rutas a las tres redes IPv6 remotas.

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S   2001:DB8:ACAD:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/1/0, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
S   2001:DB8:CAFE:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
S   2001:DB8:CAFE:2::/64 [1/0]
     via 2001:DB8:ACAD:2::2
L   FF00::/8 [0/0]
     via Null0, receive
```

- ***Ruta estática IPV4 conectada directamente***

Al configurar una ruta estática, otra opción es utilizar la interfaz de salida para especificar la dirección del siguiente salto. La figura 74 muestra de nuevo la topología.

Se configuran tres rutas estáticas conectadas directamente en el R1 mediante la interfaz de salida.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 s0/1/0
R1(config)# ip route 192.168.1.0 255.255.255.0 s0/1/0
R1(config)# ip route 192.168.2.0 255.255.255.0 s0/1/0
```

La tabla de routing para el R1 muestra que cuando un paquete está destinado a la red 192.168.2.0/24, el R1 busca una coincidencia en la tabla de routing y encuentra que puede reenviar el paquete desde su interfaz serial 0/0/0.

Nota: Generalmente se recomienda utilizar una dirección de salto siguiente. Las rutas estáticas conectadas directamente solo deben usarse con interfaces seriales punto a punto, como en este ejemplo.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 is directly connected, Serial0/1/0
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.1/32 is directly connected, Serial0/1/0
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 is directly connected, Serial0/1/0
S     192.168.2.0/24 is directly connected, Serial0/1/0
```

- ***Ruta estática IPV6 conectada directamente***

En el ejemplo, se configuran tres rutas estáticas conectadas directamente en el R1 mediante la interfaz de salida.

```
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0
R1(config)# ipv6 route 2001:db8:cafe:1::/64 s0/1/0
R1(config)# ipv6 route 2001:db8:cafe:2::/64 s0/1/0
```

La tabla de routing IPv6 para el R1 en el ejemplo muestra que cuando un paquete está destinado a la red 2001:db8:cafe:2::/64, el R1 busca una coincidencia en la tabla de routing y encuentra que puede reenviar el paquete desde su interfaz serial 0/0/0.

Nota: Generalmente se recomienda utilizar una dirección de salto siguiente. Solo se deben utilizar rutas estáticas conectadas directamente con interfaces seriales de punto a punto, como se muestra en este ejemplo.

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
```

```
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S   2001:DB8:ACAD:1::/64 [1/0]
     via Serial0/1/0, directly connected
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/1/0, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
S   2001:DB8:CAFE:1::/64 [1/0]
     via Serial0/1/0, directly connected
S   2001:DB8:CAFE:2::/64 [1/0]
     via Serial0/1/0, directly connected
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

- ***Ruta estática completamente especificada IPV4***

Una ruta estática completamente especificada tiene determinadas tanto la interfaz de salida como la dirección IP del siguiente salto. Esta forma de ruta estática se utiliza cuando la interfaz de salida es una interfaz de acceso múltiple y se debe identificar explícitamente el siguiente salto. El siguiente salto debe estar conectado directamente a la interfaz de salida especificada. El uso de una interfaz de salida es opcional, sin embargo, es necesario utilizar una dirección de salto siguiente.

Suponga que el enlace de red entre el R1 y el R2 es un enlace Ethernet y que la interfaz GigabitEthernet 0/0/1 del R1 está conectada a dicha red, como se muestra en la Figura 74.

La diferencia entre una red Ethernet de accesos múltiples y una red serial punto a punto es que esta última solo tiene un dispositivo más en esa red, el router que se encuentra en el otro extremo del enlace. Con las redes Ethernet, es posible que existan

muchos dispositivos diferentes que comparten la misma red de accesos múltiples, incluyendo hosts y hasta routers múltiples.

Cuando la interfaz de salida sea una red Ethernet, se recomienda utilizar una ruta estática que incluya una dirección del siguiente salto. También puede usar una ruta estática completamente especificada que incluye la interfaz de salida y la dirección de siguiente salto.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
```

Al reenviar paquetes al R2, la interfaz de salida es GigabitEthernet 0/0/1 y la dirección IPv4 del siguiente salto es 172.16.2.2. como se muestra en el show ip route resultado de R1.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0/1
L        172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
S     192.168.2.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
```

- ***Ruta estática completamente especificada IPV6***

En una ruta estática IPv6 completamente especificada, se especifican tanto la interfaz de salida como la dirección IPv6 del siguiente salto. Hay una situación en IPv6 que se da cuando se debe utilizar una ruta estática completamente especificada. Si la ruta estática IPv6 usa una dirección IPv6 link-local como la dirección del siguiente salto, debe utilizarse una ruta estática completamente especificada. La figura muestra un ejemplo de una ruta estática IPv6 completamente especificada que utiliza una dirección IPv6 link-local como la dirección del siguiente salto.

Figura 75

Ruta especificad IPV6

Nota. Ruta completamente especificada en protocolo IPV6.

```
R1(config)# ipv6 route 2001:db8:acad:1::/64 fe80::2
%Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0 fe80::2
```

En el ejemplo, se configura una ruta estática completamente especificada con la dirección link-local del R2 como dirección del siguiente salto. Observe que el IOS requiere que se especifique una interfaz de salida.

La razón por la cual se debe utilizar una ruta estática completamente especificada es que las direcciones IPv6 link-local no están incluidas en la tabla de routing IPv6. Las direcciones link-local solo son exclusivas en una red o un enlace dados. La dirección link-local del siguiente salto puede ser una dirección válida en varias redes conectadas al router. Por lo tanto, es necesario que la interfaz de salida se incluya.

El siguiente ejemplo muestra la entrada de la tabla de routing IPv6 para esta ruta. Observe que la dirección link-local del siguiente salto y la interfaz de salida están incluidas.

```
R1# show ipv6 route static | begin 2001:db8:acad:1::/64
S   2001:DB8:ACAD:1::/64 [1/0]
    via FE80::2, Seria0/1/0
```

- ***Verificador de una ruta estática***

Junto con show ip route, show ipv6 route, ping y traceroute, otros comandos útiles para verificar las rutas estáticas son los siguientes:

- show ip route static
- show ip route network

- show running-config | section ip route

Reemplace ip con ipv6 para las versiones IPv6 del comando.

Haga referencia a la Figura 74, al revisar los ejemplos de comandos.

Mostrar solo rutas estáticas IPV4

Esta salida muestra sólo las rutas estáticas IPv4 en la tabla de enrutamiento. También tenga en cuenta dónde el filtro comienza la salida, excluyendo todos los códigos.

```
R1# show ip route static | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S 172.16.1.0/24 [1/0] via 172.16.2.2
S 192.168.1.0/24 [1/0] via 172.16.2.2
S 192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

Mostrar una red IPV4 especifica

Este comando mostrará la salida sólo para la red especificada en la tabla de enrutamiento.

```
R1# show ip route 192.168.2.1
Routing entry for 192.168.2.0/24
  Known via "static", distance 1, metric 0
  Bloques descriptores de enrutamiento:
  * 172.16.2.2
      La métrica de la ruta es 0, y el conteo del tráfico compartido es 1.
```

Mostrar la configuración de la ruta estática IPV4

Este comando filtra la configuración en ejecución sólo para rutas estáticas IPv4..

```
R1# show running-config | section ip route
ip route 172.16.1.0 255.255.255.0 172.16.2.2
ip route 192.168.1.0 255.255.255.0 172.16.2.2
ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

Mostrar solo rutas estáticas IPV6

Este resultado muestra sólo las rutas estáticas IPv6 en la tabla de enrutamiento. También tenga en cuenta dónde el filtro comienza la salida, excluyendo todos los códigos.

```
R1# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, LA - LISP away, le - LISP extranet-policy
       a - Application
S 2001:DB8:ACAD:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
S 2001:DB8:CAFE:1: :/64 [1/0]
     via 2001:DB8:ACAD:2::2
S 2001:DB8:CAFE:2: :/64 [1/0]
     via 2001:DB8:ACAD:2::2
R1#
```

Mostrar una red IPV6 especifica

Este comando mostrará la salida de la red especificada en la tabla de routing únicamente.

```
R1# show ipv6 route 2001:db8:cafe:2::
Routing entry for 2001:DB8:CAFE:2::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Rutas de enrutamiento:
    2001:DB8:ACAD:2::2
      Última actualización hace 00:23:55
R1#
```

Mostrar la configuración de la ruta estática IPV6

Este comando filtra la configuración en ejecución sólo para rutas estáticas IPv6.

```
R1# show running-config | section ipv6 route
ipv6 route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:2::2
ipv6 route 2001:DB8:CAFE:1::/64 2001:DB8:ACAD:2::2
ipv6 route 2001:DB8:CAFE:2::/64 2001:DB8:ACAD:2::2
R1#
```

4.3.11. Autoevaluación

a) ¿Cuál ataque encripta los datos en los hosts con el propósito de extraer un pago monetario de la víctima?

- DDoS
- Malware

- Ransomware

b) ¿Cuál de las siguientes técnicas de mitigación previene suplantación de direcciones MAC e IP?

- DAI
- DHCP Snooping
- IPSG

c) Un actor de amenaza solicita todas las direcciones IP disponibles en una subred. ¿Qué tipo de ataque es este?

- Agotamiento DHCP
- Suplantación de direcciones
- Ataque de STP

d) ¿Qué acción tomará un router en un paquete con una dirección IP de destino que se encuentra en una red remota?

- Reenviara el paquete a un conmutador ethernet
- Reenviara el paquete a un router de siguiente salto
- Descarta el paquete

e) ¿Qué metrica utiliza OSPF para determinar la mejor ruta?

- Conteo de saltos
- Costo
- Ancho de banda y retraso

4.3.12. Actividad Propuesta

Figura 76

Actividad propuesta 3

Topología

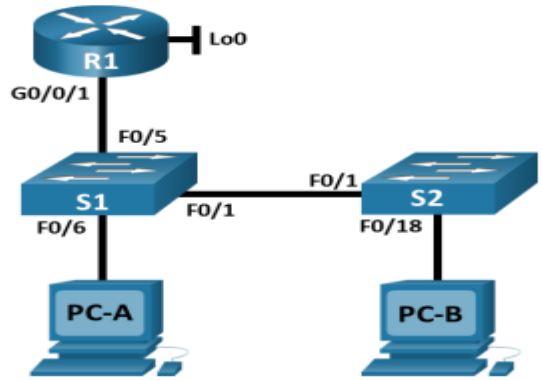


Tabla de asignación de direcciones

de red	Interface / VLAN	Dirección IP	Máscara de subred
R1	G0/0/1	192.168.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

Nota. Topología y tabla de direccionamiento ip para el ejercicio de la actividad.

Objetivos

Part 1: Configurar los dispositivos de red.

- Conecte la red.
- Configurar R1
- Configurar y verificar los parámetros básicos del switch

Part 2: Configurar las VLAN en los Switches.

- Configurar la VLAN 10.
- Configurar el SVI para VLAN 10.
- Configurar la VLAN 333 con el nombre Native en S1 y S2.
- Configurar la VLAN 999 con el nombre ParkingLot en S1 y S2.

Parte 3: Configurar la seguridad del Switch.

- Implemente el enlace troncal 802.1Q.
- Configurar puertos de acceso.
- Asegure y deshabilite los puertos del switch no utilizados.
- Documentar e implementar funciones de seguridad de los puertos
- Implemente la seguridad de DHCP snooping.
- Implemente PortFast y la protección BPDU.
- Verifique la conectividad de extremo a extremo.

Antecedentes/Escenario

Este es un laboratorio completo para revisar las características de seguridad de Capa 2 cubiertas anteriormente.

Nota: Los routers que se utilizan en los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.3 (universalk9 imagen). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 Router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.3 o comparable)
- 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Instrucciones

Parte 1: Configurar los dispositivos de red.

Paso 1: Conecte la red.

a. Realice el cableado de red tal como se muestra en la topología.
b. Inicializar los dispositivos.

Paso 2: Configurar R1

a. Verifique la configuración en ejecución en R1 con el siguiente comando:
b. Verifique que el direccionamiento IP y las interfaces estén en un estado UP/UP (solucione los problemas según sea necesario).

Paso 3: Configure y verifique os parámetros básicos del switch

a. Configure el nombre de host para los switches S1 y S2.
b. Evite búsquedas DNS no deseadas en ambos switches
c. Configure las descripciones de interfaz para los puertos que están en uso en S1 y S2.

d. Establezca la puerta de enlace predeterminada para la VLAN de administración en 192.168.10.1 en ambos switches.

Parte 2: Configure las VLAN en los Switches.

Paso 1: Configure la VLAN 10.

Agregue la VLAN 10 a S1 y S2 y asigne el nombre Management. a la VLAN de administración.

Paso 2: Configure el SVI para VLAN 10.

Configure la dirección IP de acuerdo con la Tabla de direccionamiento para SVI para VLAN 10 en S1 y S2. Habilite las interfaces SVI y proporcione una descripción para la interfaz.

Paso 3: Configure la VLAN 333 con el nombre Native en S1 y S2.

Paso 4: Configure la VLAN 999 con el nombre ParkingLot en S1 y S2.

Parte 3: Configure la seguridad del Switch.

Paso 1: Implemente el enlace 802.1Q.

a. En ambos switches, configure el enlace troncal en F0/1 para usar la VLAN 333 como la VLAN nativa.
b. Verifique que el enlace troncal esté configurado en ambos
c. Deshabilite la negociación DTP en F0/1 en S1 y S2.
d. Verifique con el comando show interfaces.

Paso 2: Configure puertos de acceso.

a. En S1, configure F0/5 y F0/6 como puertos de acceso asociados con la VLAN 10.
b. En S2, configure F0/18 como un puerto de acceso asociado con la VLAN 10.

Paso 3: Asegure y deshabilite los puertos del switch no utilizados.

a. En S1 y S2, mueva los puertos no utilizados de la VLAN 1 a la VLAN 999 y desactive los puertos no utilizados.
b. Verifique que los puertos no utilizados estén deshabilitados y asociados con la VLAN 999 emitiendo el comando show interfaces status.

Paso 4: Documente e implemente seguridad de puertos (port security).

Las interfaces F0/6 en S1 y F0/18 en S2 están configuradas como puertos de acceso. En este paso, también configurará la seguridad del puerto en estos dos puertos de acceso.

a. En S1, ejecute el comandoshow port-security interface f0/6 para mostrar la configuración de seguridad de puerto predeterminada para la interfaz F0/6. Registre sus respuestas en la tabla a continuación.

Configuración predeterminada de puertos	
Característica (Feature)	**Configuración predeterminada (Default Setting)**
Seguridad de Puertos(Port Security)	
Número máximo de direcciones MAC (Maximum number of MAC addresses)	
Modo de Violacion (Violation Mode)	
Tiempo de Vencimiento (Aging Time)	
Tipo de Vencimiento (Aging Type)	
Antigüedad segura de direcciones estáticas (Secure Static Address Aging)	
Dirección MAC segura persistente (Sticky MAC Address)	

b. En S1, habilite la seguridad de puerto (port security) en F0/6 con la siguiente configuración:
   - Número máximo de direcciones MAC: 3
   - Tipo de violación (Violation type): restrict
   - Tiempo de vencimiento (Aging time): 60 min
   - Tipo de vencimiento (Aging type): inactivity

c. Verifique la seguridad de puerto (port security) en S1 F0/6.

d. Habilite la seguridad de puerto (port security) para F0/18 en S2. Configure el puerto para agregar direcciones MAC, aprendidas automáticamente, a la configuración.

e. Configure las siguientes la seguridad de puerto (port security) en S2 F 0/18:

   - Número máximo de direcciones MAC: 2
   - Tipo de Violación (Violation type): Protect
   - Tiempo de vencimiento (Aging time): 60 min

f. Verifique la seguridad de puerto (port security) en S2 F0/18.

Paso 5: Implemente DHCP snooping.

a. En S2, habilite DHCP snooping y configúrelo para la VLAN 10.

b. Configure el puerto troncal en S2 como un puerto confiable (trusted ported).

c. Limite el puerto no confiable, F18 en S2, a cinco paquetes DHCP por segundo.

d. Verifique DHCP snooping en S2.

Paso 6: BPDU.

a. Configure PortFast en todos los puertos de acceso que están en uso en ambos switches.

b. Habilite BPDU guard, en los puertos de acceso de VLAN 10 conectados a la PC-A y PC-B.
c. Verifique que BPDU guard y PortFast estén habilitados en los puertos apropiados.

Paso 7: Verifique la conectividad de extremo a extremo

Verifique la conectividad PING entre todos los dispositivos en la tabla de direccionamiento IP. Verifique la conectividad PING entre todos los dispositivos en la tabla de direccionamiento IP.

Preguntas de reflexión

1. En referencia a Port Security en S2, ¿por qué cuando se configuró el aprendizaje permanente, no se establecio un temporizador para darle seguimiento al timempo de vencimiento restante?
2. En referencia a Port Security en S2, si carga el archivo de configuración en S2, ¿por qué la PC-B en el puerto 18 nunca obtendrá una dirección IP a través de DHCP?
3. En referencia a Port Security, ¿cuál es la diferencia entre el tipo de envejecimiento absoluto y el tipo de envejecimiento por inactividad?

4.4.RIP V1 Y RIP V2

Esta unidad permitirá a los estudiantes, conocer, configurar y verificar los protocolos de RIP V1, V2 mediante comandos y resolución de problemas.

4.4.1. Conceptos básicos de RIP V1

- ***Características***

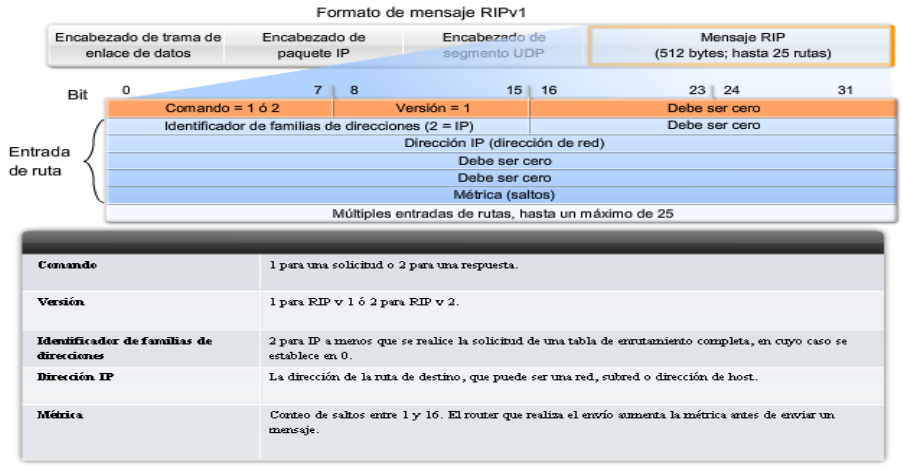
RIP es un protocolo de enrutamiento de vector de distancia (DV) classful, su métrica se mide en conteo de saltos, considerando que, las rutas con un conteo de saltos superior a 15 no se pueden alcanzar, y mientras su funcionamiento, se envía un broadcast de las actualizaciones cada 30 segundos.

- ***Formato de mensaje RIP***

EL mensaje RIP consta de un encabezado de 3 campos: campo de comando, campo de versión, debe ser cero. De la misma manera, la entrada de ruta tiene 3 campos: identificador de familia de direcciones, direcciones IP y métrica, como se muestra en la Figura 77.

Figura 77

Formato mensaje RIP



Comando	1 para una solicitud o 2 para una respuesta.
Versión	1 para RIP v 1 ó 2 para RIP v 2.
Identificador de familias de direcciones	2 para IP a menos que se realice la solicitud de una tabla de enrutamiento completa, en cuyo caso se establece en 0.
Dirección IP	La dirección de la ruta de destino, que puede ser una red, subred o dirección de host.
Métrica	Conteo de saltos entre 1 y 16. El router que realiza el envío aumenta la métrica antes de enviar un mensaje.

Nota. Descripción de mensaje RIP v1

- ***Funcionamiento***

El protocolo RIP usa 2 tipos de mensajes:

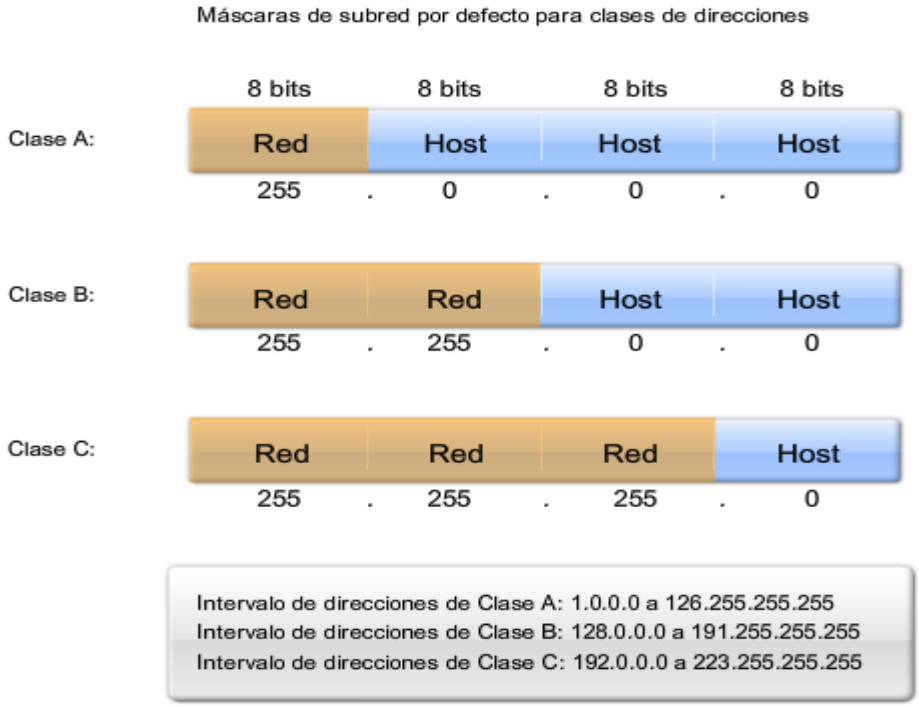
Mensaje de solicitud. - Cada interfaz habilitada con RIP lo envía en el inicio, además, solicita a todos los vecinos con RIP habilitado que envíen la tabla de enrutamiento.

Mensaje de respuesta. -El mensaje es enviado al router solicitante con la tabla de enrutamiento.

Las direcciones IP inicialmente se dividieron en 3 clases, que son A,B y C, ya que RIP es un protocolo de classful, asimismo, no envía las máscaras de subred durante las actualizaciones de enrutamiento.

Figura 78

Clases de direcciones IP



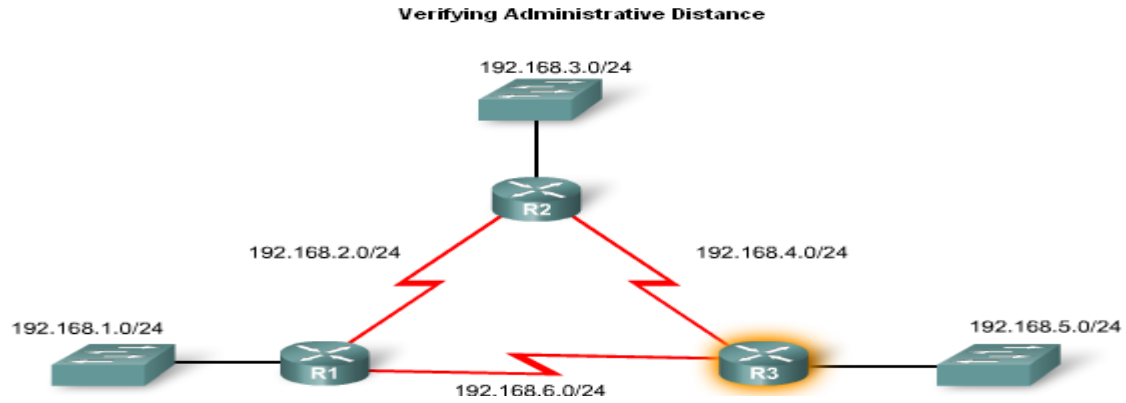
Nota. Intervalos de direcciones IP entre las tres clases.

- ***Distancia administrativa***

La distancia administrativa por defecto de RIP es de 120.

Figura 79

Distancia administrativa



Nota. Topología de tres redes conectadas entre sí.

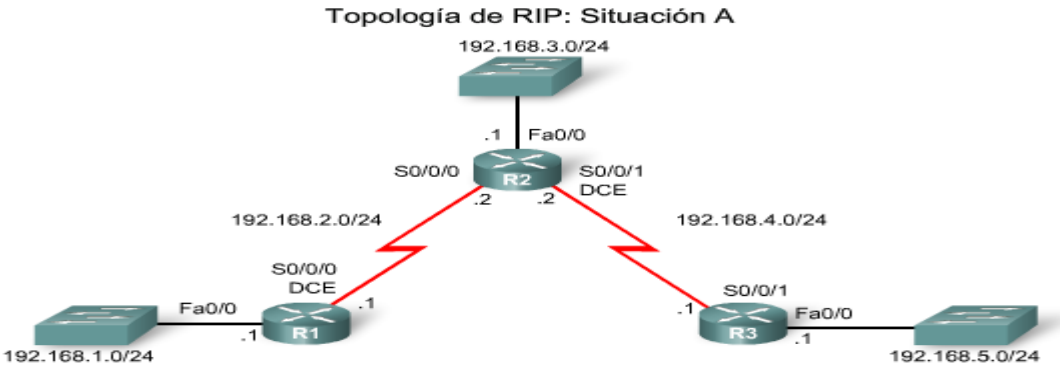
4.4.2. Configuración básica de RIP V1

- ***Topología***

Una topología típica adecuada para RIPV1 incluye: Configuración de tres routers, ninguna PC conectada a las LAN y el uso de 5 subredes IP diferentes, como se muestra en la figura 80.

Figura 80

Topología Básica



Nota. Topología típica para el enrutamiento RIP.

Figura 81

Tabla de direccionamiento IP

Tabla de direccionamiento: Situación A

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/0	192.168.1.1	255.255.255.0
	S0/0/0	192.168.2.1	255.255.255.0
R2	Fa0/0	192.168.3.1	255.255.255.0
	S0/0/0	192.168.2.2	255.255.255.0
	S0/0/1	192.168.4.2	255.255.255.0
R3	Fa0/0	192.168.5.1	255.255.255.0
	S0/0/1	192.168.4.1	255.255.255.0

Nota. Tabla de direcciones IP para la topología de la Figura 80.

- **Comando Router RIP**

Para habilitar el protocolo RIP, escriba **router rip** en el indicador de configuración global, como se indica en la Figura 82.

Figura 82

Comando router rip

```
R1#conf t
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)#router ?
  bgp         Border Gateway Protocol (BGP)
  egp         Exterior Gateway Protocol (EGP)
  eigrp       Enhanced Interior Gateway Protocol (EIRGP)
  igrp        Interior Gateway Routing Protocol (IGRP)
  isis        ISO IS-IS
  iso-igrp    IGRP for OSI networks
  mobile      Mobile routes
  odr         On Demand stub Routes
  ospf        Open Shortest Path First (OSPF)
  rip         Routing Information Protocol (RIP)

R1(config)#router rip
R1(config-router)#
```

Nota. El indicador será similar a R1 (config – router) #

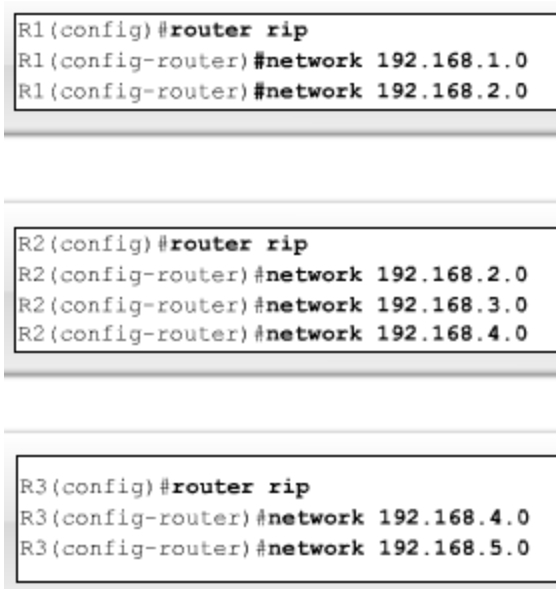
- ***Especificaciones de redes***

Se debe utilizar el comando **network** para habilitar RIP en todas las interfaces que pertenecen a la red, asimismo, se utiliza para publicar la red en las actualizaciones RIP, que se envían a otros routers cada 30 segundos.

Para el caso de la Figura 80, se debe aplicar lo siguiente:

Figura 83

Configuración RIP



Nota. Configuración rip de la topología mostrada en la figura 80.

4.4.3. RIPV1 y ruta por defecto

- ***Rutas por defecto***

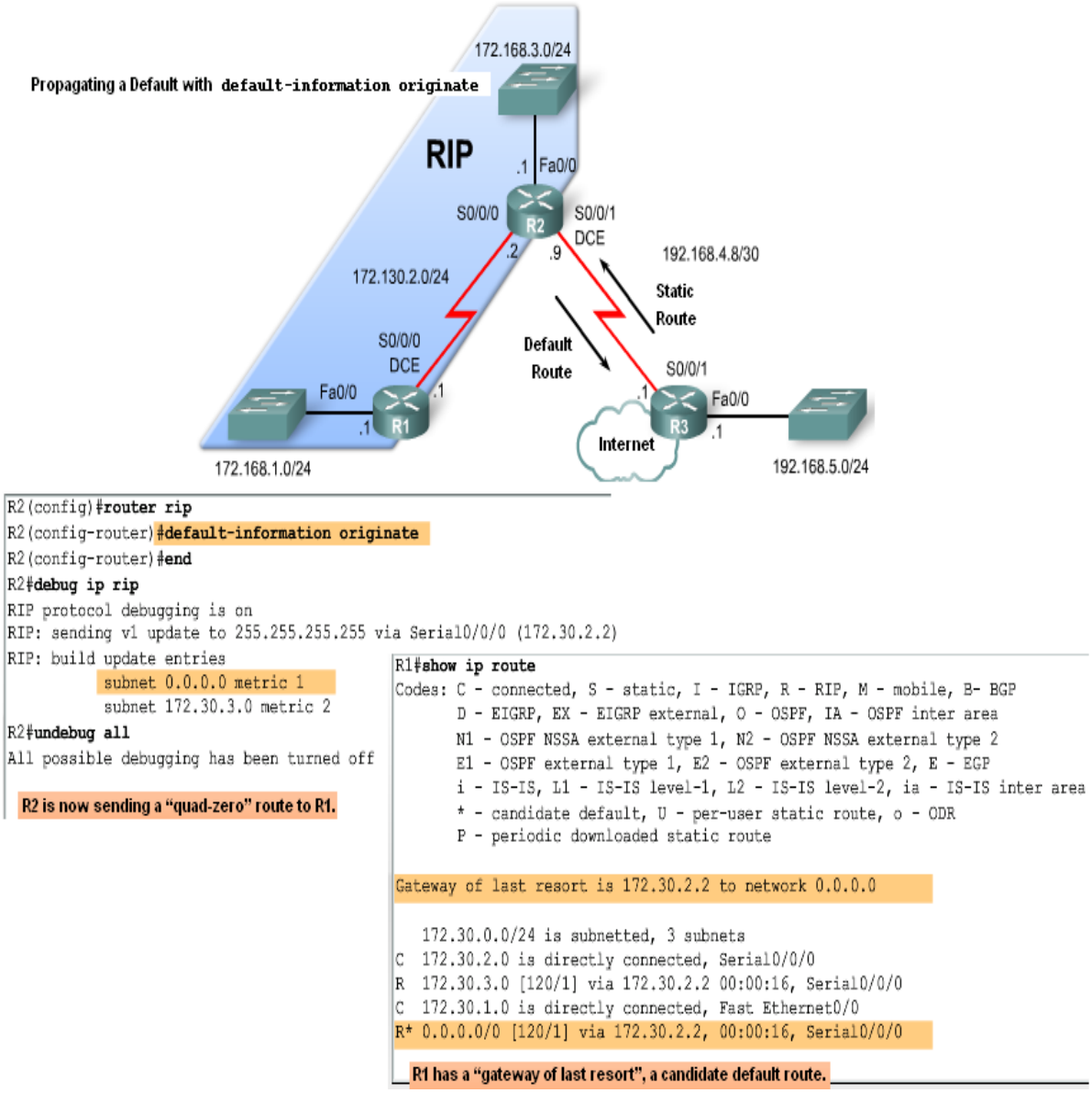
Los paquetes que no se definan específicamente en la tabla de enrutamiento irán a la interfaz determinada de la ruta por defecto. Por ejemplo, los routers clientes usan las rutas por defecto para conectarse a un router ISP, y el comando usado para configurar una ruta por defecto es:

ip route 0.0.0.0 0.0.0.0 s0/0/1

El Comando Default-information originate- Este comando se usa para especificar que el router va a originar información por defecto mediante la propagación de la ruta estática por defecto en la actualización RIP. Muy posiblemente, estos ataques envuelven una o más de las siguientes

Figura 84

Ruta por defecto en RIPv1



Nota. Propagación de la ruta por defecto.

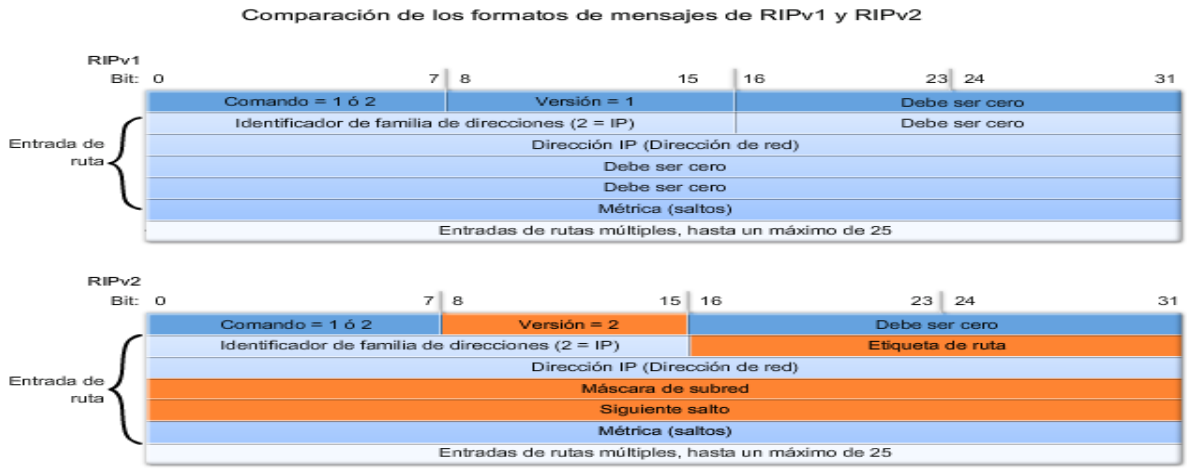
4.4.4. Configuración de RIPV2

- ***Comparación entre formatos de mensajes de RIPV1 y RIPV2***

El formato de mensajes de RIPV2 es similar al de RIPV1, pero tiene dos extensiones que son la máscara de red y la dirección del siguiente salto.

Figura 85

Formato de mensaje RIPV2



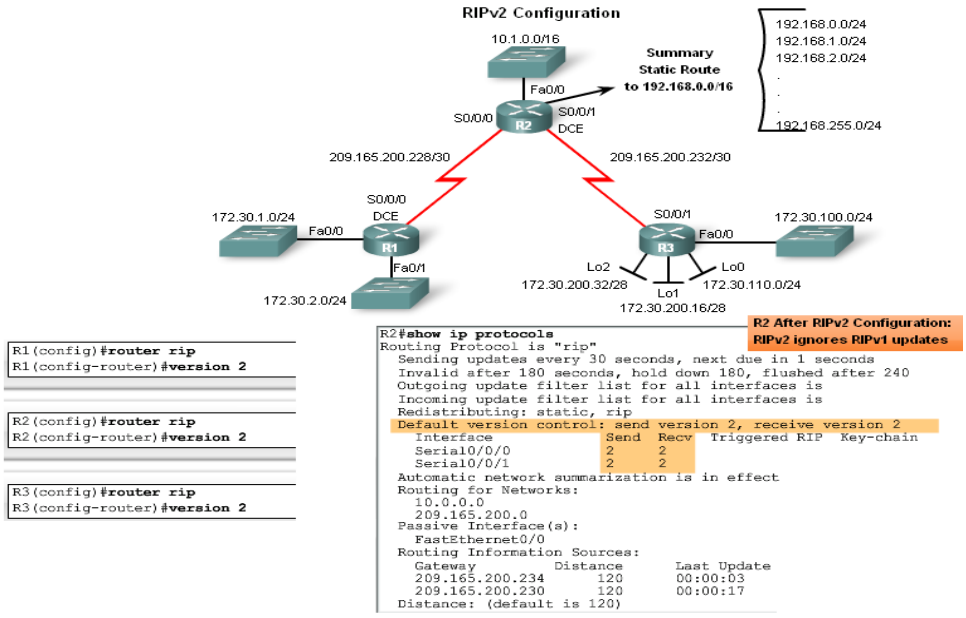
Nota. En el formato de mensaje de RIPV2 tiene la mascara de subred y la ip del siguiente salto.

- **Configuración de RIPV2 en cisco**

En primera instancia se debe habilitar y verificar RIPV2, ya que por defecto se esta ejecutando RIPV1, para verificar que RIPV2 está configurado se utiliza el comando **show ip protocols**

Figura 86

Configuración de ripv2



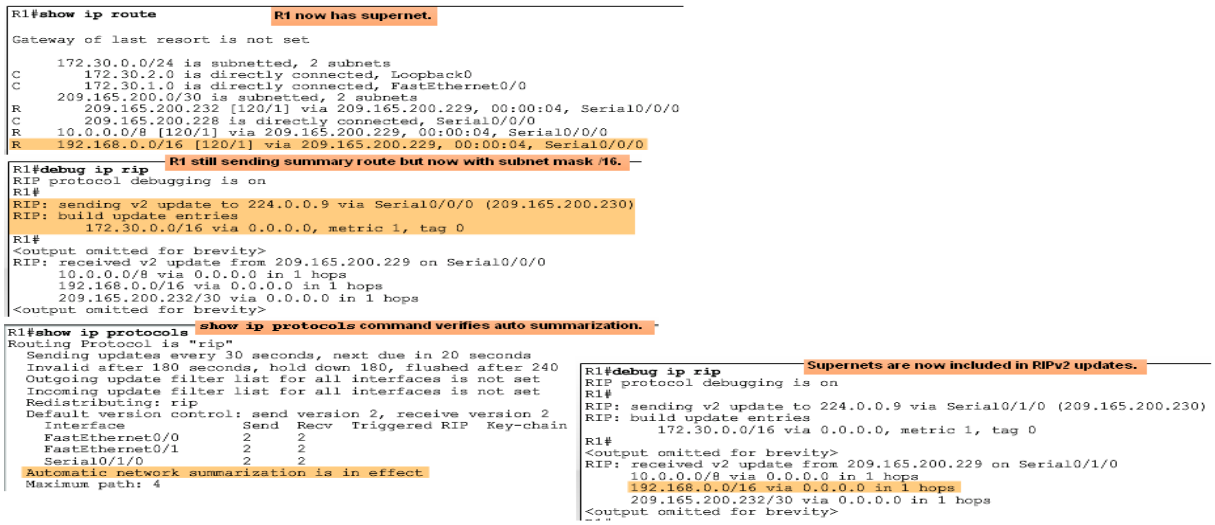
Nota. Requiere el uso de un comando versión 2.

- ***Sumarización automática de RIPV2***

RIPV2 resumirá automáticamente las rutas en los límites de red principales y también puede resumir rutas con una mascará de subred más pequeña que la máscara de subred classful.

Figura 87

Sumarización



Nota. Sumarización automática.

Para inhabilitar la sumarización automática en RIPV2, se debe ejecutar el comando **no auto-summary.**

- **Verificación de las actualizaciones de RIPV2**

Cuando se utiliza RIPV2 con la sumarización automática desactivada, cada subred (y cada mascara) tiene sus propias entradas, junto con la interfaz de salida y la dirección del siguiente salto, para alcanzar la subred. Asimismo, para verificar la información que envía RIPV2, utilice el comando **debug ip rip**.

4.4.5. Verificación y resolución de problemas de RIPV2

- ***Pasos básicos para la resolución de problemas.***

1. Verifique el estado de todos los enlaces
2. Verifique el cableado
3. Verifique la dirección IP y la configuración de la máscara de subred
4. Quite los comandos de configuración innecesarios

- ***Comandos utilizados para verificar el funcionamiento correcto de RIPv2:***

- Show ip interfaces brief
- Show ip protocols
- Debug ip rip
- Show ip route

- ***Problemas comunes de RIPV2***

Cuando resuelva problemas de RIPv2, analice lo siguiente:

- Versión: Asegúrese de estar utilizando la versión 2
- Sentencias de red: Las sentencias de red pueden estar mal escritas o pueden faltar
- Sumarización automática: Si no son necesarias las rutas resumidas, deshabilite la sumarización automática

- ***Razones por las que es conveniente autenticar la información de enrutamiento:***

- Previene la posibilidad de aceptar actualizaciones de enrutamiento no válidas
- Los contenidos de las actualizaciones de enrutamiento están encriptados

- ***Tipos de protocolos de enrutamiento que pueden utilizar la autenticación:***

- RIPv2
- EIGRP

- OSPF
- IS-IS
- BGP

4.4.6. Autoevaluación

a. ¿Cuál es la distancia administrativa de RIP?

- 120
- 150
- 179

b. ¿Qué comando se utiliza para habilitar el protocolo RIP?

- router ripp
- ip route
- router rip

c. ¿Qué comando se utiliza para habilitar RIP en todas las interfaces de la red?

- networking ip
- network
- ip network

d. ¿Qué comando se utiliza para deshabilitar la sumarización en RIPV2?

- No auto-summary
- No auto summary
- No auto-rip

e. ¿Qué comando se utiliza para verificar la información que envia RIPV2?

- debug ip-rip
- debug ip rip
- no auto-debug

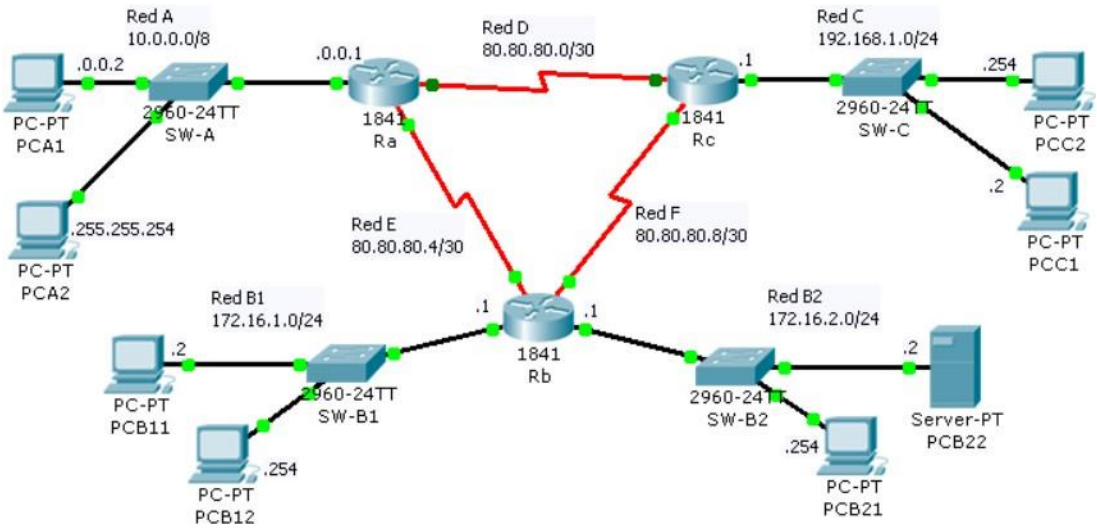
4.4.7. Actividad Propuesta

Configuración, activación y análisis del protocolo RIP

Utilizando el simulador Cisco Packet Tracer, se pide crear la topología de red que se muestra en el esquema siguiente. Configure los parámetros de red de acuerdo con las indicaciones del esquema para las siete redes presentes. Compruebe la conectividad entre los host de una misma red y verifique que las tablas de enrutamiento de los routers incluyen las entradas correspondientes a las redes conectadas.

Figura 88

Actividad propuesta 4



Nota. Topología de la red usada para esta actividad

La activación del protocolo RIP debe llevarse a cabo en cada uno de los routers bajo una administración común. El proceso es el que se describe a continuación:

1. Acceder a la programación del router en modo consola (CLI). El sistema mostrará el prompt con el nombre del equipo: Router>
2. Entrar en el modo de ejecución de usuario privilegiado Router> enable Router#

Dispositivo	Interfaz	Red	IP	Máscara	Gateway
Router Ra	Fa0/0	A	10.0.0.1	255.0.0.0	---
	S0/0/0	D	200.0.1.1	255.0.0.0	---
	S0/0/1	E	200.0.2.1	255.0.0.0	---
Router Rb	Fa0/0	B1	172.16.1.1	255.255.255.0	---
	Fa0/1	B2	172.16.2.1	255.255.255.0	---
	S0/0/0	E	200.0.2.2	255.255.255.252	---
	S0/0/1	F	200.0.3.1	255.255.255.252	---
Router Rc	Fa0/0	C	192.168.1.1	255.255.255.0	---
	S0/0/0	D	200.0.1.2	255.255.255.252	---
	S0/0/0	F	200.0.3.2	255.255.255.252	---

PCA1	NIC	A	10.0.0.2	255.0.0.0	10.0.0.1
PCA2	NIC	A	10.255.255.254	255.0.0.0	10.0.0.1
PCB11	NIC	B1	172.16.1.2	255.255.255.0	172.16.1.1
PCB12	NIC	B1	172.16.1.254	255.255.255.0	172.16.1.1
PCB21	NIC	B2	172.16.2.2	255.255.255.0	172.16.2.1
PCB22	NIC	B2	172.16.2.254	255.255.255.0	172.16.2.1
PCC1	NIC	C	192.168.1.2	255.255.255.0	172.168.1.1
PCC2	NIC	C	192.168.1.254	255.255.255.0	172.168.1.1

3. Entrar en el modo de configuración global Router# configure terminal Router(config)#

4. Activar el protocolo de enrutamiento RIP en su versión 2 (RIPv2) y sin realizar la sumarización de subredes

Router(config)> router rip

Router(config-router)# version 2

Router(config-router)#no auto-summary

Router(config-router)#

5. Señalar las interfaces que conectan a redes finales, en las que no hay ningún router, con objeto de que por ellas no se publiquen los broadcasts del protocolo

Router(config-router)# passive-interface FastEthernet0/X

Router(config-router)# passive-interface FastEthernet0/Y

Router(config-router)# ...

6. Señalar las redes que conectan al router con sus vecinos para que sean destino de sus broadcast de publicación de la tabla de enrutamiento.

   Router(config-router)# network XXX.XXX.XXX.XXX

   Router(config-router)# network XXX.XXX.XXX.XXX

   Router(config-router)#...

7. Una vez finalizado el proceso de configuración del protocolo de enrutamiento, entre en el modo simulación y filtre los paquetes por protocolo RIP. Analice el tráfico RIP que se produce en la red.
8. Espere un tiempo prudencial antes de verificar que las tablas de enrutamiento de los routers han incorporado las rutas hasta las redes remotas. Observe el contenido de dichas tablas (analice los distintos campos y extraiga las conclusiones oportunas acerca de cada una de las entradas en esastablas) utilizando la herramienta lupa del simulador Packet Tracer y desde la CLI de cada router mediante el siguiente comando: Router# show ip router
9. Como RIP es originalmente un protocolo de enrutamiento con clase, realiza por defecto procesos de sumarización de manera automática. Analice nuevamente las tablas de enrutamiento (con el comando del apartado anterior) centrándose en el análisis de las entradas cuyo destino son las subredes B1 y B2, después de haber reactivado la sumarización de rutas:

   Router(config-router)# auto-summary

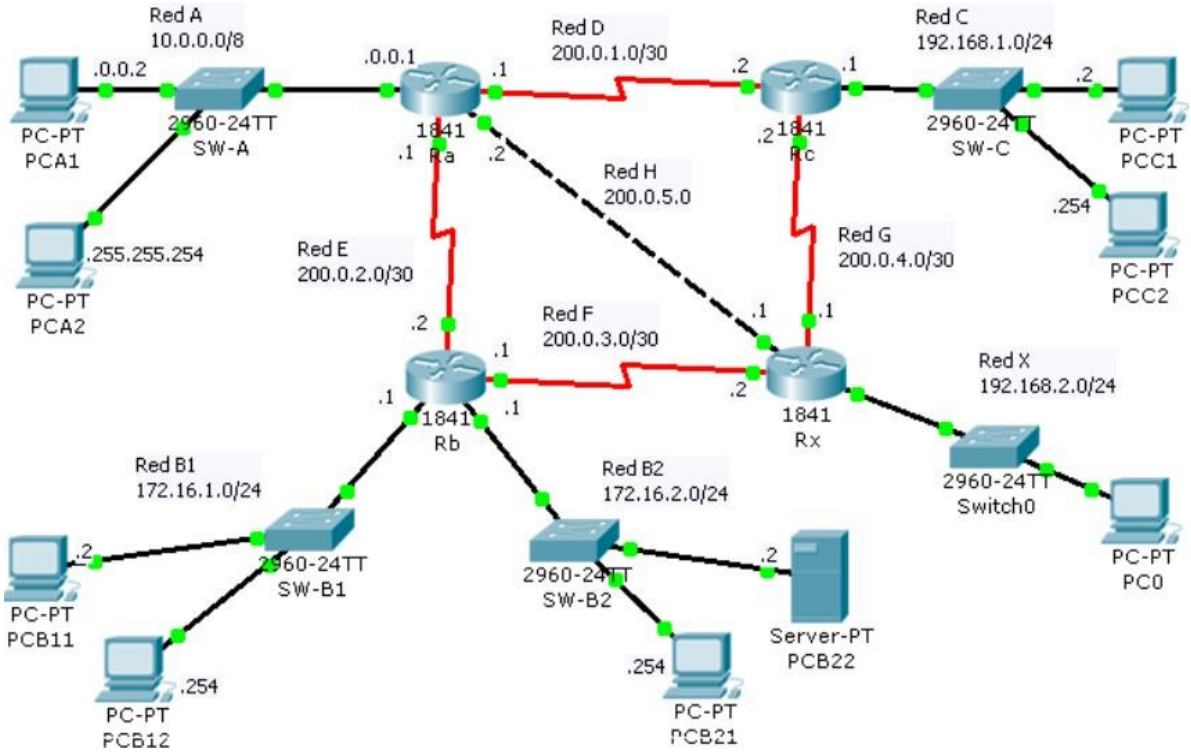
10. Desconecte una de las interfaces serie de uno de los routers de manera que el enlace correspondiente aparezca caído. Tras el correspondiente proceso de

convergencia, analice cómo han actualizado los tres routers su tabla de enrutamiento según las nuevas circunstancias de la red. Observe que se mantiene la conectividad entre todos los equipos, pero el coste de alcanzar las redes no adyacentes ha aumentado.

11. Amplíe la red de acuerdo con el esquema que se muestra en la anterior y, tras programar adecuadamente el protocolo RIP en todos los routers y esperar a la convergencia de los mismos, verifique la conectividad entre todos los hosts y analice las nuevas entradas en las tablas de enrutamiento.

Figura 89

Red ampliada



Nota. Topología de la Figura 88 ampliada con una conexión de otra red.

4.5. Fiber to the home (FTTH) y X Passive Optical Network XPON

Esta unidad ayudará a los estudiantes a identificar los diferentes protocolos y comunicaciones de redes mediante el estudio de sus características y procedimientos que permitan el desarrollo de análisis comparativos entre aquellos.

4.5.1. Historia y Futuro de la fibra a FTTX

- ***Proyección para Servicios de Datos***

El intercambio de información por medio de redes del tipo P2P, el crecimiento de los juegos on-line, aplicaciones en telemedicina y unidades del tipo SOHO pronostican la necesidad de un ancho de banda elevado. Ancho de banda previsto: 15 Mbps

- ***Proyección para Servicios de Video***

A futuro se planifica brindar el servicio HDTV con un estándar de tasa de compresión de datos de 20 Mbps por canal de alta definición y un promedio de 3 TV por hogar. Ancho de banda previsto: 60 Mbps

- ***Proyección para Servicio Telefónico***

Es servicio no representará un problema en cuando al ancho de banda a utilizar, existen CODECs cuyo ancho de banda es menor a los 64 Kbps.

- Ancho de banda previsto (servicio básico): 128 Kbps
- Ancho de banda previsto (servicio video llamado): 384 Kbps

- ***Evolución Tecnológica y Ancho de banda***

Tecnología PON: Tiene un ancho de banda de 100 M a 1G y es multicanal HDTV/VoD.

Tecnología VDSL2: Tiene un ancho de banda de 15 a 50 M y es Multimedia Home SDTV / VoD.

Tecnología ADSL 2+: Tiene un ancho de banda de 1 a 12 M y permite Internet Rápido, Medio de streaming, teletrabajo.

Dial Modem ISDN: Tiene un ancho de banda de 56 a 128 K y Text based internet.

4.5.2. Introducción a FFTH

- ***¿Qué es FTTx?***

Describe un conjunto de topologías utilizadas en las redes de acceso por fibra óptica.

- ***Elementos que determinan esta clasificación***

Alcance. – Longitud de fibra óptica

Medios de transmisión. – Fibra óptica y combinación de fibra óptica y par de cobre trenzado.

Componentes de Red. – Terminales de usuarios (ópticos) y equipos concentradores (DSL).

4.5.3. Características de FTTH

- ***Velocidades de conexión ultra rápidas:*** FTTH ofrece velocidades de conexión simétricas (misma velocidad de subida y bajada), que pueden alcanzar cientos de Mbps e incluso Gigabits por segundo (Gbps). Esto permite una navegación web rápida, descargas rápidas de archivos y transmisión de contenido multimedia sin interrupciones.
- ***Fiabilidad y estabilidad:*** Las conexiones FTTH son más estables y menos susceptibles a interferencias electromagnéticas que las conexiones basadas en cobre (como DSL). Esto se debe a la transmisión de datos a través de cables de fibra óptica, que son inmunes a las interferencias eléctricas y pueden soportar distancias más largas sin degradación de la señal.
- ***Menor latencia***: La fibra óptica tiene una menor latencia en comparación con las tecnologías de acceso basadas en cobre. Esto es crucial para aplicaciones que requieren respuestas rápidas y tiempo de latencia reducido, como juegos en línea, videoconferencias y aplicaciones en tiempo real.

4.5.4. Arquitecturas de FTTH

FTTH (Fiber to the Home) es una tecnología que permite llevar conexiones de fibra óptica directamente hasta la vivienda del usuario final. Existen diferentes arquitecturas para implementar FTTH, cada una con sus características particulares. Aquí te menciono las arquitecturas más comunes:

4.5.4.1. Punto a Punto (Point-to-Point):

- En esta arquitectura, cada hogar conectado tiene una conexión física dedicada directamente a un nodo central de la red.
- Cada cliente tiene su propio cable de fibra óptica desde el nodo central hasta su casa.
- Permite ofrecer velocidades de conexión simétricas y altamente confiables.
- Es escalable, ya que cada cliente tiene su propia fibra óptica, lo que facilita la gestión del ancho de banda.

4.5.4.2. Redes PON (Passive Optical Network):

- Las redes PON son más comunes debido a su eficiencia y costos más bajos en comparación con el punto a punto.
- En una PON, la fibra óptica se comparte entre múltiples usuarios utilizando divisores pasivos (splitters).

Hay dos tipos principales de PON:

- **GPON (Gigabit Passive Optical Network):** Utiliza divisiones pasivas para compartir el ancho de banda entre múltiples usuarios, con velocidades simétricas de hasta 2.5 Gbps de bajada y 1.25 Gbps de subida por usuario.
- **EPON (Ethernet Passive Optical Network):** Utiliza Ethernet como protocolo de acceso, con velocidades de hasta 1 Gbps simétricas.

Las redes PON permiten alcanzar un gran número de usuarios con una infraestructura de fibra óptica compartida, lo que reduce los costos de implementación y mantenimiento.

4.5.4.3. Punto a Multipunto (Point-to-Multipoint):

- Similar a PON, pero en este caso, la fibra óptica desde el nodo central se divide en varias ramificaciones que llegan a diferentes puntos (múltiples hogares).
- Cada rama puede tener un número limitado de conexiones, generalmente gestionadas por divisores pasivos o activos.
- Es una opción utilizada en áreas menos densamente pobladas donde no se justifica una red PON completa.

Cada una de estas arquitecturas tiene ventajas y desventajas dependiendo de las necesidades específicas del proveedor de servicios de Internet y las condiciones de despliegue (densidad poblacional, costos, distancia, etc.). La elección entre estas arquitecturas también puede verse influenciada por consideraciones regulatorias y de infraestructura existente en cada área de despliegue de FTTH.

4.5.5. Arquitecturas de red, opciones, beneficios y consideraciones

Las arquitecturas de red se refieren a las estructuras y configuraciones que los proveedores de servicios de Internet (ISP) utilizan para implementar redes de acceso de alta velocidad, como FTTH (Fiber to the Home). Aquí te presento varias opciones comunes, junto con sus beneficios y consideraciones:

4.5.5.1. Punto a Punto (Point-to-Point)

Descripción: En esta arquitectura, cada hogar tiene una conexión directa y dedicada a un nodo central de la red mediante un cable de fibra óptica.

Beneficios:

- **Velocidades Simétricas:** Permite ofrecer velocidades simétricas de alta velocidad (misma velocidad de subida y bajada).
- **Fiabilidad:** Menor probabilidad de congestión de red debido a la dedicación de recursos.
- **Seguridad:** Mayor seguridad de la red debido a la conexión dedicada.

Consideraciones:

- **Costos:** Puede ser más costoso implementar y mantener debido a la necesidad de fibra óptica dedicada para cada hogar.
- **Escalabilidad:** Puede ser más difícil de escalar en áreas con un crecimiento rápido de usuarios.

4.5.5.2. Redes PON (Passive Optical Network)

Descripción: Las redes PON utilizan divisores ópticos pasivos para compartir la fibra óptica entre múltiples usuarios.

Beneficios:

- **Eficiencia de Costos:** Reduce los costos de implementación y mantenimiento al compartir infraestructura de fibra óptica.
- **Escalabilidad:** Puede escalar fácilmente para soportar más usuarios agregando divisores ópticos adicionales.
- **Flexibilidad:** Puede soportar diferentes velocidades de servicio para diferentes tipos de usuarios.

Consideraciones:

- **Ancho de Banda Compartido:** El ancho de banda total se comparte entre múltiples usuarios, lo que puede causar congestión en momentos de alta demanda.
- **Latencia:** Puede haber una ligera latencia adicional debido al uso de divisores ópticos.

4.5.5.3. Punto a Multipunto (Point-to-Multipoint)

Descripción: Similar a las redes PON, pero en lugar de usar divisores ópticos, las conexiones se ramifican desde un nodo central a múltiples puntos (hogares).

Beneficios:

- **Simplicidad:** Es más fácil de implementar en áreas menos densamente pobladas donde se justifica una menor inversión en infraestructura.
- **Control de Capacidad:** Puede proporcionar un control más directo sobre la capacidad de la red para cada rama.

Consideraciones:

- **Limitaciones de Escalabilidad:** Puede ser menos escalable que las redes PON para grandes despliegues.
- **Eficiencia Espectral:** Puede requerir una planificación cuidadosa del espectro para evitar interferencias entre ramificaciones.

4.5.6. Una mirada más de cerca a la Red Pasiva Óptica (PON)

La Red Pasiva Óptica (PON, por sus siglas en inglés: Passive Optical Network) es una arquitectura de red ampliamente utilizada para implementar FTTH (Fiber to the

Home) y proporcionar conexiones de alta velocidad a los usuarios finales. Aquí tienes una mirada más detallada a cómo funciona y cuáles son sus componentes principales:

4.5.6.1. Componentes Principales de una Red PON

OLT (Optical Line Terminal):

- El OLT es el punto de inicio de la red PON y se encuentra en el lado del proveedor de servicios.
- Es responsable de gestionar y controlar múltiples conexiones de red con los ONUs (Optical Network Units) en los hogares de los usuarios.
- Convierte los datos de Ethernet u otros protocolos de red en señales ópticas que se transmiten a través de la fibra óptica.

ONU (Optical Network Unit):

- Cada hogar o usuario final está equipado con una ONU, que es el equivalente del módem o terminal de red en una red PON.
- La ONU recibe las señales ópticas del OLT y las convierte de nuevo a señales eléctricas que pueden ser utilizadas por dispositivos de red y computadoras en el hogar.
- Gestiona la interfaz entre la red óptica y la red local del usuario final, distribuyendo el servicio de Internet y otros servicios de telecomunicaciones.

Divisor Óptico (Splitter):

- Es un componente pasivo clave en una red PON que permite compartir la señal óptica entre múltiples ONUs.

- Los splitters dividen la señal óptica entrante en múltiples señales más débiles que se distribuyen a diferentes ONUs.
- Los splitters pueden ser de diferentes configuraciones (por ejemplo, 1:2, 1:4, 1:8, etc.), lo que determina la cantidad de ONUs que pueden ser soportadas por cada OLT.

4.5.6.2. Funcionamiento de una Red PON

Transmisión de Datos:

- El OLT transmite datos a través de una única fibra óptica hacia un splitter, que divide la señal para enviarla a múltiples ONUs.
- Cada ONU recibe la señal óptica correspondiente y convierte los datos ópticos en datos eléctricos que pueden ser utilizados por los dispositivos del usuario final.

Arquitectura de Fibra Óptica Compartida:

- Una característica clave de la PON es su arquitectura de fibra óptica compartida, lo que significa que la fibra óptica desde el OLT hasta el splitter es compartida entre múltiples usuarios.
- Esto reduce significativamente los costos de implementación y mantenimiento de la infraestructura de fibra óptica en comparación con las redes punto a punto.

Downstream y Upstream:

- **Downstream**: Refiere al flujo de datos desde el OLT hacia las ONUs.
- **Upstream**: Refiere al flujo de datos desde las ONUs hacia el OLT.

- En una red PON típica, el downstream suele tener un ancho de banda mayor que el upstream, ya que la mayoría de las aplicaciones de los usuarios requieren más ancho de banda para la descarga de datos que para la carga.

4.5.6.3. Beneficios de una Red PON

- **Costo Eficiente**: La utilización de divisores ópticos pasivos reduce significativamente los costos de despliegue y mantenimiento en comparación con las redes punto a punto.

- **Escalabilidad**: Puede soportar un gran número de usuarios al agregar más ONUs y splitters según sea necesario.

- **Flexibilidad**: Permite diferentes velocidades de conexión y servicios para diferentes usuarios a través de la misma infraestructura de fibra óptica.

4.5.6.4. Consideraciones

- **Ancho de Banda Compartido**: Aunque la fibra óptica ofrece un ancho de banda considerable, la capacidad total se comparte entre todos los usuarios conectados a través de un splitter.

- **Latencia**: Puede haber una leve latencia adicional debido al proceso de conversión óptica-electrica en las ONUs.

- **Planificación de la Red**: Requiere una planificación cuidadosa de la topología de la red y la ubicación de los splitters para optimizar el rendimiento y minimizar la pérdida de señal.

4.5.8. Autoevaluación

a) ¿Cuál no es una arquitectura de red?

- Punto a punto
- Punto a multipunto
- Multipunto a malla

b) ¿Cuál es un beneficio de la red PON?

- Costo Eficiente
- Menor Escalabilidad
- Inflexibilidad

c) ¿Cuál es el concepto de la arquitectura de punto a multipunto?

- La fibra óptica desde el nodo central se divide en varias ramificaciones que llegan a un punto (un hogar).
- Cada rama puede tener un número limitado de conexiones, generalmente gestionadas por divisores pasivos o activos.
- Es una opción no utilizada en áreas menos densamente pobladas donde no se justifica una red PON completa.

d) ¿Cuál no es una característica de la arquitectura FTTH?

- Velocidades de conexión ultra rápidas
- Fiabilidad y estabilidad
- Mayor Latencia

e) Selecciona si es verdadero o falso el siguiente enunciado

El OLT es el punto de inicio de la red PON y se encuentra en el lado del proveedor de servicios.

- Verdadero

- Falso

4.5.9. Actividad Propuesta

4.6. Norma técnica de diseño y construcción en edificios y urbanizaciones de acuerdo a CNT.

Esta unidad permitirá a los estudiantes, conocer e identificar las normativas de CNT para el diseño y construcción de proyectos telefónicos.

4.6.1. Que normativas existen en CNT

CNT (Corporación Nacional de Telecomunicaciones) es una empresa estatal de telecomunicaciones en Ecuador. Las normativas que rigen su funcionamiento y las regulaciones que debe cumplir están determinadas por varias leyes y entidades reguladoras en el país. Aquí te menciono algunas de las normativas relevantes:

- **Ley Orgánica de Telecomunicaciones:** Esta ley establece el marco regulatorio general para el sector de las telecomunicaciones en Ecuador, incluyendo disposiciones sobre licencias, derechos y obligaciones de los operadores, y los derechos de los usuarios de servicios de telecomunicaciones.
- **Reglamento General de la Ley Orgánica de Telecomunicaciones**: Define los detalles específicos y procedimientos para la implementación de la Ley Orgánica, incluyendo aspectos técnicos, administrativos y financieros.

- **Regulación de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL):** ARCOTEL es la entidad reguladora que supervisa y regula el sector de las telecomunicaciones en Ecuador. Sus regulaciones incluyen aspectos como:

- Condiciones para la prestación de servicios de telecomunicaciones.
- Asignación y uso de espectro radioeléctrico.
- Protección de los derechos de los usuarios de servicios de telecomunicaciones.
- Monitoreo y cumplimiento de las normas técnicas y de calidad de servicio.

- **Normativas específicas para servicios y tecnologías:** Dependiendo de los servicios específicos que ofrece CNT (como telefonía fija, móvil, Internet, televisión por cable, etc.), existen regulaciones adicionales que pueden aplicarse. Por ejemplo, normativas sobre calidad de servicio, tarifas, cobertura, entre otras.
- **Normativas ambientales y de seguridad:** CNT también está sujeta a normativas relacionadas con la protección ambiental y la seguridad en la instalación y mantenimiento de infraestructuras de telecomunicaciones.

4.6.2. Que es un proyecto telefónico

Un proyecto telefónico es un término general que se refiere a cualquier iniciativa planificada y ejecutada para establecer, mejorar, o expandir un sistema de telecomunicaciones que incluya servicios de voz, especialmente en entornos empresariales o de infraestructuras públicas. Aquí te explico algunos aspectos clave que suelen involucrar los proyectos telefónicos:

Elementos de un Proyecto Telefónico

- **Diseño y Planificación:**

- ***Requerimientos y Análisis:*** Identificación de las necesidades específicas de comunicación de la organización o comunidad que requiere el servicio telefónico.
- ***Diseño de la Red:*** Elaboración de un plan detallado que incluya la infraestructura necesaria (cableado, equipos, centrales telefónicas, etc.) y la topología de la red telefónica.

- **Implementación:**
  - ***Instalación de Infraestructura:*** Puesta en marcha física de la red, incluyendo la instalación de cables, equipos de conmutación (PBX, VoIP, etc.), y dispositivos terminales (teléfonos).
  - ***Configuración y Pruebas:*** Configuración de equipos y sistemas, y realización de pruebas para asegurar que la red funcione correctamente y cumpla con los estándares de calidad requeridos.
- **Gestión del Proyecto:**
  - Control y Seguimiento: Monitoreo constante del avance del proyecto para asegurar que se cumplan los plazos y presupuestos establecidos.
  - Gestión de Recursos: Administración de recursos humanos, financieros y materiales para garantizar la efectividad y eficiencia del proyecto.

A. Integración y Mantenimiento:

- Integración con Sistemas Existentes: Asegurar la interoperabilidad y compatibilidad con otros sistemas de comunicación existentes.
- Mantenimiento y Soporte: Establecer procedimientos de mantenimiento preventivo y correctivo para garantizar la continuidad del servicio telefónico.

Tipos de Proyectos Telefónicos

- **Implementación de PBX**: Instalación de centralitas privadas (PBX) para gestionar las llamadas internas y externas en una organización.
- **Migración a VoIP:** Transición de sistemas tradicionales de telefonía a tecnologías de Voz sobre IP (VoIP) para reducir costos y mejorar la flexibilidad.
- **Expansión de Infraestructura:** Ampliación de la capacidad telefónica para cubrir nuevas áreas geográficas o aumentar la capacidad de usuarios.
- **Mejora de la Calidad de Servicio:** Proyectos orientados a mejorar la calidad de las llamadas, reducir la congestión de la red y optimizar la experiencia del usuario.

Consideraciones Importantes

- **Normativas y Regulaciones**: Cumplimiento con las normativas locales y regulaciones de telecomunicaciones que afectan la implementación y operación de servicios telefónicos.
- **Seguridad:** Implementación de medidas de seguridad para proteger la integridad de las comunicaciones y la privacidad de los usuarios.
- **Capacitación y Soporte**: Provisión de capacitación adecuada para los usuarios finales y personal de soporte técnico para asegurar el uso efectivo y mantenimiento del sistema telefónico.

4.6.4. Actividad Propuesta: Realizar un diseño telefónico de acuerdo a las normativos CNT

Supongamos que estás diseñando el sistema telefónico para una oficina con 50 empleados. Necesitas:

- 50 extensiones telefónicas.
- 5 líneas telefónicas externas.
- Fax y servicio de conferencias.
- Uso de telefonía IP con central telefónica virtual.

Pasos a seguir:

- Utiliza cableado Cat 6 para conectar todos los teléfonos a un switch PoE.
- Configura una central telefónica IP que soporte hasta 100 extensiones.
- Asigna direcciones IP estáticas para cada teléfono y configura un servidor DHCP para otros dispositivos de red.
- Implementa medidas de seguridad como contraseñas fuertes y cifrado de comunicaciones.
- Realiza pruebas de conectividad y calidad de voz antes de poner en operación el sistema.
- Documenta todo el diseño y configuración para futuras referencias y mantenimiento.

4.8. Actividad Propuesta

Descripción del ejercicio: Configuración de una red LAN

Objetivo: Configurar una red de área local (LAN) simple utilizando dispositivos básicos de red y asignación de direcciones IP.

Pasos a seguir:

A. Diseño de la topología:

- Decide la topología de red que deseas implementar: puede ser en estrella, en bus, en anillo, etc.
- Determina cuántos dispositivos (computadoras, impresoras, etc.) estarán en la red y cómo se conectarán entre sí.

B. Selección de equipos:

Elige los dispositivos necesarios, como routers, switches, cables de red, y dispositivos finales (computadoras, impresoras, etc.).

Asegúrate de tener suficientes cables Ethernet y adaptadores de red si es necesario.

Configuración de direcciones IP:

- Decide un rango de direcciones IP para tu red. Por ejemplo, podrías usar el rango 192.168.1.1 - 192.168.1.254 con máscara de subred 255.255.255.0.
- Asigna manualmente direcciones IP estáticas a cada dispositivo o configura un servidor DHCP para la asignación automática de direcciones IP dinámicas.

Conexión y configuración de dispositivos:

- Conecta físicamente todos los dispositivos de acuerdo con la topología elegida.
- Configura los dispositivos de red (switches, routers) con direcciones IP estáticas si es necesario, o configura los parámetros de red como la puerta de enlace predeterminada y la máscara de subred.

Pruebas de conectividad:

Verifica la conectividad entre todos los dispositivos en la red. Intenta hacer ping desde una computadora a otra para asegurarte de que estén correctamente conectadas y configuradas.

Implementación de seguridad:

- Configura las políticas de seguridad básicas, como contraseñas para dispositivos de red y cortafuegos si es necesario.
- Asegúrate de que los dispositivos sólo tengan acceso a los recursos de red necesarios.

Documentación:

Documenta la configuración de la red, incluyendo la topología, las direcciones IP asignadas y cualquier otra configuración importante.

Esto será útil para referencia futura y para la resolución de problemas.

Notas adicionales:

Si te encuentras con problemas durante la configuración, como problemas de conectividad o configuración incorrecta de direcciones IP, utiliza herramientas de diagnóstico como el comando ping, ipconfig o ifconfig según el sistema operativo que estés utilizando.

No olvides tomar en cuenta aspectos como el rendimiento de la red y la escalabilidad según las necesidades futuras de expansión de la red.

5. Créditos y Responsables

En este apartado se debe colocar el perfil del docente responsable de la elaboración, emisión, control, vigilancia de la creación del manual; así como también, quien es el responsable de la revisión y aprobación del mismo.

¿Como se realiza el perfil de un docente?

Se debe colocar una breve descripción del perfil profesional, formación Profesional (títulos, cursos, seminarios de relevancia), experiencia laboral e investigaciones realizadas.

Autor: _____

Año: _____

Editorial: _____

Institución: _____-

Cuidad: _____

ISBN: _____

Responsable:

_____
Jorge David Herrera Sarango

Revisado y aprobado por:

_____
Xxxxxxxxxxxxxxxx

6. Glosario

- **Topología:** Configuración física o lógica de una red de computadoras.
- **LAN:** Red de área local, que conecta dispositivos en un área limitada.
- **WAN**: Red de área amplia, que conecta redes LAN a través de distancias extensas.
- **Router:** Dispositivo que interconecta redes y dirige el tráfico de datos entre ellas.
- **Switch:** Dispositivo de red que conecta varios dispositivos en una red LAN y gestiona el tráfico de datos.
- **Gateway:** Punto de entrada o salida entre dos redes que utiliza diferentes protocolos de comunicación.
- **Firewall:** Dispositivo o software que protege una red al controlar el tráfico entrante y saliente.
- **Protocolo:** Conjunto de reglas y estándares que define cómo los dispositivos se comunican en una red.
- **IP Address:** Dirección numérica única asignada a cada dispositivo en una red para identificación y enrutamiento.
- **Subnet:** Subdivisión de una red IP más grande en segmentos más pequeños para mejorar la gestión y la seguridad.

8. Referencias

CISCO. (2022). *switching VLANS y enrutamiento entre redes VLAN*. Obtenido de https://www.netacad.com/portal/learning