**CAPÍTULO 0**

**La capa física**

La capa física se preocupa por la transmisión de los ceros y unos. El número de voltios a utilizar para O y 1, el número de bits por segundo que se pueden enviar, el hecho de que la transmisión se lleve a cabo en ambas direcciones en forma simultánea, son todos aspectos clave en la capa física. Además, el tamaño y forma del conector en la red (enchufe), así como el número de pins y el significado de cada uno son los temas de interés aquí.

El protocolo de la capa física se encarga de la estandarización de las interfaces eléctricas, mecánicas v de señalización, de forma que, cuando una máquina envíe un bit 0, sea en realidad recibido como un bit0 y no como un bit l. Se han desarrollado muchos estándares de la capa física (para medios distintos); por ejemplo, el estándar RS-232-C para las líneas de comunicación serial.

**La capa de enlace datos**

La capa física sólo envía bits. Mientras no ocurran errores, todo está bien. Sin embargo, las redes reales de comunicación están sujetas a errores, por lo que es necesario cierto mecanismo para detectarlos y corregirlos. Este mecanismo es la tarea principal de la capa de enlace de datos. Lo que hace es agrupar los bits en unidades, que a veces se llaman **marcos,** y revisar que cada marco se reciba en forma correcta.

La capa de enlace de datos realiza su trabajo por medio de la colocación de un patrón especial de bits al inicio y al final de cada marco, para señalarlos, a la vez que calcula una **suma de verificación,** mediante la suma de todos los bytes del marco de cierta forma. La capa de enlace de datos añade la suma de verificación al marco. Al llegar el marco, el receptor vuelve a calcular la suma de verificación a partir de los datos y compara el resultado con la suma de verificación que sigue después del marco. Si coinciden, se considera que el marco es correcto y se le acepta. En caso contrario, el receptor pide al emisor que los vuelva a transmitir. Los marcos tienen asignados números secuenciales (en el encabezado), de forma que se pueda saber con exactitud cuál es cuál.

**La capa de red**

En una LAN, por lo general, no existe la necesidad de que el emisor localice al receptor.

Sólo tiene que colocar el mensaje en la red y el receptor lo recibe. Sin embargo, tina red de área amplia consta de un gran número de máquinas, cada una de ellas con cierto número de líneas hacia otras máquinas, un poco como un mapa a gran escala, que muestra las ciudades y caminos principales que los conectan. Para que un mensaje llegue del emisor al receptor, tiene que hacer un cierto número de saltos y, en cada uno de ellos, elegir una línea por utilizar. La cuestión de la elección de la mejor ruta se llama **ruteo** y es la tarea principal de la capa de red.

El problema se complica con el hecho de que la ruta más corta no siempre es la mejor.

Lo que importa en realidad es la cantidad de retraso en una ruta dada, lo cual, a su vez, se relaciona con la cantidad de tráfico y el número de mensajes formados para la transmisión en las distintas líneas. Así, el retraso puede cambiar con el curso del tiempo. Algunos algoritmos de ruteo intentan adaptarse a cargas cambiantes, mientras que otros se conforman con tomar decisiones coi1 base en promedios a largo plazo.

Dos protocolos en la capa de red tienen un uso amplio, uno orientado hacia las conexiones y otro sin conexión. El orientado hacia las conexiones se llama **X.25** y es favorecido por los operadores de las redes públicas, como las compañías telefónicas y las PTT europeas.

En primer lugar, el usuario de X.25 envía una *solicitud de llamada* a un destino, el cual puede aceptar o rechazar la conexión propuesta. Si se acepta la conexión, quien hace la llamada obtiene un identificador de conexión para usarlo en las solicitudes posteriores. En muchos casos, la red escoge una ruta del emisor al receptor durante esta configuración y la utiliza para el tráfico posterior.

El protocolo sin conexión se denomina IP (Protocolo Internet) y es parte de la serie de protocolos DoD (Departamento de Defensa de los Estados Unidos). Un **paquete** IP (el término técnico para u11 mensaje en la capa de red) se puede enviar sin configuración alguna.

Cada paquete IP tiene una ruta hacia su destino independiente de los demás paquetes. No se selecciona ruta interna alguna ni se recuerda ésta, como ocurre a menudo con X.25.

**La capa de transporte**

Los paquetes se pueden perder en el camino del emisor al receptor. Aunque ciertas aplicaciones pueden controlar su propia recuperación de los errores, otras prefieren una conexión confiable. La tarea de la capa de transporte es proporcionar este servicio. La idea es que la capa de sesión pueda enviar un mensaje a la capa de transporte, con la esperanza de que sea entregado sin pérdida alguna.

Al recibir un mensaje de la capa de sesión, la capa de transporte lo divide en pequeñas partes, de forma que cada una se ajuste a un paquete, asigna a cada uno un número secuencia1 y después los envía. La discusión en el encabezado de la capa de transporte se refiere a los paquetes que han sido enviados, a los paquetes recibidos, el número de paquetes que puede aceptar el receptor y temas similares.

Las conexiones confiables de transporte (que por definición están orientadas hacia la conexión) se pueden construir por arriba de X.25 o IP. En el primer caso, todos los paquetes llegarán en el orden correcto (si ***es*** que llegan), pero en el segundo caso es posible que un paquete tome una ruta diferente y llegue primero que el paquete enviado antes de él. El software de la capa de transporte se encarga de ponerlo todo en orden, para mantener la ilusión de que una conexión de transporte es como un gran tubo: sólo hay que colocar los mensajes en él y éstos llegan sin daño alguno, en el orden en el que fueron enviados. El protocolo de transporte oficial ISO tiene cinco variantes, conocidas como **TPO** hasta**TP4.**

Las diferencias se relacionan con el control de los errores y la capacidad de enviar varias conexiones de transporte mediante una conexión X.25. La elección de cuál utilizar depende de las propiedades de la capa de red subyacente.

El protocolo de transporte DoD se llama **TCP** (Transmission Control Protocol [protocolo para el control de transmisiones)]. Es similar a TP4. La combinación TCPIIP se utiliza con amplitud en las universidades y en la mayoría de los sistemas UNIX La serie de protocolos DoD también soportan un protocolo de transporte sin conexión llamado **UDP**

(Universal Datagrama Protocol [protocolo datagrama universal)], que en esencia es igual a IP con ciertas adiciones menores. Los programas del usuario que no necesitan un protocolo orientado hacia las conexiones utilizan por lo general UDP.

**La capa de sesión**

La capa de sesión es en esencia una versión mejorada de la capa de transporte. Proporciona el control del diálogo, con el fin de mantener un registro de la parte que está hablando en cierto momento, y proporciona facilidades en la sincronización. Esto último es útil para permitir a los usuarios que inserten puntos de verificación en las transferencias de gran tamaño, de modo que si ocurre una falla, sólo sea necesario regresar al último punto de verificación, en vez de recorrer todo el camino hasta el principio. En la práctica, pocas aplicaciones están interesadas en la capa de sesión y rara vez se le soporta. Ni siquiera está presente en la serie de protocolo DoD.

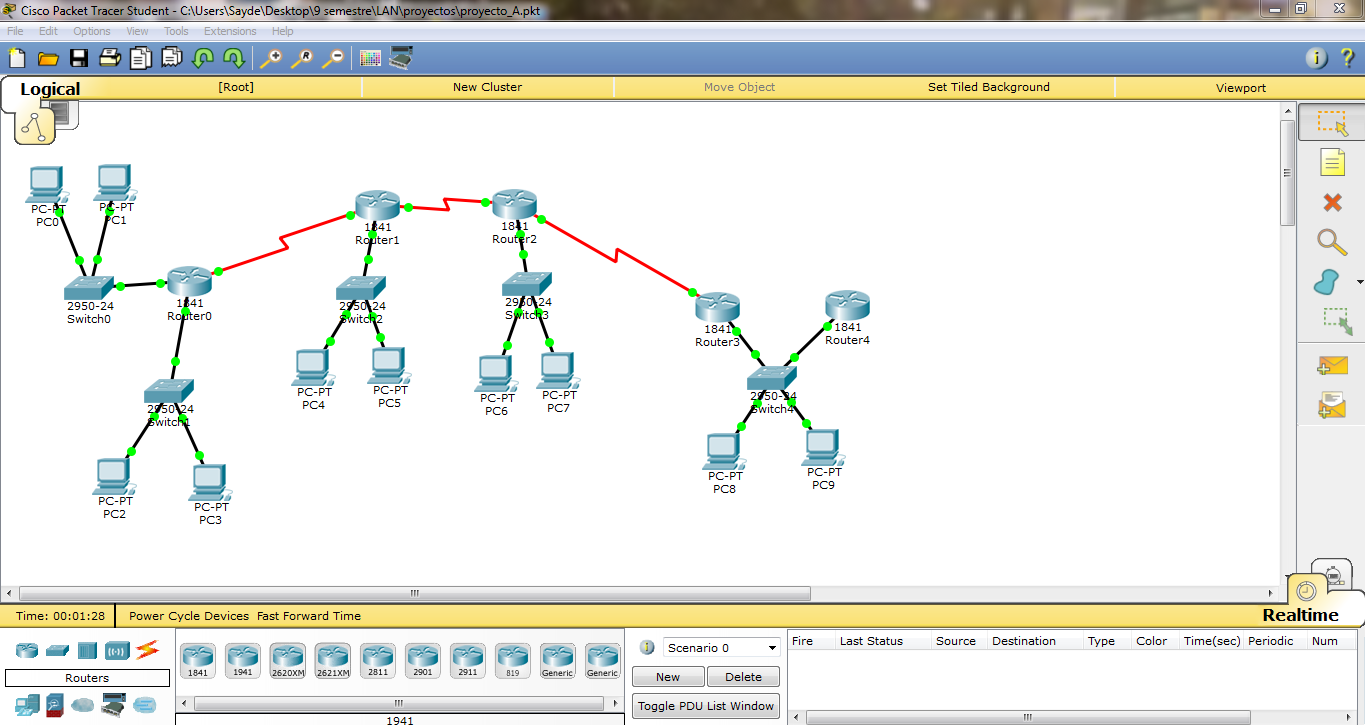
**La capa de presentación**

Adiferencia de las capas inferiores, preocupadas por la obtención de los bits del emisor al receptor en forma confiable y eficaz, la capa de presentación se preocupa por el significado de los bits. La mayoría de los mensajes no constan de una cadena aleatoria de bits, sino de información más estructurada, corno nombres de personas, sus direcciones, cantidades de dinero, etc. En la capa de presentación es posible definir registros que contengan campos como éstos y que entonces el emisor notifique al receptor que un mensaje contiene un registro particular en cierto formato. Esto facilita la comunicación entre las máquinas con distintas representaciones internas.

**La capa de aplicación**

La capa de aplicación es en realidad una colección de varios protocolos para actividades comunes, como el correo electrónico, la transferencia de archivos y la conexión entre terminales remotas a las computadoras en una red. Los más conocidos de éstos son el protocolo de correo electrónico X.400 y el servidor de directorios X.500.

**EJERCICIOS**

**clase A**

**ROUTER: 1**

Router>ena

Router#sh run

Building configuration...

Current configuration : 791 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 77.0.0.1 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

ip address 65.0.0.1 255.0.0.0

duplex auto

speed auto

interface Serial0/0/0

ip address 110.0.0.1 255.0.0.0

clock rate 56000

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router rip

network 65.0.0.0

network 77.0.0.0

network 110.0.0.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 2**

Router>ena

Router#sh run

Building configuration...

Current configuration : 786 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 85.0.0.1 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 100.0.0.1 255.0.0.0

clock rate 56000

interface Serial0/1/0

ip address 110.0.0.2 255.0.0.0

interface Vlan1

no ip address

shutdown

router rip

network 85.0.0.0

network 100.0.0.0

network 110.0.0.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER 3:**

Router>ena

Router#sh run

Building configuration...

Current configuration : 786 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 120.0.0.1 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 10.0.0.1 255.0.0.0

clock rate 56000

interface Serial0/1/0

ip address 100.0.0.2 255.0.0.0

interface Vlan1

no ip address

shutdown

router rip

network 10.0.0.0

network 100.0.0.0

network 120.0.0.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER 4:**

Router>ena

Router#sh run

Building configuration...

Current configuration : 678 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 99.0.0.1 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

ip address 10.0.0.2 255.0.0.0

interface Vlan1

no ip address

shutdown

router rip

network 10.0.0.0

network 99.0.0.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 5**

Router>ena

Router#sh run

Building configuration...

Current configuration : 643 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 99.0.0.2 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip flow-export version 9

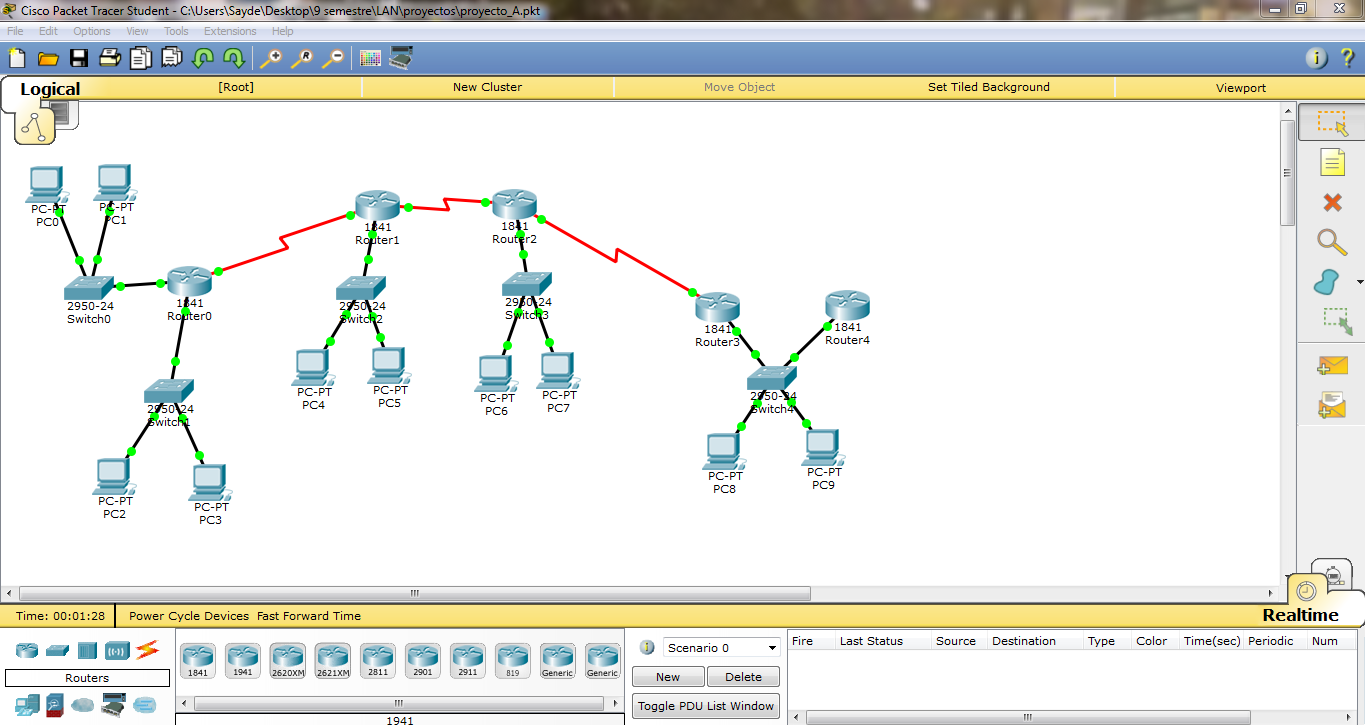
line con 0

line aux 0

line vty 0 4

login

end

**clase B**

**ROUTER: 1**

Router>ena

Router#sh run

Building configuration...

Current configuration : 803 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 168.5.0.1 255.255.0.0

duplex auto

speed auto

interface FastEthernet0/1

ip address 157.7.0.1 255.255.0.0

duplex auto

speed auto

interface Serial0/0/0

ip address 139.100.0.1 255.255.0.0

clock rate 56000

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router rip

network 139.5.0.0

network 157.7.0.0

network 168.5.0.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 2**

Router>ena

Router#sh run

Building configuration...

Current configuration : 800 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

no ip address

duplex auto

speed auto

shutdown

interface FastEthernet0/1

ip address 129.17.0.1 255.255.0.0

duplex auto

speed auto

interface Serial0/0/0

ip address 180.6.0.1 255.255.0.0

clock rate 56000

interface Serial0/1/0

ip address 139.100.0.2 255.255.0.0

interface Vlan1

no ip address

shutdow

router rip

network 129.17.0.0

network 139.100.0.0

network 180.6.0.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 3**

Router>ena

Router#sh run

Building configuration...

Current configuration : 798 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 134.8.0.1 255.255.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 147.204.0.1 255.255.0.0

clock rate 56000

interface Serial0/1/0

ip address 180.6.0.2 255.255.0.0

interface Vlan1

no ip address

shutdown

router rip

network 134.8.0.0

network 147.204.0.0

network 180.6.0.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 4**

Router>ena

Router#sh run

Building configuration...

Current configuration : 761 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 155.93.0.1 255.255.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

no ip address

clock rate 2000000

shutdown

interface Serial0/1/0

ip address 147.204.0.2 255.255.0.0

interface Vlan1

no ip address

shutdown

router rip

network 147.204.0.0

network 155.93.0.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 5**

Router>ena

Router#sh run

Building configuration...

Current configuration : 647 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 155.93.0.2 255.255.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip flow-export version 9

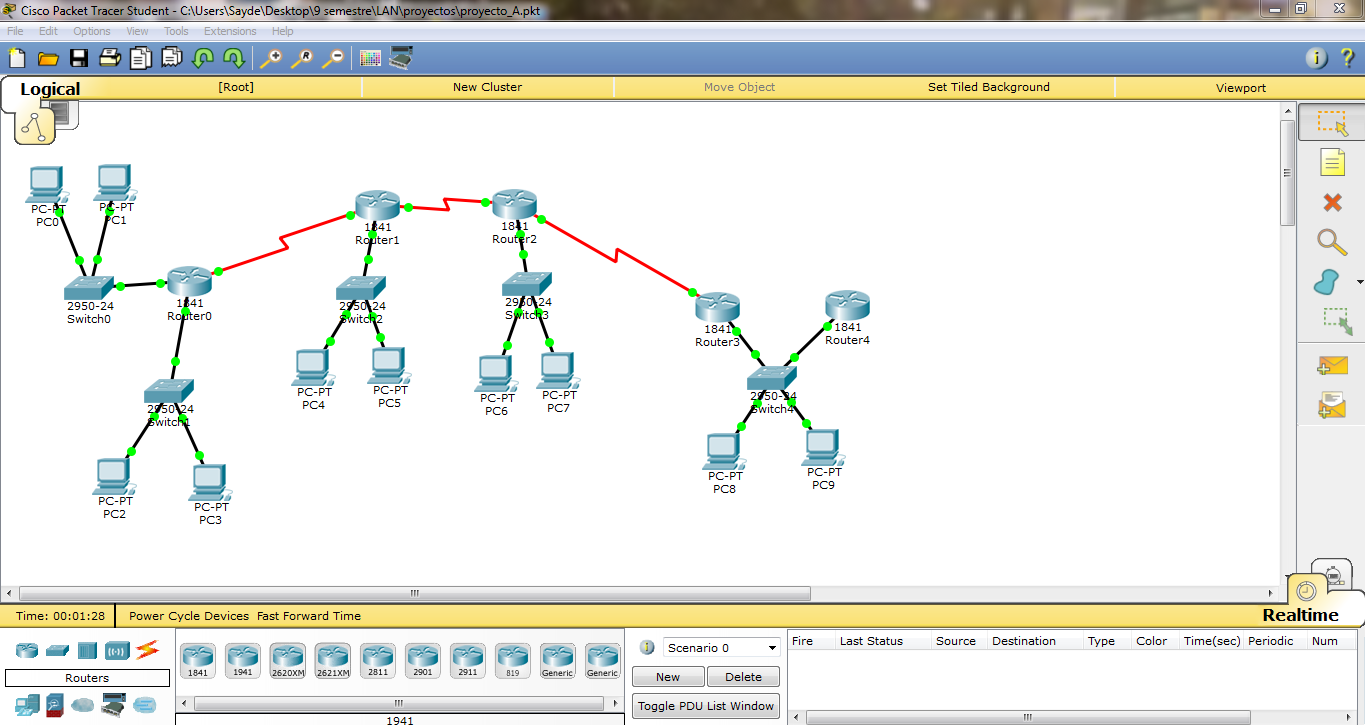
line con 0

line aux 0

line vty 0 4

login

end

**clase C**

**ROUTER: 1**

Router>ena

Router#sh run

Building configuration...

Current configuration : 813 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 205.7.5.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

ip address 192.5.5.1 255.255.255.0

duplex auto

speed auto

interface Serial0/0/0

ip address 201.100.11.1 255.255.255.0

clock rate 56000

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router rip

network 192.5.5.0

network 201.100.11.0

network 205.7.5.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 2**

Router>ena

Router#sh run

Building configuration...

Current configuration : 801 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 219.17.100.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 199.6.13.1 255.255.255.0

clock rate 56000

interface Serial0/1/0

ip address 201.100.11.2 255.255.255.0

interface Vlan1

no ip address

shutdown

router rip

network 199.6.13.0

network 201.100.11.0

network 219.17.100.0

ip classless

ip flow-export version 9

!line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 3**

Router>ena

Router#sh run

Building configuration...

Current configuration : 810 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 223.8.151.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 204.204.7.1 255.255.255.0

clock rate 56000

interface Serial0/1/0

ip address 199.6.13.2 255.255.255.0

interface Vlan1

no ip address

shutdown

router rip

network 199.6.13.0

network 204.204.7.0

network 223.8.151.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 4**

Router>ena

Router#sh run

Building configuration...

Current configuration : 713 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1spanning-tree mode pvst

interface FastEthernet0/0

ip address 210.93.105.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

ip address 204.204.7.2 255.255.255.0

interface Vlan1

no ip address

shutdown

router rip

network 204.204.7.0

network 210.93.105.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 5**

Router>ena

Router#sh run

Building configuration...

Current configuration : 699 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 210.93.105.2 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router rip

network 210.93.105.0

ip classless

ip flow-export version 9

no cdp run

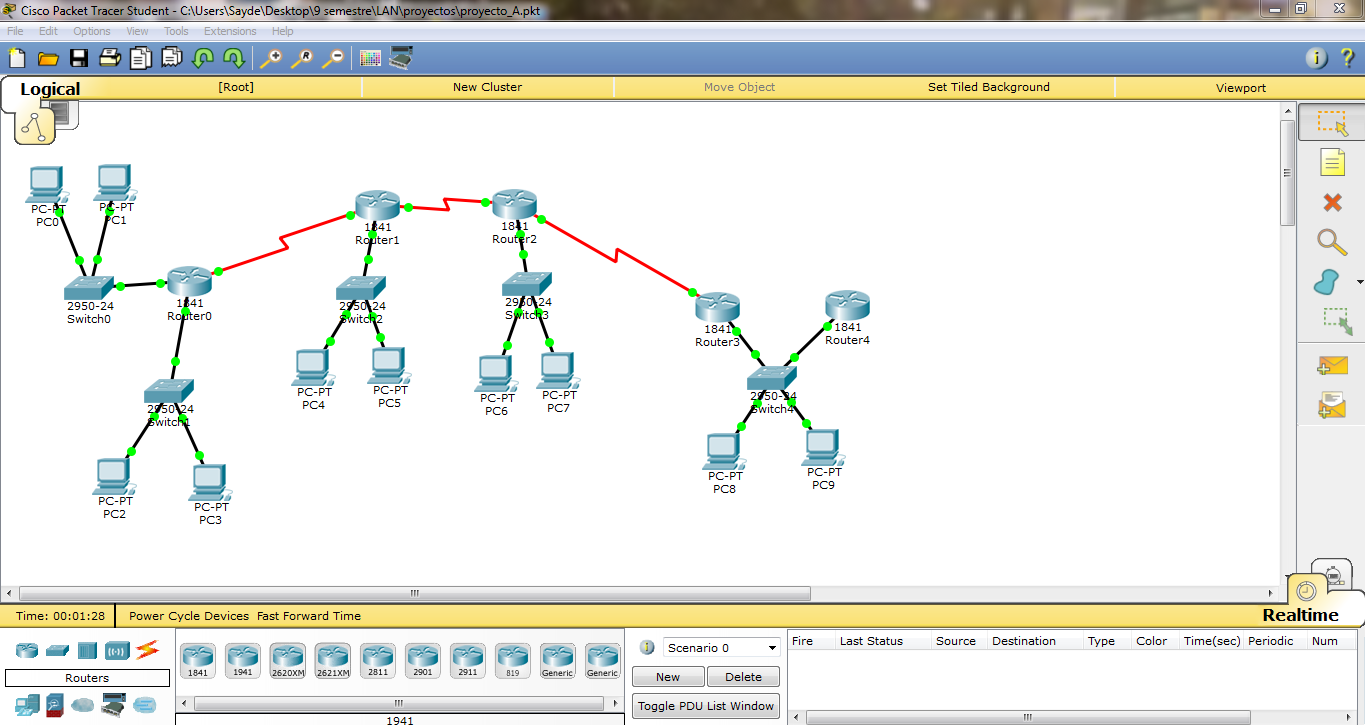
line con 0

line aux 0

line vty 0 4

login

end

**clase MIXTA**

**ROUTER: 1**

Router>ena

Router#sh run

Building configuration...

Current configuration : 795 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 118.0.0.1 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

ip address 177.5.0.1 255.255.0.0

duplex auto

speed auto

!

interface Serial0/0/0

ip address 33.0.0.1 255.0.0.0

clock rate 56000

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router rip

network 33.0.0.0

network 118.0.0.0

network 177.5.0.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 2**

Router>ena

Router#sh run

Building configuration...

Current configuration : 798 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 200.17.100.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 187.6.0.1 255.255.0.0

clock rate 56000

interface Serial0/1/0

ip address 33.0.0.2 255.0.0.0

interface Vlan1

no ip address

shutdown

router rip

network 33.0.0.0

network 187.6.0.0

network 200.17.100.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 3**

Router>ena

Router# sh run

Building configuration...

Current configuration : 796 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 10.0.0.1 255.0.0.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 221.204.7.1 255.255.255.0

clock rate 56000

interface Serial0/1/0

ip address 187.6.0.2 255.255.0.0

interface Vlan1

no ip address

shutdown

router rip

network 10.0.0.0

network 187.6.0.0

network 221.204.7.0

ip classless

ip flow-export version 9

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 4**

Router>ena

Router#sh run

Building configuration...

Current configuration : 769 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 215.93.105.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

no ip address

clock rate 2000000

shutdown

interface Serial0/1/0

ip address 221.204.7.2 255.255.255.0

interface Vlan1

no ip address

shutdown

router rip

network 215.93.105.0

network 221.204.7.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**ROUTER: 5**

Router>ena

Router#sh run

Building configuration...

Current configuration : 686 bytes

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Router

ip cef

no ipv6 cef

ip ssh version 1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 215.93.105.2 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router rip

network 215.93.105.0

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

**PRACTICAS**

Práctica #1: **Interconexión de la PC al switch**

**Integrantes del equipo:**

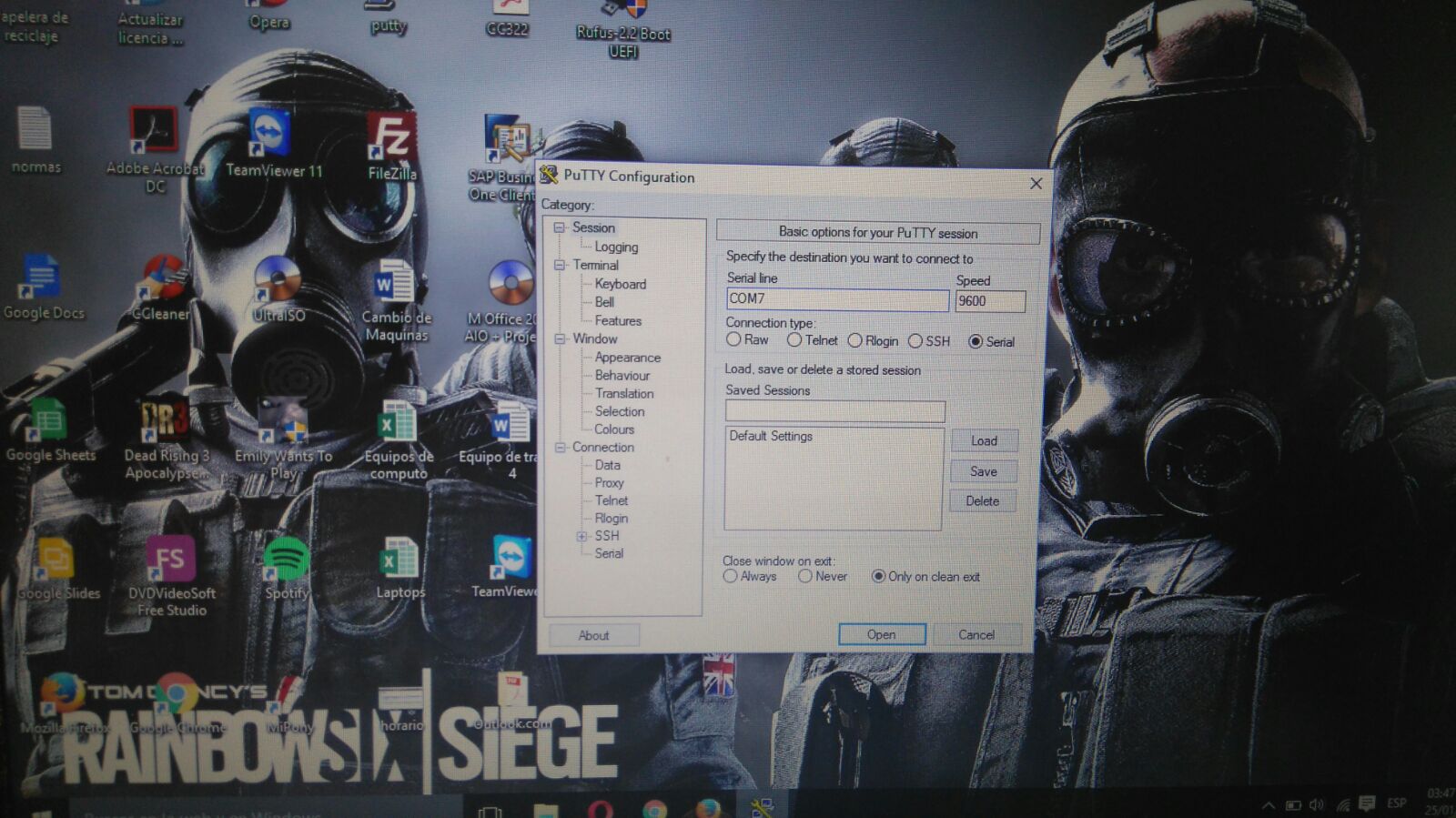
* Gómez García Jonathan Daniel
* Gutiérrez González Virginia Sayde
* Moguel Ortiz Álvaro Luis
* Padilla Villaseñor José Alejandro
* Píz Guzmán Christian
* Valdez Lomelí Manuel Alejandro

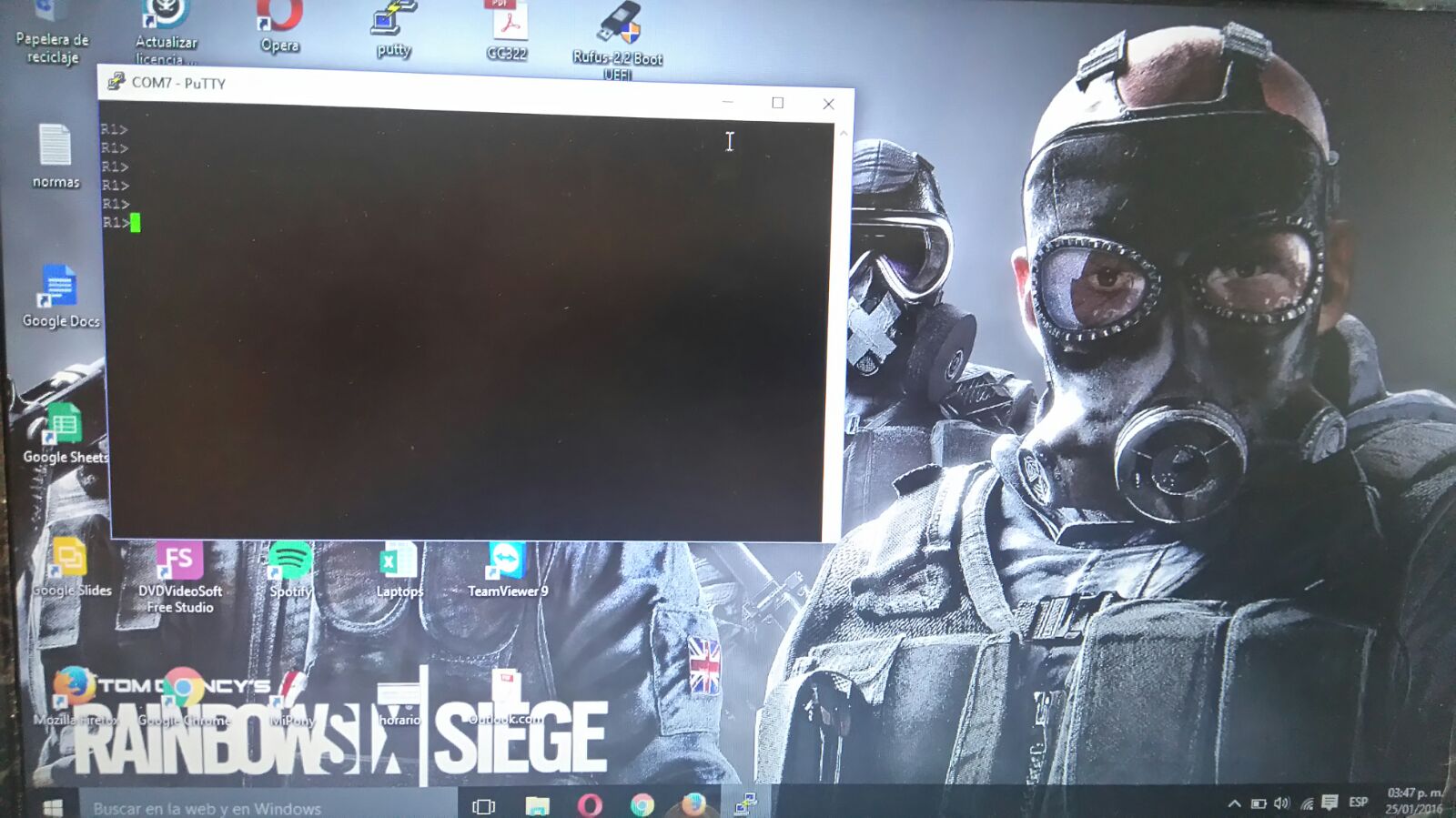
**Material:**

* 2 adaptadores de USB QdB9
* 2 cables de dB9 a RJ45
* 2 cables UTP cruzado, lineal y de consola

**Desarrollo:**

Se realizó la descarga del programa putty el cual nos ayuda a ingresar a la consola del router, para ello se necesitó la conexión de un cable db9 a RJ45 y un adaptador a USB, para tener la comunicación de la Pc al router, teniendo ya la comunicación, con ello se descargaron los drivers del cable. Teniendo los requisitos necesarios para la configuración se procedió a ejecutar el programa putty y a su vez de identifico el puerto de conexión (COM5), se le cambio el tipo de conexión a serial, y con ello apareciendo la línea de conexión y su velocidad, al tener esto se cambió la línea de conexión (COM5). Finalizando al presionar open, esto nos llevó a la consola del router.





**Problemas que se presentaron:**

No podíamos establecer una conexión entre el host y el router, mediante los cables de consola y convertidor de serial a USB ya que no contábamos con los drivers instalados en la computadora, recurrimos a una conexión a internet y es así como se pudo descargar los drivers e instalarlos en la computadora con la que estábamos trabajando.

**Conclusiones:**

Con el trabajo anterior se concibió, cuales son los requerimientos para conectar un host a un router y de esta forma configurarlo, se aprendió a utilizar el programa putty para realizar la conexión y con ello la existencia del material que nos puede ayudar a encaminar los datos entre el host y el router.

Práctica #2: **Configuración de routers**

**Integrantes del equipo:**

* Gómez García Jonathan Daniel
* Gutiérrez González Virginia Sayde
* Moguel Ortiz Álvaro Luis
* Padilla Villaseñor José Alejandro
* Píz Guzmán Christian
* Valdez Lomelí Manuel Alejandro

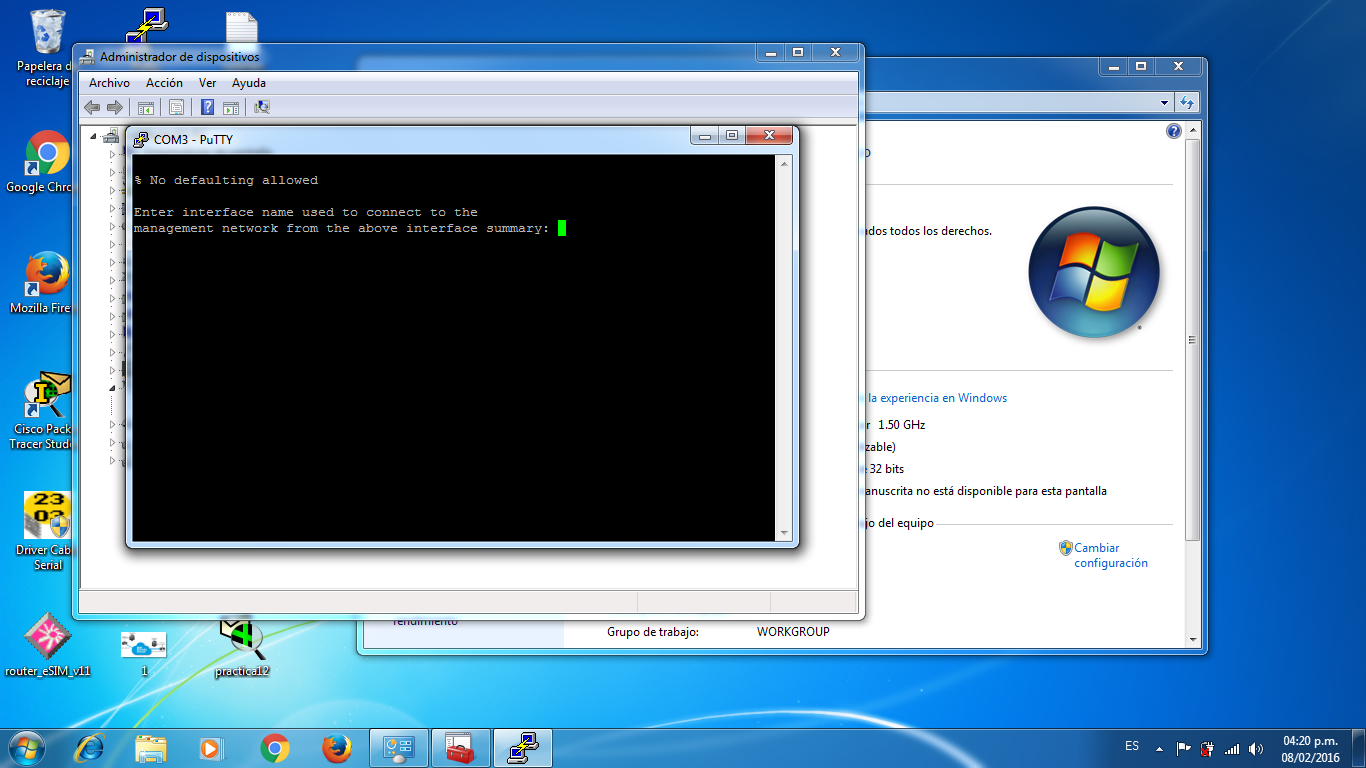
**Material:**

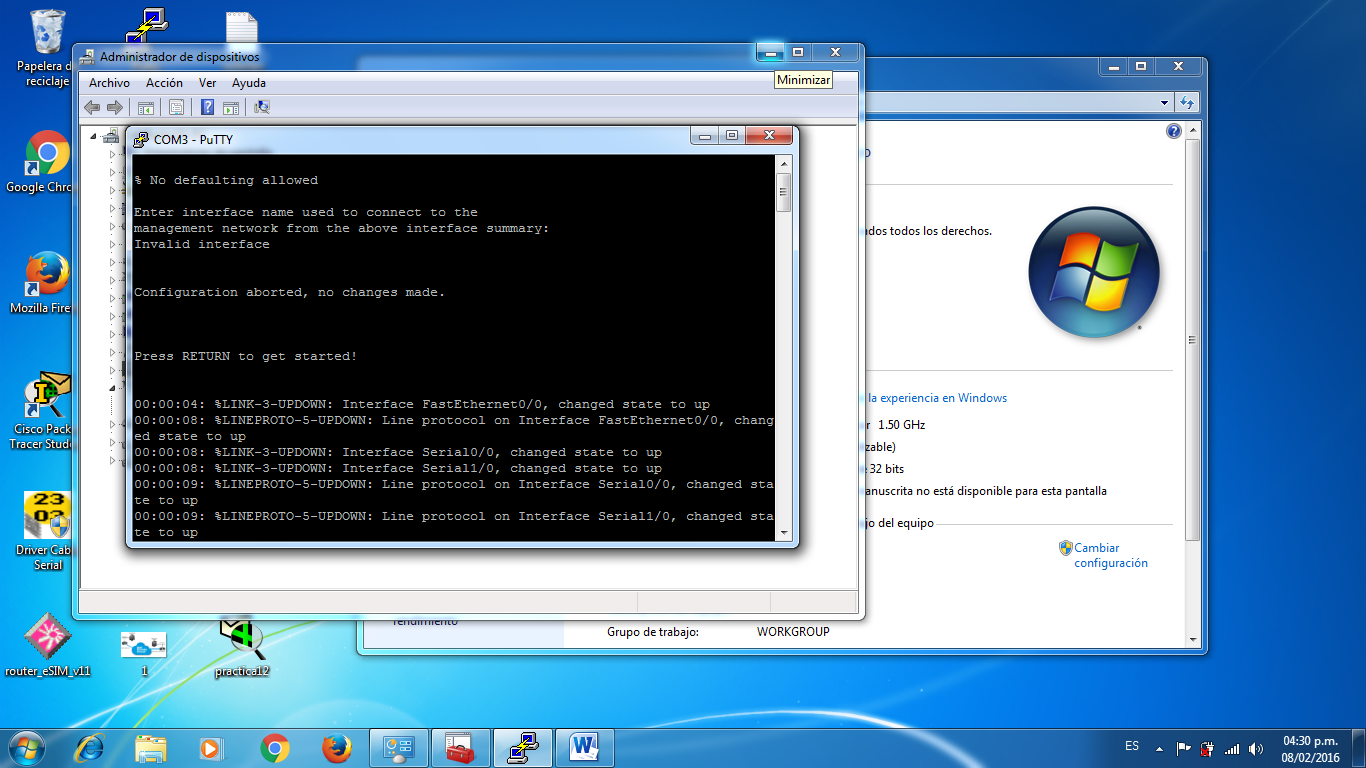
* 2 adaptadores de USB QdB9
* 2 cables de dB9 a RJ45
* 2 cables UTP cruzado, lineal y de consola

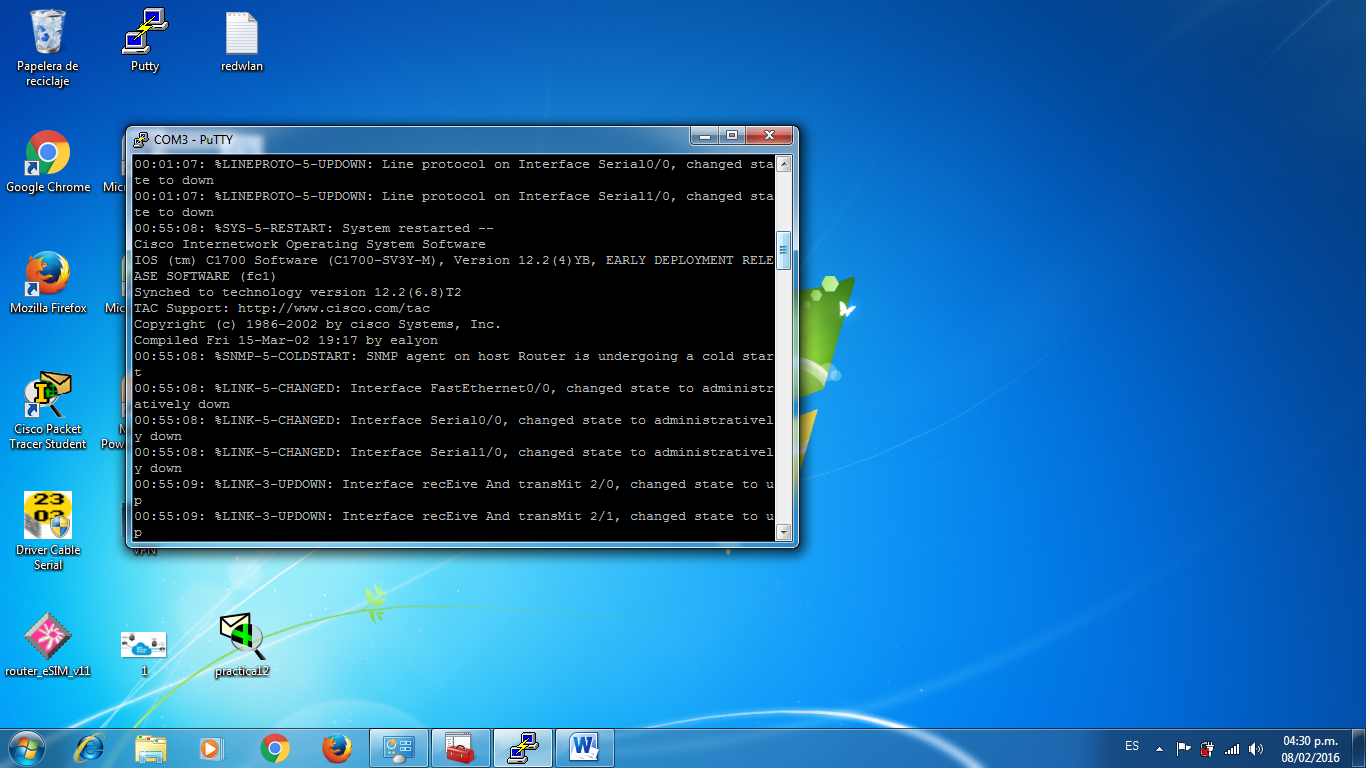
**Desarrollo:**

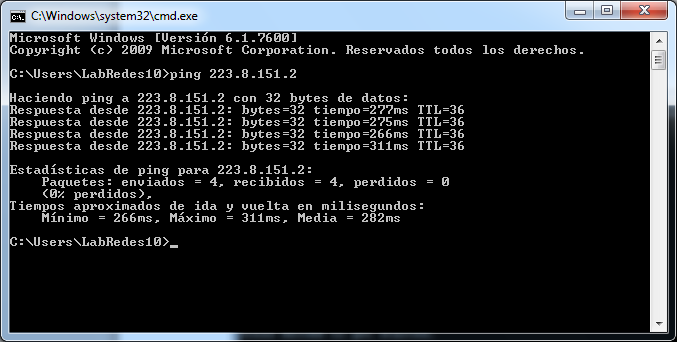
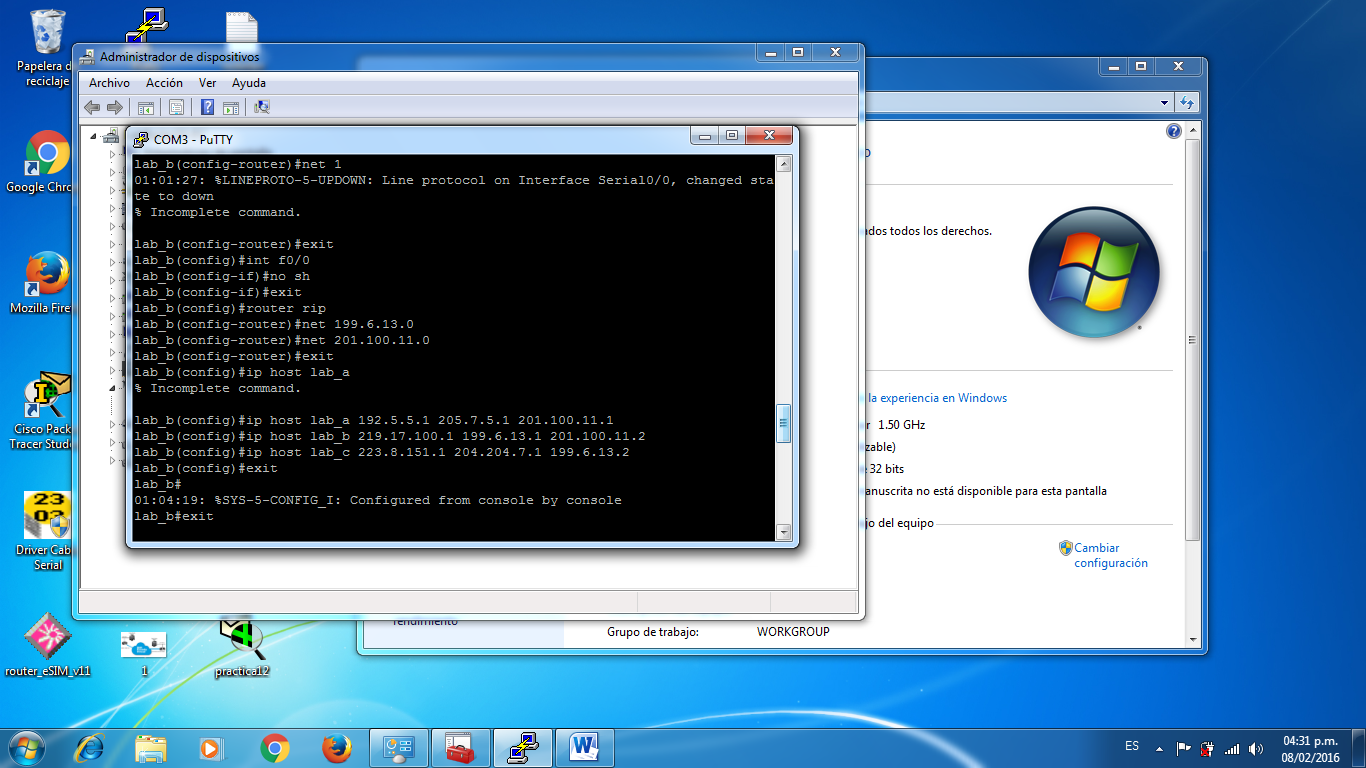
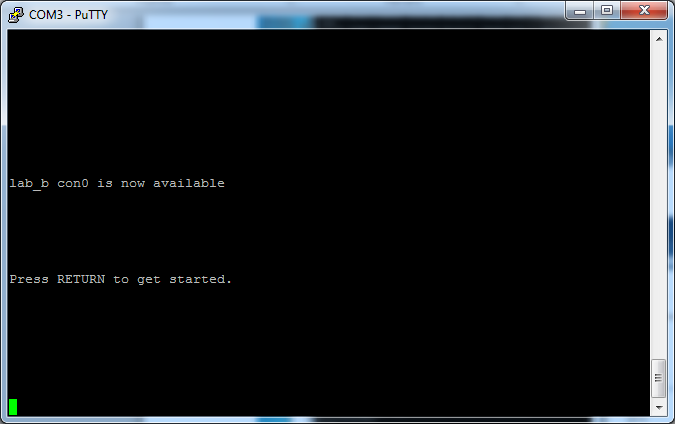
Se realizó la descarga del programa putty el cual nos ayuda a ingresar a la consola del router, para ello se necesitó la conexión de un cable db9 a RJ45 y un adaptador a USB, para tener la comunicación de la Pc al router, teniendo ya la comunicación, con ello se descargaron los drivers del cable. Teniendo los requisitos necesarios para la configuración se procedió a ejecutar el programa putty y a su vez de identifico el puerto de conexión (COM5), se le cambio el tipo de conexión a serial, y con ello apareciendo la línea de conexión y su velocidad, al tener esto se cambió la línea de conexión (COM5). Finalizando al presionar open, esto nos llevó a la consola del router.

Ya en la consola se configuró el routers A, mientras que otro equipo configuraba el router B, para ello nos auxiliarnos en el diseño de la red de eSIM (programa de cisco para la configuración de routers), después de la configuración de los routers, se hizo la llamada a la función ping con la ip del otro dispositivo configurada previamente y con ello respondiendo al ping.









**Problemas que se presentaron:**

El ping no respondía ya que los drivers no eran los correctos, se conectó un cable lineal en lugar de un cable cruzado en el router.

Al final de hacer intentos para la configuración de routers, nos percatamos que ya estaban previamente configurados los routes.

**Conclusiones:**

A pesar de que no se pudo hacer el enlace por la configuración que ya estaba establecía en los routers, se entendió como hacer la configuración de ellos.

Por el problema que se dio por la previa configuración de los routers, comprendimos y visualizamos el problema en consola.

**Conclusiones**

Este capítulo fue más que nada un repaso de la materia de teoría de redes de computadoras, lo cual fue bueno ya que con ello reforzamos nuestros conocimientos. Además se dio información adicional de la importancia de cada dispositivo que se emplea en la red y con ello su configuración. También se hicieron varias prácticas en el laboratorio para comprender más el funcionamiento de los routers

El aprender a configurar los routers, fue algo nuevo e interesante.

**CAPÍTULO 1**

**VPN**

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN. En conjunto con lo anterior, una implementación correcta de esta tecnología permite asegurar la **confidencialidad e integridad** de la información.

**Características de seguridad de una VPN**

Entre las principales características de seguridad que presentan las redes VPN se encuentran las siguientes:

* Sistemas de control de acceso.
* Autentificación y Autorización de usuarios.
* Auditoría y registro de actividades.
* Integridad.
* Confidencialidad y privacidad.
* Control de acceso.

Todas estas características aseguran que los datos están protegidos ante cualquier usuario no autorizado a ingresar a la **VPN**, lo que convierte a este tipo de red en una opción viable para empresas, organismos privados, centros de investigación y cualquier grupo de usuarios que requieran mantener protegidos sus datos, con altos estándares de seguridad.

**Tipos de VPN**

Existen varios tipos de **VPN**, según el tipo de acceso que se tenga. Estos, son los siguientes:

* VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en [usuarios](https://es.wikipedia.org/wiki/Usuario) o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, [hoteles](https://es.wikipedia.org/wiki/Hotel), [aviones](https://es.wikipedia.org/wiki/Avi%C3%B3n) preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la [red local](https://es.wikipedia.org/wiki/Red_local) de la empresa. Muchas empresas han reemplazado con esta [tecnología](https://es.wikipedia.org/wiki/Tecnolog%C3%ADa) su infraestructura [dial-up](https://es.wikipedia.org/wiki/Dial-up) ([módems](https://es.wikipedia.org/wiki/M%C3%B3dem) y líneas telefónicas).

* VPN Punto a Punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El [servidor](https://es.wikipedia.org/wiki/Servidor) VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de [banda ancha](https://es.wikipedia.org/wiki/Banda_ancha). Esto permite eliminar los costosos vínculos punto a puntos tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel [*tunneling*](https://es.wikipedia.org/wiki/Tunneling).

* Tunneling.

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una [PDU](https://es.wikipedia.org/wiki/PDU) (unidades de datos de protocolo) determinada dentro de otra [PDU](https://es.wikipedia.org/wiki/PDU)con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la [PDU](https://es.wikipedia.org/wiki/PDU) encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser [SSH](https://es.wikipedia.org/wiki/SSH).

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios *multicast*, la redirección de tráfico, etc.

* VPN Overland.

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local ([LAN](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local)) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas ([WiFi](https://es.wikipedia.org/wiki/WiFi)).

Como puede suponerse, a través de una VPN pasa información privada y confidencial que en las manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando un Wi-Fi público sin protección. Afortunadamente, este problema puede ser mitigado cifrando los datos que se envían y reciben. Para poder lograr este objetivo, se pueden utilizar los siguientes protocolos:

* [IPsec](http://es.wikipedia.org/wiki/IPsec) (*Internet Protocol Security*): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (triple DES).
* [PPTP](http://es.wikipedia.org/wiki/PPTP)/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo *Microsoft Point to Point Encryption* (MPPE). **PPTP por sí solo no cifra la información**.
* [L2TP](http://es.wikipedia.org/wiki/L2TP)/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, **L2TP no cifra la información por sí mismo**.

Parte de la protección de la información que viaja por una VPN es el cifrado, no obstante, verificar que la misma se mantenga íntegra es igual de trascendental. Para lograr esto, IPsec emplea un mecanismo que si detecta alguna modificación dentro de un paquete, procede a descartarlo. Proteger la confidencialidad e integridad de la información utilizando una VPN es una buena medida para navegar en Wi-Fi públicos e inseguros incluso si no se desea acceder a un recurso corporativo.

Por otro lado, aquellos usuarios hogareños que deseen utilizar una red VPN, pueden elegir entre servicios gratuitos y otros de pago. Es importante mencionar que aquellos libres suelen funcionar más lento que uno que no lo es.

**PSTN**

La red telefónica pública conmutada (PSTN, Public Switched Telephone Network) es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. Cuando llama a alguien, cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada. PSTN garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito hasta que la persona que llama cuelgue.

Se trata de la red telefónica clásica, en la que los terminales telefónicos (teléfonos) se comunican con una central de conmutación a través de un solo canal compartido por la señal del micrófono y del auricular. En el caso de transmisión de datos hay una sola señal en el cable en un momento dado compuesta por la de subida más la de bajada, por lo que se hacen necesarios supresores de eco.

La voz va en banda base, es decir sin modulación (la señal producida por el micrófono se pone directamente en el cable). Las señales de control (descolgar, marcar y colgar) se realizaban, desde los principios de la telefonía automática, mediante aperturas y cierre del bucle de abonado. En la actualidad, las operaciones de marcado ya no se realizan por apertura y cierre del bucle, sino mediante tonos que se envían por el terminal telefónico a la central a través del mismo par de cable que la conversación.

En los años 70 se produjo un creciente proceso de digitalización influyendo en los sistemas de transmisión, en las centrales de conmutación de la red telefónica, manteniendo el bucle de abonados de manera analógica. Por lo tanto cuando la señal de voz, señal analógica llega a las centrales que trabajan de manera digital aparece la necesidad de digitalizar la señal de voz.

El sistema de codificación digital utilizado para digitalizar la señal telefónica fue la técnica de modulación por impulsos codificados, cuyos parámetros de digitalización son:

* Frecuencia de muestreo:8000 Hz
* Número de bits: 8
* Ley A (Europa)
* Ley µ (USA y Japón)

El tratamiento que se aplica a la señal analógica es: filtrado, muestreo y codificación de las muestras. La frecuencia de muestreo Fs es siempre superior a la Nyquist.

**Características de la PSTN**

Las Características esenciales de la RTC son:

* Ofrece a cada usuario un circuito para señales analógicas con una banda base de 4KHz para cada conversación entre dos domicilios. Esta banda incluye espacios para banda de guarda anti-traslape (anti-aliasing) y para eliminación de interferencias provenientes de las líneas de «Distribución domiciliar de potencia eléctrica»
* Única red con cobertura y capilaridad nacional, donde por capilaridad se entiende la capacidad que tiene la red para ramificarse progresivamente en conductores que llevan cada vez menor tráfico.
* Capacidad de interconexión con las redes móviles. Es decir, la telefonía básica es entre aparatos fijos.
* El costo para el usuario por la ocupación del circuito depende de la distancia entre los extremos y la duración de la conexión
* Normalización para interconexión de RTCs.
* Consta de Medios de transmisión y Centrales de conmutación. Los Medios de transmisión entre centrales se conocen como **Troncales**, y en la actualidad transportan principalmente señales digitales sincronizadas, usando tecnologías modernas, sobre todo ópticas. En cambio, los medios de transmisión entre los equipos domiciliarios y las centrales, es decir, las **líneas de acceso** a la red, continúan siendo pares de cobre, y se les sigue llamando líneas de abonado (abonado proviene del Francés y significa subscriptor). Las demás formas de acceder del domicilio a la central local, tales como enlaces inalámbricos fijos, enlaces por cable coaxial o fibra óptica, u otros tipos de lìneas de abonado que trasportan señales digitales (como ISDN o xDSL), no se consideran telefonía básica.

## **Arquitectura de la PSTN**

Los componentes incluidos en la arquitectura de toda RTC son:

* Terminal de abonado y línea telefónica de abonado (bucle local).
* Centrales de Conmutación de circuitos
* Sistema de transmisión
* Sistema de Señalización

Esto correspondería exclusivamente al funcionamiento del teléfono.

Para poder transmitir datos por una Red Telefónica Conmutada, se necesita añadir otro elemento a la disponibilidad en tantos sitios de la infraestructura de la RTC la constituye en la solución más apropiada para introducir rápidamente cualquier Servicio de Telecomunicación nuevo.

### Conexión básica a la PSTN

Para acceder a la Red Publica sólo necesitaremos dos hilos (un par de cables) que forman una línea telefonica basica, en la transmision de datos es necesario un módem, ya sea interno o externo.

A lo largo del tiempo se han ido desarrollando varios métodos de transmisión de datos utilizando la RTC y así obtener un mejor aprovechamiento de la misma en el afan de conseguir mayores velocidades. Con el paso del tiempo los desarrolladores consiguieron pasar de los pocos miles de bits por segundo, como la norma V.21 o V.22, a las velocidades actuales.

* El estándar V.32 desarrollada en 1991 conseguía velocidades de 14400 bps.
* El estándar V.34 conseguía velocidades de hasta 28800 bps en 1994, y hasta 33600 la V.34+
* La conexión en la actualidad tiene una velocidad de 56 kbps en bajada y 33.6 kbps en subida y se realiza directamente desde un PC bajo la norma V.90 desarrollada entre 1998 y 1999.
* La norma V.92 ha conseguido aumentar la velocidad de subida a 48 kbps.

**IDS**

Los sistemas de detección de intrusos basados en la red operan de una forma diferente que aquellos IDSes basados en host. La filosofía de diseño de un IDS basado en la red es escanear los paquetes de red al nivel del enrutador o host, auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información extendida. Basándose en estos paquetes sospechosos, un IDS basado en la red puede escanear su propia base de datos de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete. Si los niveles de severidad son lo suficientemente altos, se enviará un correo electrónico o un mensaje de pager de advertencia a los miembros del equipo de seguridad para que ellos puedan investigar la naturaleza de la anomalía.

Los IDSes basados en la red se han vuelto muy populares a medida en que la Internet ha crecido en tamaño y tráfico. Los IDSes que son capaces de escanear grandes volúmenes de actividad en la red y exitósamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escaners, huzmeadores y otras herramientas de auditoria y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como:

* Engaño de direcciones IP (IP Spoofing)
* ataques de rechazo de servicio (DoS)
* envenenamiento de caché arp
* Corrupción de nombres DNS
* ataques de hombre en el medio

**IPS**

En la prensa especializada cada vez resuena más el término **IPS** (*Sistema de prevención de intrusiones*) que viene a sustituir al IDS "tradicional" o para hacer una distinción entre ellos.

Los sistemas de prevención de intrusiones detectan y bloquean cualquier intento de intrusión, transmisión de código malicioso o amenazas a través de la red, sin impacto alguno sobre su rendimiento. La solución de Interoute puede soportar caudales desde los 100 Mbps hasta los 10 Gbps en su configuración estándar.

Un IPS es un sistema de prevención/protección para defenderse de las intrusiones y no sólo para reconocerlas e informar sobre ellas, como hacen la mayoría de los IDS. Hay dos características principales que distinguen a un IDS (de red) de un IPS (de red):

* El IPS se sitúa en línea dentro de la red IPS y no sólo escucha pasivamente a la red como un IDS (tradicionalmente colocado como un [rastreador de puertos](http://es.ccm.net/contents/attaques/sniffers.php3) en la red).
* El IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes en modo nativo (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos, el bloqueo de un intruso, etc.).

El servicio funciona de manera transparente para el usuario, por lo que no requiere ninguna reconfiguración de la red existente a la que se conecta. El servicio de Prevención de intrusiones en la red de Interoute ofrece una compleja capa de protección para las empresas. Utilizando técnicas de reconocimiento de protocolos, identificación y análisis de tráfico, es capaz de detectar, identificar, alertar y proteger a su organización frente a amenazas como:

* Gusanos
* Spyware
* Peer to peer (P2P)
* Ataques de denegación de servicio individuales (DoS) o distribuidos (DDoS)
* Botnets
* Ataques dirigidos contra aplicaciones web
* Salida de datos protegidos o delicados fuera de la red
* Ejecución no autorizada de código JavaScript entre distintos dominios *(cross-site scripting)*
* Inyección de código SQL
* Desbordamiento de búferes
* Navegación por directorios de una web

**QoS**

QoS es el acrónimo de **Quality of Service**, o calidad de servicio, que establece diversos mecanismos destinados a asegurarnos la fluidez en el tráfico de la red. Para ello, lo que hace es **dar prioridad al tráfico según el tipo de datos**que transportan.

La conexión de red, tanto de área local como acceso a Internet es finita, está limitada por la capacidad de la banda ancha que tengas contratada. Este factor de escasez es el que administra QoS, para tratar de que las preferencias del tráfico se adapten a nuestras prioridades. **Si tu red va fluida, no va a suponer una gran diferencia** si el QoS está configurado o no, pero si notas algún cuello de botella puntual o latencia, en ese momento es cuando deberías plantearte su configuración.

**QoS tratará un paquete de datos de una forma u otra en función de la clase** a la que pertenezca. Aquí depende un poco del router para establecer un tipo de clasificación u otra. No todos nos dan las mismas opciones. En este sentido, lo normal es que se clasifique la pertenencia **según la dirección MAC, el puerto de origen o destino, etc**. Esto va a permitir diferenciar entre paquetes de datos que van destinados a una videoconferencia por Skype, [un juego online](http://www.anexom.es/tecnologia/mi-conexion/exprime-tu-conexion-adsl-como-mejorar-el-juego-online/) o una película que estamos viendo por streaming, por poner varios ejemplos de servicios que demandan un consumo de datos alto, tanto de bajada como también de subida, que muchas veces es el factor más escaso.

Una vez clasificados los paquetes de datos y establecidas las prioridades, **QoS lo que en realidad hace es ordenar los paquetes para su salida en diferentes colas**según sus clases. A partir de aquí, y según las prioridades establecidas, va enviando los paquetes. De esta forma, se asegura de mantener una calidad de servicio en el tráfico de red, lo que se conoce como **la gestión del ancho de banda,** una de las partes principales del QoS.

Por lo general, donde es más efectivo el QoS en su configuración en el router es en **la gestión del tráfico de subida**, que es el **segmento de la red más escaso** en comparación con el de bajada (la mayoría de las líneas de banda ancha del hogar suelen ser asimétricas). Para ello, tenemos que tener configurada esta cuestión en nuestro router, aunque, como hemos comentado antes, no todos nos ofrecen las mismas posibilidades.

### Switches capa 2

Son los Switches tradicionales, que funcionan como puentes multi-puertos. Su función principal es la de dividir una LAN en varios dominios, o en los casos de las redes anillo, segmentar la LAN en diversos anillos.

Los conmutadores de la capa 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes. Los switches de capa 2 no consiguen, sin embargo, filtrar difusiones o broadcasts, y multicasts.

**Referencia del fabricante :**

FGSD-1022P

**Fabricante[UK_PLT_SI](http://www.acalbfi.com/es/search/PLT)**

Planet

**Descripción:**

Switch gestionable PLANET de capa 2 con 8 puertos 10/100Base-TX y 2 puertos 10/100/1000Base-TX. Dispone de 2SFPs 1000Base-SX/LX/BX. Disfruta de alimentación POE bajo el estándar IEEE 802,3af en los 8 puertos 10/100Base-TX con una potencia acumulada efectiva de 180w

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
|  |  | **Avaya ERS 4850GTS-PWR+ Características:**48 puertos 10/100/1000 Gigabit con Power Over Ethernet (PoE+); sistema de chasis apilable de 1U de rack; funcionalidades de capa 2 completa, ruteo IP estático, RIP v1 y v2 además de otras capacidades de capa 3 que se pueden habilitar con licenciamiento adicional, fuente de poder redundante; desempeño de hasta 184Gps.**Disponibilidad:**Anixter, Avnet y Centro de Conectividad.**Garantía:**De por vida. |

**Principales Características:**

* Switch Administrable
* Compilación IEEE 802.3, 3u, .3ab, .3z, .3x, .1q, .1p, .1x, .1d, .1w, .1s, .3ad, .3az
* Puerto Espejo
* VLAN
* QoS
* VSM
* Modo Isolated
* Control de Ancho de Banda
* Interfaz de hardware:Voltaje de operacion: 100 - 240V
  + 24 puertos 10/100/1000 Base-T, RJ-45
  + 4 puertos 100/1000 SFP combo RJ-45
  + 2 puertos 100/1000 SFP
  + 1 boton de reset de fabrica
* Consumo: 250W
* Peso: 4.6Kg.
* Dimensiones: L300 x W442 xH44 (mm)

### Switches capa 3

Son los switches que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de routing, como por ejemplo la determinación de un camino basado en informaciones de capa de red y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc). Los conmutadores de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.

Por permitir la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la LAN, debido a la cantidad excesiva de usuarios.

|  |  |  |
| --- | --- | --- |
|  |  | **Avaya ERS 4850GTS Características:**Sistema de chasis apilable de 1U de rack, 48 puertos 10/100/1000 Gigabit Ethernet, dos puertos SFP compartidos; procesamiento a 533 MHz con 256MB en RAM; orientado a convergencia, seguridad y conectividad flexible con Ethernet; funciones de capa 3 como ruteo IP estático, consumo de energía optimizado.**Disponibilidad:**Anixter, Avnet y Centro de Conectividad.**Garantía:** De por vida. |

|  |  |  |
| --- | --- | --- |
|  |  | **Cisco Catalyst 2960-X Características:**Versiones de 24 o 48 puertos con Power Over Ethernet (PoE+) opcional, capacidades capa 3; diseño escalable de hasta 8 unidades, fuentes de poder redundantes, Netflow para ofrecer visibilidad de aplicaciones; consumo de energía optimizado, puerto USB e interfaces de gestión de Ethernet, sistema operativo Lite Cisco IOS para ruteo dinámico y más funcionalidades de capa 3.**Disponibilidad:**Comstor, Grupo Dice, Ingram Micro y Tech Data.**Garantía:** Limitada de por vida. |

Principales características:

* 12 puertos SFP 10/100/1000BASE-X
* 4 puertos 10/100/1000BASE-T
* 1 puerto consola RS232
* Ancho de banda agregado 24Gps
* Funciones L3 y L2
* VLANs
* Adminsitracion via web
* Log de eventos del sistema

**Switches para empresas pequeñas, medianas y grandes**

Un switch o conmutador es un dispositivo necesario en todas aquellas compañías que tienen la firme intención de tener todas sus redes conectadas entre sí. A partir de aquí, desarrollan su actividad en la llamada capa 2, que es la arquitectura de interconexión de sistemas de comunicaciones empleada habitualmente en el campo de las redes.

Una de las características más atractivas e interesantes que incorporan estos equipos es su capacidad para aprender y almacenar las llamadas direcciones MAC, y cuyo cometido es identificar los dispositivos de una red de manera individual: con este planteamiento, se consigue dirigir la conexión que se establece a un determinado puerto a través de una única dirección y, de esta forma, evitar algunos inconvenientes como la aparición de bucles. De igual forma, es posible detectar las estaciones conectadas a cada uno de los puertos del switch, valorando el tráfico de entrada y concluyendo las direcciones MAC de las estaciones que hay conectadas a cada puerto. Lo habitual es que un switch integre 24 ó 48 puertos. Cuando los paquetes de información se han recibido, el siguiente paso es re-direccionarlos a su dirección de destino o puerto correspondiente.

Por otra parte, y en función de la metodología de segmentación de las sub-redes utilizadas, es posible diferenciar entre modelos de 2, 3 y 4 capas. Los primeros son los más sencillos y son los encargados de dividir una red LAN en varios anillos o dominios (su decisión de envío se basa de manera casi exclusiva en direcciones MAC destino que incorpora cada una de las tramas de datos). Mientras, los modelos de capas 3 soportan las funcionalidades de los modelos de capa 2 e incorporan también características de routing como los protocolos para la construcción y el mantenimiento de las llamadas tablas de enrutamiento. En este caso, un switch de capa 3 es apropiado para las redes LAN de gran tamaño que precisan de un alto rendimiento y quieren evitar sorpresas desagradables como la falta de eficacia. Otras posibilidades son la definición de redes virtuales, servicios de autenticación, filtros y niveles de priorización. Finalmente, los modelos de capa 4 completan sus características con direcciones FTP y filtros como los puertos TCP/UDP.

**Cisco Nexus 3548**

**Altamente potente y con un rendimiento superior. Este equipo, miembro de la familia de switches Unified Fabric de Cisco, es la opción más adecuada para grandes centros de datos y corporaciones de gran tamaño que precisan de una baja latencia.**

El importe económico del modelo de Cisco proporciona alguna que otra pista sobre el tipo de empresas al que se dirige. En concreto, el switch Nexus 3548 es un equipo enfocado a entornos de transacciones de alto rendimiento y grandes centros de datos.

Una de sus características más importantes es que integra la tecnología Algo Boost en un formato compacto de una unidad de rack, prestación que permite ofrecer un alto control, visibilidad y rendimiento. Entrando en detalle, Algo Boost ayuda a obtener latencias bajas de 250 nanosegundos (ns) e, incluso, inferiores en todos los volúmenes de trabajo con independencia de las funciones aplicadas (capa 2 y 3, unidifusión o multidifusión, entre otras). Gracias a su modo Warp, el switch Nexus 3548 reduce aún más la latencia a 190 ns en las implementaciones de capa 2/3 pequeñas a medianas.

Desde el punto de vista de sus características técnicas, se han incorporado 48 puertos SFP+ 1/10 Gbps fijos y fuentes de alimentación redundantes dobles codificadas por colores que facilitan su identificación. Este sistema de colores también se ha aplicado a sus cuatro ventiladores redundantes. La capacidad de procesamiento de sus capas 2 y 3 proporciona una velocidad de línea de hasta 960 Gbps.

Este equipo es sumamente preciso, y lo consigue a través de la función SPAN remoto integrado con marca horaria en nanosegundos que ayuda a supervisar el tráfico. Además, su capacidad de supervisión activa del búfer es útil a la hora de aprovechar la volatilidad del mercado y manejar micro ráfagas de datos. La opción Traducción de Direcciones de Red (del inglés Network Address Translation, NAT) se aplicará en la ejecución de las transacciones con independencia de la ubicación y sin penalizaciones por latencia.

El sistema operativo que integra es Cisco NX-OS diseñado para centros de datos. Entre sus funciones, destacan los protocolos de multidifusión del tipo PIM-SM, PIM-SSM y MSDP. También admite protocolos de unidifusión con plenas funciones como los que ofrecen los estándares BGP (Border Gataway Protocol), para el intercambio de información de encaminamiento entre sistemas autónomos; Open (Open Shortest Path First), para el cálculo de las rutas más cortas; EIGRP (Enhanced Interior Gataway Routing), este protocolo avanzado proporciona lo mejor de los algoritmos del estado de enlace y vector de distancias; y la versión 2 de RIP (Routing Information Protocol), protocolo de puerta de enlace interna para el intercambio de información sobre redes IP.  Por último, añadir su compatibilidad con herramientas de resolución de problemas como el Analizador de puertos conmutados, calidad de servicio y listas de control de acceso por VLAN y routing. La gestión del switch se efectúa a través del programa Cisco Prime Data Center Network Management: este software ayudar a implementar y administrar de un modo eficiente los centros de datos virtualizados.

**D-Link DGS-3620**

**Esta familia, formada por cinco dispositivos, puede utilizarse como centro de conmutación de una red multinivel o como dispositivo de acceso departamental. Proporciona un completo soporte IPv6, una alta densidad de puertos, es eficiente en términos de energía y posee una ranura para tarjetas SD que permite guardar y restaurar archivos de configuración.**

Las grandes corporaciones, y también las pequeñas y medianas empresas, tienen en esta familia de switches gestionados una interesante propuesta en términos de flexibilidad, rendimiento y seguridad multinivel que logra a través de listas de control de accesos multinivel L2/L3 y L4 y autenticación de usuarios 802.1x con servidores RADIUS y TACACS+. Además, están dotados de la tecnología ZoneDefense que permite integrar una pila de switches con firewalls NetDefend de D-Link para crear  una infraestructura de seguridad proactiva y completa. A este listado de características, se suman su soporte VLAN extensivo y su motor de seguridad Safeguard Engine que mejoran el nivel de servicio y la disponibilidad, evitando el tráfico malicioso que origina un virus o un gusano. También se pueden establecer controles de banda ancha.

Por otra parte, brinda soporte completo IPv6 y conectividad 10 Gigabit de cara a posibles mejores y actualizaciones, y las tareas relativas a su despliegue y gestión carecen de complejidad.  Los cinco modelos que conforman esta gama pueden apilarse virtualmente con cualquier otro switch compatible mediante la “Gestión IP” que facilita D-Link y, de esta manera, crear una red estructurada multi-nivel a partir de servidores de alta velocidad centralizados.

Se han incluido dos imágenes de software diferentes. Por un lado, la Imagen Estándar (SI) y, por el otro, la Imagen Mejorada (EI). La primera de ellas provee de funciones que son básicas para corporaciones y grandes campus como routing, switching, multicasting o calidad de servicio avanzada. La segunda, por su parte, está indicada para las redes de proveedores de servicio y ofrece tunneling IPv6, enrutado dinámico u OAM, entre otras características.

D-Lint también plantea a las empresas la posibilidad de crear un apilado físico utilizando uno o dos puertos SFP+ de 10 Gigabit: con esta configuración, los switches son intercambiables en caliente para reducir los tiempos de caída de red en caso de reposición y suprimiendo puntos únicos de fallo. Es posible configurar una arquitectura física apilable de hasta 576 puertos Gigabit en una sola pila y, así, facilitar un mayor ancho de banda y alta densidades de puerto.

Incorpora, asimismo, un modo de ahorro de energía y un sistema de ventilación inteligente. Los switches de la serie DGS-3260 ofrecen una interfaz de usuario gráfico basada en Web, desarrollándose versiones PoE y PoE+. Finalmente, indicar su completo conjunto de protocolos de enrutado, su ranura para tarjetas SD para guardar y restaurar archivos de configuración, su alta densidad de puertos Gigabit y su soporte Gigabit SFP.

**Fibernet FIB-SWITCH-1090**

**Destaca por su densidad de puertos y por proporcionar una respuesta eficaz que permite disminuir costes operativos. Este modelo emplea, asimismo, tecnología Carrier Ethernet y un amplio abanico de funcionalidades OAM y prestaciones de nivel 2.**

Esta firma española, dedicada al desarrollo de equipos de transmisión por fibra óptica, participa en esta comparativa con el switch Carrier Ethernet FIB-SWITCH-1090. Se trata de un modelo dirigido a núcleos empresariales que requieren de grandes anchos de banda en el transporte de datos, voz, video y servicios móviles. Asimismo, cumple con los estándares que recogen las certificaciones ITU, MEF e IEEE.

Entrando en detalle, el fabricante garantiza, con esta propuesta, reducir los costes derivados de la implementación de servicios e inversión frente al transporte basado en las tecnologías SDH y SONET (adoptan la forma de un anillo de fibra óptica) y la construcción de redes, a excepción de los nodos donde se proveen servicios IP. En concreto, Fibernet apunta a equipamiento de capa 2 de agregación y acceso, reduciendo el número de máquinas desplegadas de capa 2.

¿Y qué beneficios reporta la tecnología Carrier Ethernet? A la escalabilidad y la implementación rápida (pues no requiere de personal de operación especializado), hay que sumar la interoperabilidad entre proveedores y tecnologías. Otra ventaja es que permite de forma granular y customizada controlar el servicio a nivel de redes de área local virtual, lo que facilita la entrega de servicios con SLAs (define la relación proveedor-cliente) ajustados a las necesidades del destinatario. La tecnología Carrier Ethernet también admite funcionalidades carrier-class en las tareas de operación, administración y mantenimiento.

El equipo FIB-SWITCH-1090, que destaca por su número de puertos, integra 24 puertos ópticos GbE (base FX) y 4 x 10 GbE. Basado en el protocolo de comunicación Ethernet, soporta funcionales de nivel 2 tales como la auto-negociación de velocidad de puerto, IEEE 802.3x y normas 802.1s, 802.1w y 802.1s. Asimismo, y con este switch, un circuito de 1 GbE puede ser aprovisionado de extremo a extremo mediante circuitos OAM&P y VLAN tunneling. En cuanto a la seguridad, los clientes pueden establecer topologías en anillo con un mecanismo de protección que admite la recuperación de fallos de enlace (menos de 50 ms) en comparación a otras tecnologías. FIB-SWITCH-1090 también detecta fallos relacionados con la pérdida de continuidad y señal.

En otro orden de cosas, es posible definir atributos como perfiles de ancho de banda con prioridad definida (8 CoS), clasificar el tráfico que se genera o gestionar prioridades basadas en la norma IEEE 802.1p. Finalmente, indicar que soporta un amplio abanico de funcionalidades OAM que mejora la detección y gestión de fallos.

**STP**

El Protocolo de Árbol de Extensión (**STP**) es un protocolo de capa dos publicado en la especificación IEEE 802.1.  
El objetivo del árbol de extensión es mantener una red libre de bucles. Un camino libre de bucles se consigue cuando un dispositivo es capaz de reconocer un bucle en la topología y bloquear uno o más puertos redundantes.  
El protocolo Árbol de extensión explora constantemente la red, de forma que cualquier fallo o adición en un enlace, switch o bridge es detectado al instante. Cuando cambia la topología de red, el algoritmo de árbol de extensión reconfigura los puertos del switch o el bridge para evitar una pérdida total de la conectividad.  
Los switches intercambian información (BPDU) cada dos segundos si se detecta alguna anormalidad en algún puerto STP cambiara de estado algún puerto automáticamente utilizando algún camino redundante sin que se pierda conectividad en la red.

**Proceso STP**

**Elección de un Switch Raíz:**  
En un dominio de difusión solo puede existir un switch raíz. Todos los puertos del bridge raíz se encuentran en estado enviando y se denominan puertos designados. Cuando esta en este estado, un puerto puede enviar y recibir tráfico. La elección de un switch raíz se lleva a cabo determinando el switch que posea la menor prioridad. Este valor es la suma de la prioridad por defecto dentro de un rango de 1 al 65536 (20 a 216) y el ID del switch equivalente a la dirección MAC. Por defecto la prioridad es 215 = 32768 y es un valor configurable. Un administrador puede cambiar la elección del switch raíz por diversos motivos configurando un valor de prioridad menor a 32768. Los demás switches del dominio se llaman switch no  raíz.

**Puerto Raíz:**  
El puerto raíz corresponde a la ruta de menor coste desde el Switch no raíz, hasta el Switch Raíz. Los puertos raíz se encuentran en estado de envío o retransmisión y proporcionan conectividad hacia atrás al Switch Raíz. La ruta de menor coste al switch raíz se basa en el ancho de banda.

**Puertos designados:**  
El puerto designado es el que conecta los segmentos al Switch Raíz y solo puede haber un puerto designado por segmento. Los puertos designados se encuentran en estado de retransmisión y son los responsables del reenvío de tráfico entre segmentos.  
Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de bucle.

# EtherChannel

EtherChannel entre un [*switch*](https://es.wikipedia.org/wiki/Switch) y un [servidor](https://es.wikipedia.org/wiki/Servidor).

**EtherChannel** es una tecnología de [Cisco](https://es.wikipedia.org/wiki/Cisco_Systems) construida de acuerdo con los estándares 802.3 [full-duplex](https://es.wikipedia.org/wiki/Full-duplex) [Fast Ethernet](https://es.wikipedia.org/wiki/Fast_Ethernet).[[*cita requerida*](https://es.wikipedia.org/wiki/Wikipedia:Verificabilidad)] Permite la agrupación lógica de varios enlaces físicos [Ethernet](https://es.wikipedia.org/wiki/Ethernet), esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

La tecnología EtherChannel es una extensión de una tecnología ofrecida por Kalpana en sus [*switches*](https://es.wikipedia.org/wiki/Switch) en la década de 1990.[[*cita requerida*](https://es.wikipedia.org/wiki/Wikipedia:Verificabilidad)]

Un máximo de 8 puertos Fast Ethernet, [Giga Ethernet](https://es.wikipedia.org/w/index.php?title=Giga_Ethernet&action=edit&redlink=1) o [10Gigabit Ethernet](https://es.wikipedia.org/w/index.php?title=10Gigabit_Ethernet&action=edit&redlink=1) pueden ser agrupados juntos para formar un EtherChannel. Con esta última agrupación es posible conseguir un máximo de 80 Gbps de ancho de banda. Las conexiones EtherChannel pueden interconectar *switches*, [*routers*](https://es.wikipedia.org/wiki/Router), servidores o clientes.

Los puertos usados deben tener las mismas características y configuración.

## **Ventajas**

* La tecnología EtherChannel se basa en el estándar IEEE 802.3 compatible con Ethernet mediante la agrupación múltiple, enlaces full-duplex punto a punto.
* Permite el uso en cualquier lugar de la red donde puedan ocurrir cuellos de botella.
* Permite un crecimiento escalable y a medida. Es posible agregar el ancho de banda de cualquiera de los enlaces que tenemos en el EtherChannel, aunque los enlaces no tengan la misma velocidad.
* El incremento de la capacidad no requiere una actualización del hardware.
* Permite reparto de carga. Como el enlace está compuesto por varios enlaces Ethernet, se puede hacer reparto de carga entre estos enlaces. Así se obtiene mayor rendimiento y caminos paralelos redundantes.
* Robustez y convergencia rápida. Cuando un enlace falla, la tecnología EtherChannel redirige el tráfico del enlace fallido a los otros enlaces proporcionando una recuperación automática mediante la redistribución de la carga entre los enlaces restantes. La convergencia es completamente transparente para los usuarios y las aplicaciones de red.
* La tecnología EtherChannel está disponible para todas las velocidades de los enlaces Ethernet. Permite a los administradores de red desplegar redes escalables sin problemas.
* Completamente compatible con el [Cisco IOS Software](https://es.wikipedia.org/wiki/Cisco_IOS). Las conexiones EtherChannel de Cisco son totalmente compatibles con Cisco IOS LAN virtual ([VLAN](https://es.wikipedia.org/wiki/VLAN)) y las tecnologías de enrutamiento. EtherChannel se puede configurar como enlace VLAN trunk. Cisco ISL, VTP y IEEE 802.1Q son compatibles con EtherChannel.[[*cita requerida*](https://es.wikipedia.org/wiki/Wikipedia:Verificabilidad)]
* Interoperabilidad con Coarse Wavelength Division Multiplexing ([CWDM](https://es.wikipedia.org/wiki/CWDM)). La tecnología CWDM permite el tráfico agregado en el enlace EtherChannel de Cisco para ser multiplexado en un solo hilo de fibra.

## **Configuración**

La configuración de un EtherChannel se puede hacer de dos formas diferentes: negociación o manual. En negociación se pueden identificar también dos formas, Port Aggregation Protocol (PAgP) o Link Aggregation Control Protocol (LACP).

Ambos extremos se deben de configurar en el mismo modo.

PAgP es un protocolo propietario de Cisco. El switch negocia con el otro extremo cuales son los puertos que deben ponerse activos. El propio protocolo se encarga de agrupar puertos con características similares (por velocidad, troncales, por pertenecer a una misma VLAN,…). Se puede configurar de dos modos:

* Auto. Pone el puerto en modo pasivo, solo responderá paquetes PAgP cuando los reciba y nunca iniciará una negociación.

Dos puertos auto nunca podrán formar grupo, ya que ninguno puede iniciar una negociación.

* Desirable. Establece el puerto en modo activo, negociará el estado cuando reciba paquetes PAgP y puede iniciar negociaciones con otros puertos.

LACP es muy similar a PAgP ya que también puede agrupar puertos con características similares. Es un protocolo definido en el estándar 802.3ad.

Los modos de configuración de LACP son:

* Activo. Está habilitado para iniciar negociaciones con otros puertos.
* Pasivo. No puede iniciar negociaciones, pero si responde a las negociaciones generadas por otros puertos.

Dos puertos pasivos tampoco podrán nunca formar grupo. Es necesario que al menos uno de los dos puertos sea activos.

En el modo manual toda la configuración del puerto se realiza de forma manual, no existe ningún tipo de negociación entre los puertos.

## **Limitaciones**

Una limitación de EtherChannel es que todos los puertos físicos en el grupo de agregación deben residir en el mismo conmutador. El protocolo [SMLT](https://es.wikipedia.org/wiki/SMLT) Avaya elimina esta limitación al permitir que los puertos físicos sean divididos entre dos switches en una configuración de triángulo o 4 o más switches en una configuración de malla.

## **Componentes**

* Enlaces Fast Ethernet- las conexiones EtherChannel puede consistir de uno a ocho enlaces Fast Ethernet para compartir la carga de tráfico de hasta 800 Mbps de ancho de banda utilizable. Conexiones EtherChannel puede interconectar switches, routers, servidores y clientes. La tecnología EtherChannel ofrece enlaces resistentes dentro de un canal- si los enlaces fallan, el tráfico es redirigido inmediatamente a los demás enlaces. Finalmente, la tecnología EtherChannel no depende de ningún tipo de medio de comunicación. Se puede utilizar con Ethernet que funciona con par trenzado sin blindaje (UTP), fibra monomodo y fibra multimodo.
* Los algoritmos de compartición de carga utilizados varían entre plataformas, permitiendo decisiones basadas en direcciones MAC origen o destino, direcciones IP, o los números de puerto [TCP](https://es.wikipedia.org/wiki/Transmission_Control_Protocol)/ [UDP](https://es.wikipedia.org/wiki/UDP).
* Redundancia- La tecnología EtherChannel de Cisco no requiere del uso de 802.1d Spanning Tree Protocol para mantener un estado dentro de la topología del canal. Por el contrario, utiliza un protocolo de control punto a punto que proporciona configuración automática y tiempos de convergencia para enlaces paralelos inferiores al segundo. Sin embargo, permite protocolos de alto nivel (como el Protocolo Spanning Tree) o protocolos de enrutamiento para mantener la topología.
* Gestión- La tecnología EtherChannel de Cisco se configura fácilmente mediante una interfaz de línea de comandos ([CLI](https://es.wikipedia.org/wiki/CLI)) o aplicaciones [Simple Network Management Protocol](https://es.wikipedia.org/wiki/Simple_Network_Management_Protocol) (SNMP), tales como CiscoWorks. El administrador de red necesita identificar y definir el número de puertos que conformarán el canal, y luego conectar los dispositivos. Un beneficio de la tecnología EtherChannel es la capacidad de detectar, informar y prevenir el uso de pares de interfaces incorrectas dentro del canal. Estos pueden incluir interfaces que no están configurados para full-duplex, tienen velocidades de enlace incorrectas, o están mal conectadas. Comprobaciones de coherencia antes de la activación de un canal ayudan a asegurar la integridad de la red.

## ***FIBRE CHANNEL***

Fibre Channel (FC) es una nueva tecnología desarrollada para transmisión de datos a alta velocidad entre mainframes, superordenadores, servidores de altas prestaciones y dispositivos de almacenamiento.

FC es un interfaz de transferencia de datos en serie que utiliza actualmente una velocidad de enlace de 1 Gigabit por segundo (1 Gbps) y que soporta diferentes protocolos de transporte, tanto de canal de periféricos (como puedan ser SCSI o IP) como de paquetes de red (como puedan ser IP o ATM).

Este soporte multiprotocolo permite reunir bajo una misma tecnología de interconexión las funcionalidades de las redes (networking) y las de E/S de alta velocidad (principalmente memorias de masa). Adicionalmente, esta conexión de ordenadores y dispositivos de almacenamiento directamente a la red, ha hecho posible el desarrollo de una nueva forma de implementar los servidores (SAN: Storage Area Network), en que los discos o cintas ya no están asociados físicamente a un servidor concreto, pudiendo incluso estar separados a bastante distancia. Esta tecnología tiene evidentes ventajas en cuanto a la disponibilidad del sistema, recursos compartidos, etc. (permite disponer de un conjunto de servidores con acceso a un conjunto de discos compartidos, realizar operaciones de mantenimiento sin apagar los servidores y sin impedir el acceso de éstos a otros dispositivos sobre la red, realizar copias de seguridad hacia dispositivos físicamente separados y situados en distintos lugares seguros, etc, etc.).

FC puede operar sobre cable y sobre fibra óptica a distancias de hasta 10 Kms sin uso de repetidores. Es una tecnología única en cuanto a las múltiples e interoperables topologías que soporta, que pueden ser Punto-a-punto,

Fabric conmutado y Arbitrated Loop (FC-AL), y que ofrece diferentes Clases de Servicio para un mayor control sobre las prestaciones y características de transmisión de datos de cada aplicación particular. Las Clases de Servicio incluyen servicios orientados a conexión (conmutación de circuitos) y orientados a no conexión (conmutación de paquetes), pudiendo elegir combinaciones con notificación y sin notificación de entrega, circuitos virtuales con reserva de ancho de banda y especificación de latencia máxima (QoS) y funciones de multicast, broadcast y hunt groups (cualquiera-de-un-grupo-a-cualquiera-en-otro-grupo). Por último, el tamaño de paquete variable desde 0 hasta 2,112 octetos lo hace ideal para aplicaciones de almacenamiento, video, gráficos y grandes transferencias de información con memorias de masa.

La información adicional (overhead) introducida por el protocolo, incluyendo el factor introducido por la codificación serie, es tan bajo que a la velocidad de enlace (1.0625 Gbps exactamente) se obtienen tasas de transferencias reales de datos ligeramente por encima de los 100 MB/s, lo que significa casi un 80% de eficiencia. Adicionalmente, la tecnología FC utiliza fibras independientes para transmisión y recepción, lo que permite que los dispositivos fullduplex puedan transmitir y recibir simultáneamente y puedan llegar a realizar transferencias hasta a 200 MB/s.

Comparado con protocolo SCSI Paralelo, en FC todas las transferencias se realizan a la velocidad máxima de enlace, al contrario de lo que sucede en SCSI en que sólo las transferencias de datos se realizan a la máxima velocidad, mientras que el resto de las fases (comando, estado, mensaje) se realizan de forma asíncrona y mediante la intervención del firmware de ambos dispositivos, por lo que la eficiencia es significativamente más baja que en FC.

Comparado con protocolos de red basados en un stack SW, FC es un interfaz cuya arquitectura permite realizar una cantidad significativa de proceso en HW, con lo que se obtienen unas prestaciones superiores a las de aquéllos. Por último, actualmente ya están aprobadas velocidades de enlace a 2 y 4 Gbps sobre fibra óptica, lo que unido a que la tecnología de interconexión entre nodos evita por definición las colisiones (y las correspondientes pérdidas de tiempo) tan habituales en otras topologías, hacen de FC un interfaz realmente rápido.

Este conjunto de características de soporte multiprotocolo, conectividad y velocidad, unidas a la posibilidad de interconectar más de 16 millones de nodos en un dominio, hacen de FC una tecnología ideal para interconexión de sistemas (ordenadores y dispositivos de almacenamiento) a nivel de edificios y de campus. En caso necesario, FC permite la conectividad con otras redes a través de puertas de enlace (gateways), y cuando se precisen conexiones a muy larga distancia, FC permite que se puedan implementar los enlaces entre los conmutadores (ISLs, Inter-Switch Links) por medio de enlaces no FC, como por ejemplo, alquilando los servicios de un operador de telecomunicaciones, con lo que un dominio FC puede expandirse a nivel regional, nacional o internacional.

**Capas del Canal de fibra**

El Canal de fibra es un protocolo con 5 capas, llamadas:

FC0 La capa física, que incluye los cables, la óptica de la fibra, conectores, etc.

FC1 La capa de enlace de datos, que implementa la codificación y decodificación de las señales.

FC2 La capa de red, definida por el estándar FC-PI-2, que constituye el núcleo de Fibre Channel y define los protocolos principales.

FC3 La capa de servicios comunes, una fina capa que puede implementar funciones como el cifrado o RAID.

FC4 La capa de mapeo de protocolo, en la que otros protocolos, como SCSI, se encapsulan en unidades de información que se entregan a la capa FC2.

 FC0, FC1 y FC2 también se conocen como FC-PH, las capas físicas de fibre channel.

Las implementaciones del Canal de fibra están disponibles a 1 Gbps, 2 Gbps y 4 Gbps. Un estándar a 8 Gbps está en desarrollo. Un desarrollo a 10 Gbps ha sido ratificado, pero en este momento sólo se usa para interconectar switches. No existen todavía iniciadores ni dispositivos de destino a 10 Gbps basados en el estándar. Los productos basados en los estándares a 1, 2, 4 y 8 Gbps deben ser interoperables, y compatibles hacia atrás; el estándar a 10 Gbps, sin embargo, no será compatible hacia atrás con ninguna de las implementaciones más lentas.

**Puertos**

En el Canal de fibra se definen los siguientes puertos:

E\_port es la conexión entre dos switches fibre channel. También conocida como puerto de expansión, cuando dos E\_ports entre dos switches forman un enlace, ese enlace se denomina enlace de InterSwitch o ISL.

EX\_port es la conexión entre un router de Canal de fibra y un switch de Canal de fibra. En el extremo del switch, el puerto es como el de un E\_port, pero en el extremo del router es un EX\_port.

F\_port es una conexión de medios en una topología conmutada. Un puerto F\_port no se puede utilizar para un bucle de dispositivo.

FL\_port es la conexión de medios en un bucle público en una topología de anillo arbitrado. También conocido como puerto de bucle. Nótese que un puerto de switch pude convertirse automáticamente en unF\_port o un FL\_port dependiendo de qué se esté conectando.

G\_port o puerto genérico en un switch puedo operar como E\_port o F\_port.

L\_port es el término genérco utilizado para cualquier tipo de puerto de bucle, NL\_port o FL\_port. También conocido como puerto de bucle.

N\_port es la conexión de nodo de los servidores o dispositivos de almacenamiento en una topología conmutada. También se conoce como puerto de nodo.

NL\_port es la conexión de nodo de los servidores o dispositivos de almacenamiento en una topología de anillo arbitrado. También conocido como puerto de bucle de nodo.

TE\_port es un término utilizado para múltiples puertos E\_ports unidos juntos para crear un ancho de banda mayor entre switches. También conocidos como puertos de expansión trunking.

**Access Point**

También llamado sólo AP, Access Point traducido significa punto de acceso. Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Area Network), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

|  |
| --- |
| **Características generales del Access Point** |
| + Permiten la conexión de dispositivos inalámbricos a la WLAN, como: [teléfonos celulares modernos](http://www.informaticamoderna.com/Celular.htm), [Netbook](http://www.informaticamoderna.com/Netbook.htm), [Laptop](http://www.informaticamoderna.com/Laptop.htm), [PDA](http://www.informaticamoderna.com/PDA.htm), [Notebook](http://www.informaticamoderna.com/Notebook.htm) e inclusive otros Access Point para ampliar las redes. |
| + También cuentan con soporte para redes basadas en alambre (LAN - Local Area Network), que tienen un puerto RJ45 que permite interconectarse con [Switch inalámbrico](http://www.informaticamoderna.com/Switch_inal.htm) y formar grandes redes entre dispositivos convencionales e inalámbricos. |
| + La tecnología de comunicación con que cuentan es a base de ondas de radio, capaces de traspasar muros, sin embargo entre cada obstáculo esta señal pierde fuerza y se reduce su cobertura. |
| + El Access Point puede tener otros servicios integrados como [expansor de rango](http://www.informaticamoderna.com/Expansor.htm) y ampliar la cobertura de la red. |
| + Cuentan con un alcance máximo de cobertura, esto dependiendo el modelo, siendo la unidad de medida el radio de alcance que puede estar desde 30 metros (m) hasta más de 100 m. |
| + Cuentan con una antena externa para la correcta emisión y recepción de ondas, así por ende, una correcta transmisión de la información. |
|  |

**Función Bridge**

Una red inalámbrica tiene una doble función: interconectar computadoras y dispositivos cercanos entre sí y la segunda es la de proveer de servicios de Internet a los dispositivos. Un [servidor](http://www.informaticamoderna.com/Servidor.htm) ó un Módem inalámbrico de un proveedor de Internet es el encargado de recibir la señal y distribuirla a la red local. Sin embargo, el servidor cuenta con un sistema operativo específico (Novell®, Microsoft Windows NT®, Linux Apache, etc.) y cada dispositivo que se conecta a la red cuenta con el propio.

     Los [sistemas operativos](http://www.informaticamoderna.com/Sist_Ope.htm) básicamente son incompatibles entre sí y los usuarios que acceden a la red local generalmente tendrán en sus dispositivos sistemas operativos muy diferentes a los del servidor como: MacOS® Leopard, Linux Ubuntu, GoogleOS® Chrome, Microsoft® Windows Vista, etc.; es en este momento en el que un dispositivo como el Access Point puede funcionar como puente entre todos ellos y evitar que se interrumpa la comunicación, lo que hace es permitir la comunicación entre dispositivos a pesar de las diferentes plataformas, siendo cada una la encargada de interpretar los datos recibidos.  También permite evaluar la información, realizando actividades de limpieza, seguridad y filtro con la información, así como descongestionador de redes dividiendo las redes en subredes y enviando la información de manera paralela y por lo tanto mas velozmente.

**Partes que componen un Access Point**

Internamente cuenta con todos los circuitos electrónicos necesarios para la conexión inalámbrica, externamente cuenta con las siguientes partes:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | |  | | --- | | **1.- Cubierta:** se encarga de proteger los circuitos internos y da estética al producto. | | **2.- Indicadores:** permiten visualizar la actividad en la red. | | **3.- Antena:** recibe y envía la señal de manera más fiable. | | **4.- Conector RJ45:** permite interconectar la red inalámbrica con una red basada en cables. | | **5.- Conector DC:** recibe la corriente eléctrica desde un adaptador AC/DC, necesario para su funcionamiento. | |

# Acces Point Marca Zonet Modelo Zew3003

**Características.**

* Soporta los estándares IEEE 802.11g, 802.11b
* Proporciona los modos, AP, Cliente, WDS, AP+WDS, y repetidor
* Proporcione 1 puerto LAN con Auto-Negociación 10/100M, y soporte auto MDI/MDIX
* Soporta las siguientes velocidades inalámbricas de transferencia de datos 54/48/36/24/18/12/11/9/6/5.5/2/1
* Soporta servidor DHCP
* Soporta administración remota y web
* Soporta los estándares de seguridad inalámbrica WEP 64/128 y WPA/WPA2
* Soporta actualización del firmware
* Antena desmontable (conector SMA invertido)

Funciones:

* La red inalámbrica 802.11n de gran velocidad y sumamente segura ofrece rendimiento mejorado y rango extendido para aplicaciones con uso intensivo del ancho de banda.
* La instalación y la configuración basadas en asistente permiten la implementación rápida y simple.
* La seguridad sólida, que incluye WPA2, 802.1X con autenticación RADIUS segura y detección de puntos de acceso dudosos, ayuda a proteger la información confidencial de la empresa.
* La compatibilidad con PoE permite la instalación sencilla sin los gastos relacionados con cableados adicionales.
* El modo "puente cliente" le permite expandir la red mediante conexión inalámbrica a una segunda red Ethernet.
* El diseño compacto y elegante con kit de montaje versátil y antenas internas permite la instalación en techos, paredes o escritorios.
* La QoS inteligente en todos los modelos prioriza el tráfico de la red para optimizar al máximo el rendimiento de las aplicaciones más importantes.
* Las funciones de control de puertos y modo inactivo que ahorran energía ayudan a maximizar la eficacia energética.
* El acceso sumamente seguro de usuarios temporales ayuda a ofrecer conectividad inalámbrica segura para los usuarios temporales.
* La compatibilidad con IPv6 le permitirá implementar aplicaciones de red y sistemas operativos futuros
* sin actualizaciones costosas

|  |
| --- |
| **Linksys WAP54G** |
| • **Menos es más** Agregue funciones inalámbricas a su red con cables y disfrute de la comodidad que supone eliminar la necesidad de cables. Agregue dispositivos inalámbricos a su red. Menos cables, más eficiencia.  • **Comodidad inalámbrica** Ya dispone de la red, ahora sólo tiene que mejorarla mediante un punto de acceso Wireless-G de hasta 54 Mbps. Ya puede ampliar su red añadiéndole más ordenadores, impresoras y otros dispositivos inalámbricos. Ahora es mucho más fácil y no tendrá que utilizar ni un solo cable. También es compatible con dispositivos Wireless-B. Una conexión de confianza que le permite desplazar sus ordenadores portátiles o configurar sus dispositivos desde cualquier parte de la casa o la oficina. También puede añadir puntos de acceso a dos redes distintas y crear conectividad de “cable inalámbrico” entre ellos.  • **Fácil configuración** Sólo hay que pulsar un botón para configurarlo, por lo que añadir dispositivos a su nueva red inalámbrica es muy sencillo. Pulse el botón del punto de acceso y de los demás dispositivos inalámbricos con Secure Easy Setup para crear automáticamente la conexión inalámbrica. Configurar los parámetros de seguridad y el dispositivo mediante la utilidad de configuración basada en el explorador resulta muy sencillo.  • **Seguridad completa** Trabaje con total confianza. La encriptación de seguridad industrial le ayuda a mantener protegidas y en privado sus comunicaciones. El filtro de acceso le permite controlar quién accede a su red inalámbrica. |

|  |
| --- |
| **Características Principales** |
| • IEEE 802.11g soporta velocidades de transferencia de datos de hasta 54 Mbps • Compatible con versiones anteriores de los dispositivos IEEE 802.11b existentes • Configuración inalámbrica sencilla con el botón SecureEasySetup • Soporta seguridad WPA y encriptación WEP de 64/128 bits • Interfaz de usuario web incorporada para una configuración sencilla desde cualquier explorador web • Firmware actualizable mediante explorador web • Soporta las funciones de puente inalámbrico, repetidor inalámbrico, filtrado de direcciones MAC y registro de sucesos |

**ISL**

**Inter Switch Link** (**ISL**) es un protocolo propietario de [Cisco](https://es.wikipedia.org/wiki/Cisco) que mantiene información sobre [VLANs](https://es.wikipedia.org/wiki/VLAN) en el tráfico entre routers y switches.

Este método de encapsulación sólo es soportado en los equipos Cisco a través de los enlaces Fast y Gigabit Ethernet. El tamaño de las tramas ISL puede variar entre 94 bytes y 1548 bytes debido a la sobrecarga (campos adicionales) que el protocolo crea en la encapsulación.

Es el método de encapsulación de [Cisco](https://es.wikipedia.org/wiki/Cisco) para las [VLAN](https://es.wikipedia.org/wiki/VLAN) que compite con el protocolo libre (no propietario) de [IEEE 802.1Q](https://es.wikipedia.org/wiki/IEEE_802.1Q). A pesar de que en los últimos equipos de Cisco se ha dejado de incluir este protocolo en favor del protocolo de la IEEE.

### El IEEE 802.3 (Estándar de Ethernet)

**Estándares IEEE 802.3**. Fue el primer intento para estandarizar ethernet. Aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits Ethernet), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

La especificación IEEE para [Ethernet](http://www.ecured.cu/Ethernet) es la 802.3, que define qué tipo de cableado se permite y cuáles son las características de la señal que transporta. La especificación 802.3 original utilizaba un cable coaxial grueso de 50 ohm, que permite transportar una señal de 10 Mbps a 500 m. Más tarde se añadió la posibilidad de utilizar otros tipos de cables: [Coaxial](http://www.ecured.cu/Cable_coaxial) delgado; pares de cables trenzados, y [fibra óptica](http://www.ecured.cu/Fibra_%C3%B3ptica).

## **Introducción**

Una red Ethernet puede transmitir datos a 10 Mbps sobre un solo canal de banda base, generalmente un bus coaxial o una estructura ramificada. Los segmentos de cable están limitados a un máximo de 500 m. Aunque la mayoría de fabricantes especifican un máximo de 100 estaciones en cada segmento, el límite práctico puede ser menor, dependiendo de la utilización.

El número máximo de DTEs ("Data Terminal Equipment" equipo conectado a una Ethernet.) en una red Ethernet es de 1024; pueden utilizarse repetidores para aumentar la longitud de la red conectando varios segmentos, pero el número máximo de repetidores que puede encontrar una señal es de 2.

## **Principales estándares utilizados en Ethernet**

Nota: los distintos estándares Ethernet tienen una denominación que responde a la fórmula general xBaseZ. La designación Base se refiere a "Baseband modulation", que es el método de modulación empleado. El primer número X, indica la velocidad en Megabits por segundo sobre el canal (que es distinta de la velocidad disponible para datos, ya que junto a estos se incluyen los "envoltorios"). La última cifra (o letra) Z, señala la longitud máxima del cable en centenares de metros, o el tipo de tecnología. Por ejemplo, T significa par trenzado "Twisted (pairs)", F fibra óptica "Fiber", etc.

### 10Base5

Error al crear miniatura: Falta archivo

Ethernet de coaxial grueso 10Base 5

Conocido como Ethernet de cable grueso. 10 Mbps, de banda base. Puede ser identificado por su cable amarillo. Utiliza cable coaxial grueso; el 5 viene de la longitud máxima del segmento que son 500 m. El cable debe estar unido a tierra en un solo punto.

Cada estación está unida al cable mediante un tranceptor denominado MAU ("Medium Attachment Unit") y un cable de derivación. El conector usado en los adaptadores 10Base5 se denomina AUI ("Attachment Unit Interface"). Tiene un aspecto similar al de un puerto serie con 15 patillas (DB15).

Los transceptores no deben estar situados a menos de 8.2 piés (2.5 metros) entre sí, y el cable de derivación no debe exceder de 165 piés (50 metros). Si se utiliza un cable de derivación de alta flexibilidad esta longitud deben ser reducida a 41 piés (12.5 metros).

Nota: algunos tranceptores tienen circuitos que deben ser tenidos en cuenta al contar estas longitudes; lo que se denomina "Longitud Equivalente".

### 10Base2

Conocido como Ethernet de cable fino cuya designación comercial es RG-58. 10 Mbps, banda base; utiliza conectores BNC ("Bayonet Nut connector"). Su distancia máxima por segmento es de 606 pies (185 m), aunque pueden utilizarse repetidores para aumentar esta distancia siempre que los datos no pasen por más de dos repetidores antes de alcanzar su destino.

El número de DTEs en cada segmento no debe ser mayor de 30, y deben estar separados por un mínimo de 1.6 pies (0.5 metros).

Nota: en la práctica esta distancia mínima debe ser mucho mayor. El autor ha encontrado fallos de conexión absolutamente inexplicables utilizando este tipo de cable, que sencillamente han desaparecido manteniendo esta distancia (longitud de cable) superior a 4 o 5 metros.

Utiliza cable coaxial de 50 Ohm apantallado que debe estar terminado por adaptadores resistivos de 50 Ohmios y estar conectado a tierra en un punto. El cable no debe estar conectado consigo mismo formando un anillo, y debe estar conectado al DTE mediante un adaptador "T", sin que esté permitido añadir un prolongador a dicho adaptador ni conectar directamente con el DTE eliminando el adaptador "T". Su mejor atractivo es su precio, del orden del 15% del cable grueso.

Nota: este tipo de cable, muy usado hasta fechas recientes, ha cedido protagonismo en favor de las instalaciones Base-T; actualmente solo se recomienda para instalaciones muy pequeñas.

### 10Base-T

En Septiembre de 1990, el IEEE aprobó un añadido a la especificación 802.3i, conocida generalmente como 10BaseT. Estas líneas son mucho más económicas que las anteriores de cable coaxial, pueden ser instaladas sobre los cableados telefónicos UTP ("Unshielded Twister Pairs") existentes [3], y utilizar los conectores telefónicos estándar RJ-45 (ISO 8877), lo que reduce enormemente el costo de instalación (H12.4.2).

Estos cables se conectan a una serie de "hubs", también conocidos como repetidores multipuerto, que pueden estar conectados entre sí en cadena o formando una topología arborescente, pero el camino de la señal entre dos DTEs no debe incluir más de cinco segmentos, cuatro repetidores (incluyendo AUIs opcionales), dos tranceptores (MAUs) y dos AUIs.

10 Mbps, banda base, cable telefónico UTP de 2 pares de categoría 3, 4 o 5, con una impedancia característica de 100 +/-15 ohms a 10 Mhz [4]; no debe exceder de 328 pies (100 m).

Cuando una red contenga cinco segmentos y cuatro repetidores, el número de segmentos coaxiales no debe ser mayor que tres, el resto deben ser de enlace con DTEs (es lo que se conoce como regla 5-4-3). Dicho de otra forma: Entre cualquier par de estaciones no debe haber más de 5 segmentos, 4 repetidores y 3 conexiones hub-hub. Si se utilizan segmentos de fibra óptica, no deben exceder de 1640 pies (500 metros).

Cuando una red contenga cuatro segmentos y tres repetidores utilizando enlaces de fibra óptica, los segmentos no deben exceder de 3280 pies (1000 metros).

### 10Base-F

10 Mbps, banda base, cable de fibra óptica. Longitud máxima del segmento 2000 metros.

### 100Base-T4

Fast Ethernet a 100 Mbps, banda base, que utiliza par trenzado de 4 pares de categoría 3, 4 o 5. Distancia máxima 100 m.

### 100Base-TX

Fast Ethernet a 100 Mbps, banda base, utiliza par trenzado de 2 pares de categoría 5. Distancia máxima 100 m.

### 100Base-FX

Fast Ethernet a 100 Mbps que utiliza fibra óptica. Longitud máxima del segmento 2000 metros.

### 10GBaseT

En Junio de 2006 se aprobó el estándar 10GBaseT. Como se desprende de su nombre, se refiere a conexiones de 10 Gbit por segundo (10.000 Mbps) con una longitud máxima entre Hubs o repetidores (segmento) de 100 m. Sin embargo, a la fecha de la publicación del estándar ningún cable estandarizado cumplía con los requisitos. El de categoría 6 se adoptó inicialmente para segmentos de 55 metros pero hubo que reducirla a 37 m. Se espera que el cable de categoría 7 cumpla plenamente con las exigencias de la nueva especificación.

### Árbol de extensión

El árbol de extensión ("spanning tree") es un tipo de conexión asociado a la norma IEEE 802.3 que no requiere que las estaciones de la red mantengan un registro de las direcciones, lo que implica un menor costo de cada NIC.

**PoE**

PoE son la iniciales de Power Over Ethernet y permite la transmisión de electricidad y datos a través de cable UTP/STP. Es útil en  aquellas situaciones en las que se necesita instalar un dispositivo de red (como puede ser un Punto de Acceso inalámbrico, un teléfono IP, una cámara Ip o cualquier dispositivo de red que admita este sistema  y no haya disponible una toma de electricidad

El PoE Ethernet permite la transmisión de electricidad y datos a través de un cable UTP/STP hasta 100 m. de distancia. Esto permite a los dispositivos electrónicos instalarse en el exterior o en sitios de difícil acceso y con la necesidad de estar conectado tanto a la red eléctrica como a la red Ethernet del interior.

Existen distintas normas o protocolos, la más extendida es la 802.11af, por lo que los PoE que cumplen esta norma pueden convivir con otros muchos dispositivos que también cumplen dicha norma.

**¿De qué se compone un PoE?**

**1- El Inyector de alimentación (POE-INJAF)**

Se encarga de suministrar  la energía necesaria para todo el kit. Se conecta al enchufe de pared mediante el cable de alimentación suministrado y a través del puerto Ethernet se conecta el cable UTP (cable de red) que  recibe los datos desde el Switch. Por lo que tenemos como resultado un único cable de red que lleva el voltaje y los datos hasta el otro extremo llamado Terminal o splitter.

Estos aparatos suelen tener una entrada entre 100V – AC 240V y una salida (por el cable de red) entre 15 y 48V, una eficiencia entre el 70 y 90% y en algunos casos contra cortocircuitos, sobrecargas y picos de tensión. Pueden soportar temperaturas entre 0ºC a 60ºC los de interior y de -10ºC a 70ºC los de exterior con humedades relativas entre 5% a 90%, aunque estos parámetros varían con los modelos.

**Sistemas operativos para switches**

**Cisco IOS** (originalmente **Internetwork Operating System**) es el software utilizado en la gran mayoría de [routers](https://es.wikipedia.org/wiki/Router) (encaminadores) y[switches](https://es.wikipedia.org/wiki/Switch) (conmutadores) de [Cisco Systems](https://es.wikipedia.org/wiki/Cisco_Systems) (algunos conmutadores obsoletos ejecutaban [CatOS](https://es.wikipedia.org/w/index.php?title=CatOS&action=edit&redlink=1)). IOS es un paquete de funciones de enrutamiento, conmutamiento, trabajo de internet y telecomunicaciones que se integra estrechamente con un sistema operativo [multitarea](https://es.wikipedia.org/wiki/Multitarea).

La interfaz de línea de comandos de IOS (IOS CLI) proporciona un conjunto fijo de [comandos](https://es.wikipedia.org/wiki/Comando_(inform%C3%A1tica)) de múltiples palabras. El conjunto disponible se determina mediante el "modo" y el nivel de privilegios del usuario actual. El modo "Global configuration" proporciona comandos para cambiar la configuración del sistema y el modo "interface configuration" a su vez, proporciona comandos para cambiar la configuración de una interfaz específica. A todos los comandos se les asigna un *nivel de privilegios*, de 0 a 15, y pueden ser accedidos por usuarios con los privilegios necesarios. A través de la CLI, se pueden definir los comandos disponibles para cada nivel de privilegio.

## **Arranque del IOS**

Al arrancar un dispositivo de Cisco este realiza un Bootstrap (comprobación de hardware).

Después intentará cargar una imagen IOS desde la memoria Flash o desde un servidor TFTP. En el caso de no hallarla ejecutará una versión reducida de la IOS ubicada en la ROM.

Tras el arranque del sistema localizará la configuración del mismo, generalmente en texto simple. Puede estar ubicada en la memoria NVRAM o en un servidor de TFTP. En el caso de no encontrarla iniciará un asistente de instalación (modo Setup).

Con la siguiente imagen puede quedar más claro:

## **VLAN**

Una red de área local (LAN) está definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder tener una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente. La solución a este problema era la división de la LAN en segmentos físicos los cuales fueran independientes entre si, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma. La necesidad de confidencialidad como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs. Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación.

La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control más inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

## **Ventajas de la VLAN**

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

* mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores;
* aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza;
* disminución en la transmisión de tráfico en la red.

## Segmentación

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica microsegmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Una de las ventajas que se pueden notar en las VLAN es la reducción en el trafico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol (VTP) es el que se utiliza para esta conexión, el VTP puede ser utilizado en todas las líneas de conexión incluyendo ISL, IEEE 810.10. IEEE 810.1Q y ATM LANE.

## **Tipos de VLAN**

### VLAN de puerto central

Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

### VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo.

### Por puerto

Se configura por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. Para la Figura 1 tendríamos en el Switch 9 puertos de los cuales el 1,5 y 7 pertenecen a la VLAN 1; el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3

Ventajas:

* Facilidad de movimientos y cambios.
* Microsegmentación y reducción del dominio de Broadcast.
* Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

* Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

### Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

Ventajas:

* Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
* Multiprotocolo.
* Se pueden tener miembros en múltiples VLANs.

Desventajas:

* Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.
* Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

### Por protocolo

Asigna a un protocolo una VLAN. El switch se encarga de dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente (Figura 4).

Ventajas:

* Segmentación por protocolo.
* Asignación dinámica.

Desventajas

* Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
* No soporta protocolos de nivel 2 ni dinámicos.

### Por direcciones IP

Está basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Ventajas:

* Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

Desventajas:

* El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
* Pérdida de tiempo en la lectura de las tablas.
* Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

### Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

Ventajas:

* Facilidad de movimiento de los integrantes de la VLAN.
* Multiprotocolo.

Desventajas:

* En corporaciones muy dinámicas la administración de las tablas de usuarios.

### VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

### Capa de Red: ELAN o Redes LAN Emuladas

Si bien el concepto de VLAN se creó para las redes LAN, la necesidad llevo a ampliar los horizontes con el crecimiento de las redes ATM. Para los administradores de las VLAN se crearon una serie de estándares para simular en una red ATM una VLAN. Por un lado una tecnología orientada a no conexión, qué es el caso de las LANS y por el otro una orientada a conexión como en el caso de ATM. En el caso de las LANS se trabaja con direcciones MAC, mientras en ATM se usan direcciones ATM y se establecen circuitos virtuales permanentes, por esta razón se requiere hacer cambios de direcciones MAC a ATM.

Ventajas:

* Facilidad de administración.
* Facilidad de movimientos y cambios.
* Multiprotocolo.

Desventajas:

* Aplicable solo a Ethernet y Token Ring.
* No explota la calidad de Calidad de servicio (QoS) de ATM.

### Enrutamiento entre VLANs

Cuando creamos VLANs, agrupamos varios dispositivos en un mismo dominio de broadcast, totalmente aislado del resto. Por ello, cada VLAN debe tener un direccionamiento IP **diferente** al de todas las demás.

Si queremos que puedan comunicarse las VLANs entre sí, es necesario contar con un dispositivo de capa 3 que enrute los paquetes, ya sea un switch multicapa o un **router**.

Si conectamos un router a un switch para que sean capaz de enrutar estos paquetes, la interfaz del router será un enlace troncal con el switch configurado como **“router-on-a-stick**” que, básicamente, es una única interfaz física con una serie de subinterfaces para comunicar una VLAN con otra. Su funcionamiento es simple, acepta las tramas etiquetadas a través del troncal y las conmuta entre las diferentes subinterfaces (interfaces lógicas o virtuales que pertenecen a cada una de las VLANs configuradas en el switch) para enviarlas a la VLAN que corresponda.

Cada una de las subinterfaces deberá tener una dirección IP del rango de la VLAN a la que pertenece y hará de su **puerta de enlace**.

Si en lugar de un router conectamos un **switch multicapa**, no necesitamos un dispositivo dedicado para este enrutamiento, sino que el propio switch puede llevar a cabo esa labor porque trabaja con las capa 2 y 3. Para ello, el switch debe tener habilitado el enrutamiento IP.

Un switch multicapa tiene ciertas **ventajas** con respecto a un router, como por ejemplo que puede enrutar más rápido el tráfico entre VLANs ya que lo hace internamente a nivel de hardware, mientras que un router tiene que compartir un solo enlace troncal para todas las VLANs. En ese caso, será la propia velocidad del enlace la que marque la velocidad de transmisión.

Sin embargo, también hay **desventajas**: un router puede tener funcionalidades de seguridad que un switch multicapa no tiene.

### Enrutamiento entre VLANs heredado

Antiguamente, para poder realizar el enrutamiento entre diferentes VLANs, la única posibilidad era que el router conectado al switch tuviera una interfaz física por cada una de las VLANs. Estas**interfaces físicas**estaban configuradas como interfaces de acceso y no troncales, como si se tratara de un dispositivo final con una IP del rango de cada VLAN. Esta IP sería la puerta de enlace correspondiente a cada una de las VLANs para el resto de dispositivos.

Para **configurar** este tipo de enrutamiento, simplemente debemos configurar, por ejemplo, todos los puertos pertenencientes a la VLAN 10, incluyendo uno de los enlaces con el router como si fuera un puesto de trabajo más, con el siguiente comando en el switch:  
sw1(config-if)# switchport access vlan 10 (Esto creará la VLAN 10 automáticamente en el switch)  
Y configurar la interfaz del router como se hace normalmente, aplicándole una IP del rango de la VLAN 10 y levantándola con:  
R1(config-if)# ip address 172.17.10.1 255.255.255.0  
R1(config-if)# no shutdown

### Enrutamiento entre VLANs router-on-a-stick

El problema principal del enrutamiento heredado es que, cuando tenemos muchas VLANs creadas en el entorno, necesitamos el mismo número de interfaces en el router, y esto a veces es **inviable**.

Por ello, se usa este modo de configuración de enrutamiento entre VLANs, donde se asignan interfaces lógicas, o **subinterfaces**, a una única interfaz física como troncal y todo el tráfico VLAN pasa por ellas.

Cada una de estas subinterfaces se configura de manera independiente, con una dirección IP y máscara del **rango de red** de la VLAN a la que pertenece.

El **funcionamiento** real es el mismo que en el enrutamiento heredado, cuando se recibe un paquete, se comprueba la dirección IP de destino y se enruta, según la información que tenga el router en su tabla de enrutamiento, pero por la subinterfaz correspondiente, en lugar de la interfaz física.

Para **configurarlo**, primero es necesario hacer que el enlace entre el router y el switch sea troncal. Para ello usamos el siguiente comando (el router no acepta DTP):  
Sw1(config-if)# switchport mode trunk

Una vez que ya tenemos el enlace como troncal y, asumiendo que la VLAN nativa es la 1, por defecto, vamos a configurar el router.  
Creamos cada una de las **subinterfaces** sobre la interfaz gigabitEthernet 0/0. Para ello se suele usar el mismo número que la VLAN a la que pertenecerá para una mejor organización:  
R1(config)# interface g0/0.10  
Debemos configurar la encapsulación 802.1Q en la subinterfaz para la VLAN a la que pertenecerá (en el ejemplo la 10):  
R1(config-if)# encapsulation dot1q 10  
Configuramos una IP y su máscara del rango de la VLAN:  
R1(config-if)# ip address 172.17.10.1 255.255.255.0

No es necesario habilitar las subinterfaces una a una, sino que debemos **levantar** la interfaz física para habilitarlas todas a la vez:  
R1(config)# interface g0/0  
R1(config-if)# no shutdown

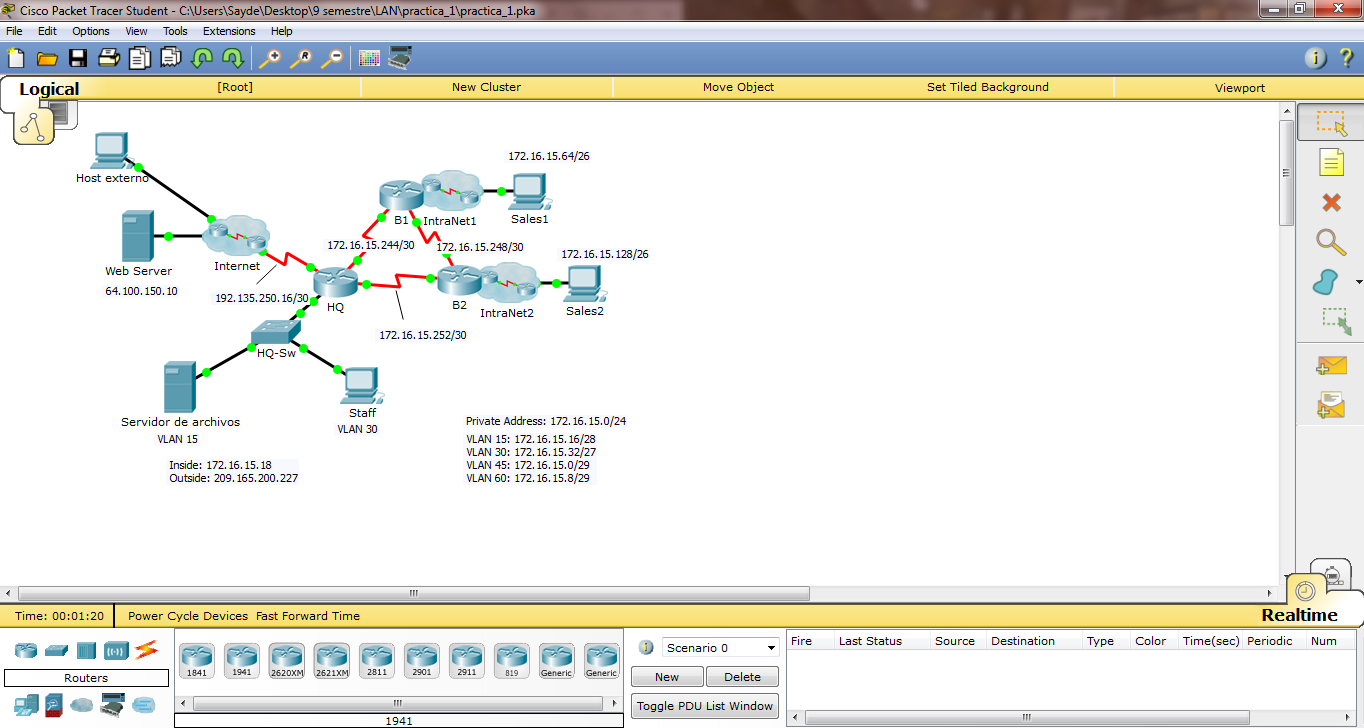
#### **Verificando la configuración**

Con el comando show vlans podemos ver todas las VLANs configuradas en el router y a qué subinterfaz está asociada, incluyendo el tipo de encapsulación que se lleva a cabo y la IP de la subinterfaz. En la imagen se aprecian las VLANs 10 y 30.

Para verificar la **conectividad** entre VLANs, lo ideal es realizar un ping o un tracert de un PC de una VLAN al de otra.

Un error común al configurar una subinterfaz es introducir el **ID de VLAN** erróneo. Con el comando show interfaces, también podemos comprobarlo.

**#1.3.1.3**



**SWITCH HQ-SW:**

HQ-Sw#sh run

Building configuration...

Current configuration : 2919 bytes

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

hostname HQ-Sw

ip ssh version 2

ip ssh authentication-retries 2

ip ssh time-out 60

ip domain-name cisco.com

!

username Admin privilege 1 password 7 082D495A041C0C19

username HQadmin privilege 1 password 7 0822455D0A16061B13181F

spanning-tree mode pvst

!

interface FastEthernet0/1

switchport access vlan 30

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security violation restrict

switchport port-security mac-address sticky 0001.C90E.8923

!

interface FastEthernet0/2

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/3

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/5

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/6

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/7

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/8

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/10

switchport access vlan 30

switchport mode access

shutdown

!

interface FastEthernet0/11

switchport access vlan 15

switchport mode access

!

interface FastEthernet0/12

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/19

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 15

switchport mode access

shutdown

!

interface FastEthernet0/21

shutdown

!

interface FastEthernet0/22

shutdown

!

interface FastEthernet0/23

shutdown

!

interface FastEthernet0/24

shutdown

interface GigabitEthernet0/1

switchport trunk native vlan 45

switchport mode trunk

interface GigabitEthernet0/2

shutdown

interface Vlan1

no ip address

shutdown

interface Vlan60

ip address 172.16.15.10 255.255.255.248

ip default-gateway 172.16.15.9

line con 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

end

**ROUER HQ:**

HQ>ena

HQ#sh run

Building configuration...

Current configuration : 2151 bytes

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname HQ

ip dhcp excluded-address 172.16.15.33

ip dhcp pool LAN

network 172.16.15.32 255.255.255.224

default-router 172.16.15.33

ip cef

no ipv6 cef

license udi pid CISCO1941/K9 sn FTX1524OT6M

spanning-tree mode pvst

interface GigabitEthernet0/0

no ip address

duplex auto

speed auto

!

interface GigabitEthernet0/0.15

encapsulation dot1Q 15

ip address 172.16.15.17 255.255.255.240

ip nat inside

!

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 172.16.15.33 255.255.255.224

ip nat inside

!

interface GigabitEthernet0/0.45

encapsulation dot1Q 45 native

ip address 172.16.15.1 255.255.255.248

ip nat inside

!

interface GigabitEthernet0/0.60

encapsulation dot1Q 60

ip address 172.16.15.9 255.255.255.248

ip nat inside

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 172.16.15.245 255.255.255.252

ip nat inside

clock rate 2000000

!

interface Serial0/0/1

ip address 172.16.15.254 255.255.255.252

ip nat inside

!

interface Serial0/1/0

ip address 192.135.250.18 255.255.255.252

ip nat outside

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

interface Vlan1

no ip address

shutdown

router ospf 1

router-id 1.1.1.1

log-adjacency-changes

passive-interface GigabitEthernet0/0

passive-interface Serial0/1/0

passive-interface GigabitEthernet0/0.15

passive-interface GigabitEthernet0/0.30

passive-interface GigabitEthernet0/0.45

passive-interface GigabitEthernet0/0.60

network 172.16.15.0 0.0.0.255 area 0

default-information originate

ip nat pool Public 209.165.200.225 209.165.200.226 netmask 255.255.255.224

ip nat inside source list 1 pool Public overload

ip nat inside source static 172.16.15.18 209.165.200.227

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/1/0

ip flow-export version 9

access-list 1 permit 172.16.15.0 0.0.0.255

line con 0

exec-timeout 0 0

line aux 0

line vty 0 4

login

end

**CAPÍTULO 2**

**STP**

**Tormenta de broadcast**

Una tormenta de broadcast es una descripción del marco de comportamiento de las inundaciones que se produce bajo condiciones especiales en una red Ethernet. Durante una tormenta de broadcast las tramas Ethernet se encuentran atrapadas en un bucle sin fin y siguen siendo retransmitidos hasta que el conmutador de red se siente colapsado o el bucle se termina.

### El broadcast es un riesgo permanente en nuestra red, ¿porqué?

* Porque inunda la red utilizando ancho de banda innecesariamente.
* Porque insume recursos de los dispositivos que deben procesar este broadcast.
* Porque insume recursos de las terminales y servidores que reciben el broadcast y deben analizarlo.

Adicionalmente, problemas de configuración o fallos de los dispositivos o de las terminales pueden provocar la presencia de montos muy importantes de broadcast en la red que quitan recursos para el procesamiento del tráfico de datos o la operación regular de la red, bajando de modo notable su performance.  
  
Una tormenta de difusión puede consumir suficientes recursos de red con el fin de hacer que la red no puede transportar el tráfico normal.

### Causas

Por lo general la causa es un circuito de conmutación en la topología de cableado Ethernet. Como broadcast y multicast se transmiten por medio de interruptores fuera cada puerto, el conmutador o conmutadores retransmitirán repetidamente mensajes de difusión e inundar la red.  
  
En algunos casos, una tormenta de difusión puede ser instigado a los efectos de una denegación de servicio a través de uno de los ataques de amplificación de paquetes, como el ataque pitufo o ataque Fraggle, donde pitufo envía una gran cantidad de tráfico ICMP Echo Pide a una dirección de difusión, con cada paquete de eco ICMP contiene la dirección de origen de la parodia de la máquina víctima. Cuando el paquete falso llega a la red de destino, todas las máquinas de la red responden a la dirección falsa. La solicitud de eco inicial se multiplica por el número de máquinas de la red. Esto genera una tormenta de respuestas al host víctima inmovilización de ancho de banda de red, utilizando recursos de la CPU o, posiblemente, rompiendo la víctima.  
  
En las redes inalámbricas un paquete disociación falsificado con la fuente a la del punto de acceso inalámbrico y enviado a la dirección de difusión puede generar una disociación ataque DOS difusión.

El control de tormentas se configura para el switch como un todo, pero opera por puerto.  
  
El control de tormentas se encuentra inhabilitado por defecto.  
  
La prevención de las tormentas de broadcast mediante el establecimiento de valores demasiado altos o bajos de umbral descarta el tráfico MAC excesivo de broadcast, multicast o unicast. Además, la configuración de valores para elevar umbrales en un switch puede desactivar el puerto.

### Supresión de broadcast con Cisco IOS

Los switches Cisco IOS brindan un feature que permite con facilidad limitar la porción de ancho de banda que puede ser ocupada por tráfico de broadcast en cada puerto del switch. Esta función está deshabilitada por defecto. Esta función permite adicionalmente definir el modo en que cada puerto debe manejar el tráfico de broadcast que recibe: se puede descartar el tráfico de broadcast excedente por un tiempo limitado o hasta que el tráfico de broadcast que llega disminuya.

#### Un ejemplo de cómo configurar esta función en un switch Catalyst 2950:

Switch(config)#interface fastethernet 0/10  
Switch(config-if)#storm-control broadcast level 50  
Switch(config-if)#storm-control action trap  
  
El primer comando es el único requerido. En esa línea se define el tráfico que se desea limitar (también se puede utilizar para limitar tráfico de multicast o de unicast) y hasta qué nivel se tolera el mismo.  
  
La segunda línea indica la acción que se desea tomar. Si la opción buscada es que el puerto sea inhabilitado completamente, el comando será: storm-control action shutdown. Si no se especifica nada, por defecto, el comando descarta el tráfico de broadcast. También se puede solicitar que envíe un aviso de SNMP a una estación de management.

**STP y los loops**

Este protocolo se utiliza cuando nos encontramos en redes con topologías redundantes. Es en este tipo de redes que se pueden producir bucles (loops o lazos), los cuales pueden producir los siguientes problemas: • Tormentas o Inundaciones de Broadcast o Multicast. Los Broadcast en la red son enviados una y otra vez circulando sin fin en la misma, dado que en Ethernet no existe como en IP un campo TTL. Lógicamente al no eliminarse la situación se agrava con cada nuevo Broadcast. • Copias múltiples de Tramas. Con la redundancia es muy probable que un host reciba una trama repetida, dado que la trama podría llegar por dos enlaces diferentes. • Inestabilidad o Inconsistencia de Tablas de Direcciones MAC (Media Access Control, Control de Acceso al Medio). Una trama que proviene de una dirección MAC en particular podría llegar desde enlaces diferentes. Como efecto de estos problemas se reduce el tráfico de usuario y la red parecerá estar inactiva o extremadamente lenta.

**TTL**

Tiempo de Vida o Time To Live (TTL) es un concepto usado en redes de computadores para indicar por cuántos [nodos](https://es.wikipedia.org/wiki/Nodo_(inform%C3%A1tica)) pueden pasar un [paquete](https://es.wikipedia.org/wiki/Paquete_de_datos) antes de ser descartado por la red o devuelto a su origen.

El TTL como tal es un campo en la estructura del paquete del protocolo IP. Sin este campo, paquetes enviados a través de rutas no existentes, o a direcciones erróneas, estarían vagando por la red de manera infinita, utilizando ancho de banda sin una razón positiva.

El TTL o TimeToLive, es utilizado en el paquete IP de manera que los routers puedan analizarlo y actuar según su contenido. Si un router recibe un paquete con un TTL igual a uno o cero, no lo envía a través de sus puertos, sino que notifica vía [ICMP](https://es.wikipedia.org/wiki/ICMP) a la dirección IP origen que el destino se encuentra "muy alejado" y procede a descartar dicho paquete. Si un paquete es recibido por un router que no es el destino, éste decrementa el valor del TTL en uno y envía el paquete al siguiente router (next hop). En el [protocolo IP](https://es.wikipedia.org/wiki/Protocolo_IP), esta información se almacena en un campo de 8 [bits](https://es.wikipedia.org/wiki/Bit). El valor óptimo para aprovechar el rendimiento en Internet es de 128.

# Direccionamiento MAC

En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el organizationally unique identifier. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas burned-in addresses, en inglés.

En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet, usándose esta sólo a niveles internos de la red. Sin embargo, es posible añadir un control de hardware en un conmutador o un punto de acceso inalámbrico, para permitir sólo a unas MAC concretas el acceso a la red. En este caso, deberá saberse la MAC de los dispositivos para añadirlos a la lista. Dicho medio de seguridad se puede considerar un refuerzo de otros sistemas de seguridad, ya que teóricamente se trata de una dirección única y permanente, aunque en todos los sistemas operativos hay métodos que permiten a las tarjetas de red identificarse con direcciones MAC distintas de la real.

La dirección MAC es utilizada en varias tecnologías entre las que se incluyen:

* Ethernet
* 802.3 CSMA/CD
* 802.5 o redes en anillo a 4 Mbps o 16 Mbps
* 802.11 redes inalámbricas (Wi-Fi).
* Asynchronous Transfer Mode

MAC opera en la capa 2 del modelo OSI, encargada de hacer fluir la información libre de errores entre dos máquinas conectadas directamente. Para ello se generan tramas, pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

**IEEE 802.1 X**

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. Se caracteriza por tener tres participantes en su proceso: 1. Suplicante o cliente, que desea conectarse con la red. 2. El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 3. El autenticador, que es el equipo de red (switch, Acces Point) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

802.1X utiliza el Protocolo de autenticación extensible (EAP) para el intercambio de mensajes durante el proceso de autenticación y el Protocolo de autenticación extensible utilizado en la LAN (EAPoL, EAP Over LAN) usado para transportar EAP. Con EAP se utilizan métodos de autenticación arbitrarios, como contraseñas, tarjetas inteligentes o certificados para autenticar la conexión inalámbrica. La compatibilidad que 802.1x ofrece con los tipos de EAP le permite utilizar cualquiera de los siguientes métodos de autenticación.

**Balanceo de cargas en un switch**

Configurar un esquema del balanceo de carga Última actualización: De octubre el 28 de 2011 Este módulo contiene la información sobre el Cisco Express Forwarding y describe las tareas para configurar un esquema del balanceo de carga para el tráfico del Cisco Express Forwarding. El balanceo de carga permite que usted optimice los recursos distribuyendo el tráfico sobre los trayectos múltiples. Cisco Express Forwarding es una avanzada tecnología de switching IP de Capa 3. Optimiza el rendimiento y la escalabilidad de todos los tipos de redes: los que llevan pequeñas cantidades de tráfico y los que llevan grandes cantidades de tráfico en patrones complejos, como Internet y las redes caracterizados por aplicaciones en Internet o sesiones interactivas intensivas. Encontrar la información de la característica Requisitos previos para un esquema del balanceo de carga Restricciones para un esquema del balanceo de carga Información sobre un esquema del balanceo de carga. Su versión de software puede no soportar todas las características documentadas en este módulo. Para la última información y advertencias de la característica, vea los Release Note para su plataforma y versión de software. Para encontrar la información sobre las características documentadas en este módulo, y ver una lista de las versiones en las cuales se soporta cada característica, vea la tabla de información de la característica en el extremo de este documento. Utilice el Cisco Feature Navigator para encontrar la información sobre el soporte del Soporte de la plataforma y de la imagen del software de Cisco. Para acceder el Cisco Feature Navigator, vaya a www.cisco.com/go/cfn. Una cuenta en Cisco.com no se requiere. Requisitos previos para un esquema del balanceo de carga El Cisco Express Forwarding o el Distributed Cisco Express Forwarding se debe habilitar en su Switch o router. Si usted habilita el Equilibrio de carga por paquete para el tráfico que va a un destino determinado, todas las interfaces que pueden remitir el tráfico a ese destino se deben habilitar para el Equilibrio de carga por paquete. Restricciones para un esquema del balanceo de carga Usted debe global configurar el Equilibrio de carga en el linecards del Cisco 12000 Series Router E2 de la misma manera: en el por destino o el modo por paquete. No es posible (como en otras plataformas basadas en software del Cisco IOS) configurar algunos prefijos del paquete en el modo del por destino y otros en el modo por paquete. Información sobre un esquema del balanceo de carga Soporte de Plataforma de Cisco para el CEF central y el dCEF Descripción del balanceo de carga CEF Equilibrio de la carga por destino Equilibrio de carga por paquete Algoritmos del balanceo de carga Soporte de Plataforma de Cisco para el CEF central y el dCEF Cisco Express Forwarding se habilita de forma predeterminada en la mayoría de las plataformas Cisco que ejecutan el software Cisco IOS versión 12.0 o posterior. Cuando Cisco Express Forwarding se habilita en un router, el Procesador de ruteo (RP) realiza el Express Forwarding. Para descubrir si el Cisco Express Forwarding se habilita en su plataforma, ingrese el cefcommand del IP de la demostración. Si se ha habilitado Cisco Express Forwarding, la salida recibida será similar a la siguiente: Router# show ip cef Prefix Next Hop Interface [...] 10.2.61.8/24 192.168.100.1 FastEthernet1/0/0 192.168.101.1 FastEthernet6/1 [...] Si el Cisco Express Forwarding no se habilita en su plataforma, la salida para el cefcommand del IP de la demostración parece esto: Router# show ip cef %CEF not running El Distributed Cisco Express Forwarding se habilita por abandono en el Catalyst 6500 Series Switch, el Cisco 7500 Series Router, y el Cisco 12000 Series Router. Cuando se habilita Cisco Express Forwarding distribuido en su plataforma, las tarjetas de línea realizan el reenvío express. Si el Cisco Express Forwarding no se habilita en su plataforma, utilice el cefcommand del IP para habilitar el Cisco Express Forwarding (de la central) o el comando ip cef distributed de habilitar el Distributed Cisco Express Forwarding. Descripción del balanceo de carga CEF El Equilibrio de carga del Cisco Express Forwarding se basa en una combinación de origen y una información del paquete del destino; permite que usted optimice los recursos distribuyendo el tráfico sobre los trayectos múltiples. Usted puede configurar el Equilibrio de carga en un por destino o una base por paquete. Porque las decisiones de balance de carga se toman en la interfaz de salida, el Equilibrio de carga se debe configurar en la interfaz de salida. Equilibrio de la carga por destino El equilibrio de la carga por destino permite que el router utilice los trayectos múltiples para alcanzar la carga a compartir a través de las pares del host múltiples del origen de destino. Los paquetes para las pares del host dadas del origen de destino se garantizan para tomar la misma trayectoria, incluso si los trayectos múltiples están disponibles. Los flujos de tráfico destinados para diversos pares tienden a tomar diversas trayectorias. El balanceo de carga por destino se habilita de forma predeterminada al habilitar Cisco Express Forwarding. Para utilizar la carga por destino que equilibra, usted no realiza ninguna tarea adicional una vez que se habilita el Cisco Express Forwarding. El por destino es el método de balance de carga de opción para la mayoría de las situaciones. **ARP**

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo.

El protocolo de resolución de direcciones es responsable de convertir la dirección de protocolo de alto nivel (direcciones IP) a direcciones de red físicas. Primero, consideremos algunas cuestiones generales acerca de Ethernet.

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red. De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador.

Si una aplicación desea enviar datos a una determinado dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un "router") y el dispositivo hardware al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador (el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

##### ARP y subredes

El protocolo ARP es el mismo aunque haya subredes. Recordar que cada datagrama IP pasa primero por el algoritmo de encaminamiento IP. Este algoritmo selecciona el manejador de dispositivo que debería enviar el paquete. Sólo entonces se consulta al módulo ARP asociado con ese manejador.

**ICMP**

El Protocolo de Mensajes de Control y Error de Internet, ICMP, es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

El protocolo ICMP solamente informa de incidencias en la entrega de paquetes o de errores en la red en general, pero no toma decisión alguna al respecto. Esto es tarea de las capas superiores.

Los mensajes ICMP se transmiten como datagramas IP normales, con el campo de cabecera "protocolo" con un valor 1, y comienzan con un campo de 8 bits que define el tipo de mensaje de que se trata. A continuación viene un campo código, de o bits, que a veces ofrece una descripción del error concreto que se ha producido y después un campo suma de control, de 16 bits, que incluye una suma de verificación de errores de transmisión. Tras estos campos viene el cuerpo del mensaje, determinado por el contenido del campo "tipo". Contienen además los 8 primeros bytes del datagrama que ocasionó el error.  
Los principales tipos de mensaje ICMP son los siguientes:

**Mensajes informativos**

Entre estos mensajes hay algunos de suma importancia, como los mensajes de petición de ECO (tipo 8) y los de respuesta de Eco (tipo 0). Las peticiones y respuestas de eco se usan en redes para comprobar si existe una comunicación entre dos host a nivel de capa de red, por lo que nos pueden servir para identificar fallos en este nivel, ya que verifican si las capas física (cableado), de enlace de datos (tarjeta de red) y red (configuración IP) se encuentran en buen estado y configuración.

**Mensajes de error**

En el caso de obtener un mensaje ICMP de destino inalcanzable, con campo "tipo" de valor 3, el error concreto que se ha producido vendrá dado por el valor del campo "código", pudiendo presentar los siguientes valores que se muestran en la parte derecha.

Este tipo de mensajes se generan cuando el tiempo de vida del datagrama a llegado a cero mientras se encontraba en tránsito hacia el host destino (código=0), o porque, habiendo llegado al destino, el tiempo de reensamblado de los diferentes fragmentos expira antes de que lleguen todos los necesarios (código=1).

Los mensajes ICMP de tipo= 12 (problemas de parámetros) se originan por ejemplo cuando existe información inconsistente en alguno de los campos del datagrama, que hace que sea imposible procesar el mismo correctamente, cuando se envían datagramas de tamaño incorrecto o cuando falta algún campo obligatorio.

Por su parte, los mensajes de tipo=5 (mensajes de redirección) se suelen enviar cuando, existiendo dos o más routers diferentes en la misma red, el paquete se envía al router equivocado. En este caso, el router receptor devuelve el datagrama al host origen junto con un mensaje ICMP de redirección, lo que hará que éste actualice su tabla de enrutamiento y envíe el paquete al siguiente router.

**PDU**

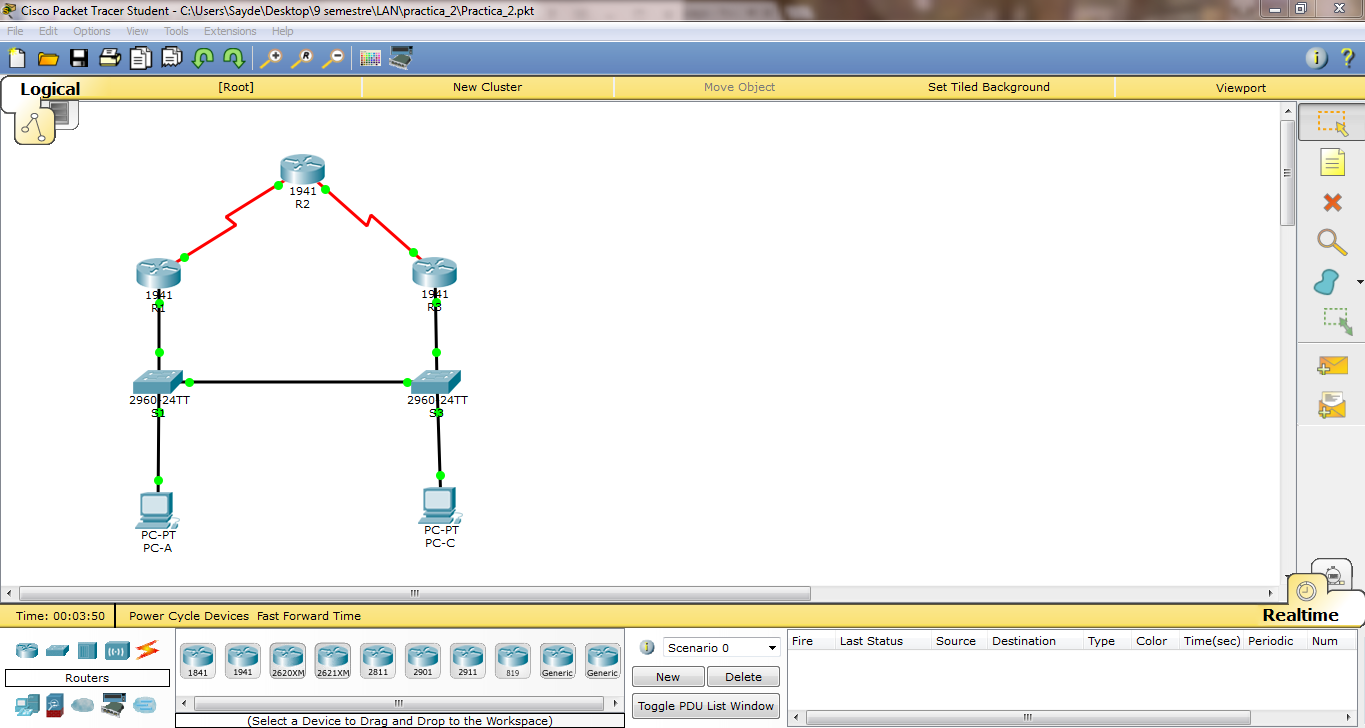
Las **unidades de datos de protocolo**, también llamadas **PDU**, se utilizan para el intercambio de datos entre unidades disparejas, dentro de una capa del [modelo OSI](https://es.wikipedia.org/wiki/Modelo_OSI). Existen dos clases:

* PDU de datos, que contiene los datos del usuario principal (en el caso de la capa de aplicación) o la PDU del nivel inmediatamente inferior.
* PDU de control, que sirven para gobernar el comportamiento completo del [protocolo](https://es.wikipedia.org/wiki/Protocolo_de_comunicaciones) en sus funciones de establecimiento y unión de la conexión, control de flujo, control de errores, etc. No contienen información alguna proveniente del nivel N+1.

Cada capa del modelo OSI en el origen debe comunicarse con capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicación de par-a-par.

Durante este proceso, cada protocolo de capa intercambia información en lo que no se conoce como unidades de datos, entre capas iguales. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

**#2.4.3.4**



**S1**

Switch>ena

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostaname S1

^

% Invalid input detected at '^' marker.

Switch(config)#hostname S1

S1(config)#int vlan 1

S1(config-if)#ip add 192.168.1.11 255.255.255.0

S1(config-if)#exit

S1(config)#ip default.gateway 192.168.1.1

^

% Invalid input detected at '^' marker.

S1(config)#ip default-gateway 192.168.1.1

S1(config)#

S1>ena

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#ip default-gateway 192.168.1.254

S1(config)#

**S2**

Switch>ena

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname S3

S3(config)#int vlan 1

S3(config-if)#ip add 192.168.1.13 255.255.255.0

S3(config-if)#exit

S3(config)#ip default.gateway 192.1.3

^

% Invalid input detected at '^' marker.

S3(config)#ip default-gateway 192.1.3

^

% Invalid input detected at '^' marker.

S3(config)#ip default-gateway 192.1658.1.3

^

% Invalid input detected at '^' marker.

S3(config)#ip default-gateway 192.168.1.3

S3(config)#

S3>ena

S3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S3(config)#ip default-gateway 192.168.1.254

S3(config)#

S3#

%SYS-5-CONFIG\_I: Configured from console by console

**R1**

Router>ena

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hpstname R1

^

% Invalid input detected at '^' marker.

Router(config)#hostname R1

R1(config)#int g0/1

R1(config-if)#ip add 192.168.1.1 255.255.255.0

R1(config-if)#no sh

R1(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#int s0/0/0

R1(config-if)#ip add 10.1.1.1 255.255.255.252

R1(config-if)#clock rate 128000

R1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R1(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R1(config-if)#exit

R1(config)#router eigrp 1

R1(config-router)#networ 192.168.1.0 0.0.0255

^

% Invalid input detected at '^' marker.

R1(config-router)#networ 192.168.1.0 0.0.0.255

R1(config-router)#network 10.1.1.0 0.0.0.3

R1(config-router)#no auto-summary

R1(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.3 (GigabitEthernet0/1) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.1.2 (Serial0/0/0) is up: new adjacency

R1(config-router)#exit

R1(config)#exit

R1#

%SYS-5-CONFIG\_I: Configured from console by console

R1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

D 10.2.2.0/30 [90/2172416] via 192.168.1.3, 00:08:25, GigabitEthernet0/1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1

L 192.168.1.1/32 is directly connected, GigabitEthernet0/1

D\*EX 0.0.0.0/0 [170/3449856] via 10.1.1.2, 00:01:54, Serial0/0/0

R1#

R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#int g0/1

R1(config-if)#standby 1 ip 192.168.1.254

R1(config-if)#standby 1 priority 150

R1(config-if)#

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active

R1(config-if)#standby preempt

R1(config-if)#end

R1#

%SYS-5-CONFIG\_I: Configured from console by console

R1#show standby

GigabitEthernet0/1 - Group 1 (version 2)

State is Active

4 state changes, last state change 00:54:12

Virtual IP address is 192.168.1.254

Active virtual MAC address is 0000.0C9F.F001

Local virtual MAC address is 0000.0C9F.F001 (v2 default)

Hello time 3 sec, hold time 10 sec

Next hello sent in 1.249 secs

Preemption disabled

Active router is local

Standby router is 192.168.1.3

Priority 150 (configured 150)

Group name is hsrp-Gig0/1-1 (default)

R1#show standby brief

P indicates configured to preempt.

|

Interface Grp Pri P State Active Standby Virtual IP

Gig0/1 1 150 Active local 192.168.1.3 192.168.1.254

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#in g0/1

R1(config-if)#no stanby 1

^

% Invalid input detected at '^' marker.

R1(config-if)#no standby 1

R1(config-if)#

**R2**

Router>ena

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R2

R2(config)#int s0/0/0

R2(config-if)#ip add 10.1.1.2 255.255.255.252

R2(config-if)#no sh

R2(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#int s0/0/0/1

^

% Invalid input detected at '^' marker.

R2(config-if)#int s0/0/1

R2(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

R2(config-if)#

R2(config-if)#ip add 10.2.2.2 255.255.255.252

R2(config-if)#clock rate 128000

This command applies only to DCE interfaces

R2(config-if)#no sh

R2(config-if)#int lo1

R2(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R2(config-if)#ip add 209.165.200.225 255.255.255.252

R2(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R2(config-if)#exit

R2(config)#router eifrp 1

^

% Invalid input detected at '^' marker.

R2(config)#router eigrp 1

R2(config-router)#network 10.1.1.0 0.0.0.3

R2(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

R2(config-router)#network 10.2.2.0 0.0.0.3

R2(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.2.2.1 (Serial0/0/1) is up: new adjacency

R2(config-router)#no auto-summary

R2(config-router)#

R2(config-router)#exit

R2(config)#ip route 0.0.0.0.0.0.0.0 lo1

^

% Invalid input detected at '^' marker.

R2(config)#ip route 0.0.0.0 0.0.0.0 lo1

%Default route without gateway, if not a point-to-point interface, may impact performance

R2(config)#router eigrp 1

R2(config-router)#redistribute static

R2(config-router)#exit

R2(config)#exit

R2#

%SYS-5-CONFIG\_I: Configured from console by console

R2#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.2/32 is directly connected, Serial0/0/0

C 10.2.2.0/30 is directly connected, Serial0/0/1

L 10.2.2.2/32 is directly connected, Serial0/0/1

D 192.168.1.0/24 [90/2172416] via 10.1.1.1, 00:06:04, Serial0/0/0

[90/2172416] via 10.2.2.1, 00:05:23, Serial0/0/1

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/30 is directly connected, Loopback1

L 209.165.200.225/32 is directly connected, Loopback1

S\* 0.0.0.0/0 is directly connected, Loopback1

**R3**

Router>ena

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R3

R3(config)#int g0/1

R3(config-if)#ip add 192.168.1.3 255.255.255.0

R3(config-if)#no sh

R3(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R3(config-if)#int s0/0/1

R3(config-if)#ip add 10.2.2.1 255.255.255.252

R3(config-if)#no sh

R3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#exit

R3(config)#router eigrp 1

R3(config-router)#network 192.168.1.0 0.0.0.255

R3(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.1 (GigabitEthernet0/1) is up: new adjacency

R3(config-router)#network 10.2.2.0 0.0.0.3

R3(config-router)#no auto-summary

R3(config-router)#

R3(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency

R3 con0 is now available

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int g0/1

R3(config-if)#standby 1 ip 192.168.1.254

R3(config-if)#

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak -> Standby

R3(config-if)#exit

R3(config)#exit

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int g0/1

R3(config-if)#do show standby

GigabitEthernet0/1 - Group 1 (version 2)

State is Standby

3 state changes, last state change 00:48:02

Virtual IP address is 192.168.1.254

Active virtual MAC address is 0000.0C9F.F001

Local virtual MAC address is 0000.0C9F.F001 (v2 default)

Hello time 3 sec, hold time 10 sec

Next hello sent in 1.581 secs

Preemption disabled

Active router is 192.168.1.1

Standby router is local

Priority 100 (default 100)

Group name is hsrp-Gig0/1-1 (default)

R3(config-if)#show stand by brief

^

% Invalid input detected at '^' marker.

R3(config-if)#do show standby brief

P indicates configured to preempt.

Interface Grp Pri P State Active Standby Virtual IP

Gig0/1 1 100 Standby 192.168.1.1 local 192.168.1.254

R3(config-if)#

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active

R3(config-if)#exit

R3(config)#int g0/1

R3(config-if)#no standby 1

R3(config-if)#

**CAPÍTULO 3**

Tal vez sea posible usar enlaces más rápidos (por ejemplo, de 10 Gb/s) en el enlace agregado entre los switches de capa de acceso y de distribución. Sin embargo, agregar enlaces más rápidos es costoso. Además, como la velocidad aumenta en los enlaces de acceso, ni siquiera el puerto más rápido posible en el enlace agregado es lo suficientemente rápido para agregar el tráfico proveniente de todos los enlaces de acceso.

También es posible multiplicar la cantidad de enlaces físicos entre los switches para aumentar la velocidad general de la comunicación switch a switch. Sin embargo, STP está habilitado de manera predeterminada en los dispositivos de switch. STP bloquea los enlaces redundantes para evitar los bucles de routing.

Las agregaciones de enlaces tienen las siguientes funciones:

* **Ancho de banda ampliado**: la capacidad de varios enlaces se combina en un enlace lógico.
* **Conmutación por error y conmutación por recuperación automáticas**: gracias a la compatibilidad con la detección de fallos basada en enlaces, el tráfico que proviene de un enlace con errores se conmuta a otros enlaces que estén funcionando en la agregación.
* **Administración mejorada**: todos los enlaces subyacentes se administran como una única unidad.
* **Menos drenaje en la agrupación de direcciones de red**: puede asignarse una dirección IP a la agregación completa.
* **Protección de enlaces**: puede configurar la propiedad de enlace de datos que activa la protección de enlaces para los paquetes que fluyen por la agregación.
* **Gestión de recursos**: las propiedades de enlace de datos para los recursos de red y las definiciones de flujos le permiten regular el uso de los recursos de red que hacen las aplicaciones.

**Tamaño del Ancho de Banda.**

El *trunking* se convierte en una tecnología ineficaz más allá de cierto tamaño de banda, dependiendo del número total de puertos en el equipo del [interruptor](https://es.wikipedia.org/wiki/Interruptor). Los 24 interruptores del Gigabit con dos enlaces de 8 Gigabites están utilizando dieciséis de sus puertos disponibles apenas para los dos enlaces, y salen de solamente ocho de sus puertos de 1 Gigabit para otros [dispositivos](https://es.wikipedia.org/wiki/Hardware). Esta misma configuración en un interruptor de puerto del [Gigabit](https://es.wikipedia.org/wiki/Gigabit) 48 deja 32 puertos de 1 Gigabit disponibles, y así que es mucho más eficiente (suponiendo por supuesto que esos puertos son realmente necesarios en la localización el interruptor).

Cuando el 40-50% de los puertos del interruptor se está utilizando para el *trunking*, el aumento a un interruptor con más puertos o una velocidad de funcionamiento base más alta puede ser una opción mejor que simplemente agregando más interruptores, especialmente si el viejo interruptor se puede reutilizar por otra parte en una pieza crítica del funcionamiento de la [red](https://es.wikipedia.org/wiki/Red).

**Restricciones de implementación.**

El EtherChannel proporciona un ancho de banda full-duplex de hasta 800 Mb/s (Fast EtherChannel) u 8 Gb/s (Gigabit EtherChannel) entre un switch y otro switch o host. En la actualidad, cada EtherChannel puede constar de hasta ocho puertos Ethernet configurados de manera compatible. El switch con IOS de Cisco actualmente puede admitir seis EtherChannels. Sin embargo, a medida que se desarrollan nuevos IOS y cambian las plataformas, algunas tarjetas y plataformas pueden admitir una mayor cantidad de puertos dentro de un enlace EtherChannel, así como una mayor cantidad de Gigabit EtherChannels. El concepto es el mismo, independientemente de las velocidades o la cantidad de enlaces que estén involucrados. Cuando se configure EtherChannel en los switches, tenga en cuenta los límites y las especificaciones de la plataforma de hardware. El propósito original de EtherChannel es aumentar la capacidad de velocidad en los enlaces agregados entre los switches. Sin embargo, el concepto se extendió a medida que la tecnología EtherChannel adquirió más popularidad, y ahora muchos servidores también admiten la agregación de enlaces con EtherChannel. EtherChannel crea una relación de uno a uno, es decir, un enlace EtherChannel conecta solo dos dispositivos. Se puede crear un enlace EtherChannel entre dos switches o entre un servidor con EtherChannel habilitado y un switch. Sin embargo, no se puede enviar el tráfico a dos switches diferentes a través del mismo enlace EtherChannel.

La configuración de los puertos individuales que forman parte del grupo EtherChannel debe ser coherente en ambos dispositivos. Si los puertos físicos de un lado se configuran como enlaces troncales, los puertos físicos del otro lado también se deben configurar como enlaces troncales dentro de la misma VLAN nativa. Además, todos los puertos en cada enlace EtherChannel se deben configurar como puertos de capa 2.

### Agregaciones de troncos

Las agregaciones de troncos otorgan beneficios a diversas redes con diferentes cargas de tráfico. Por ejemplo, si un sistema de la red ejecuta aplicaciones con un gran volumen de tráfico distribuido, puede dedicar una agregación de troncos al tráfico de dicha aplicación para aprovechar el aumento del ancho de banda. Para ubicaciones con espacio de direcciones IP limitado pero que requieren una gran cantidad de ancho de banda, sólo se necesita una dirección IP para una gran agregación de interfaces. Para ubicaciones que necesitan ocultar la existencia de interfaces internas, la dirección IP de la agregación oculta las interfaces a aplicaciones externas.

Una agregación de troncos normalmente alcanza para satisfacer los requisitos de una configuración de red. Sin embargo, una agregación de troncos está limitada a trabajar solo con un conmutador. Por lo tanto, el conmutador se convierte en un único punto de fallo para la agregación del sistema. Las soluciones anteriores que permiten que las agregaciones abarquen varios conmutadores tienen sus propias desventajas:

* Las soluciones que se implementan en los conmutadores son específicos del proveedor, no son estándares. Si se utilizan varios conmutadores de diferentes proveedores, puede que la solución de un proveedor tal vez no se aplique a los productos de otros proveedores.
* Combinar agregaciones de enlaces con las rutas múltiples de IP (IPMP) es muy complejo, sobre todo en el contexto de la virtualización de redes que implica zonas globales y zonas no globales. La complejidad aumenta a medida que se escalan las configuraciones, por ejemplo, en un escenario que incluye una gran cantidad de sistemas, zonas, NIC, NIC virtuales (VNIC) y grupos IPMP. Esta solución también exige hacer configuraciones en la zona global y en cada zona no global de todos los sistemas.
* Incluso si se implementa una combinación de agregaciones de enlaces e IPMP, la configuración no se beneficia de las otras ventajas de trabajar en la capa de enlace sola; por ejemplo, la protección de enlaces, los flujos definidos por el usuario y la capacidad de personalizar las propiedades de enlace, como el ancho de banda.

El Sistema A tiene una agregación que consta de dos interfaces, net1 y net2. Estas interfaces están conectadas al nodo mediante puertos agregados. El Sistema B tiene una agregación de cuatro interfaces, de net1 a net4. Estas interfaces también están conectadas mediante puertos agregados del nodo.

En esta topología de agregación de enlaces, el conmutador debe admitir la tecnología de agregaciones. En consecuencia, sus puertos de conmutador deben estar configurados para gestionar el tráfico de los sistemas.

Las agregaciones de troncos también admiten la configuración de extremo a extremo. En lugar de utilizar un conmutador, se conectan directamente dos sistemas entre sí para ejecutar agregaciones paralelas.

**EtherChannel.**

En los inicios, Cisco desarrolló la tecnología EtherChannel como una técnica switch a switch LAN para agrupar varios puertos Fast Ethernet o Gigabit Ethernet en un único canal lógico. Cuando se configura un EtherChannel, la interfaz virtual resultante se denomina “canal de puertos”. Las interfaces físicas se agrupan en una interfaz de canal de puertos.

Un máximo de 8 puertos Fast Ethernet, [Giga Ethernet](https://es.wikipedia.org/w/index.php?title=Giga_Ethernet&action=edit&redlink=1) o [10Gigabit Ethernet](https://es.wikipedia.org/w/index.php?title=10Gigabit_Ethernet&action=edit&redlink=1) pueden ser agrupados juntos para formar un EtherChannel. Con esta última agrupación es posible conseguir un máximo de 80 Gbps de ancho de banda. Las conexiones EtherChannel pueden interconectar switches, [routers](https://es.wikipedia.org/wiki/Router), servidores o clientes. Los puertos usados deben tener las mismas características y configuración.

[Spanning Tree Protocol](https://es.wikipedia.org/wiki/Spanning_Tree_Protocol) (STP) se puede utilizar con EtherChannel. STP trata a todos los enlaces como uno solo y únicamente se envían las BPDU por uno de los enlaces. Sin el uso de un EtherChannel, STP efectivamente bloquearía los enlaces redundantes entre switches y solo se utilizarían ante la caída de una conexión. Es por esta razón por la que EtherChannel es aconsejable ya que permite el uso completo de todos los enlaces disponibles entre dos dispositivos. Con EtherChannel la capacidad sería el doble en funcionamiento normal y ante una caída no es necesario esperar a la convergencia del STP porque sigue funcionando con el otro enlace. La creación de EtherChannel es recomendable en enlaces sobre puertos de acceso, uno por VLAN. Es preferible tener un EtherChannel y convertir el enlace resultante en trunk 802.1Q para transportar todas las VLAN aprovechando así las ventajas de multiplexación estadística del tráfico.

La tecnología EtherChannel tiene muchas ventajas:

* La mayoría de las tareas de configuración se pueden realizar en la interfaz EtherChannel en lugar de en cada puerto individual, lo que asegura la coherencia de configuración en todos los enlaces.
* El EtherChannel depende de los puertos de switch existentes. No es necesario actualizar el enlace a una conexión más rápida y más costosa para tener más ancho de banda.
* El balanceo de carga ocurre entre los enlaces que forman parte del mismo EtherChannel. Según la plataforma de hardware, se pueden implementar uno o más métodos de balanceo de carga. Estos métodos incluyen balanceo de carga de la MAC de origen a la MAC de destino o balanceo de carga de la IP de origen a la IP de destino, a través de enlaces físicos.
* EtherChannel crea una agregación que se ve como un único enlace lógico. Cuando existen varios grupos EtherChannel entre dos switches, STP puede bloquear uno de los grupos para evitar los bucles de switching. Cuando STP bloquea uno de los enlaces redundantes, bloquea el EtherChannel completo. Esto bloquea todos los puertos que pertenecen a ese enlace EtherChannel. Donde solo existe un único enlace EtherChannel, todos los enlaces físicos en el EtherChannel están activos, ya que STP solo ve un único enlace (lógico).
* EtherChannel proporciona redundancia, ya que el enlace general se ve como una única conexión lógica. Además, la pérdida de un enlace físico dentro del canal no crea ningún cambio en la topología, por lo que no es necesario volver a calcular el árbol de expansión. Suponiendo que haya por lo menos un enlace físico presente, el EtherChannel permanece en funcionamiento, incluso si su rendimiento general disminuye debido a la pérdida de un enlace dentro del EtherChannel.

Una limitación de EtherChannel es que todos los puertos físicos en el grupo de agregación deben residir en el mismo conmutador. El protocolo SMLT Avaya elimina esta limitación al permitir que los puertos físicos sean divididos entre dos switches en una configuración de triángulo o 4 o más switches en una configuración de malla.

Todas las interfaces dentro de un EtherChannel deben tener la misma configuración de velocidad y modo dúplex, de VLAN nativas y permitidas en los enlaces troncales, y de la VLAN de acceso en los puertos de acceso.

* Asigne todos los puertos en el EtherChannel a la misma VLAN o configúrelos como enlace troncal. Los puertos con VLAN nativas diferentes no pueden formar un EtherChannel.
* Cuando se configure un EtherChannel desde puertos de enlace troncal, verifique que el modo de enlace troncal sea el mismo en todos los enlaces troncales. Los modos de enlace troncal incoherentes en los puertos EtherChannel pueden hacer que EtherChannel no funcione y que se desactiven los puertos (estado errdisable).
* Un EtherChannel admite el mismo rango permitido de VLAN en todos los puertos. Si el rango permitido de VLAN no es el mismo, los puertos no forman un EtherChannel, incluso cuando PAgP se establece en modo automatic o desirable.
* Las opciones de negociación dinámica para PAgP y LACP se deben configurar de manera compatible en ambos extremos del EtherChannel.

**Componentes**

* Enlaces Fast Ethernet- las conexiones EtherChannel puede consistir de uno a ocho enlaces Fast Ethernet para compartir la carga de tráfico de hasta 800 Mbps de ancho de banda utilizable. Conexiones EtherChannel puede interconectar switches, routers, servidores y clientes. La tecnología EtherChannel ofrece enlaces resistentes dentro de un canal- si los enlaces fallan, el tráfico es redirigido inmediatamente a los demás enlaces. Finalmente, la tecnología EtherChannel no depende de ningún tipo de medio de comunicación. Se puede utilizar con Ethernet que funciona con par trenzado sin blindaje (UTP), fibra monomodo y fibra multimodo.
* Los algoritmos de compartición de carga utilizados varían entre plataformas, permitiendo decisiones basadas en direcciones MAC origen o destino, direcciones IP, o los números de puerto [TCP](https://es.wikipedia.org/wiki/Transmission_Control_Protocol)/ [UDP](https://es.wikipedia.org/wiki/UDP).
* Redundancia- La tecnología EtherChannel de Cisco no requiere del uso de 802.1d Spanning Tree Protocol para mantener un estado dentro de la topología del canal. Por el contrario, utiliza un protocolo de control punto a punto que proporciona configuración automática y tiempos de convergencia para enlaces paralelos inferiores al segundo. Sin embargo, permite protocolos de alto nivel (como el Protocolo Spanning Tree) o protocolos de enrutamiento para mantener la topología.
* Gestión- La tecnología EtherChannel de Cisco se configura fácilmente mediante una interfaz de línea de comandos ([CLI](https://es.wikipedia.org/wiki/CLI)) o aplicaciones [Simple Network Management Protocol](https://es.wikipedia.org/wiki/Simple_Network_Management_Protocol) (SNMP), tales como CiscoWorks. El administrador de red necesita identificar y definir el número de puertos que conformarán el canal, y luego conectar los dispositivos. Un beneficio de la tecnología EtherChannel es la capacidad de detectar, informar y prevenir el uso de pares de interfaces incorrectas dentro del canal. Estos pueden incluir interfaces que no están configurados para full-duplex, tienen velocidades de enlace incorrectas, o están mal conectadas. Comprobaciones de coherencia antes de la activación de un canal ayudan a asegurar la integridad de la red.

**Protocolos para la agregación de puertos.**

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

**PAgP**

Es un protocolo exclusivo de Cisco que ayuda en la creación automática de enlaces EtherChannel. Cuando se configura un enlace EtherChannel mediante PAgP, se envían paquetes PAgP entre los puertos aptos para EtherChannel para negociar la formación de un canal. Cuando PAgP identifica enlaces Ethernet compatibles, agrupa los enlaces en un EtherChannel. El EtherChannel después se agrega al árbol de expansión como un único puerto. Cuando se habilita, PAgP también administra el EtherChannel. Los paquetes PAgP se envían cada 30 segundos. PAgP revisa la coherencia de la configuración y administra los enlaces que se agregan, así como las fallas entre dos switches. Cuando se crea un EtherChannel, asegura que todos los puertos tengan el mismo tipo de configuración.

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

**Encendido:** este modo obliga a la interfaz a proporcionar un canal sin PAgP. Las interfaces configuradas en el modo encendido no intercambian paquetes PAgP.

**PAgP deseado:** este modo PAgP coloca una interfaz en un estado de negociación activa en el que la interfaz inicia negociaciones con otras interfaces al enviar paquetes PAgP.

**PAgP automático:** este modo PAgP coloca una interfaz en un estado de negociación pasiva en el que la interfaz responde a los paquetes PAgP que recibe, pero no inicia la negociación PAgP.

Los modos deben ser compatibles en cada lado. Si se configura un lado en modo automático, se lo coloca en estado pasivo, a la espera de que el otro lado inicie la negociación del EtherChannel. Si el otro lado se establece en modo automático, la negociación nunca se inicia y no se forma el canal EtherChannel. Si se deshabilitan todos los modos mediante el comando no o si no se configura ningún modo, entonces se deshabilita el EtherChannel.

El modo encendido coloca manualmente la interfaz en un EtherChannel, sin ninguna negociación. Funciona solo si el otro lado también se establece en modo encendido. Si el otro lado se establece para negociar los parámetros a través de PAgP, no se forma ningún EtherChannel, ya que el lado que se establece en modo encendido no negocia.

Los modos deben ser compatibles en ambos lados para que se forme el enlace EtherChannel. Se repite el modo encendido, ya que crea la configuración de EtherChannel incondicionalmente, sin la negociación dinámica de PAgP. Para establecer un enlace PAgP entre dos dispositivos Cisco las combinaciones posibles son:

|  |  |  |
| --- | --- | --- |
| SwitchA | SwitchB | Description |
| desirable | desirable | Recommended |
| auto | desirable | Link aggregation occurs if negotiation is successful. |
| Desirable | auto | Link aggregation occurs if negotiation is successful. |

**LACP.**

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

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

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

Al igual que con PAgP, los modos deben ser compatibles en ambos lados para que se forme el enlace EtherChannel. Se repite el modo encendido, ya que crea la configuración de EtherChannel incondicionalmente, sin la negociación dinámica de PAgP o LACP.

La agregación manual de enlaces requiere de configuración manual de los grupos de agregación.

Las siguientes configuraciones deben realizarse para configurar un grupo de agregación manual:

* Crear o eliminar un grupo.
* Añadir o eliminar un puerto Ethernet.
* Configurar o eliminar una descripción.

**Configuración**

Las siguientes pautas y restricciones son útiles para configurar EtherChannel:

* **Soporte de EtherChannel:** todas las interfaces Ethernet en todos los módulos deben admitir EtherChannel, sin necesidad de que las interfaces sean físicamente contiguas o estén en el mismo módulo.
* **Velocidad y dúplex:** configure todas las interfaces en un EtherChannel para que funcionen a la misma velocidad y en el mismo modo dúplex, como se muestra en la ilustración.
* **Coincidencia de VLAN:** todas las interfaces en el grupo EtherChannel se deben asignar a la misma VLAN o se deben configurar como enlace troncal, lo que también se muestra en la ilustración.
* **Rango de VLAN:** un EtherChannel admite el mismo rango permitido de VLAN en todas las interfaces de un EtherChannel de enlace troncal. Si el rango permitido de VLAN no es el mismo, las interfaces no forman un EtherChannel, incluso si se establecen en modo automático o deseado.

Si se deben modificar estos parámetros, configúrelos en el modo de configuración de interfaz de canal de puertos. Después de configurar la interfaz de canal de puertos, cualquier configuración que se aplique a esta interfaz también afecta a las interfaces individuales. Sin embargo, las configuraciones que se aplican a las interfaces individuales no afectan a la interfaz de canal de puertos. Por ello, realizar cambios de configuración a una interfaz que forma parte de un enlace EtherChannel puede causar problemas de compatibilidad de interfaces.

La configuración de EtherChannel con LACP se realiza en dos pasos:

**Paso 1.** Especifique las interfaces que componen el grupo EtherChannel mediante el comando interface range *interface* del modo de configuración global. La palabra clave range le permite seleccionar varias interfaces y configurarlas a la vez. Se recomienda comenzar desactivando esas interfaces, de modo que ninguna configuración incompleta cree actividad en el enlace.

**Paso 2.** Cree la interfaz de canal de puertos con el comando channel-group *identifier* mode active en el modo de configuración de rango de interfaces. El identificador especifica el número del grupo del canal. Las palabras clave mode active identifican a esta configuración como EtherChannel LACP.

Para cambiar la configuración de capa 2 en la interfaz de canal de puertos, ingrese al modo de configuración de interfaz de canal de puertos mediante el comando interface port-channel, seguido del identificador de la interfaz. En el ejemplo, el EtherChannel está configurado como interfaz de enlace troncal con VLAN permitidas específicas.

**Verificacion de EtherChannel.**

Existe una variedad de comandos para verificar una configuración EtherChannel. Primero, el comando **show interface port-channel** muestra el estado general de la interfaz de canal de puertos.

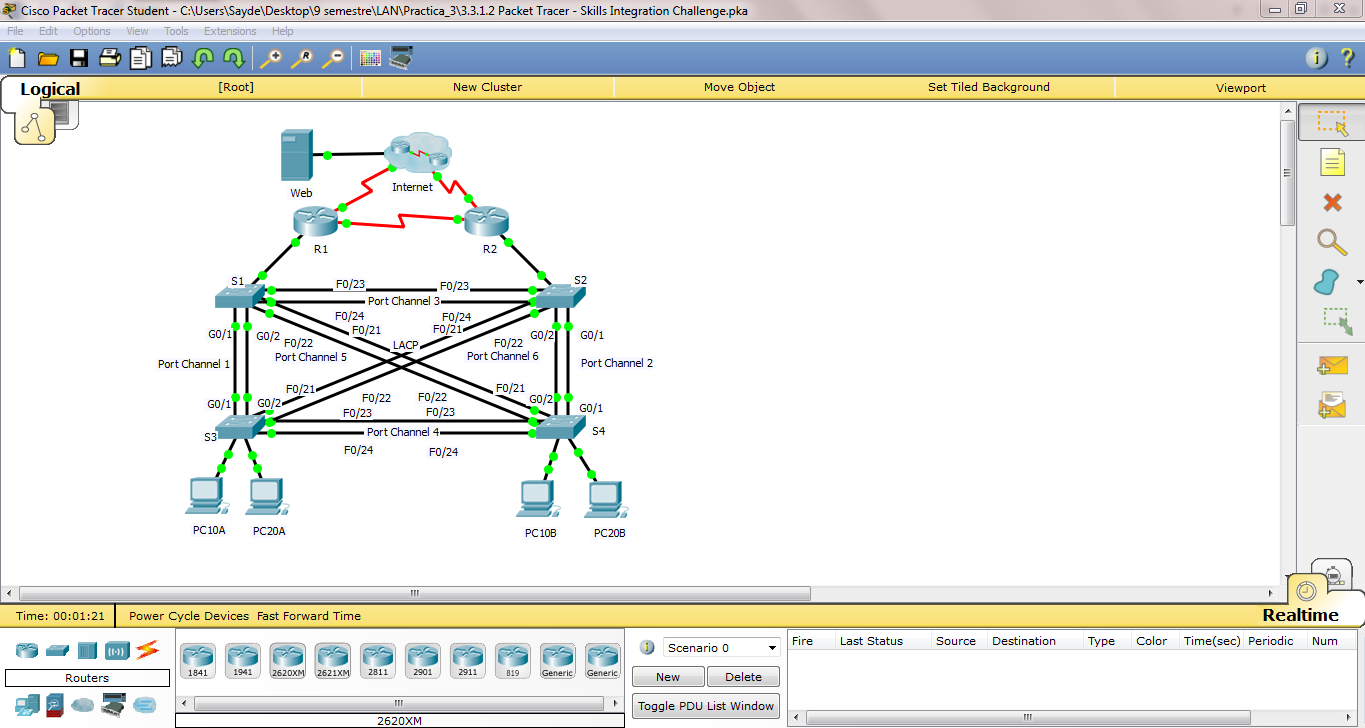
Cuando se configuren varias interfaces de canal de puertos en el mismo dispositivo, use el comando **show etherchannel summary** para mostrar una única línea de información por canal de puertos.

El grupo de interfaces consta de las interfaces FastEthernet0/1 y FastEthernet0/2. El grupo es un EtherChannel de capa 2 y está en uso, según lo indican las letras SU junto al número de canal de puertos.

Use el comando **show etherchannel port-channel** para mostrar la información sobre una interfaz de canal de puertos específica, como se muestra en la figura 3. En el ejemplo, la interfaz de canal de puertos 1 consta de dos interfaces físicas, FastEthernet0/1 y FastEthernet0/2. Esta usa LACP en modo activo. Está correctamente conectada a otro switch con una configuración compatible, razón por la cual se dice que el canal de puertos está en uso.

En cualquier miembro de una interfaz física de un grupo EtherChannel, el comando **show interfaces etherchannel** puede proporcionar información sobre la función de la interfaz en el EtherChannel, como se muestra en la figura 4. La interfaz FastEthernet0/1 forma parte del grupo EtherChannel 1. El protocolo para este EtherChannel es LACP.

**#3.3.1.2**



**R1**

R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#int g0/0.1

R1(config-subif)#encapsulation dot1q 99 native

R1(config-subif)#ip add 192.168.99.1 255.255.255.0

R1(config-subif)#int g0/0.10

R1(config-subif)#encapsulation dot1q 10

R1(config-subif)#ip add 192.168.10.1 255.255.255.0

R1(config-subif)#int g0/0.20

R1(config-subif)#encapsulation dot1q 20

R1(config-subif)#ip add 192.168.10.1 255.255.255.0

% 192.168.10.0 overlaps with GigabitEthernet0/0.10

R1(config-subif)#ip add 192.168.20.1 255.255.255.0

R1(config-subif)#exit

R1(config)#

R1(config)#in g0/0

R1(config-if)#no shut

R1(config-if)#

R1(config-if)#exit

R1(config)#router ospf 1

R1(config-router)#network 192.168.99.0 0.0.0.255 area 0

R1(config-router)#network 192.168.10.0 0.0.0.255 area 0

R1(config-router)#network 192.168.20.0 0.0.0.255 area 0

R1(config-router)#pass

% Incomplete command.

R1(config-router)#passive-interface g0/0.1

R1(config-router)#passive-interface g0/0.10

R1(config-router)#passive-interface g0/0.20

R1(config-router)#

R1#

**R2**

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#int g0/0.1

R2(config-subif)#encapsulation dot1q 99 native

R2(config-subif)#ip add 192.168.99.2 255.255.255.0

R2(config-subif)#int g0/0.10

R2(config-subif)#encapsulation dot1q 10

R2(config-subif)#ip add 192.168.10.2 255.255.255.0

R2(config-subif)#int g0/0.20

R2(config-subif)#encapsulation dot1q 20

R2(config-subif)#ip add 192.168.20.2 255.255.255.0

R2(config-subif)#exit

R2(config)#int g0/0

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#router ospf 1

R2(config-router)#network 192.168.99.0 0.0.0.255 area 0

R2(config-router)#network 192.168.10.0 0.0.0.255 area 0

R2(config-router)#network 192.168.20.0 0.0.0.255 area 0

R2(config-router)#passive-interface g0/0.1

R2(config-router)#passive-interface g0/0.10

R2(config-router)#passive-interface g0/0.20

R2(config-router)#

**S1**

S1>ena

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#vlan 10

S1(config-vlan)#vlan 20

S1(config-vlan)#vlan 99

S1(config-vlan)#

S1>ena

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#vlan 10

S1(config-vlan)#vlan 20

S1(config-vlan)#vlan 99

S1(config-vlan)#exit

S1(config)#in range fa0/1-9

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 10

S1(config-if-range)#in range fa0/10-19

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 20

S1(config-if-range)#in range fa0/20-24, g1/1-2

interface range not validated - command rejected

S1(config)#in range fa0/20-24, g0/1-2

S1(config-if-range)#switchport mode trunk

S1(config-if-range)#

S1(config-if-range)#switchport trunk native vlan 99

S1(config)#int range g0/1-2

S1(config-if-range)#channel-group 1 mode active

S1(config-if-range)#

Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

S1(config-if-range)#int range g0/23-24

interface range not validated - command rejected

S1(config)#int range f0/23-24

S1(config-if-range)#channel-group 3 mode active

S1(config-if-range)#

Creating a port-channel interface Port-channel 3

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

S1(config-if-range)#int range f0/21-22

S1(config-if-range)#channel-group 5 mode active

S1(config-if-range)#

Creating a port-channel interface Port-channel 5

**S2**

S2>ena

S2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)#vlan 10

S2(config-vlan)#vlan 99

S2(config-vlan)#vlan 20

S2(config-vlan)#exit

S2(config)#int range fa0/1-9

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 10

S2(config-if-range)#int range fa0/10-9

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (1), with S1 FastEthernet0/23 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1), with S1 FastEthernet0/24 (99).

S2(config-if-range)#int range fa0/10-19

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 20

S2(config-if-range)#int range fa0/20-24, g0/1-2

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (1), with S1 FastEthernet0/23 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1), with S1 FastEthernet0/24 (99).

S2(config-if-range)#int range fa0/20-24, g0/1-2

S2(config-if-range)#switchport mode trunk

S2(config-if-range)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

S2(config-if-range)#switchport trunk native vlan

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (1), with S1 FastEthernet0/23 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1), with S1 FastEthernet0/24 (99).

S2(config-if-range)#switchport trunk native vlan 99

**S3**

S3>ena

S3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S3(config)#vlan 10

S3(config-vlan)#vlan 99

S3(config-vlan)#vlan 20

S3(config-vlan)#

S3(config)#int range fa0/1-9

S3(config-if-range)#switch

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with S1 GigabitEthernet0/1 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1), with S1 GigabitEthernet0/2 (99).

S3(config-if-range)#switchport mode access

S3(config-if-range)#switchport access vlan 10

S3(config-if-range)#int range fa0/10-20

S3(config-if-range)#switchport access vlan 10

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (1), with S2 FastEthernet0/21 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/22 (1), with S2 FastEthernet0/22 (99).

S3(config-if-range)#switchport access vlan 10

S3(config-if-range)#switchport mode access

S3(config-if-range)#switchport access vlan 20

S3(config-if-range)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with S1 GigabitEthernet0/1 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1), with S1 GigabitEthernet0/2 (99).

S3(config-if-range)#in range fa0/21-24, g0/1-2

S3(config-if-range)#switchport mode access

S3(config-if-range)#switchport mode trunk

S3(config-if-range)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

S3(config-if-range)#switchport trunk native vlan 99

**S4**

S4>ena

S4#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S4(config)#vlan 10

S4(config-vlan)#vlan 99

S4(config-vlan)#vlan 20

S4(config-vlan)#

**CAPÍTULO 4**

**Beneficios de las redes LAN inalámbricas**

Las redes LAN inalámbricas ofrecen beneficios tanto de corto como de largo plazo entre las que destacan:

* **Comodidad:** Todas las computadoras portátiles y muchos teléfonos móviles están equipados con la tecnología WiFi necesaria para conectarse directamente a redes LAN inalámbricas. Los empleados pueden usar una red LAN inalámbrica para acceder en forma segura a los recursos de red desde cualquier lugar en sus instalaciones.
* **Movilidad:** Los empleados pueden permanecer conectados a la red a través de una red LAN inalámbrica, incluso cuando no están en sus escritorios. Las personas en reuniones pueden acceder a documentos y aplicaciones con una red LAN inalámbrica. Los vendedores pueden usar una LAN inalámbrica para buscar en la red datos importantes desde cualquier lugar.
* **Productividad:** Las redes LAN inalámbricas ofrecen al personal y otras personas un cómodo acceso a información y aplicaciones importantes de la empresa. Los visitantes (tales como clientes, contratistas o proveedores) pueden usar la red LAN inalámbrica para acceder en forma segura como usuarios temporales a Internet y a sus datos comerciales.
* **Facilidad de configuración:** Como las redes LAN inalámbricas no requieren tender cables físicos, se pueden instalar en forma rápida y económica. Con las redes LAN inalámbricas también es más fácil llevar conectividad a lugares de difícil acceso, como bodegas o plantas de producción.
* **Escalabilidad:** Generalmente, las redes LAN inalámbricas pueden ampliarse con equipos existentes, mientras que las redes cableadas pueden requerir cables y otros materiales adicionales.
* Seguridad: Controlar y administrar el acceso a la red LAN inalámbrica es importante para su éxito. Los avances en tecnología WiFi proporcionan una sólida protección, para que sólo las personas que usted permita puedan acceder fácilmente a sus datos.
* **Costo:** Puede costar menos operar una red LAN inalámbrica, que elimina o reduce los costos de cableado durante los traslados de oficina, reconfiguraciones o expansiones.

**Tipos de LAN inalámbricas.**

La combinación de tecnologías inalámbricas se expande continuamente, este análisis se centra en las redes inalámbricas que permiten que los usuarios se muevan. En términos generales, las redes inalámbricas se clasifican en los siguientes tipos:

* **Redes de área personal inalámbrica (WPAN):** tienen un alcance de unos pocos metros. En las WPAN, se utilizan dispositivos con Bluetooth o Wi-Fi Direct habilitado.
* **LAN inalámbricas (WLAN):** tienen un alcance de unos 30 m, como en una sala, un hogar, una oficina e incluso un campus.
* **Redes de área extensa inalámbrica (WWAN):** tienen un alcance de kilómetros, como un área metropolitana, una jerarquía de datos móviles o incluso los enlaces entre ciudades mediante retransmisiones de microondas.
* **Bluetooth:** originalmente era un estándar de WPAN IEEE 802.15 que usa un proceso de emparejamiento de dispositivos para comunicarse a través de distancias de hasta 0,05 mi (100 m). El Bluetooth Special Interest Group estandariza las versiones más recientes de Bluetooth.
* **Fidelidad inalámbrica (Wi-Fi):** es un estándar de WLAN IEEE 802.11 que se implementa generalmente para proporcionar acceso a la red a los usuarios domésticos y empresariales, que permite incluir tráfico de datos, voz y video a distancias de hasta 300 m (0,18 mi)
* **Interoperabilidad mundial para el acceso por microondas (WiMAX):** es un estándar de WWAN IEEE 802.16 que proporciona acceso a servicios de banda ancha inalámbrica hasta 30 mi (50 km) WiMAX es una alternativa a las conexiones de banda ancha por cable y DSL. Se agregó la movilidad a WiMAX en 2005, y los proveedores de servicios ahora la pueden usar para proporcionar banda ancha de datos móviles.
* **Banda ancha celular:** consta de varias organizaciones empresariales, nacionales e internacionales que usan el acceso de datos móviles de un proveedor de servicios para proporcionar conectividad de red de banda ancha celular. Disponible por primera vez en 1991 con los teléfonos celulares de segunda generación (2G), con mayores velocidades disponibles en 2001 y 2006 como parte de la tercera (3G) y la cuarta (4G) generación de la tecnología de comunicaciones móviles.
* **Banda ancha satelital:** proporciona acceso de red a sitios remotos mediante el uso de una antena parabólica direccional que se alinea con un satélite específico en la órbita geoestacionaria (GEO) de la Tierra. Normalmente es más costosa y requiere una línea de vista despejada.

**Usos de una LAN inalámbrica.**

Existen muchos beneficios de admitir redes inalámbricas en el entorno empresarial y doméstico. Algunos de los beneficios incluyen el aumento de la flexibilidad y la productividad, la reducción de costos y la capacidad de crecer y adaptarse a requisitos cambiantes.

Estas son algunas de las ventajas que las redes LAN inalámbricas ofrecen a las empresas:

* **Mayor movilidad y colaboración:** los empleados que usan redes LAN inalámbricas pueden recorrer sus oficinas o ir a un piso diferente sin perder su conectividad. De manera similar, la tecnología de voz sobre red LAN inalámbrica les otorga comunicaciones de voz itinerantes.
* **Mayor capacidad de respuesta:** una red LAN inalámbrica puede mejorar el servicio al cliente conectando a los empleados con la información que necesitan.
* **Mejor acceso a información:** una red LAN inalámbrica permite a las empresas proporcionar acceso en áreas que serían difíciles de conectar con una red cableada.
* **Expansión de red más fácil:** las empresas que necesitan agregar empleados o reconfigurar oficinas con frecuencia pueden beneficiarse de la flexibilidad que ofrecen las redes LAN inalámbricas.
* **Mejor acceso de usuarios temporales:** las redes LAN inalámbricas permiten a las empresas proporcionar acceso inalámbrico seguro a Internet a usuarios temporales, como clientes o partners comerciales.

Otro beneficio importante de las redes inalámbricas es la capacidad para adaptarse a las necesidades y las tecnologías cambiantes. Agregar nuevos equipos a la red es muy sencillo con las redes inalámbricas. Considere la conectividad inalámbrica en el hogar. Los usuarios pueden navegar la Web desde la mesa de la cocina, la sala o incluso en exteriores. Los usuarios domésticos conectan nuevos dispositivos, como smartphones, smartpads, computadoras portátiles y televisores inteligentes.

**Estándares 802.11.**

El estándar de WLAN IEEE 802.11 define cómo se usa la RF en las bandas de frecuencia ISM sin licencia para la capa física y la subcapa MAC de los enlaces inalámbricos.

Con el correr de los años, se desarrollaron varias implementaciones del estándar IEEE 802.11. A continuación, se presentan estos estándares:

* **802.11:** lanzado en 1997 y ahora obsoleto, es la especificación de WLAN original que funcionaba en la banda de 2,4 GHz y ofrecía velocidades de hasta 2 Mb/s. Cuando se lanzó, las LAN conectadas por cable funcionaban a 10 Mb/s, por lo que la nueva tecnología inalámbrica no se adoptó con entusiasmo. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas.
* **IEEE 802.11a:** lanzado en 1999, funciona en la banda de frecuencia de 5 GHz, menos poblada, y ofrece velocidades de hasta 54 Mb/s. Posee un área de cobertura menor y es menos efectivo al penetrar estructuras edilicias ya que opera en frecuencias superiores. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas. Los dispositivos que funcionan conforme a este estándar no son interoperables con los estándares 802.11b y 802.11g. Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas*.*
* **IEEE 802.11b:** lanzado en 1999, funciona en la banda de frecuencia de 2,4 GHz y ofrece velocidades de hasta 11 Mb/s. Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejor las estructuras edilicias que los dispositivos basados en 802.11a. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas. 802.11b es usualmente usada en configuraciones punto y multipunto como en el caso de los AP que se comunican con una antena omnidireccional con uno o más clientes que se encuentran ubicados en un área de cobertura alrededor del AP. El rango típico en interiores es de 32 metros a 11 Mbit/s y 90 metros a 1 Mbit/s. Con antenas de alta ganancia externas el protocolo puede ser utilizado en arreglos fijos punto a punto típicamente rangos superiores a 8 Km incluso en algunos casos de 80 a 120 km siempre que haya línea de visión. Esto se hace usualmente para reemplazar el costoso equipo de líneas o el uso de quipos de comunicaciones de microondas.
* **IEEE 802.11g:** lanzado en 2003, funciona en la banda de frecuencia de 2,4 GHz y ofrece velocidades de hasta 54 Mb/s. Por lo tanto, los dispositivos que implementan este estándar funcionan en la misma radiofrecuencia y en el mismo rango que 802.11b, pero con el ancho de banda de 802.11a. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas. Es compatible con el estándar anterior 802.11b. Sin embargo, cuando admite un cliente 802.11b, se reduce el ancho de banda general.

|  |
| --- |
| **IEEE 802.11n:** lanzado en 2009, funciona en las bandas de frecuencia de 2,4 GHz y 5 GHz, y se conoce como “dispositivo de doble banda”. Las velocidades de datos típicas van desde150 Mb/s hasta 600 Mb/s, con un alcance de hasta 70 m (0,5 mi). Sin embargo, para lograr mayores velocidades, los AP y los clientes inalámbricos requieren varias antenas con tecnología de múltiple entrada múltiple salida (MIMO). MIMO usa varias antenas como transmisor y receptor para mejorar el rendimiento de la comunicación. Se pueden admitir hasta cuatro antenas. El estándar 802.11n es compatible con dispositivos 802.11a/b/g anteriores. Sin embargo, si se admite un entorno mixto, se limitan las velocidades de datos previstas. Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Muchos de los productos de banda dual 802.11a/b se convirtieron de banda dual a modo triple soportando a (a, b y g) en un solo adaptador móvil o AP. A pesar de su mayor aceptación 802.11g sufre de la misma interferencia de 802.11b en el rango ya saturado de 2.4 GHz por dispositivos como hornos microondas, dispositivos bluetooth y teléfonos inalámbricos |

|  |
| --- |
|  |

* **IEEE 802.11ac:** lanzado en 2013, funciona en la banda de frecuencia de 5 GHz y proporciona velocidades de datos que van desde 450 Mb/s hasta 1,3 Gb/s (1300 Mb/s). Usa la tecnología MIMO para mejorar el rendimiento de la comunicación. Se pueden admitir hasta ocho antenas. El estándar 802.11ac es compatible con dispositivos 802.11a/n anteriores; sin embargo, admitir un entorno mixto limita las velocidades de datos esperadas.
* **IEEE 802.11ad:** programado para su lanzamiento en 2014 y también conocido como “WiGig”, utiliza una solución de Wi-Fi de triple banda con 2,4 GHz, 5 GHz y 60 GHz, y ofrece velocidades teóricas de hasta 7 Gb/s. Sin embargo, la banda de 60 GHz es una tecnología de línea de vista y, por lo tanto, no puede penetrar las paredes. Cuando un usuario se mueve, el dispositivo cambia a las bandas más bajas de 2,4 GHz y 5 GHz. Es compatible con dispositivos Wi-Fi anteriores existentes. Sin embargo, si se admite un entorno mixto, se limitan las velocidades de datos previstas.

**Certificaciones WI-FI**

Los estándares aseguran interoperabilidad entre dispositivos hechos por diferentes fabricantes. Las tres organizaciones que influyen en los estándares de WLAN en todo el mundo son las siguientes:

* **ITU-R:** regula la asignación del espectro de RF y las órbitas satelitales.
* **IEEE:** especifica cómo se modula la RF para transportar la información. Mantiene los estándares para las redes de área local y metropolitana (MAN) con la familia de estándares de LAN y MAN IEEE 802. Los estándares dominantes en la familia IEEE 802 son Ethernet 802.3 y WLAN 802.11. Si bien el IEEE especificó los estándares para los dispositivos de modulación de RF, no especificó los estándares de fabricación; por lo tanto, las interpretaciones de los estándares 802.11 por parte de los diferentes proveedores pueden causar problemas de interoperabilidad entre los dispositivos.
* **Wi-Fi Alliance:** Wi-Fi Alliance® es una asociación comercial global del sector sin fines de lucro dedicada a promover el crecimiento y la aceptación de las redes WLAN. Es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de los productos basados en el estándar 802.11 mediante la certificación de los proveedores por el cumplimiento de las normas del sector y la observancia de los estándares. No todos los dispositivos compatibles con [IEEE 802.11](https://es.wikipedia.org/wiki/IEEE_802.11) son presentados para la certificación de la Wi-Fi Alliance, a veces debido a los costes asociados al proceso de certificación. La falta del logotipo Wi-Fi no implica necesariamente que un dispositivo sea incompatible con dispositivos Wi-Fi. La Wi-Fi Alliance es propietaria de la [marca registrada](https://es.wikipedia.org/wiki/Marca_%28registro%29) *Wi-Fi*. Los fabricantes pueden utilizar la marca para etiquetar los productos que han sido certificados para la interoperabilidad.

Wi-Fi Alliance certifica la compatibilidad de Wi-Fi con los siguientes productos:

* Compatibilidad con IEEE 802.11a/b/g/n/ac/ad
* IEEE 802.11i seguro con WPA2™ y el protocolo de autenticación extensible (EAP)
* Configuración protegida de Wi-Fi (WPS) para simplificar la conexión de los dispositivos
* Wi-Fi Direct para compartir medios entre dispositivos
* Wi-Fi Passpoint para simplificar de forma segura la conexión a las redes de zona de cobertura Wi-Fi
* Wi-Fi Miracast para mostrar video sin inconvenientes entre dispositivos

**Comparación entre WLAN y LAN.**

Las WLAN comparten un origen similar con las LAN Ethernet. El IEEE adoptó la cartera 802 LAN/MAN de estándares de arquitectura de red de computadoras. Los dos grupos de trabajo 802 dominantes son Ethernet 802.3 y WLAN 802.11. Sin embargo, hay diferencias importantes entre ellos. En principio, colocar los puntos de acceso dentro del servidor de seguridad implica que cualquier usuario que sea capaz de autenticarse en alguno pueda tener acceso a cualquier sistema de la red interna. Probablemente haya implementado controles de acceso en sus sistemas más importantes (y, si no es así, ¿por qué no lo ha hecho?), pero es mejor filtrar el tráfico no deseado en el perímetro de la red. Al colocar los puntos de acceso fuera del servidor de seguridad simplemente se obliga a los usuarios de la WLAN a usar una VPN para entrar, lo que, por supuesto, les resulta menos cómodo que usar una conexión ordinaria. También el uso de esta solución supone otra desventaja: el gran tráfico de datos generado por la WLAN podría sobrepasar la capacidad del servidor de seguridad o del servidor VPN. Una solución habitual es optar por un enfoque intermedio y poner un PA fuera del servidor de seguridad y el resto dentro. El punto de acceso “exterior” puede ser utilizado por los usuarios que no sean de confianza o por invitados (aunque los usuarios de confianza puedan entrar mediante una VPN a la red interna), mientras que los usuarios autenticados pueden usar los puntos de acceso “interiores”. Naturalmente, esta configuración no se recomienda a menos que se use un mecanismo muy seguro de autenticación (como 802.1x) en los puntos de acceso “interiores”.

Una red inalámbrica tiene una doble función: interconectar computadoras y dispositivos cercanos entre sí y la segunda es la de proveer de servicios de Internet a los dispositivos. Un [servidor](http://www.informaticamoderna.com/Servidor.htm) ó un Módem inalámbrico de un proveedor de Internet es el encargado de recibir la señal y distribuirla a la red local. Sin embargo, el servidor cuenta con un sistema operativo específico (Novell®, Microsoft Windows NT®, Linux Apache, etc.) y cada dispositivo que se conecta a la red cuenta con el propio.

     Los [sistemas operativos](http://www.informaticamoderna.com/Sist_Ope.htm) básicamente son incompatibles entre sí y los usuarios que acceden a la red local generalmente tendrán en sus dispositivos sistemas operativos muy diferentes a los del servidor como MacOS® Leopard, Linux Ubuntu, GoogleOS® Chrome, Microsoft® Windows Vista, etc.; es en este momento en el que un dispositivo como el Router inalámbrico puede funcionar como puente entre todos ellos y evitar que se interrumpa la comunicación, lo que hace es permitir la comunicación entre dispositivos a pesar de las diferentes plataformas, siendo cada una la encargada de interpretar los datos recibidos.  También permite evaluar la información, realizando actividades de limpieza, seguridad y filtro con la información, así como descongestionador de redes dividiendo las redes en subredes y enviando la información de manera paralela y por lo tanto mas velozmente.

Las WLAN usan RF en lugar de cables en la capa física y la subcapa MAC de la capa de enlace de datos. Comparada con el cable, la RF tiene las siguientes características:

* La RF no tiene límites, como los límites de un cable envuelto. Esto permite que las tramas de datos que se transmiten a través de los medios de RF estén disponibles para cualquier persona que pueda recibir la señal de RF.
* La señal RF no está protegida de señales exteriores, como sí lo está el cable en su envoltura aislante. Las radios que funcionan de manera independiente en la misma área geográfica, pero con una RF igual o similar, pueden interferir entre sí.
* La transmisión RF está sujeta a los mismos desafíos inherentes a cualquier tecnología basada en ondas, como la radio comercial. Por ejemplo, a medida que la radio se aleja del origen, es posible que las emisoras de radio comiencen a reproducirse una por encima de la otra y que aumente el ruido estático. Finalmente, la señal se pierde por completo. Las LAN conectadas tienen cables que son del largo apropiado para mantener la fuerza de la señal.
* Las bandas RF se regulan en forma diferente en cada país. La utilización de las WLAN está sujeta a regulaciones adicionales y a conjuntos de estándares que no se aplican a las LAN conectadas por cable.

Las WLAN también difieren de las LAN conectadas por cable de la siguiente manera:

* Las WLAN conectan clientes a la red mediante puntos de acceso (AP) inalámbrico o un router inalámbrico, en lugar de hacerlo mediante un switch Ethernet.
* Las WLAN conectan los dispositivos móviles que, en general, están alimentados por batería, en lugar de los dispositivos conectados de la LAN. Las NIC inalámbricas tienden a reducir la duración de la batería de los dispositivos móviles.
* Las WLAN admiten hosts que se disputan el acceso a los medios RF (bandas de frecuencia). Para evitar proactivamente las colisiones dentro de los medios, el estándar 802.11 recomienda la prevención de colisiones (CSMA/CA) en lugar de la detección de colisiones (CSMA/CD) para el acceso a los medios.
* Las WLAN utilizan un formato de trama diferente al de las LAN Ethernet conectadas por cable. Las WLAN requieren información adicional en el encabezado de la Capa 2 de la trama.
* Las WLAN son más lentas, en general, que las LAN. El estándar 802.11b permite una conectividad de hasta 11 Mb/s, mientras que 802.11a y 802.11g alcanzan los 54 Mb/s. Compare esta velocidad con los 100 Mb/s del hardware común de LAN o con los 1000 Mb/s que disfruta Gigabit Ethernet y parece que se queda bastante atrás, especialmente si recuerda que la velocidad de la conexión de una WLAN puede reducirse (hasta los 2 Mb/s) como resultado de las interferencias en las señales.
* Las WLAN requieren configuración. Con las LAN basta con conectar los conmutadores y los concentradores para empezar a trabajar. Por el contrario, los puntos de acceso de las WLAN deben configurarse. Aunque la configuración de un punto de acceso no es difícil, implica que debe ocuparse de ello, de asignar una contraseña y de realizar los cambios que la red pueda precisar y que pueden hacer necesario volver a modificar la configuración en algún momento posterior.
* Las WLAN tienen mayores inconvenientes de privacidad debido a que las frecuencias de radio pueden salir fuera de las instalaciones. Las WLAN son más lentas, en general, que las LAN. El estándar 802.11b permite una conectividad de hasta 11 Mb/s, mientras que 802.11a y 802.11g alcanzan los 54 Mb/s. Compare esta velocidad con los 100 Mb/s del hardware común de LAN o con los 1000 Mb/s que disfruta Gigabit Ethernet y parece que se queda bastante atrás, especialmente si recuerda que la velocidad de la conexión de una WLAN puede reducirse (hasta los 2 Mb/s) como resultado de las interferencias en las señales.

**Componentes de WLAN.**

La red inalámbrica más simple requiere, como mínimo, dos dispositivos. Cada dispositivo debe tener un transmisor de radio y un receptor de radio sintonizados en las mismas frecuencias.

**NIC Inalámbrica.**

Una tarjeta de red o adaptador de red permite la comunicación con aparatos conectados entre si y también permite compartir recursos entre dos o más[computadoras](http://es.wikipedia.org/wiki/Computadora) . A las tarjetas de red también se les llama NIC (por *network interface card*; en español “tarjeta de interfaz de red”). Aunque el término tarjeta de red se suele asociar a una [tarjeta de expansión](http://es.wikipedia.org/wiki/Tarjeta_de_expansi%C3%B3n) insertada en una ranura interna de un [computador](http://es.wikipedia.org/wiki/Computadora) o [impresora](http://es.wikipedia.org/wiki/Impresora), se suele utilizar para referirse también a dispositivos integrados en la [placa madre](http://es.wikipedia.org/wiki/Placa_madre) del equipo, como las interfaces presentes en las [videoconsolas](http://es.wikipedia.org/wiki/Videoconsola) [Xbox](http://es.wikipedia.org/wiki/Xbox) o las [computadoras portátiles](http://es.wikipedia.org/wiki/Computadora_port%C3%A1til).

Se denomina también NIC al [circuito integrado](http://es.wikipedia.org/wiki/Circuito_integrado) de la tarjeta de red que se encarga de servir como interfaz de [Ethernet](http://es.wikipedia.org/wiki/Ethernet) entre el medio físico (por ejemplo un [cable coaxial](http://es.wikipedia.org/wiki/Cable_coaxial)) y el equipo (por ejemplo una [computadora personal](http://es.wikipedia.org/wiki/Computadora_personal) o una [impresora](http://es.wikipedia.org/wiki/Impresora)). Es un circuito integrado usado en computadoras o periféricos tales como las tarjetas de red, impresoras de red o sistemas integrados, para conectar dos o más dispositivos entre sí a través de algún medio, ya sea conexión inalámbrica, cable UTP, cable coaxial, [fibra óptica](http://es.wikipedia.org/wiki/Fibra_%C3%B3ptica), etc.

Las características de la tarjeta de red definen en parte, las características de la red. Al escoger e instalar una NIC se debe tener en cuenta lo siguiente:

* Velocidad de conexión. (10/100/1000) Megabits por segundo.
* Tipo de conexión (ISA, PCI, PCMCIA, USB, Inalámbrica…).
* Conectores y Topología (AUI, BNC, RJ45).
* Wake-On-LAN (WOL).
* Indicadores de estado (LED) (Conexión, actividad de la red).
* Soporte Full-duplex (para doblar la velocidad de comunicación).
* Normas compatibles. (Novell NE, Ethernet, IEEE 802.x…).
* Controladores de LAN (Sistemas operativos en que funciona).
* Precio.

Sin embargo, la mayoría de las implementaciones inalámbricas requieren lo siguiente:

* Terminales con NIC inalámbricas
* Dispositivo de infraestructura, como un router o un AP inalámbricos

Para comunicarse de forma inalámbrica, los terminales requieren una NIC inalámbrica que incorpore un transmisor o un receptor de radio y el controlador de software necesario para que funcione. Las computadoras portátiles, las tablet PC y los smartphones ahora incluyen NIC inalámbricas integradas. Sin embargo, si un dispositivo no tiene una NIC inalámbrica integrada, se puede usar un adaptador inalámbrico USB.

El controlador de la tarjeta de red debe indicarle al sistema operativo las opciones de configuración de **Dirección Base de I/O,** Interrupción **(IRQ)** y Dirección de Acceso a Memoria (**DMA**) de esta forma se controla la comunicación Hardware la tarjeta de red. En ocasiones la conexion a la red se puede realizar mediante otros procedimientos: Modem, Wifi, WiMax, bluetooth, electricidad… por lo que es aconsejable analizar los pros y contras de todos los sistemas de comunicacion.  
**En ocasiones** la conexión a la red se puede realizar mediante otros procedimientos: Modem, Wifi, WiMax, bluetooth, electricidad… por lo que es aconsejable analizar los pros y contras de todos los sistemas de comunicación.

**Router Inalámbrico.**

Un router inalámbrico o ruteador inalámbrico es un dispositivo hogareño que realiza las funciones de un [router](https://es.wikipedia.org/wiki/Router), pero también incluye las funciones de un [punto de acceso inalámbrico](https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico). Se utiliza comúnmente para proporcionar acceso a Internet o a una red informática. No se requiere un enlace por cable, ya que la conexión se realiza sin cables, a través de ondas de radio. Puede funcionar en una LAN cableada ([local area network](https://es.wikipedia.org/wiki/Local_area_network)), en una LAN sólo-inalámbrica ([WLAN](https://es.wikipedia.org/wiki/WLAN)), o en una red mixta cableada/inalámbrica, dependiendo del fabricante y el modelo.

Cuando emplea un router inalámbrico, su red se denomina "red de Infraestructura inalámbrica". El router inalámbrico es el principal componente de una red doméstica. El router inalámbrico puede compararse con la base de un teléfono inalámbrico. El resto de dispositivos inalámbricos de la red, como los ordenadores y las impresoras, son como los teléfonos inalámbrico. Todas las comunicaciones en la red inalámbrica se realizan a través del router inalámbrico, que permite que los dispositivos conectados hablen entre sí y con el mundo exterior. Muchos routers inalámbricos incorporan un firewall para evitar el acceso no deseado a su red.

Muchos routers inalámbricos también permiten que los dispositivos se conecten a la red con un cable Ethernet. Así que una red doméstica con un router inalámbrico puede tener dispositivos inalámbricos y conectados por cable conectados a la misma.

El tipo de dispositivo de infraestructura al que se asocia una terminal y con el que se autentica varía según el tamaño y los requisitos de la WLAN.

Por ejemplo, un usuario doméstico normalmente interconecta dispositivos inalámbricos mediante un pequeño router inalámbrico integrado. Estos routers integrados más pequeños funcionan como lo siguiente:

* **Punto de acceso:** proporciona acceso inalámbrico 802.11a/b/g/n/ac.
* **Switch:** proporciona un switch Ethernet 10/100/1000, full-duplex, de cuatro puertos para conectar dispositivos por cable.
* **Router:** proporciona un gateway predeterminado para la conexión a otras infraestructuras de la red.

**Características.**

Las características principales de un router inalámbrico son:

|  |
| --- |
| * Permiten la conexión a la WLAN de dispositivos inalámbricos como [teléfonos celulares modernos](http://www.informaticamoderna.com/Celular.htm), [Netbook](http://www.informaticamoderna.com/Netbook.htm), [Laptop](http://www.informaticamoderna.com/Laptop.htm), [PDA](http://www.informaticamoderna.com/PDA.htm), [Notebook](http://www.informaticamoderna.com/Notebook.htm) y [Access Point](http://www.informaticamoderna.com/Acces_point.htm) para proveer de servicios de Internet. |
| * También cuentan con soporte para redes basadas en alambre (LAN - *Local Area Network*), esto es tienen un puerto RJ45 que permite interconectarse con Switches y formar grandes redes entre dispositivos convencionales e inalámbricos para su conexión a Internet. |
| * La tecnología de comunicación con que cuentan es a base de ondas de radio, capaces de traspasar muros, sin embargo entre cada obstáculo esta señal pierde fuerza y se reduce su cobertura. |
| * Permiten la conexión ADSL (Asymmetric Digital Subscriber Line), la cuál permite el manejo de Internet de banda ancha y ser distribuido hacia otras computadoras sin necesidad de cables e incluso hacia redes por medio de puerto RJ45. |
| * El Router inalámbrico puede tener otras funciones como [servidor de impresión](http://www.informaticamoderna.com/Print_serv_ina.htm) y permitir de manera inalámbrica la generación de documentos físicos por medio de una impresora. |
| * Cuentan con una antena externa para la correcta emisión y recepción de ondas, así por ende, un correcto flujo de datos. |

**Puntos de Acceso Inalámbrico.**

Un punto de acceso inalámbrico (en inglés: *Wireless Access Point*, conocido por las siglas WAP o AP), en una [red de computadoras](https://es.wikipedia.org/wiki/Red_de_computadoras), es un [dispositivo de red](https://es.wikipedia.org/wiki/Red_de_computadoras#Dispositivos_de_red) que interconecta equipos de comunicación inalámbricos, para formar una [red inalámbrica](https://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica) que interconecta [dispositivos móviles](https://es.wikipedia.org/wiki/Dispositivos_m%C3%B3viles) o [tarjetas de red](https://es.wikipedia.org/wiki/Tarjetas_de_red) inalámbricas.

Son dispositivos que son configurados en redes de tipo inalámbricas que son intermediarios entre una computadora y una red (Internet o local) Facilitan conectar varias máquinas cliente sin la necesidad de un cable (mayor portabilidad del equipo) y que estas posean una conexión sin limitárseles tanto su ancho de banda. Los WAP son dispositivos que permiten la conexión inalámbrica de un [dispositivo móvil](https://es.wikipedia.org/wiki/Dispositivo_m%C3%B3vil) de cómputo ([computadora](https://es.wikipedia.org/wiki/Computadora), [tableta](https://es.wikipedia.org/wiki/Tableta_%28computadora%29), [*smartphone*](https://es.wikipedia.org/wiki/Tel%C3%A9fono_inteligente)) con una [red](https://es.wikipedia.org/wiki/Red_de_computadoras). Normalmente, un WAP también puede conectarse a una [red cableada](https://es.wikipedia.org/wiki/Ethernet), y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos.

Generalmente, los AP tienen como función principal permitir la conectividad con la red, delegando la tarea de ruteo y direccionamiento a servidores, [ruteadores](https://es.wikipedia.org/wiki/Router) y [*switches*](https://es.wikipedia.org/wiki/Switch). La mayoría de los AP siguen el estándar de comunicación, [802.11](https://es.wikipedia.org/wiki/802.11) de la [IEEE](https://es.wikipedia.org/wiki/IEEE), lo que permite una compatibilidad con una gran variedad de equipos inalámbricos. Algunos equipos incluyen tareas como la configuración de la función de ruteo, de direccionamiento de puertos, seguridad y administración de usuarios. Estas funciones responden ante una configuración establecida previamente. Al fortalecer la interoperabilidad entre los servidores y los AP, se pueden lograr mejoras en el servicio que ofrecen, por ejemplo, la respuesta dinámica ante cambios en la red y ajustes de la configuración de los dispositivos.

Los AP son el enlace entre las redes cableadas y las inalámbricas. El uso de varios AP permite el servicio de *roaming*. El surgimiento de estos dispositivos ha permitido el ahorro de nuevos cableados de red. Un AP con el estándar IEEE [802.11b](https://es.wikipedia.org/wiki/802.11b) tiene aproximadamente un radio de 100 m.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la [red de área local inalámbrica](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local_inal%C3%A1mbrica) ([WLAN](https://es.wikipedia.org/wiki/WLAN)) y la [red de área local](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local) ([LAN](https://es.wikipedia.org/wiki/Local_Area_Network)) cableada.

Un único AP puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros. Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red [WLAN](https://es.wikipedia.org/wiki/WLAN) a través de [adaptadores](https://es.wikipedia.org/wiki/Adaptador_%28inform%C3%A1tica%29) situados en sus equipos (computadora, tableta, teléfono inteligente, [*smart TV*](https://es.wikipedia.org/wiki/Smart_TV), [radio por Internet](https://es.wikipedia.org/wiki/Radio_por_Internet), etcétera). Estos proporcionan una interfaz entre el [sistema operativo de red](https://es.wikipedia.org/wiki/Sistema_operativo_de_red) del cliente ([NOS](https://es.wikipedia.org/wiki/Sistema_operativo_de_red): *Network Operating System*) y las ondas, mediante una [antena](https://es.wikipedia.org/wiki/Antena) inalámbrica.

Los AP se pueden categorizar de las siguientes maneras:

* **AP autónomos**: Los AP autónomos, a veces denominados “AP pesados”, son dispositivos autónomos que se configuran mediante la CLI de Cisco o una GUI. Los AP autónomos son útiles en situaciones en las que solo se requiere un par de AP en la red. De manera optativa, se pueden controlar varios AP mediante los servicios de dominio inalámbrico (WDS) y se pueden administrar mediante el motor de soluciones de LAN inalámbricas (WLSE) CiscoWorks.
* **AP basados en controladores:** Los AP basados en controladores son dispositivos que dependen del servidor y no requieren una configuración inicial. Cisco ofrece dos soluciones basadas en controladores. Los AP basados en controladores son útiles en situaciones en las que se requieren muchos AP en la red. A medida que se agregan más AP, un controlador de WLAN configura y administra cada AP automáticamente. El beneficio del controlador es que se puede usar para administrar muchos AP.

**Antenas Inalámbricas.**

La mayoría de los AP de clase empresarial requieren el uso de antenas externas para convertirlas en unidades de funcionamiento pleno. Cisco desarrolló antenas diseñadas específicamente para usar con AP 802.11 y que admiten condiciones de implementación específica, incluida la disposición física, la distancia y la estética.

Los AP Cisco Aironet pueden usar lo siguiente:

* **Antenas Wi-Fi omnidireccionales:** con frecuencia, el engranaje Wi-Fi de fábrica usa antenas dipolos básicos, conocidos como “antenas de goma”, similares a aquellas usadas en las radios walkie-talkie. Las antenas omnidireccionales proporcionan cobertura de 360° y son ideales para áreas de oficinas abiertas, pasillos, salas de conferencias y exteriores. Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones con menor alcance.  
  Las antenas Omnidireccionales “envían” la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté, ya que no requieren orientarlas. En contrapartida, el alcance de estas antenas es menor que el de las antenas direccionales.
* **Antenas Wi-Fi direccionales:** las antenas direccionales concentran la señal de radio en un sentido determinado. Esto mejora la señal desde y hasta el AP en el sentido que apunta la antena, lo que proporciona una mayor potencia de señal en un sentido, así como una menor potencia de señal en todos los demás sentidos. orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, actúa de forma parecida a un foco de luz que emite un haz concreto y estrecho pero de forma intensa (más alcance).  Generalmente el haz o apertura y el alcance son inversamente proporcionales, esto es a mayor apertura menos alcance y a menor apertura más alcance. El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. Dentro de las antenas direccionales podemos distinguir varios tipos.
* **Antenas Yagi:** son un tipo de antena de radio direccional que se puede usar para las redes Wi-Fi de larga distancia. Normalmente, estas antenas se usan para extender el alcance de las zonas de cobertura exteriores en un sentido específico o para llegar a un edificio externo. El uso de esta antena en Japón solo comenzó a utilizarse durante la [Segunda Guerra Mundial](https://es.wikipedia.org/wiki/Segunda_Guerra_Mundial), cuando fue descubierto que la invención de Yagi era utilizada como antena de radar por los ejércitos aliados. Se puede demostrar que las propiedades ([impedancia](https://es.wikipedia.org/wiki/Impedancia), [ganancia](https://es.wikipedia.org/wiki/Ganancia_%28electr%C3%B3nica%29), etc.) de una antena cualquiera son las mismas tanto en emisión como en recepción. Como es más fácil de comprender el funcionamiento de una antena Yagi-Uda en transmisión que en recepción, comenzaremos por una antena en transmisión.

una antena Yagi-Uda está formada por un elemento alimentado (conectado al emisor o al receptor) formado por un simple [dipolo](https://es.wikipedia.org/wiki/Dipolo_%28antena%29) o un [dipolo doblado](https://es.wikipedia.org/wiki/Dipolo_%28antena%29#Dipolo_doblado) llamado también "radiador" de manera inapropiada, ya que en la antena Yagi-Uda todos los elementos irradian de manera comparable. Además de ese elemento, la antena tiene uno o varios elementos aislados llamados, injustamente, elementos parásitos. La corriente que circula en el elemento alimentado irradia un campo electromagnético, el cual induce corrientes en los "elementos parásitos" de la antena. Las corrientes inducidas en esos elementos irradian también campos electromagnéticos que a su vez inducen corrientes en los demás. Finalmente la corriente que circula en cada uno de los elementos es el resultado de la interacción entre todos los elementos. El elemento alimentado. La fase de la corriente que circula en el elemento parásito dependerá de la distancia entre los dos elementos y de la longitud y diámetro de este último. La amplitud también dependerá de lo mismo pero mucho menos y será, de todas maneras, de la misma magnitud que la corriente del elemento alimentado.

**Seguridad de LAN Inalámbrica.**

Las dificultades para mantener segura una red conectada por cable se multiplican con una red inalámbrica. La seguridad debe ser una prioridad para cualquiera que utilice o administre redes.

Una WLAN está abierta a cualquier persona dentro del alcance de un AP con las credenciales correspondientes para asociarse a él. Con una NIC inalámbrica y conocimientos de técnicas de decodificación, un atacante no tendrá que entrar físicamente al espacio de trabajo para obtener acceso a una WLAN.

Las preocupaciones de seguridad son aún más importantes cuando se lidia con redes empresariales, ya que el sustento de la empresa depende de la protección de su información. En estos casos, las violaciones a la seguridad pueden tener graves repercusiones, sobre todo si la empresa guarda información financiera relacionada con sus clientes. Cada vez se implementan más redes inalámbricas en las empresas y, en muchos casos, estas redes evolucionaron de ser una conveniencia a ser una parte de la red imprescindible para cumplir con los objetivos. Si bien las WLAN siempre fueron un blanco de los ataques, debido al aumento constante de su popularidad, ahora son un blanco principal.

Las personas ajenas a la empresa, los empleados insatisfechos e incluso otros empleados, involuntariamente, pueden generar los ataques. Las redes inalámbricas son específicamente vulnerables a varias amenazas, incluido lo siguiente:

* Intrusos inalámbricos
* Aplicaciones no autorizadas
* Intercepción de datos
* Ataques DoS

La seguridad de este tipo de redes se ha basado en la implantación de la autenticación del punto de acceso y los clientes con tarjetas inalámbricas permitiendo o denegando los accesos a los recursos de la red.

**MECANISMOS DE SEGURIDAD PARA REDES WLAN.**

 La especificación del estándar 802.11 originalmente utiliza tres métodos para la protección de la red. SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Cada uno de los clientes debe tener configurado el SSID correcto para acceder a la red inalámbrica. Filtrado de direcciones MAC. Se definen tablas que contienen las direcciones MAC de los clientes que accesarán a la red.

WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11.  El IEEE creo el estándar 802.X diseñado para dar controlar los accesos a los dispositivos inalámbricos clientes, Access point y servidores. Este método emplea llaves dinámicas y requiere de autentificación por ambas partes. Requiere de un servidor que administre los servicios de autentificación de usuarios entrantes. El WPA añade una mayor capacidad de encriptación así como métodos de identificación de usuarios que no se contemplaron en el estándar 802.X.

**Ataque DoS.**

Los ataques de **denegación de servicio (DoS)** son probablemente uno de los tipos de ataques más sencillos de llevar a cabo y a la vez uno de los más complicados de contrarrestar. Estos hechos han provocado en los últimos tiempos que este tipo de ataques informáticos se hayan convertido en recurso habitual para todo tipo de **hackers,** aunque también nos pueden servir a los administradores de red como test para comprobar hasta qué punto pueden llegar a responder nuestros sistemas.

La **denegación de servicio (Dos**) consiste básicamente y a grandes rasgos en enviar un gran número de peticiones a un servidor de manera que los usuarios legítimos del servicio no puedan acceder a esos recursos, por ejemplo cuando se satura una web a través de un ataque DoS un usuario que quiera consultar esa web la encontrará caída

Para minimizar el riesgo de un ataque DoS debido a dispositivos mal configurados o ataques malintencionados, proteja todos los dispositivos y las contraseñas, cree copias de seguridad y asegúrese de que todos los cambios de configuración se incorporen fuera del horario de operación.

La interferencia accidental solo ocurre cuando se agrega otro dispositivo inalámbrico. La mejor solución consiste en controlar la WLAN para detectar cualquier problema de interferencia y abordarlo cuando aparezca. Debido a que la banda de 2,4 GHz es más proclive a la interferencia, la banda de 5 GHz se podría usar en áreas con tendencia a la interferencia. Algunas soluciones de WLAN permiten que los AP ajusten automáticamente los canales y usen la banda de 5 GHz para compensar la interferencia. Por ejemplo, algunas soluciones 802.11n/ac/ad se ajustan de manera automática para contrarrestar la interferencia. La tecnología Cisco CleanAir permite que los dispositivos identifiquen y ubiquen las fuentes de interferencia que no son 802.11. Crea una red que tiene la capacidad de ajustarse de forma automática a los cambios en el entorno.

Si bien es poco probable, un usuario malintencionado podría iniciar intencionalmente un ataque DoS mediante bloqueadores de RF que producen interferencia accidental. Es más probable que intenten manipular las tramas de administración para consumir los recursos del AP y mantener los canales demasiado ocupados como para admitir el tráfico de usuarios legítimos.

Las tramas de administración se pueden manipular para crear varios tipos de ataque DoS. Los dos tipos de ataques comunes a las tramas de administración incluyen lo siguiente:

* **Un ataque de desconexión suplantada:** esto ocurre cuando un atacante envía una serie de comandos de “desasociación” a los clientes inalámbricos dentro de un BSS. Estos comandos hacen que todos los clientes se desconecten. Al desconectarse, los clientes inalámbricos inmediatamente intentan volver a asociarse, lo que crea un estallido de tráfico. El atacante continúa enviando tramas de desasociación, y el ciclo se repite.
* **Una saturación con CTS:** esto ocurre cuando un atacante aprovecha el método de contienda CSMA/CA para monopolizar el ancho de banda y denegar el acceso de todos los demás clientes inalámbricos al AP. Para lograr esto, el atacante satura repetidamente el BSS con tramas de Listo para enviar (CTS) a una STA falsa. Todos los demás clientes inalámbricos que comparten el medio de RF reciben las CTS y retienen sus transmisiones hasta que el atacante deja de transmitir las tramas CTS.

**Ataque Man-In-The-Middle.**

En el mundo de la [seguridad informática](http://bitelia.com/tag/seguridad-informatica), un **ataque “**man in the middle**“** o si lo traducimos literalmente a “hombre en el medio”, es un tipo de amenaza que se aprovecha de un intermediario. El atacante en este caso, tiene la habilidad de **desviar o controlar las comunicaciones entre dos partes**. Por ejemplo, si se tratase de un ataque MITM a tu correo, el perpetrador podría desviar todos los e-mails a una dirección alterna para leer o alterar toda la información antes de enviarla al destinatario correcto.

Uno de los ataques más sofisticados que un usuario malintencionado puede usar se denomina “ataque man-in-the-middle” (MITM, intermediario). Existen varias maneras de crear un ataque MITM. Un popular ataque MITM inalámbrico se denomina “ataque con AP de red intrusa”, en el que un atacante introduce un AP no autorizado y lo configura con el mismo SSID que el de un AP legítimo. Las ubicaciones que ofrecen Wi-Fi gratuito, como los aeropuertos, los cafés y los restaurantes, son focos para este tipo de ataque, debido a la autenticación abierta. Los clientes que se conectan a una red inalámbrica verían dos AP que ofrecen acceso inalámbrico. Aquellos que están cerca del AP no autorizado detectan la señal más intensa y es más probable que se asocien a este AP de red intrusa. El tráfico de usuarios ahora se envía al AP no autorizado, que a su vez captura los datos y los reenvía al AP legítimo. El tráfico de retorno del AP legítimo se envía al AP no autorizado, se captura y se reenvía a la STA desprevenida. El atacante puede robar la contraseña del usuario y su información personal, obtener acceso a la red y comprometer el sistema del usuario. Vencer un ataque MITM depende de la sofisticación de la infraestructura WLAN y la vigilancia de la actividad de monitoreo de red. El proceso comienza con la identificación de los dispositivos legítimos en la WLAN. Para hacer esto, se deben autenticar los usuarios. Una vez que se conocen todos los dispositivos legítimos, se puede monitorear la red para detectar los dispositivos o el tráfico anormales.

Las WLAN de empresas que utilizan dispositivos WLAN de tecnología avanzada proveen herramientas a los administradores que trabajan juntas como un sistema de prevención de intrusión inalámbrica (IPS). Estas herramientas incluyen escáneres que identifican las redes ad hoc y los AP no autorizados, así como la administración de recursos de radio (RRM), que controla la banda de RF para vigilar la actividad y la carga de AP. Un AP que está más ocupado de lo normal advierte al administrador sobre posible tráfico no autorizado.

**Como Prevenir ataques.**

La seguridad siempre fue un motivo de preocupación con la tecnología Wi-Fi, debido a que se movió el límite de la red. Las señales inalámbricas pueden trasladarse a través de la materia sólida, como los techos, los pisos, las paredes, fueran del hogar o de la oficina. Sin medidas de seguridad estrictas, instalar una WLAN equivale a colocar puertos Ethernet en todas partes, incluso en exteriores.

Para abordar las amenazas relacionadas con mantener alejados a los intrusos inalámbricos y proteger los datos, en un principio se usaron dos características de seguridad:

* **Ocultamiento del SSID:** los AP y algunos routers inalámbricos permiten que se deshabilite la trama de señal del SSID. Los clientes inalámbricos deben identificar manualmente el SSID para conectarse a la red.
* **Filtrado de direcciones MAC:** un administrador puede permitir o denegar el acceso inalámbrico a los clientes de forma manual según la dirección MAC del hardware físico.

Si bien estas dos características pueden disuadir a la mayoría de los usuarios, la realidad es que ni el ocultamiento del SSID ni el filtrado de direcciones MAC podrían disuadir a un intruso hábil. Los SSID se descubren con facilidad, incluso si los AP no los transmiten por difusión, y las direcciones MAC se pueden suplantar. Se introdujeron dos tipos de autenticación con el estándar 802.11 original:

**Autenticación de sistema abierto:** cualquier cliente inalámbrico se debe poder conectar con facilidad, y este método solo se debe usar en situaciones en las que la seguridad no es motivo de preocupación, como en los lugares que proporcionan acceso gratuito a Internet, como cafés, hoteles y áreas remotas. La autenticación de sistema abierto no es realmente una autenticación, porque todo lo que hace es identificar un nodo inalámbrico mediante su dirección de hardware de adaptador inalámbrico. Una dirección de hardware es una dirección asignada al adaptador de red durante su fabricación y se utiliza para identificar la dirección de origen y de destino de las tramas inalámbricas.

Para el modo de infraestructura, aunque algunos puntos de acceso inalámbricos permiten configurar una lista de direcciones de hardware permitidas para la autenticación de sistema abierto, resulta bastante sencillo para un usuario malintencionado capturar las tramas enviadas en la red inalámbrica para determinar la dirección de hardware de los nodos inalámbricos permitidos y, a continuación, utilizar la dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica.

Para el modo ad hoc, no existe equivalencia para la configuración de la lista de direcciones de hardware permitidas en Windows XP. Por lo tanto, se puede utilizar cualquier dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica basada en el modo ad hoc.

**Autenticación mediante clave compartida:** proporciona mecanismos como WEP, WPA o WPA2 para autenticar y cifrar datos entre un cliente y un AP inalámbricos. Sin embargo, la contraseña se debe compartir previamente entre las dos partes para que estas se conecten.

Existen tres técnicas de autenticación mediante clave compartida:

* **Privacidad equiparable a la de redes cableadas (WEP):** especificación 802.11 original, diseñada para proporcionar una privacidad similar a la de conectarse a una red mediante una conexión por cable. Los datos se protegen mediante el método de cifrado RC4 con una clave estática. Sin embargo, la clave nunca cambia al intercambiar paquetes, por lo que es fácil de descifrar.
* **Acceso protegido Wi-Fi (WPA):** un estándar de Wi-Fi Alliance que usa WEP, pero protege los datos con un algoritmo de cifrado del protocolo de integridad de clave temporal (TKIP), que es mucho más seguro. TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar.
* **IEEE 802.11i/WPA2**: IEEE 802.11i es un estándar del sector para proteger las redes inalámbricas. La versión de Wi-Fi Alliance se denomina WPA2. Tanto 802.11i como WPA2 usan el estándar de cifrado avanzado (AES). En la actualidad, se considera que AES es el protocolo de cifrado más seguro.

Ya no se recomienda WEP. Se comprobó que las claves WEP compartidas presentan errores y, por lo tanto, no se lo debe usar nunca. Para contrarrestar la debilidad de las claves WEP compartidas, el primer enfoque de las empresas fue probar técnicas, como el ocultamiento de los SSID y el filtrado de las direcciones MAC. Se comprobó que estas técnicas también son demasiado débiles.

Luego de las debilidades de una seguridad basada en WEP, hubo un período de medidas de seguridad interinas. Los proveedores como Cisco, que quieren responder a la demanda de mejor seguridad, desarrollaron sus propios sistemas y, al mismo tiempo, ayudaron con la evolución del estándar 802.11i. En el camino hacia 802.11i, se creó el algoritmo de cifrado TKIP, que se unió al método de seguridad WPA de Wi-Fi Alliance.

Las redes inalámbricas modernas siempre deben usar el estándar 802.11i/WPA2. WPA2 es la versión Wi-Fi de 802.11i y, por lo tanto, los términos WPA2 y 802.11i se suelen usar de manera indistinta.

**Autenticación de Usuario Doméstico.**

En la ilustración, se muestran las opciones del modo de seguridad del router inalámbrico Linksys EA6500. Observe cómo el Security mode (Modo de seguridad) para la red de 2,4 GHz usa autenticación abierta (es decir, None [Ninguna]) y no requiere una contraseña, mientras que la opción de Security mode para la red de 5 GHz usa una autenticación WPA2/WPA Mixed Personal (WPA2/WPA personal combinado) y requiere una contraseña. En la lista desplegable de Security mode de la red de 2,4 GHz, se muestran los métodos de seguridad disponibles en el router Linksys EA6500. Se indica desde el método más débil (es decir, None) al más seguro (es decir, WPA2/WPA Mixed Enterprise [WPA2/WPA empresarial combinado]). La red de 5 GHz incluye la misma lista desplegable.

WPA y WPA2 admiten dos tipos de autenticación:

* **Personal:** diseñada para las redes domésticas o de oficinas pequeñas; los usuarios se autentican mediante una clave previamente compartida (PSK). Los clientes inalámbricos se autentican con el AP mediante una contraseña previamente compartida. No se requiere ningún servidor de autenticación especial.
* **Enterprise (Empresarial):** diseñada para las redes empresariales, pero requiere un servidor de servicio de autenticación remota telefónica de usuario (RADIUS). Si bien su configuración es más complicada, proporciona seguridad adicional. El servidor RADIUS debe autenticar el dispositivo y, a continuación, se deben autenticar los usuarios mediante el estándar 802.1X, que usa el protocolo de autenticación extensible (EAP).

**Autenticación Empresarial**

En las redes que tienen requisitos de seguridad más estrictos, se requiere una autenticación o un inicio de sesión adicionales para otorgar acceso a los clientes inalámbricos. Las opciones del modo de seguridad Enterprise requieren un servidor RADIUS con autenticación, autorización y contabilidad (AAA).

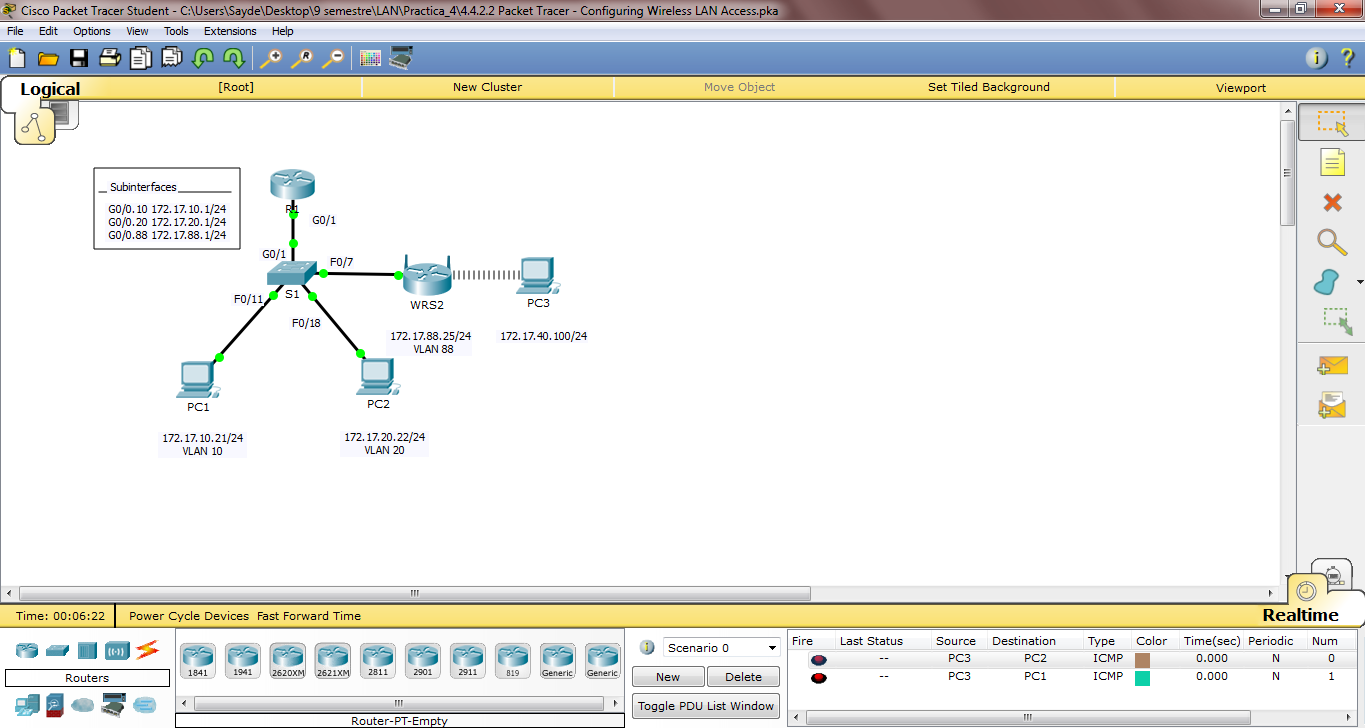
Estos campos son necesarios para proporcionar al AP la información requerida para contactar al servidor AAA:

* **Dirección IP del servidor RADIUS:** esta es la dirección del servidor RADIUS a la que se puede llegar.
* **Números de puerto UDP:** los números de puerto UDP asignados oficialmente son 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS, pero también pueden funcionar mediante los números de puerto UDP 1645 y 1646.
* **Clave compartida:** se usa para autenticar el AP con el servidor RADIUS.

La clave compartida no es un parámetro que se debe configurar en una STA. Solo se requiere en el AP para autenticar con el servidor RADIUS.

El proceso de inicio de sesión 802.1X usa EAP para comunicarse con el AP y el servidor RADIUS. El EAP es una estructura para autenticar el acceso a la red. Puede proporcionar un mecanismo de autenticación seguro y negociar una clave privada segura que después se puede usar para una sesión de cifrado inalámbrico mediante el cifrado TKIP o AES.

**#4.4.2.2**



**R1**

R1>en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#int g0/1.10

R1(config-subif)#encap

% Incomplete command.

R1(config-subif)#encap dot1Q 10

R1(config-subif)#ip add 172.17.10.1 255.255.255.0

R1(config-subif)#int g0/1.20

R1(config-subif)#encap dot1Q 10

%Configuration of multiple subinterfaces of the same main

interface with the same VID (10) is not permitted.

This VID is already configured on GigabitEthernet0/1.10.

R1(config-subif)#encap dot1Q 20

R1(config-subif)#ip add 172.17.20.1 255.255.255.0

R1(config-subif)#int g0/1.88

R1(config-subif)#encap dot1Q 88

R1(config-subif)#ip add 172.17.88.1 255.255.255.0

R1(config-subif)#int g0/1.99

R1(config-subif)#encap dot1Q 99 native

R1(config-subif)#ip add 172.17.99.1 255.255.255.0

R1(config-subif)#exit

R1(config)#int g0/1

R1(config-if)#no sh

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp pool ?

WORD Pool name

R1(config)#ip dhcp pool VLAN10

R1(dhcp-config)#default-router 172.17.10.1

R1(dhcp-config)#ip dhcp pool VLAN20

R1(dhcp-config)#default-router 172.17.20.1

R1(dhcp-config)#ip dhcp pool VLAN88

R1(dhcp-config)#default-router 172.17.88.1

R1(dhcp-config)#exit

R1(config)#ip dhcp excluded-address 172.17.10.1 172.17.10.20

R1(config)#ip dhcp excluded-address 172.17.20.1 172.17.20.20

R1(config)#ip dhcp excluded-address 172.17.88.1 172.17.88.10

R1(config)#ip dhcp pool VLAN10

R1(dhcp-config)#network 172.17.10.0 255.255.255.0

R1(dhcp-config)#ip dhcp pool VLAN20

R1(dhcp-config)#network 172.17.20.0 255.255.255.0

R1(dhcp-config)#ip dhcp pool VLAN88

R1(dhcp-config)#network 172.17.88.0 255.255.255.0

R1(dhcp-config)#

**S2**

S2(config)#vlan 999

S2(config-vlan)#name Blak

S2(config-vlan)#name Blackhole

S2(config-vlan)#exit

S2(config)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with S3 FastEthernet0/3 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S3 FastEthernet0/4 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 FastEthernet0/3 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 FastEthernet0/4 (99).

S2(config)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with S3 FastEthernet0/3 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S3 FastEthernet0/4 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 FastEthernet0/4 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 FastEthernet0/3 (99).

S2(config)#spanning-tree mode rapid-pvst

S2(config)#

S2(config)#int range fa0/4-1

S2(config-if-range)#exit

S2(config)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S3 FastEthernet0/4 (99).

S2(config)#int range fa0/1-4

S2(config-if-range)#switchport trunk native vlan 99

S2(config)#int range fa0/1-4

S2(config-if-range)#switchport trunk native vlan 99

S2(config-if-range)#sw

% Incomplete command.

S2(config-if-range)#switchport mode trunk

S2(config)#int fa0/7

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 88

S2(config-if)#int fa0/18

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 20

S2(config-if)#int fa0/11

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 10

S2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)#int fa0/7

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 88

S2(config-if)#int fa0/18

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 20

S2(config-if)#int fa0/11

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 10

S2(config-if)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, fa0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 999

S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S2(config-if-range)#exit

S2(config)#int range g1/1-2

interface range not validated - command rejected

S2(config)#int range g0/1-2

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 999

S2(config-if-range)#shutdown

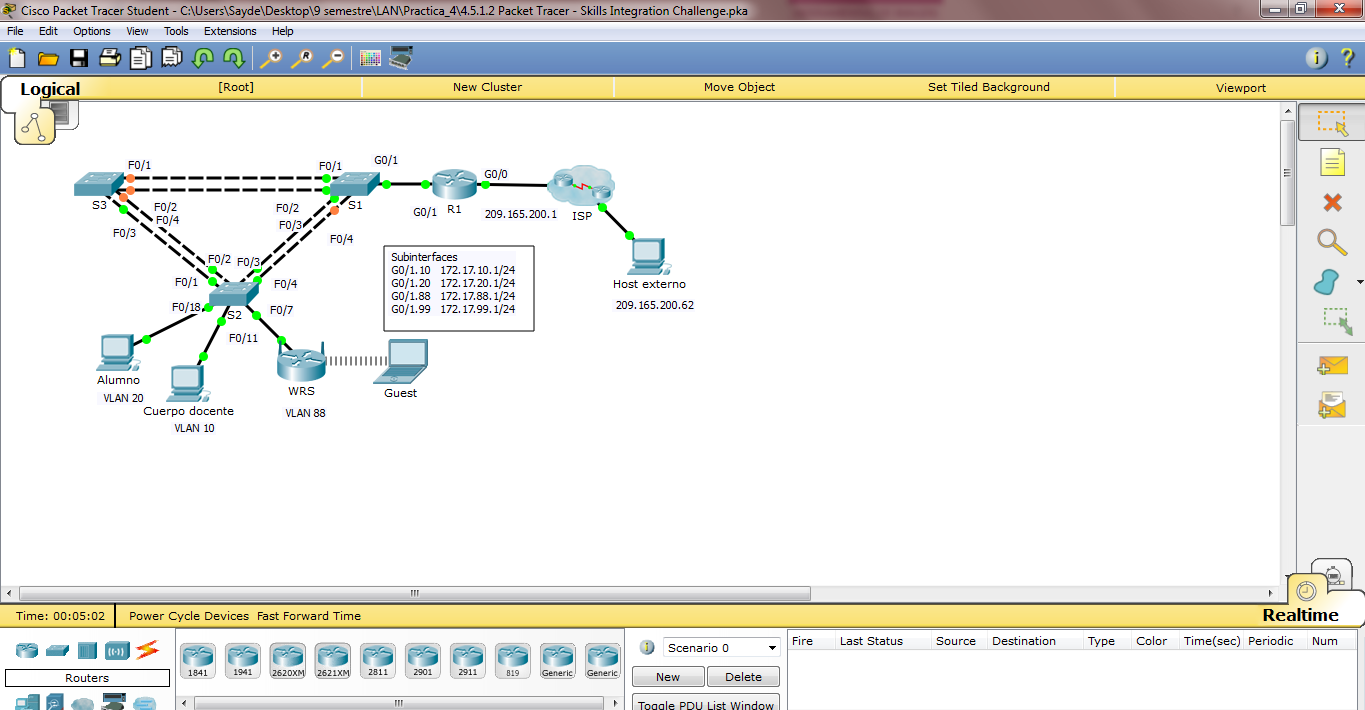
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S2(config-if-range)#end

S2#

**Proyecto: #4.5.1.2**



**R1**

R1>en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#int g0/1.10

R1(config-subif)#encap

% Incomplete command.

R1(config-subif)#encap dot1Q 10

R1(config-subif)#ip add 172.17.10.1 255.255.255.0

R1(config-subif)#int g0/1.20

R1(config-subif)#encap dot1Q 10

%Configuration of multiple subinterfaces of the same main

interface with the same VID (10) is not permitted.

This VID is already configured on GigabitEthernet0/1.10.

R1(config-subif)#encap dot1Q 20

R1(config-subif)#ip add 172.17.20.1 255.255.255.0

R1(config-subif)#int g0/1.88

R1(config-subif)#encap dot1Q 88

R1(config-subif)#ip add 172.17.88.1 255.255.255.0

R1(config-subif)#int g0/1.99

R1(config-subif)#encap dot1Q 99 native

R1(config-subif)#ip add 172.17.99.1 255.255.255.0

R1(config-subif)#exit

R1(config)#int g0/1

R1(config-if)#no sh

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp pool ?

WORD Pool name

R1(config)#ip dhcp pool VLAN10

R1(dhcp-config)#default-router 172.17.10.1

R1(dhcp-config)#ip dhcp pool VLAN20

R1(dhcp-config)#default-router 172.17.20.1

R1(dhcp-config)#ip dhcp pool VLAN88

R1(dhcp-config)#default-router 172.17.88.1

R1(dhcp-config)#exit

R1(config)#ip dhcp excluded-address 172.17.10.1 172.17.10.20

R1(config)#ip dhcp excluded-address 172.17.20.1 172.17.20.20

R1(config)#ip dhcp excluded-address 172.17.88.1 172.17.88.10

R1(config)#ip dhcp pool VLAN10

R1(dhcp-config)#network 172.17.10.0 255.255.255.0

R1(dhcp-config)#ip dhcp pool VLAN20

R1(dhcp-config)#network 172.17.20.0 255.255.255.0

R1(dhcp-config)#ip dhcp pool VLAN88

R1(dhcp-config)#network 172.17.88.0 255.255.255.0

R1(dhcp-config)#

**S2**

S2(config)#vlan 999

S2(config-vlan)#name Blak

S2(config-vlan)#name Blackhole

S2(config-vlan)#exit

S2(config)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with S3 FastEthernet0/3 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S3 FastEthernet0/4 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 FastEthernet0/3 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 FastEthernet0/4 (99).

S2(config)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with S3 FastEthernet0/3 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S3 FastEthernet0/4 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 FastEthernet0/4 (99).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 FastEthernet0/3 (99).

S2(config)#spanning-tree mode rapid-pvst

S2(config)#

S2(config)#int range fa0/4-1

S2(config-if-range)#exit

S2(config)#

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S3 FastEthernet0/4 (99).

S2(config)#int range fa0/1-4

S2(config-if-range)#switchport trunk native vlan 99

S2(config)#int range fa0/1-4

S2(config-if-range)#switchport trunk native vlan 99

S2(config-if-range)#sw

% Incomplete command.

S2(config-if-range)#switchport mode trunk

S2(config)#int fa0/7

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 88

S2(config-if)#int fa0/18

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 20

S2(config-if)#int fa0/11

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 10

S2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)#int fa0/7

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 88

S2(config-if)#int fa0/18

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 20

S2(config-if)#int fa0/11

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 10

S2(config-if)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, fa0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24, g1/1-2

interface range not validated - command rejected

S2(config)#int range fa0/5-6, fa0/8-10, fa0/12-17, f0/19-24

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 999

S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S2(config-if-range)#exit

S2(config)#int range g1/1-2

interface range not validated - command rejected

S2(config)#int range g0/1-2

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 999

S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S2(config-if-range)#end

S2#

**CAPÍTULO 5**

# Comparación entre routing y switching

Las redes escalables requieren un diseño de red jerárquico. El eje central de los capítulos anteriores fueron las capas de acceso y de distribución. Como se muestra en la figura 1, los switches de capa 2, la agregación de enlaces, la redundancia LAN y las LAN inalámbricas son tecnologías que le proporcionan al usuario acceso a los recursos de la red o mejoran dicho acceso.

Las redes escalables también requieren que la posibilidad de conexión entre sitios sea óptima. La posibilidad de conexión de una red remota es proporcionada por los routers y los switches de capa 3 que operan en las capas de distribución y de núcleo, como se muestra en la figura 2. Los routers y los switches de capa 3 descubren las redes remotas de una de las dos maneras siguientes:

* **Manualmente:** las redes remotas se introducen manualmente en la tabla de rutas por medio de rutas estáticas.
* **Dinámicamente:** las rutas remotas se descubren automáticamente por medio de un protocolo de routing dinámico, como el protocolo de routing de gateway interior mejorado (EIGRP) o el protocolo OSPF (Open Shortest Path First).

**Routing estático**

Un administrador de red puede configurar una ruta estática manualmente para alcanzar una red específica. A diferencia de un protocolo de routing dinámico, las rutas estáticas no se actualizan automáticamente, y se deben volver a configurar manualmente cada vez que cambia la topología de la red. Una ruta estática no cambia hasta que el administrador la vuelve a configurar en forma manual.

El routing estático tiene tres usos principales:

* Facilita el mantenimiento de la tabla de routing en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
* Proporciona routing hacia las redes de rutas internas y desde estas. Una red de rutas internas es aquella a la cual se accede a través un de una única ruta y cuyo router tiene solo un vecino.
* Utiliza una única ruta predeterminada para representar una ruta hacia cualquier red que no tenga una coincidencia más específica con otra ruta en la tabla de routing. Las rutas predeterminadas se utilizan para enviar tráfico a cualquier destino que esté más allá del próximo router ascendente.

# Protocolos de routing dinámico

**Enrutamiento dinámico**

Los protocolos de routing permiten que los routers compartan información sobre redes remotas de forma dinámica, como se muestra en la ilustración. Los routers que reciben la actualización agregan esa información automáticamente a sus propias tablas de routing. A continuación, los protocolos de routing determinan la mejor ruta hacia cada red. 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.

En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, usar protocolos de routing dinámico implica el costo de dedicar parte de los recursos de un router a la operación del protocolo, incluidos tiempo de CPU y ancho de banda del enlace de red. Pese a los beneficios del enrutamiento dinámico, el enrutamiento estático aún ocupa su lugar. En algunas ocasiones el enrutamiento estático es más apropiado, mientras que en otras, el enrutamiento dinámico es la mejor opción. Sin embargo, es importante comprender que 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.

Los dos protocolos de routing dinámico más comunes son EIGRP y OSPF. Este capítulo se centra en OSPF.

**Nota:** todos los protocolos de routing dinámico tienen capacidad para anunciar y propagar rutas estáticas en las actualizaciones de routing.

OSPF es un protocolo de routing de estado de enlace que se implementa con frecuencia y se desarrolló como un reemplazo para el protocolo de routing vector distancia RIP. Sin embargo, OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.

Las características de OSPF, que se muestran en la ilustración, incluyen lo siguiente:

* **Sin clase:** fue concebido como un protocolo sin clase, de modo que admite VLSM y CIDR.
* **Eficaz:** los cambios de routing desencadenan actualizaciones de routing (no hay actualizaciones periódicas). Usa el algoritmo SPF para elegir la mejor ruta.
* **Convergencia rápida:** propaga rápidamente los cambios que se realizan a la red.
* **Escalable:** funciona bien en redes pequeñas y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.
* **Seguro:** admite la autenticación de síntesis del mensaje 5 (MD5). Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de routing cifradas de peers con la misma contraseña compartida previamente.

**Verificación de OSPF de área única**

Algunos de los comandos útiles para verificar OSPF son los siguientes:

* **show ip ospf neighbor**: comando para verificar que el router formó una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.
* **show ip protocols:** comando que proporciona una manera rápida de verificar información fundamental de configuración de OSPF. Esta incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es de 110.
* **show ip ospf:**comando que se usa para mostrar la ID del proceso OSPF y la ID del router, así como el SPF de OSPF y la información de área OSPF.
* **show ip ospf interface:** comando que proporciona una lista detallada de cada interfaz con OSPF habilitado y es muy útil para determinar si las instrucciones **network** se compusieron correctamente.
* **show ip ospf interface brief:** comando útil para mostrar un resumen y el estado de las interfaces con OSPF habilitado.

Algunos de los comandos útiles para verificar OSPFv3 son los siguientes:

* **show ipv6 ospf neighbor**: comando para verificar que el router formó una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.
* **show ipv6 protocols:** este comando proporciona una manera rápida de verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.
* **show ipv6 route ospf:** este comando proporciona datos específicos sobre rutas OSPFv3 en la tabla de routing.
* **show ipv6 ospf interface brief:** comando útil para mostrar un resumen y el estado de las interfaces con OSPFv3 habilitado.

**Tipos de redes OSPF**

Para configurar los ajustes de OSPF, empiece por una implementación básica del protocolo de routing OSPF.

OSPF define cinco tipos de redes, como se muestra en las figuras 1 a 5:

* **Punto a punto:** dos routers interconectados por medio de un enlace común. No hay otros routers en el enlace. Con frecuencia, esta es la configuración en los enlaces WAN.
* **Multiacceso con difusión:** varios routers interconectados por medio de una red Ethernet.
* **Multiacceso sin difusión (NBMA):** varios routers interconectados en una red que no permite transmisiones por difusión, como Frame Relay.
* **Punto a multipunto:** varios routers interconectados en una topología hub-and-spoke por medio de una red NBMA. Con frecuencia, se usa para conectar sitios de sucursal (spokes, que significa “rayo”) a un sitio central (hub, que significa “concentrador”).
* **Enlaces virtuales:** una red OSPF especial que se usa para interconectar áreas OSPF distantes al área de red troncal.

Una red de accesos múltiples es una red con varios dispositivos en los mismos medios compartidos, que comparten comunicaciones. Las LAN Ethernet son el ejemplo más común de redes multiacceso con difusión. En las redes de difusión, todos los dispositivos en la red pueden ver todas las tramas de difusión y de multidifusión. Son redes de accesos múltiples ya que puede haber gran cantidad de hosts, impresoras, routers y demás dispositivos que formen parte de la misma red.

**Desafíos en redes de accesos múltiples**

Las redes de accesos múltiples pueden crear dos retos para OSPF en relación con la saturación de las LSA:

* **Creación de varias adyacencias:** las redes Ethernet podrían interconectar muchos routers OSPF con un enlace común. La creación de adyacencias con cada router es innecesaria y no se recomienda, ya que conduciría al intercambio de una cantidad excesiva de LSA entre routers en la misma red.
* **Saturación intensa con LSA:** los routers de estado de enlace saturan con sus paquetes de estado de enlace cuando se inicializa OSPF o cuando se produce un cambio en la topología. Esta saturación puede llegar a ser excesiva.

Para calcular la cantidad de adyacencias requeridas, se puede usar la siguiente fórmula. La cantidad de adyacencias requeridas para cualquier cantidad de routers (designada como *n*) en una red de accesos múltiples es la siguiente:

*n* (*n* – 1) / 2

La solución para administrar la cantidad de adyacencias y la saturación con LSA en una red de accesos múltiples es el DR. En las redes de accesos múltiples, OSPF elige un DR para que funcione como punto de recolección y distribución de las LSA enviadas y recibidas. También se elige un BDR en caso de que falle el DR. El BDR escucha este intercambio en forma pasiva y mantiene una relación con todos los routers. Si el DR deja de producir paquetes de saludo, el BDR se asciende a sí mismo y asume la función de DR.

Todos los otros routers que no son DR ni BDR se convierten en DROthers.

Para verificar las adyacencias OSPF, utilice el comando **show ip ospf neighbor**, como se muestra en la figura 1.

A diferencia de los enlaces seriales que solo muestran un estado de FULL/-, el estado de los vecinos en redes de accesos múltiples puede ser uno de los siguientes:

* FULL/DROTHER: se trata de un router DR o BDR que tiene plena adyacencia con un router que no es DR ni BDR. Estos dos vecinos pueden intercambiar paquetes de saludo, actualizaciones, consultas, respuestas y acuses de recibo.
* FULL/DR: el router tiene plena adyacencia con el vecino DR indicado. Estos dos vecinos pueden intercambiar paquetes de saludo, actualizaciones, consultas, respuestas y acuses de recibo.
* FULL/BDR: el router tiene plena adyacencia con el vecino BDR indicado. Estos dos vecinos pueden intercambiar paquetes de saludo, actualizaciones, consultas, respuestas y acuses de recibo.
* 2-WAY/DROTHER: el router que no es DR ni BDR tiene una relación de vecino con otro router que no es DR ni BDR. Estos dos vecinos intercambian paquetes de saludo.

En general, el estado normal de un router OSPF esFULL. Si un router está atascado en otro estado, es un indicio de que existen problemas en la formación de adyacencias. La única excepción a esto es el estado 2-WAY, que es normal es una red multiacceso con difusión.

En redes de accesos múltiples, los DROthers solo forman adyacencias FULL con el DR y el BDR. Sin embargo, forman adyacencias de vecino 2-WAY con cualquier otro DROther que se una a la red. Esto significa que todos los routers DROther en la red de accesos múltiples siguen recibiendo paquetes de saludo de todos los otros routers DROther. De esta manera, éstos conocen a todos los routers de la red. Cuando dos routers DROther forman una adyacencia de vecino, el estado de vecino aparece como 2-WAY/DROTHER.

La decisión de elección del DR y el BDR OSPF se hace según los siguientes criterios, en orden secuencial:

1. Los routers en la red seleccionan como DR al router con la prioridad de interfaz más alta. El router con la segunda prioridad de interfaz más alta se elige como BDR. La prioridad puede configurarse para que sea cualquier número entre 0 y 255. Cuanto mayor sea la prioridad, más probabilidades hay de que se elija al router como DR. Si la prioridad se establece en 0, el router no puede convertirse en el DR. La prioridad predeterminada de las interfaces de difusión de accesos múltiples es 1. Por lo tanto, a menos que se configuren de otra manera, todos los routers tienen un mismo valor de prioridad y deben depender de otro método de diferenciación durante la elección del DR/BDR.

2. Si las prioridades de interfaz son iguales, se elige al router con la ID más alta como DR. El router con la segunda ID de router más alta es el BDR.

Recuerde que la ID del router se determina de tres maneras:

* La ID del router se puede configurar manualmente.
* Si no hay una ID de router configurada, la ID del router la determina la dirección IP de loopback más alta.
* Si no hay interfaces loopback configuradas, la ID del router la determina la dirección IPv4 activa más alta.

La elección del DR y el BDR OSPF no se basa en prelación. Si se agregan a la red un router nuevo con una prioridad más alta o una ID del router más alta después de la elección del DR y el BDR, el router agregado no se apropia de la función de DR o BDR. Esto se debe a que esas funciones ya se asignaron. La incorporación de un nuevo router no inicia un nuevo proceso de elección.

Una vez que se elige el DR, permanece como tal hasta que se produce una de las siguientes situaciones:

* El DR falla.
* El proceso OSPF en el DR falla o se detiene.
* La interfaz de accesos múltiples en el DR falla o se apaga.

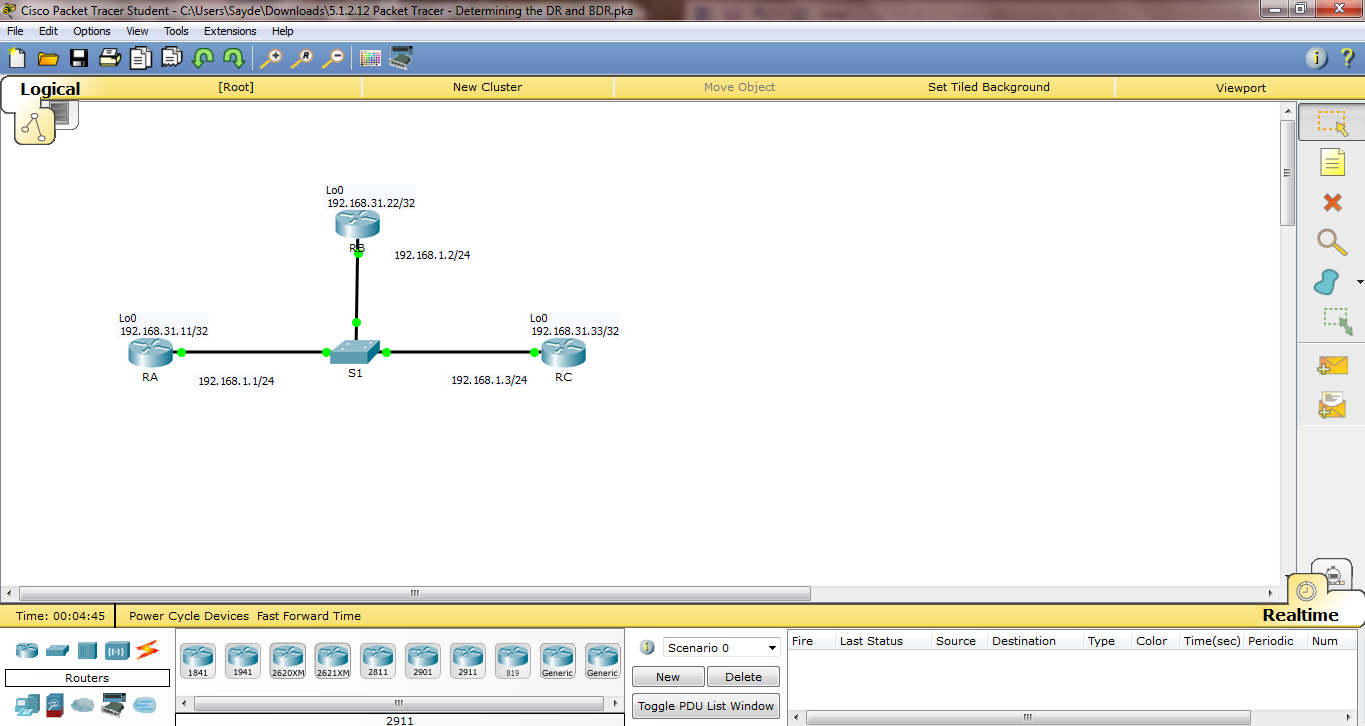
Si el DR falla, el BDR se asciende automáticamente a DR. Esto ocurre así incluso si se agrega otro DROther con una prioridad o ID de router más alta a la red después de la elección inicial de DR/BDR. Sin embargo, después del ascenso de un BDR a DR, se lleva a cabo otra elección de BDR y se elige al DROther con la prioridad o la ID de router más alta como el BDR nuevo.

# La prioridad OSPF

El DR se convierte en el centro de la recopilación y distribución de LSA, por lo tanto, dicho router debe contar con suficiente capacidad de memoria y de CPU para manejar la carga de trabajo. Es posible influenciar el proceso de elección de DR/BDR mediante configuraciones.

Si las prioridades de interfaz son iguales en todos los routers, se elige al router con la ID más alta como DR. Es posible configurar la ID del router para manipular la elección de DR/BDR. Sin embargo, el proceso solo funciona si hay un plan riguroso para establecer la ID de router de todos los routers. En las redes grandes, esto puede ser engorroso.

En vez de depender de la ID del router, es mejor controlar la elección mediante el establecimiento de prioridades de interfaz. Las prioridades son un valor específico de cada interfaz, lo que significa que proporcionan un mejor control en una red de accesos múltiples. Esto también permite que un router sea el DR en una red y un DROther en otra.

**#5.1.2.12**

**RA**

RA>ena

RA#undebug all

All possible debugging has been turned off

RA#conf t

Enter configuration comands, one per line. End with CNTL/2.

RA(config)#int g0/0

RA(config-if)#ip ospf priority 200

RA(config-if)#

**RB**

RB#conf t

Enter configuration comands, one per line. End with CNTL/2.

RB(config)#int g0/0

RB(config-if)#ip ospf priority 100

RB(config-if)#

**RC**

RC>ena

RC#conf t

Enter configuration comands, one per line. End with CNTL/2.

RC(config)#int g0/0

RC(config-if)#do undebug all

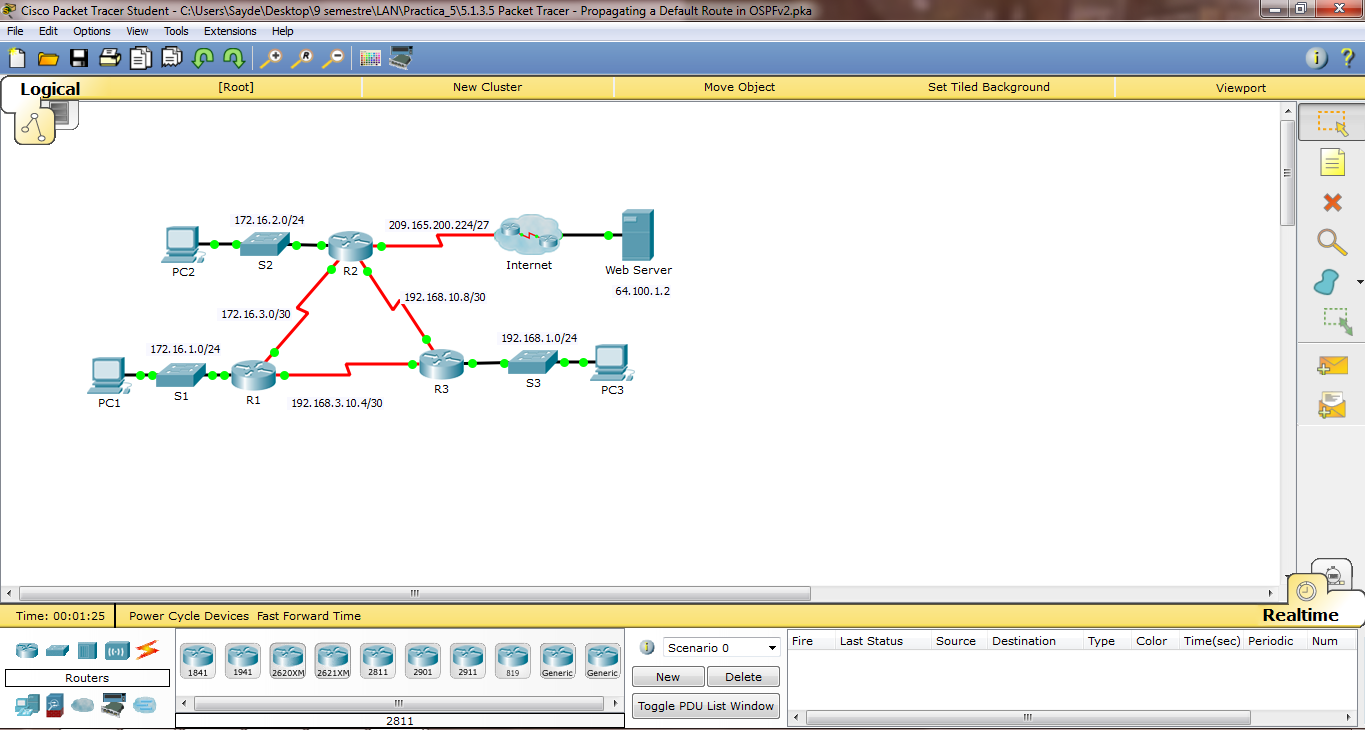
All possible debugging has been turned off

RC(config-if)#int g0/0

RC(config-if)#ip ospf priority 1

RC(config-if)#

**#5.1.3.5**



**R2**

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0

%Default route without gateway, if not a point-to-point interface, may impact performance

R2(config)#end

R2#

%SYS-5-CONFIG\_I: Configured from console by console

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router ospf

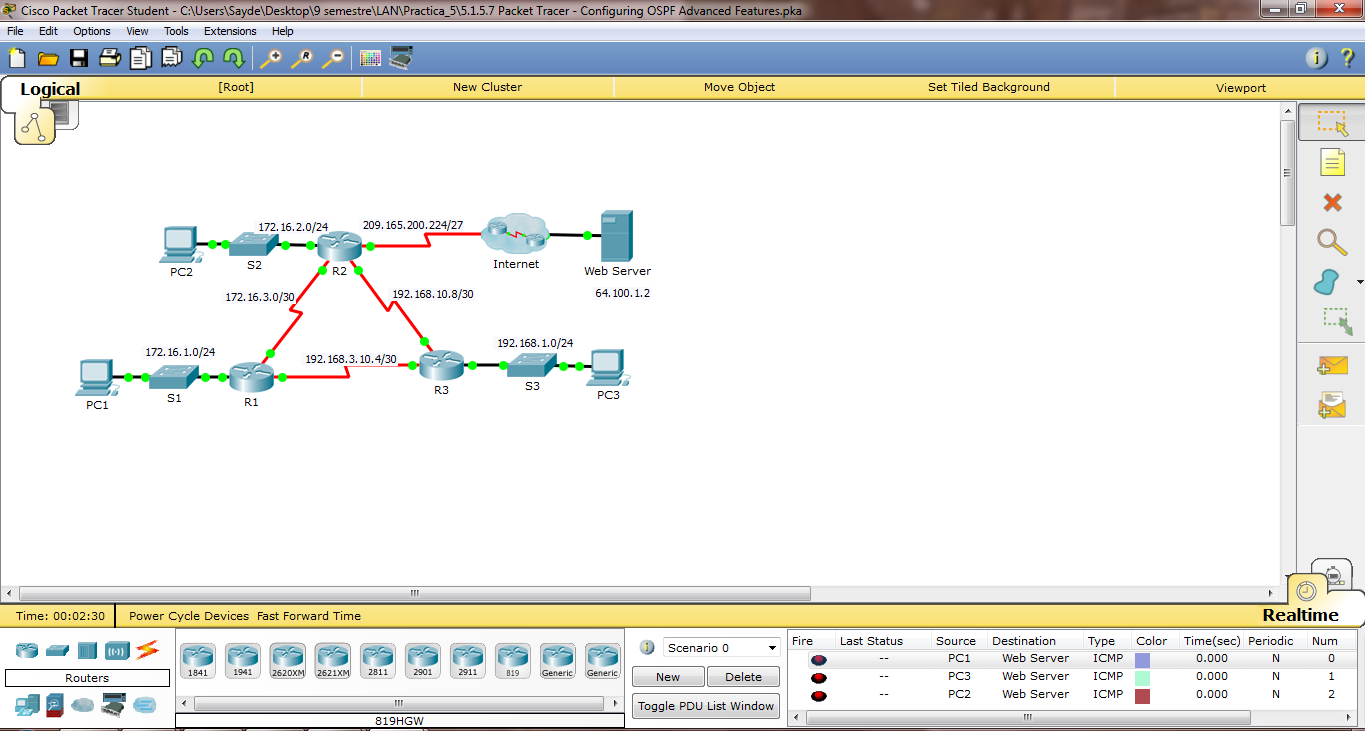
% Incomplete command.

R2(config)#router ospf 1

R2(config-router)#default-information originate

R2(config-router)#

**#5.1.5.7**



**R1**

R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#interface s0/0/0

R1(config-if)#ip ospf hello-interval 15

R1(config-if)#ip ospf dead-interval 60

R1(config-if)#

R1(config)#interface s0/0/0

R1(config-if)#bandwidth 64

R1(config)#router ospf 1

R1(config-router)#area 0 authentication message-digest

R1(config-router)#int s0/0/0

R1(config-if)#ip ospf message-digest-key 1 md5 R1-R2

R1(config-if)#int s0/0/1

R1(config-if)#ip ospf message-digest-key 1 md5 R1-R3

R1(config-if)#

**R2**

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#interface s0/0/0

R2(config-if)#ip ospf hello-interval 15

R2(config-if)#ip ospf dead-interval 60

R2(config-if)# R2(config-if)#router ospf 1

R2(config-router)#area 0 authentication message-digest

R2(config-router)#int s0/0/0

R2(config-if)#ip ospf message-digest-key 1 md5 R1-R2

R2(config-if)#

R2(config-if)#int s0/0/1

R2(config-if)#

R2(config-if)#ip ospf message-digest-key 1 md5 R2-R3

**R3**

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router ospf 1

R3(config-router)#area 0 authentication message-digest

R3(config-router)#int s0/0/0

R3(config-if)#ip ospf message-digest-key 1 md5 R1-R3

R3(config-if)#int s0/0/1

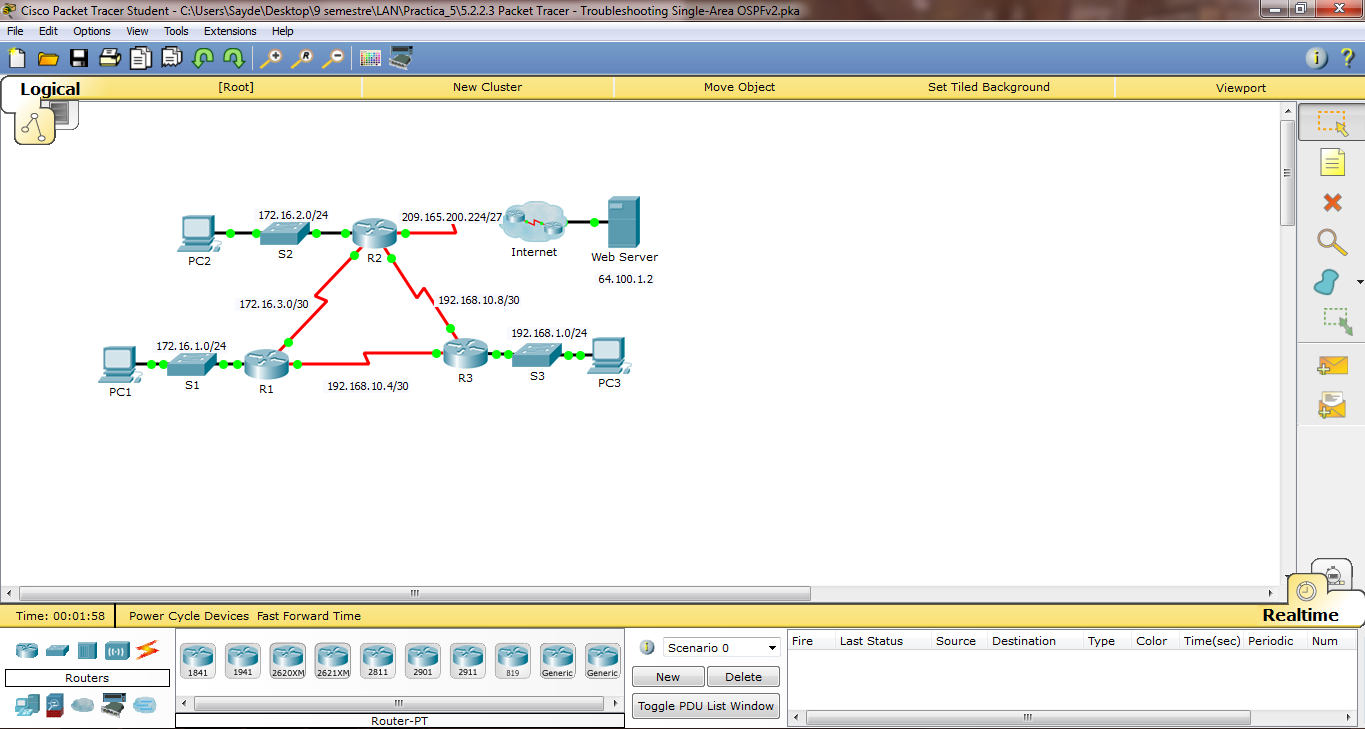
R3(config-if)#

00:19:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from LOADING to FULL, Loading Done

R3(config-if)#ip ospf message-digest-key 1 md5 R2-R3

R3(config-if)#

**#5.2.2.3**



**R1**

R1>ena

R1#debug ip ospf events

OSPF events debugging is on

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#no network 172.16.10.4 0.0.0.3 area 0

R1(config-router)#network 192.168.10.4 0.0.0.3 area 0

R1(config-router)#exit

R1(config)#

**R2**

R2(config)#

R2(config)#router ospf 1

R2(config-router)#default-information originate

**R3**

R3>ena

R3#conf t

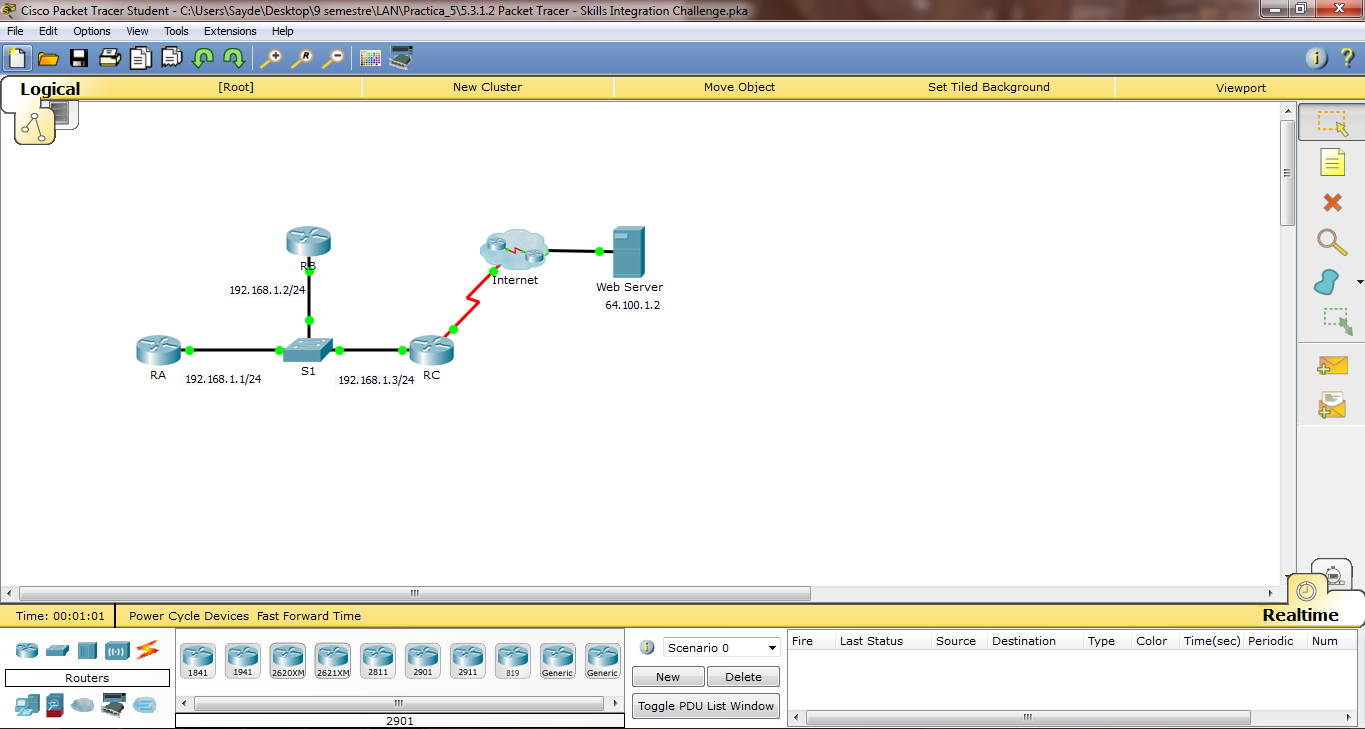
Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int s0/0/1

R3(config-if)#ip ospf hello-interval 10

R3(config-if)#

**#5.3.1.2**



**RA**

RA>en

RA#sh run

Building configuration...

Current configuration : 740 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname RA

!

ip cef

no ipv6 cef

!

license udi pid CISCO1941/K9 sn FTX1524NCYI

!

ip ssh version 1

no ip domain-lookup

!

spanning-tree mode pvst

!

interface Loopback0

no ip address

shutdown

!

interface GigabitEthernet0/0

description Link to Multiaccess LAN

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

ip flow-export version 9

!

line con 0

!

line aux 0

!

line vty 0 4

no login

!

end

RA#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RA(config)#router ospf 1

RA(config-router)#network 192.168.1.0 0.0.0.255 area 0

RA(config-router)#area 0 authentication message-digest

RA(config-router)#exit

RA(config)#int g0/0

RA(config-if)#ip ospf priority 150

RA(config-if)#ip ospf message-digest-key 1 md5 cisco

RA(config-if)#ip ospf hello-interval 5

RA(config-if)#ip ospf dead-interval 20

RA(config-if)#

**RB**

RB>ena

RB#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RB(config)#router ospf 1

RB(config-router)#network 192.168.1.0 0.0.0.255 area 0

RB(config-router)#area 0 authentication message-digest

RB(config-router)#exit

RB(config)#int g0/0

RB(config-if)#ip ospf priority 100

RB(config-if)#ip ospf message-digest-key 1 md5 cisco

RB(config-if)#ip ospf hello-interval 5

RB(config-if)#ip ospf hello-interval 20

RB(config-if)#

RB>ena

RB#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RB(config)#int g0/0

RB(config-if)#ip ospf hello-interval 5

RB(config-if)#ip ospf dead-interval 20

RB(config-if)#

00:24:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

**RC**

RC#sh run

Building configuration...

Current configuration : 1132 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname RC

!

ip cef

no ipv6 cef

!

license udi pid CISCO1941/K9 sn FTX152449P8

!

spanning-tree mode pvst

!

interface Loopback0

no ip address

shutdown

!

interface GigabitEthernet0/0

description Link to Mulitaccess LAN

ip address 192.168.1.3 255.255.255.0

ip ospf message-digest-key 1 md5 cisco

ip ospf hello-interval 20

ip ospf priority 50

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 209.165.200.225 255.255.255.252

!

interface Serial0/0/1

no ip address

clock rate 2000000

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

area 0 authentication message-digest

passive-interface default

no passive-interface GigabitEthernet0/0

network 192.168.1.0 0.0.0.255 area 0

default-information originate

!

ip classless

!

ip flow-export version 9

!

line con 0

!

line aux 0

!

line vty 0 4

no login

!

end

RC#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RC(config)#router ospf 1

RC(config-router)#network 192.168.1.0 0.0.0.255 area 0

RC(config-router)#area 0 authentication message-digest

RC(config-router)#passive-interface default

RC(config-router)#no passive-interface g0/0

RC(config-router)#default-information originate

RC(config-router)#exit

RC(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

%Default route without gateway, if not a point-to-point interface, may impact performance

RC(config)#int g0/0

RC(config-if)#ip ospf priority 50

RC(config-if)#ip ospf message-digest-key 1 md5 cisco

OSPF: Key 1 already exists

RC(config-if)#ip ospf hello-interval 5

RC(config-if)#ip ospf dead-interval 20

RC(config-if)#

RC(config-if)#

00:36:41: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

00:36:41: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

**CAPÍTULO 6**

OSPF de área única es útil en redes más pequeñas, donde la red de enlaces entre routers es simple y las rutas a los destinos individuales se deducen con facilidad.

No obstante, si un área crece demasiado, se deben resolver los siguientes problemas de inmediato (consulte la ilustración para obtener un ejemplo):

* **Tablas de routing extensas:** OSPF no realiza la sumarización de rutas de manera predeterminada. Si las rutas no se resumen, la tabla de routing se vuelve muy extensa, según el tamaño de la red.
* **Bases de datos de estado de enlace (LSDB) muy grandes:** debido a que la LSDB abarca la topología de toda la red, cada router debe mantener una entrada para cada red en el área, incluso aunque no se seleccionen todas las rutas para la tabla de routing.
* **Cálculos frecuentes del algoritmo SPF:** en las redes grandes, las modificaciones son inevitables, por lo que los routers pasan muchos ciclos de CPU volviendo a calcular el algoritmo SPF y actualizando la tabla de routing.

Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área de OSPF es un grupo de routers que comparten la misma información de estado de enlace en las bases de datos de estado de enlace.

**OSPF multiárea**

Cuando se divide un área OSPF grande en áreas más pequeñas, esto se denomina “OSPF multiárea”. OSPF multiárea es útil en implementaciones de red más grandes, ya que reduce la sobrecarga de procesamiento y de memoria.

Por ejemplo, cada vez que un router recibe información nueva acerca de la topología, como la adición, la eliminación o la modificación de un enlace, el router debe volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar la tabla de routing. El algoritmo SPF representa una gran exigencia para el CPU y el tiempo que le toma realizar los cálculos depende del tamaño del área. Si hubiera demasiados routers en un área, la LSDB sería más grande y se incrementaría la carga en la CPU. Por lo tanto, la disposición de los routers en distintas áreas divide de manera eficaz una base de datos potencialmente grande en bases de datos más pequeñas y más fáciles de administrar.

OSPF multiárea requiere un diseño de red jerárquico. El área principal se denomina “de red troncal” (área 0) y el resto de las áreas deben estar conectadas a esta. Con el routing jerárquico, se sigue produciendo el routing entre áreas (routing interárea), y muchas de las tediosas operaciones de routing, como volver a calcular la base de datos, se guardan en un área.

Las posibilidades de topología jerárquica de OSPF multiárea presentan las siguientes ventajas:

* **Tablas de routing más pequeñas:** hay menos entradas de la tabla de routing, ya que las direcciones de red pueden resumirse entre áreas. Por ejemplo, el R1 resume las rutas del área 1 al área 0 y el R2 resume las rutas del área 51 al área 0. Además, el R1 y el R2 propagan una ruta estática predeterminada a las áreas 1 y 51.
* **Menor sobrecarga de actualización de estado de enlace:** minimiza los requisitos de procesamiento y memoria, ya que hay menos routers que intercambian LSA.
* **Menor frecuencia de cálculos de SPF:** localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de una actualización de routing, porque la inundación de LSA se detiene en la frontera del área.

**Jerarquía de área de OSPF de dos capas**

El OSPF de diversas áreas se implementa con una jerarquía de área de dos capas:

* **Área de red troncal (de tránsito):** un área OSPF cuya función principal es la transmisión rápida y eficaz de los paquetes IP. Las áreas de red troncal se interconectan con otros tipos de área de OSPF. En general, los usuarios finales no se encuentran en un área de red troncal. El área de red troncal también se denomina “área OSPF 0”. En las redes jerárquicas, se define al área 0 como el núcleo al que se conectan directamente todas las demás áreas (figura 1).
* **Área común (no de red troncal):** conecta usuarios y recursos. Las áreas regulares se configuran generalmente en grupos funcionales o geográficos. De manera predeterminada, un área regular no permite que el tráfico de otra área utilice sus enlaces para alcanzar otras áreas. Todo el tráfico de otras áreas debe atravesar un área de tránsito (figura 2).

**Nota:** las áreas comunes pueden tener una variedad de subtipos, incluidas un área estándar, un área de rutas internas, un área exclusiva de rutas internas y un área no exclusiva de rutas internas (NSSA). Las áreas de rutas internas, las áreas exclusivas de rutas internas y las áreas NSSA exceden el ámbito de este capítulo.

OSPF aplica esta rígida jerarquía de área de dos capas. La conectividad física subyacente de la red se debe asignar a la estructura del área de dos capas, con solo áreas que no son de red troncal conectadas directamente al área 0. Todo el tráfico que se transfiere de un área a la otra debe atravesar el área de red troncal. Este tráfico se denomina “tráfico interárea”.

La cantidad óptima de routers por área depende de factores como la estabilidad de la red, pero Cisco recomienda tener en cuenta las siguientes pautas:

* Un área no debe tener más de 50 routers.
* Un router no debe estar en más de tres áreas.
* Ningún router debe tener más de 60 vecinos.

**Tipos de routers de OSPF**

Distintos tipos de routers OSPF controlan el tráfico que entra a las áreas y sale de estas. Los routers OSPF se categorizan según la función que cumplen en el dominio de routing.

Existen cuatro tipos diferentes de routers de OSPF:

* **Router interno:** es un router cuyas interfaces están todas en la misma área. Todos los routers internos de un área tienen LSDB idénticas. (figura 1).
* **Router de respaldo:** es un router que se encuentra en el área de red troncal. Por lo general, el área de red troncal se configura como área 0. (figura 2).
* **Router de área perimetral.** **(ABR):** es un router cuyas interfaces se conectan a varias áreas. Debe mantener una LSDB para cada área a la que está conectado; puede hacer routing entre áreas. Los ABR son puntos de salida para cada área. Esto significa que la información de routing que se destina hacia otra área puede llegar únicamente mediante el ABR del área local. Es posible configurar los ABR para resumir la información de routing que proviene de las LSDB de las áreas conectadas. Los ABR distribuyen la información de routing en la red troncal. Luego, los routers de red troncal reenvían la información a otros ABR. En una red de diversas áreas, un área puede tener uno o más ABR. (figura 3).
* **Router limítrofe del sistema autónomo (ASBR):**es un router que tiene al menos una interfaz conectada a una internetwork externa (otro sistema autónomo), por ejemplo, una red que no es OSPF. Un ASBR puede importar información de una red no OSPF hacia una red OSPF, y viceversa, mediante un proceso que se llama "redistribución de rutas". (figura 4).

La redistribución en OSPF de diversas áreas ocurre cuando un ASBR conecta diferentes dominios de routing (por ejemplo, EIGRP y OSPF) y los configura para intercambiar y anunciar información de routing entre dichos dominios de routing.

Un router se puede clasificar como uno o más tipos de router. Por ejemplo, si un router se conecta a las áreas 0 y 1, y además mantiene información de routing de otra red que no es OSPF, se ubica en tres categorías diferentes: router de respaldo, ABR y ASBR.

# Tipos de LSA de OSPF

Las LSA son los bloques funcionales de la LSDB de OSPF. De manera individual, funcionan como registros de la base de datos y proporcionan detalles específicos de las redes OSPF. En conjunto, describen toda la topología de un área o una red OSPF.

LSA de tipo 1 y reenvía la información de su red a los vecinos OSPF. El LSA contiene una lista de interfaces con conexión directa, tipos de enlace y estados de enlace.

A los LSA de tipo 1 también se los denomina "entradas de enlace de router".

Los LSA de tipo 1 solo inundan el área que los origina. Los ABR, a la vez, anuncian a otras áreas las redes descubiertas a partir de las LSA de tipo 1 como LSA de tipo 3.

El Id. de router que origina el área identifica el Id. de enlace de un LSA de tipo 1.

Un LSA de tipo 2 solo existe para redes de diversos accesos y redes sin diversos accesos ni difusión (NBMA) en donde se selecciona un DR y al menos dos routers en el segmento de diversos accesos. La LSA de tipo 2 contiene la ID del router y la dirección IP del DR, además de la ID del router de todos los demás routers en el segmento de accesos múltiples. Se crea una LSA de tipo 2 para cada red de accesos múltiples en el área.

El propósito de una LSA de tipo 2 es proporcionar a otros routers información sobre las redes de accesos múltiples dentro de la misma área.

El DR inunda los LSA de tipo 2 solo en el área en que se originan. Los LSA de tipo 2 no se reenvían fuera del área.

A las LSA de tipo 2 también se las denomina “entradas de enlace de red”.

Los ABR utilizan los LSA de tipo 3 para anunciar redes de otras áreas. Los ABR recopilan LSA de tipo 1 en la LSDB. Después de que converge un área de OSPF, el ABR crea un LSA de tipo 3 para cada red de OSPF reconocida. Por lo tanto, un ABR con varias rutas OSPF debe crear un LSA de tipo 3 para cada red.

Los LSA de tipo 4 y tipo 5 se utilizan en conjunto para identificar un ASBR y anunciar redes externas que llegan a un dominio de routing de OSPF.

El ABR genera un LSA de resumen de tipo 4 solo cuando existe un ASBR en el área. Un LSA de tipo 4 identifica el ASBR y le asigna una ruta. Todo tráfico destinado a un sistema autónomo externo requiere conocimiento de la tabla de routing del ASBR que originó las rutas externas.

Los LSA externos de tipo 5 anuncian rutas a redes que se encuentran afuera del sistema autónomo de OSPF. Los LSA de tipo 5 se originan en el ASBR y se propagan hacia todo el sistema autónomo.

Los LSA de tipo 5 también se conocen como entradas de LSA externas del sistema autónomo.

# Cálculo de router de OSPF

Cada router utiliza el algoritmo SPF en virtud de la LSDB para crear un árbol SPF. El árbol de SPF se utiliza para determinar las mejores rutas.

Como se muestra en la figura, el orden en el que se calculan las mejores rutas es el siguiente:

1. Todo router calcula las mejores rutas a destinos de su área (intraárea) y agrega estas entradas a la tabla de routing. Se trata de LSA de tipo 1 y tipo 2, que se indican en la tabla de routing con el designador "O". (1)

2. Todo router calcula las mejores rutas hacia otras áreas en la internetwork. Las mejores rutas son las entradas de rutas interárea, o LSA de tipo 3 y tipo 4, y se indican con el designador de routing "O IA". (2)

3. Todo router (excepto los que se ubican en una forma de rutas internas) calcula las mejores rutas hacia destinos del sistema autónomo externo (tipo 5). Estas se indican con el designador de ruta O E1 u O E2, según la configuración. (3)

Cuando converge, un router se comunica con cualquier red dentro o fuera del sistema autónomo OSPF.

**Implementación de OSPF multiárea**

La implementación de OSPF puede ser de área única o multiárea. El tipo de implementación de OSPF que se elige depende de los requisitos específicos y de la topología existente.

Para implementar OSPF multiárea, se deben seguir cuatro pasos, los cuales se muestran en la ilustración.

Los pasos 1 y 2 forman parte del proceso de planificación.

**Paso 1. Recopile los parámetros y los requisitos de la red:** esto incluye determinar la cantidad de dispositivos host y de red, el esquema de direccionamiento IP (si ya se implementó), el tamaño del dominio y de las tablas de routing, el riesgo de los cambios en la topología y otras características de la red.

**Paso 2. Defina los parámetros de OSPF:** sobre la base de la información que recopiló en el paso 1, el administrador de red debe determinar si la implementación preferida es OSPF de área única o multiárea. Si se selecciona OSPF multiárea, el administrador de red debe tener en cuenta varias consideraciones al determinar los parámetros de OSPF, incluido lo siguiente:

* **Plan de direccionamiento IP:** este rige la manera en que se puede implementar OSPF y qué tan bien se podría escalar la implementación de OSPF. Se debe crear un plan de direccionamiento IP detallado, así como la información de división en subredes IP. Un buen plan de direccionamiento IP debe habilitar el uso de la sumarización y del diseño de OSPF multiárea. Este plan escala la red con mayor facilidad y optimiza el comportamiento de OSPF y la propagación de LSA.
* **Áreas OSPF:** la división de una red OSPF en áreas disminuye el tamaño de la LSDB y limita la propagación de las actualizaciones de estado de enlace cuando se modifica la topología. Se deben identificar los routers que van a cumplir la función de ABR y ASBR, así como los que van a realizar la sumarización o la redistribución.
* **Topología de la red:** esta consta de enlaces que conectan los equipos de red y que pertenecen a áreas OSPF diferentes en un diseño de OSPF multiárea. La topología de la red es importante para determinar los enlaces principales y de respaldo. Los enlaces principales y de respaldo se definen mediante la modificación del costo de OSPF en las interfaces. También se debe usar un plan detallado de la topología de la red para determinar las distintas áreas OSPF, el ABR y el ASBR, además de los puntos de sumarización y redistribución, si se utiliza OSPF multiárea.

**Paso 3.** Configure la implementación de OSPF multiárea según los parámetros.

**Paso 4.**Verifique la implementación de OSPF multiárea según los parámetros.

**Sumarización de rutas externas e interárea**

En OSPF, la sumarización se puede configurar solo en los ABR o los ASBR. En lugar de anunciar muchas redes específicas, los routers ABR y ASBR anuncian una ruta resumida. Los routers ABR resumen LSA de tipo 3 y los routers ASBR resumen LSA de tipo 5.

De manera predeterminada, las LSA de resumen (LSA de tipo 3) y las LSA externas (tipo 5) no contienen rutas resumidas (agregadas); es decir que, de manera predeterminada, las LSA de resumen no se resumen.

* **Sumarización de rutas interárea:** la sumarización de rutas interárea se produce en los ABR y se aplica a las rutas dentro de cada área. No se aplica a las rutas externas introducidas en OSPF mediante la redistribución. Para realizar una sumarización de rutas interárea eficaz, las direcciones de red se deben asignar de manera contigua, para que dichas direcciones se puedan resumir en una cantidad mínima de direcciones de resumen.
* **Sumarización de rutas externas:** la sumarización de rutas externas es específica de las rutas externas que se introducen en OSPF mediante la redistribución de rutas. Una vez más, es importante asegurar la contigüidad de los rangos de direcciones externas que se resumen. Por lo general, solo los ASBR resumen rutas externas. Como se muestra en la figura 2, el ASBR R2 resume las rutas externas EIGRP en una única LSA y las envía al R1 y al R3.

**Verificación de OSPF de diversas áreas**

Para verificar la topología OSPF multiárea de la ilustración, se pueden usar los mismos comandos de verificación que se utilizan para verificar OSPF de área única:

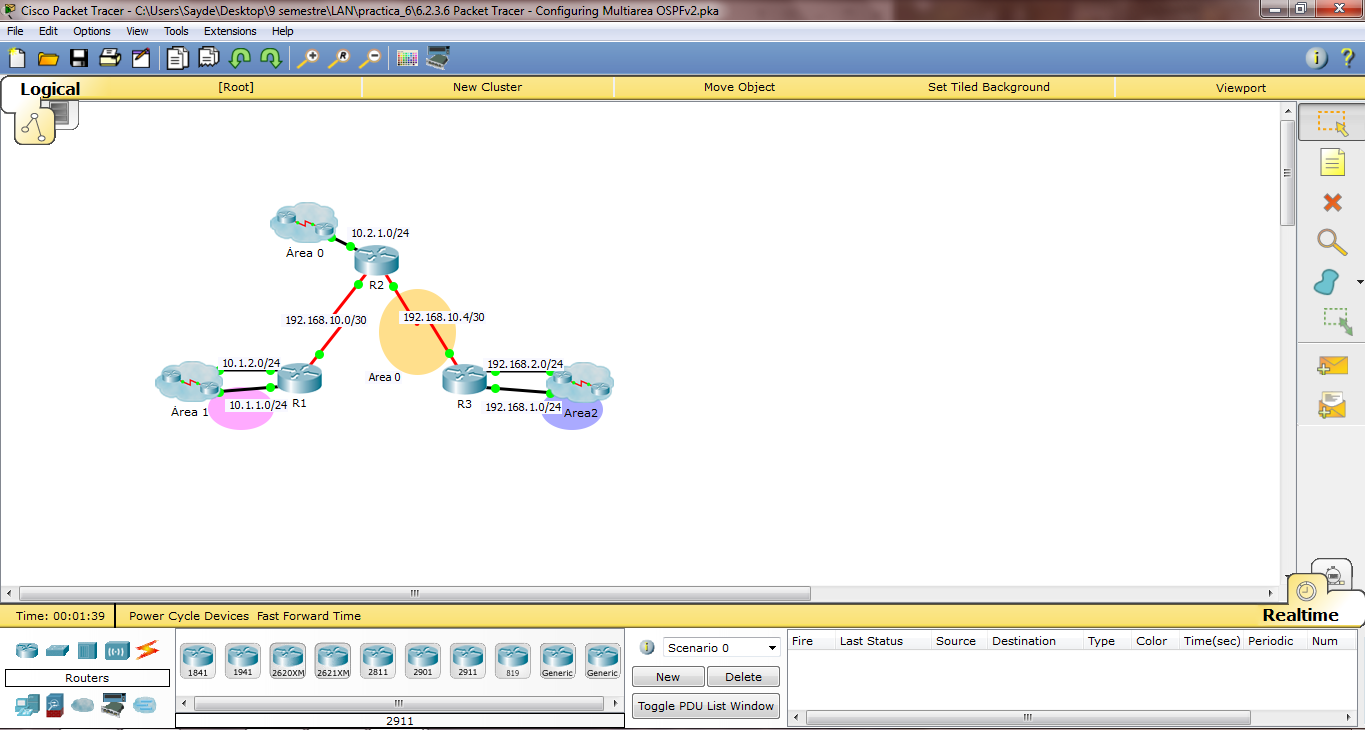
* **show ip ospf neighbor**
* **show ip ospf**
* **show ip ospf interface**

Los comandos que verifican información específica de OSPF multiárea son los siguientes:

* **show ip protocols**
* **show ip ospf interface brief**
* **show ip route ospf**
* **show ip ospf database**

**Nota:** para obtener el comando equivalente de OSPFv3, simplemente reemplace **ip** por **ipv6**.

**#6.2.3.6**



**R1**

R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1

R1(config-router)#network 10.1.1.0 0.0.0.255 area 1

R1(config-router)#network 10.1.2.0 0.0.0.255 area 1

R1(config-router)#

00:07:38: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on GigabitEthernet0/1 from LOADING to FULL, Loading Done

R1(config-router)#network 192.168.10.0 0.0.0.3 area 0

R1(config-router)#

**R2**

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router ospf 1

R2(config-router)#router-id 2.2.2.2

R2(config-router)#network 10.2.1.0 0.0.0.255 area 0

R2(config-router)#network 192.16 area 0

00:10:07: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet0/0 from LOADING trouter-id 2.2.2.2

R2(config-router)#network 192.168.10.4 0.0.0.3 area 0

R2(config-router)#network 192.168.10.0 0.0.0.3 area 0

**R3**

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router ospf 1

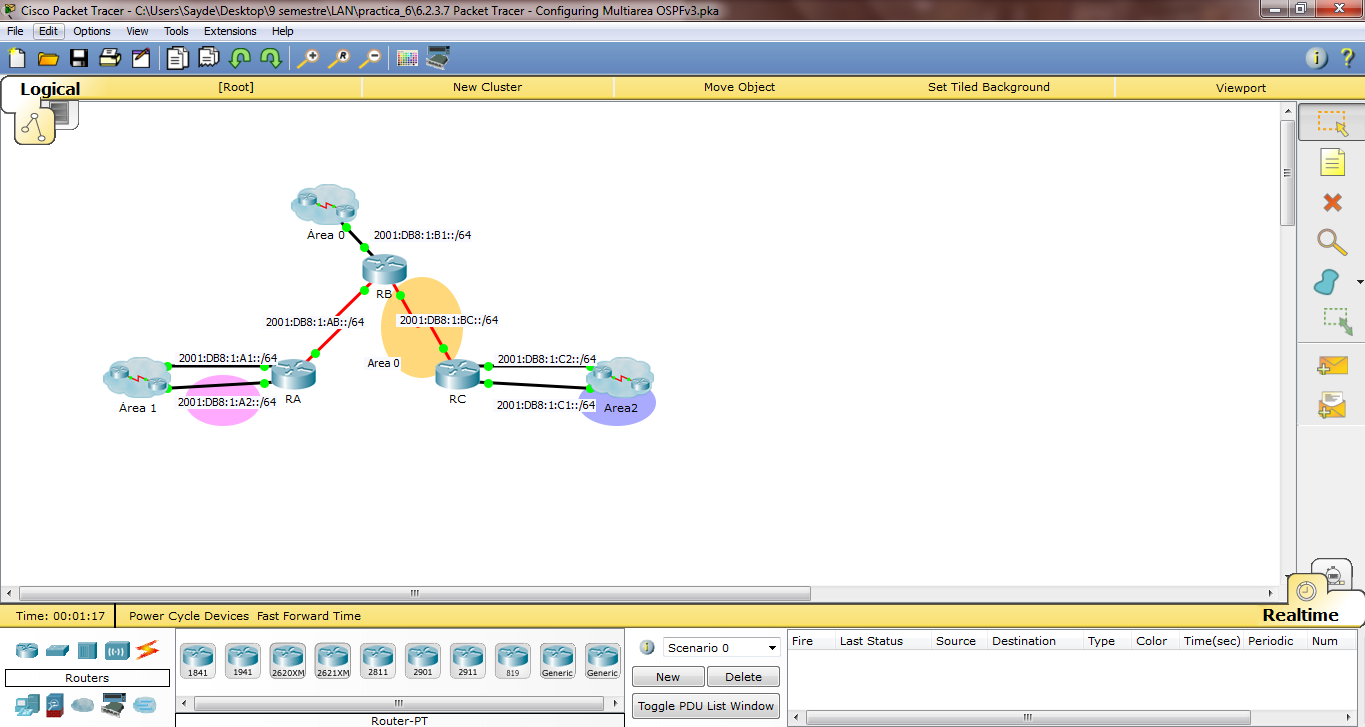
R3(config-router)#router-id 3.3.3.3

R3(config-router)#network 192.168.10.4 0.0.0.3 area 0

R3(config-router)#network 192.168.2.0 0.0.0.255 area 2

R3(config-router)#network 192.168.1.0 0.0.0.255 area 2

**#6.2.3.7**



**RA**

RA>ena

RA#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RA(config)#ipv6 unicast-routing

RA(config)#ipv6 router ospf 1

%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually

RA(config-rtr)#router-id 1.1.1.1

RA(config-rtr)#exit

RA(config)#int g0/0

RA(config-if)#ipv6 ospf 1 area 1

RA(config-if)#int g0/1

RA(config-if)#ipv6 ospf 1 area 1

RA(config-if)#int se0/0/0

RA(config-if)#ipv6 ospf 1 area 0

RA(config-if)#

**RB**

RB>ena

RB#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RB(config)#ipv6 rout

% Ambiguous command: "ipv6 rout"

RB(config)#ipv6 unicast-routing

RB(config)#ipv6 router ospf 1

RB(config-rtr)#router-id 2.2.2.2

RB(config-rtr)#exit

RB(config)#int g0/0

RB(config-if)#ipv6 ospf 1 area 0

RB(config-if)#int se0/0/0

RB(config-if)#ipv6 ospf 1 area 0

RB(config-if)#

00:07:09: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

00:07:25: %OSPFv3-5-ADJCHG: Process 1, Nbr 21.21.21.21 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

RB(config-if)#int se0/0/1

RB(config-if)#ipv6 ospf 1 area 0

RB(config-if)#

**RC**

RC>ena

RC#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RC(config)#ipv6 unicast-routing

RC(config)#ipv6 router ospf 1

%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually

RC(config-rtr)#router-id 3.3.3.3

RC(config-rtr)#exit

RC(config)#int se0/0/0

RC(config-if)#ipv6 ospf 1 area 0

OSPFv3: No IPV6 enabled on this interface

RC(config-if)#exit

RC(config)#ipv6 unicast-routing

RC(config)#int se0/0/0

RC(config-if)#ipv6 ospf 1 area 0

OSPFv3: No IPV6 enabled on this interface

RC(config-if)#int g0/0

RC(config-if)#int se0/0/1

RC(config-if)#ipv6 ospf 1 area 0

RC(config-if)#int g0/0

00:11:35: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done

RC(config-if)#int g0/0

RC(config-if)#ipv6 ospf 1 area 1

RC(config-if)#ipv6 ospf 1 area 2

00:11:54: %OSPFv3-4-AREA\_MISMATCH: Received packet with incorrect area from FE80::C1, GigabitEthernet0/0, area 0.0.0.1, packet area 0.0.0.2

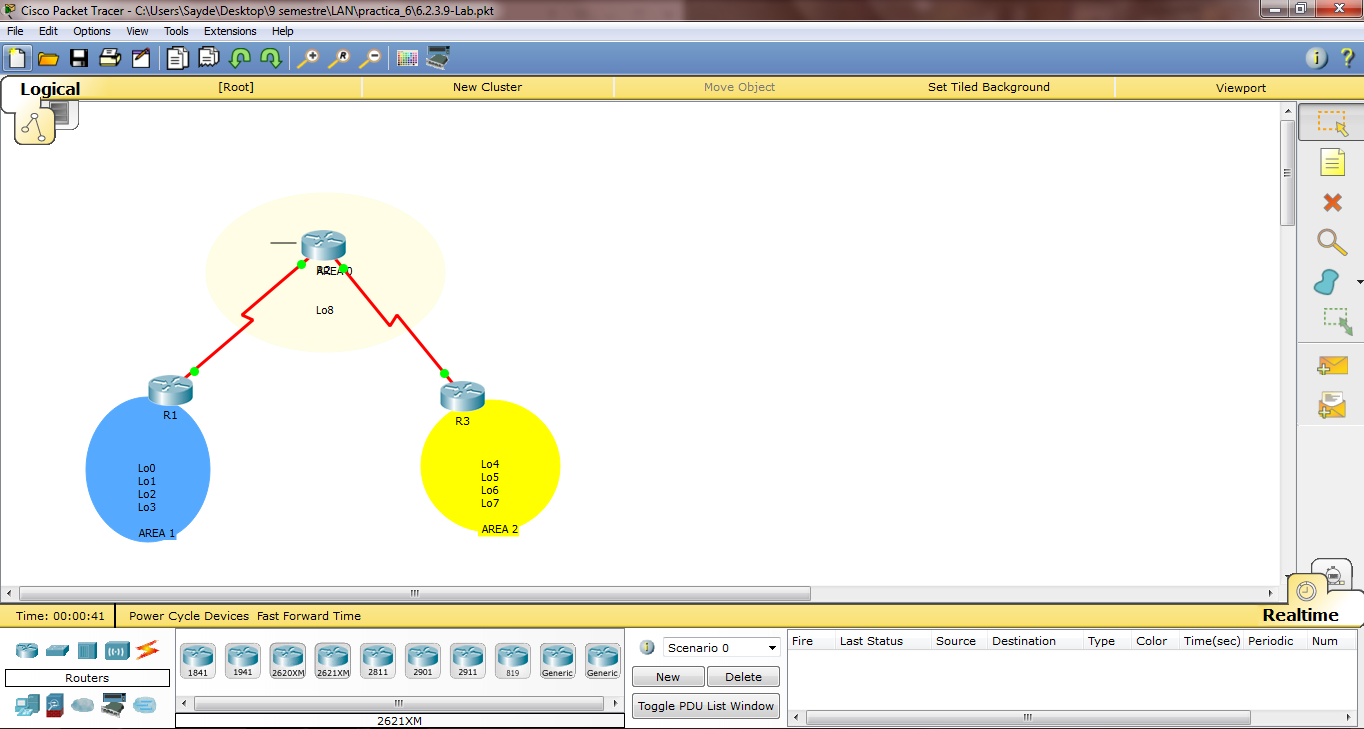
RC(config-if)#ipv6 ospf 1 area 2

RC(config-if)#int g0/1

RC(config-if)#ipv6 ospf 1 area 2

RC(config-if)#

**#6.2.3.9**



Router>EN

Router#CONF T

Router(config)#hostname R1

R1(config)#int s0/0/0

R1(config-if)#clock rate 128000

R1(config-if)#ipv6 address 2001:db8:acad:12::1/64

R1(config-if)#ipv6 address fe80::1 link-local

R1(config-if)#no shutdown

R1(config-if)#int lo0

R1(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ipv6 address 2001:db8:acad::1/64

R1(config-if)#int lo1

R1(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R1(config-if)#ipv6 address 2001:db8:acad:1::1/64

R1(config-if)#int lo2

R1(config-if)#

%LINK-5-CHANGED: Interface Loopback2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up

R1(config-if)#ipv6 address 2001:db8:acad:2::1/64

R1(config-if)#int lo3

R1(config-if)#

%LINK-5-CHANGED: Interface Loopback3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3, changed state to up

R1()#ipv6 address 2001:db8:acad:3::1/64

R1(config-if)#exit

R1(config)#ipv6 unicast-routing

R1(config)#

%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually

Router(config-rtr)#router-id 1.1.1.1

Router(config-rtr)#exit

Router(config)#int lo0

Router(config-if)#ipv6 ospf 1 area 1

Router(config-if)#ipv6 ospf network point-to-point

Router(config-if)#int lo1

Router(config-if)#ipv6 ospf 1 area 1

Router(config-if)#ipv6 ospf network point-to-point

Router(config-if)#int lo2

Router(config-if)#ipv6 ospf 1 area 1

Router(config-if)#ipv6 ospf network point-to-point

Router(config-if)#int lo3

Router(config-if)#ipv6 ospf 1 area 1

Router(config-if)#ipv6 ospf network point-to-point

Router(config-if)#int s0/0/0

Router(config-if)#ipv6 ospf 1 area 0

Router(config-if)#end

Router#

%SYS-5-CONFIG\_I: Configured from console by console

Router#show ipv6 proto

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "ospf 1"

Interfaces (Area 1)

Loopback0

Loopback1

Loopback2

Loopback3

Interfaces (Area 0)

Serial0/0/0

Redistribution:

None

Router#

00:43:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Router con0 is now available

Press RETURN to get started.

Router>en

Router#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface

2.2.2.2 0 FULL/ - 00:00:37 3 Serial0/0/0

Router#show ipv6 router ospf

^

% Invalid input detected at '^' marker.

Router#show ipv6 route ospf

IPv6 Routing Table - 18 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OI 2001:DB8:4::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:5::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:6::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:7::/64 [110/129]

via FE80::2, Serial0/0/0

O 2001:DB8:23::/64 [110/192]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:8::/64 [110/65]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:23::/64 [110/128]

via FE80::2, Serial0/0/0

Router#show ipv6 ospf database

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 1)

ADV Router Age Seq# Fragment ID Link count Bits

1.1.1.1 1462 0x80000002 0 0

Inter Area Prefix Link States (Area 1)

ADV Router Age Seq# Metric Prefix

1.1.1.1 1322 0x80000005 64 2001:DB8:ACAD:12::/64

1.1.1.1 543 0x80000006 128 2001:DB8:ACAD:23::/64

1.1.1.1 498 0x80000007 65 2001:DB8:ACAD:8::/64

1.1.1.1 493 0x80000008 192 2001:DB8:23::/64

1.1.1.1 493 0x80000009 129 2001:DB8:4::/64

1.1.1.1 493 0x8000000a 129 2001:DB8:5::/64

1.1.1.1 493 0x8000000b 129 2001:DB8:6::/64

1.1.1.1 493 0x8000000c 129 2001:DB8:7::/64

Intra Area Prefix Link States (Area 1)

ADV Router Age Seq# Link ID Ref-lstype Ref-LSID

1.1.1.1 1371 0x80000009 2 0x2001 0

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 0)

ADV Router Age Seq# Fragment ID Link count Bits

1.1.1.1 579 0x80000003 0 1 B

2.2.2.2 504 0x80000004 0 2

Router#

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ipv6 route ospf 1

^

% Invalid input detected at '^' marker.

Router(config)#ipv6 router ospf 1

Router(config-rtr)#area 1 ranger 2001:db8:acad::/62

^

% Invalid input detected at '^' marker.

Router(config-rtr)#

Router(config-rtr)#area 1 range 2001:db8:acad::/62

Router(config-rtr)#exit

Router(config)#show ipv6 route ospf

^

% Invalid input detected at '^' marker.

Router(config)#exit

Router#

%SYS-5-CONFIG\_I: Configured from console by console

Router#show ipv6 route ospf

IPv6 Routing Table - 18 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OI 2001:DB8:4::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:5::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:6::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:7::/64 [110/129]

via FE80::2, Serial0/0/0

O 2001:DB8:23::/64 [110/192]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:8::/64 [110/65]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:23::/64 [110/128]

via FE80::2, Serial0/0/0

Router#show ipv6 route ospf

IPv6 Routing Table - 18 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OI 2001:DB8:4::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:5::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:6::/64 [110/129]

via FE80::2, Serial0/0/0

OI 2001:DB8:7::/64 [110/129]

via FE80::2, Serial0/0/0

O 2001:DB8:23::/64 [110/192]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:8::/64 [110/65]

via FE80::2, Serial0/0/0

O 2001:DB8:ACAD:23::/64 [110/128]

via FE80::2, Serial0/0/0

Router#

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#Hostname R2

Router(config)#int s0/0/0

Router(config-if)#ipv6 address 2001:db8:acad:12::2/64

Router(config-if)#ipv6 address fe80::2 link-local

Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Router(config-if)#int s0/0/1

Router(config-if)#clock rate 128000

Router(config-if)#ipv6 address 2001:db8:acad:23::2/64

Router(config-if)#ipv6 address fe80::2 link-local

Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Router(config-if)#int lo8

Router(config-if)#

%LINK-5-CHANGED: Interface Loopback8, changed state to up

Router(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router(config-if)#ipv6 address 2001:db8:acad:8::1/64

R2>

R2>en

R2#show ipv6 ospf

Routing Process "ospfv3 1" with ID 2.2.2.2

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs

Retransmission pacing timer 66 msecs

Number of external LSA 0. Checksum Sum 0x000000

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Reference bandwidth unit is 100 mbps

Area BACKBONE(0)

Number of interfaces in this area is 3

SPF algorithm executed 6 times

Number of LSA 8. Checksum Sum 0x03a88c

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#int s0/0/0

R2(config-if)#ipv6 ospf 1 area 0

R2(config-if)#int s0/0/1

R2(config-if)#ipv6 ospf 1 area 0

R2(config-if)#

R2(config-if)#int lo8

R2(config-if)#ipv6 ospf 1 area 0

R2(config-if)#ipv6 ospf network point-to-point

R2(config-if)#end

R2#

%SYS-5-CONFIG\_I: Configured from console by console

R2#show ipv6 ospf interface

Serial0/0/0 is up, line protocol is up

Link Local Address FE80::2, Interface ID 3

Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2

Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:03

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1 , Adjacent neighbor count is 1

Adjacent with neighbor 1.1.1.1

Suppress hello for 0 neighbor(s)

Serial0/0/1 is up, line protocol is up

Link Local Address FE80::2, Interface ID 4

Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2

Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:01

Index 2/2, flood queue length 0

R2#

01:15:15: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done

R2#show ipv6 neighbor

R2#

R2#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface

3.3.3.3 0 FULL/ - 00:00:37 4 Serial0/0/1

1.1.1.1 0 FULL/ - 00:00:38 3 Serial0/0/0

R2#show ipv6 ospf database

OSPF Router with ID (2.2.2.2) (Process ID 1)

Router Link States (Area 0)

ADV Router Age Seq# Fragment ID Link count Bits

1.1.1.1 702 0x80000003 0 1 B

2.2.2.2 627 0x80000004 0 2

3.3.3.3 627 0x80000002 0 1 B

Inter Area Prefix Link States (Area 0)

ADV Router Age Seq# Metric Prefix

1.1.1.1 1444 0x80000005 1 2001:DB8:ACAD::/64

1.1.1.1 1444 0x80000006 1 2001:DB8:ACAD:1::/64

1.1.1.1 1444 0x80000007 1 2001:DB8:ACAD:2::/64

1.1.1.1 1444 0x80000008 1 2001:DB8:ACAD:3::/64

3.3.3.3 621 0x80000001 1 2001:DB8:4::/64

3.3.3.3 621 0x80000002 1 2001:DB8:5::/64

3.3.3.3 621 0x80000003 1 2001:DB8:6::/64

3.3.3.3 621 0x80000004 1 2001:DB8:7::/64

Link (Type-8) Link States (Area 0)

ADV Router Age Seq# Link ID Interface

2.2.2.2 701 0x80000004 3 Se0/0/0

1.1.1.1 708 0x80000003 3 Se0/0/0

2.2.2.2 629 0x80000006 4 Se0/0/1

3.3.3.3 627 0x80000002 4 Se0/0/1

Intra Area Prefix Link States (Area 0)

ADV Router Age Seq# Link ID Ref-lstype Ref-LSID

2.2.2.2 625 0x80000005 2 0x2001 0

1.1.1.1 1448 0x80000002 2 0x2001 0

3.3.3.3 629 0x80000001 2 0x2001 0

R2 con0 is now available

Press RETURN to get started.

R2>en

R2#show ipv6 router ospf

^

% Invalid input detected at '^' marker.

R2#show ipv6 route ospf

IPv6 Routing Table - 14 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OI 2001:DB8:4::/64 [110/65]

via FE80::3, Serial0/0/1

OI 2001:DB8:5::/64 [110/65]

via FE80::3, Serial0/0/1

OI 2001:DB8:6::/64 [110/65]

via FE80::3, Serial0/0/1

OI 2001:DB8:7::/64 [110/65]

via FE80::3, Serial0/0/1

O 2001:DB8:23::/64 [110/128]

via FE80::3, Serial0/0/1

OI 2001:DB8:ACAD::/62 [110/65]

via FE80::1, Serial0/0/0

OI 2001:DB8:ACAD::/64 [110/65]

via FE80::1, Serial0/0/0

R2#

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname r3

r3(config)#int s0/0/1

r3(config-if)#ipv6 address 2001:db8:acad:23::3/64

r3(config-if)#ipv6 address fe80::3 link-local

r3(config-if)#no shutdown

r3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

r3(config-if)#int lo4

r3(config-if)#ipv6 address 2001:db8:acad:4::1/64

r3(config-if)#int lo5

r3(config-if)#ipv6 address 2001:db8:acad:5::1/64

r3(config-if)#int lo6

r3(config-if)#

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

r3(config-if)#ipv6 address 2001:db8:acad:6::1/64

r3(config-if)#int lo7

r3(config-if)#

%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up

r3(config-if)#ipv6 address 2001:db8:acad:7::1/64

r3(config-if)#int lo8

r3(config-if)#

%LINK-5-CHANGED: Interface Loopback8, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback8, changed state to up

R3>en

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int lo4

R3(config-if)#ipv6 ospf 1 area 2

R3(config-if)#ipv6 ospf network point-to-point

R3(config-if)#int lo5

R3(config-if)#ipv6 ospf 1 area 2

R3(config-if)#ipv6 ospf network point-to-point

R3(config-if)#ipv6 ospf 1 area 2

R3(config-if)#ipv6 ospf network point-to-point

R3(config-if)#int lo6

R3(config-if)#ipv6 ospf 1 area 2

R3(config-if)#ipv6 ospf network point-to-point

R3(config-if)#int lo7

R3(config-if)#ipv6 ospf 1 area 2

R3(config-if)#ipv6 ospf network point-to-point

R3(config-if)#int s0/0/1

R3(config-if)#ipv6 ospf 1 area 0

R3(config-if)#

01:14:58: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-if)#end

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#show ipv6 ospf

Routing Process "ospfv3 1" with ID 3.3.3.3

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs

Retransmission pacing timer 66 msecs

Number of external LSA 0. Checksum Sum 0x000000

Number of areas in this router is 2. 2 normal 0 stub 0 nssa

Reference bandwidth unit is 100 mbps

Area 2

Number of interfaces in this area is 4

SPF algorithm executed 7 times

Number of LSA 10. Checksum Sum 0x0326f2

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

Area BACKBONE(0)

Number of interfaces in this area is 1

SPF algorithm executed 2 times

Number of LSA 14. Checksum Sum 0x07ca22

Number of DCbitless LSA 0

R3#

R3 con0 is now available

Press RETURN to get started.

R3>en

R3#show ipv6 ospf database

OSPF Router with ID (3.3.3.3) (Process ID 1)

Router Link States (Area 2)

ADV Router Age Seq# Fragment ID Link count Bits

3.3.3.3 819 0x80000001 0 0

Inter Area Prefix Link States (Area 2)

ADV Router Age Seq# Metric Prefix

3.3.3.3 693 0x80000001 64 2001:DB8:23::/64

3.3.3.3 684 0x80000002 128 2001:DB8:ACAD:12::/64

3.3.3.3 684 0x80000003 128 2001:DB8:ACAD:23::/64

3.3.3.3 684 0x80000004 65 2001:DB8:ACAD:8::/64

3.3.3.3 684 0x80000005 129 2001:DB8:ACAD::/64

3.3.3.3 684 0x80000006 129 2001:DB8:ACAD:1::/64

3.3.3.3 684 0x80000007 129 2001:DB8:ACAD:2::/64

3.3.3.3 684 0x80000008 129 2001:DB8:ACAD:3::/64

Intra Area Prefix Link States (Area 2)

ADV Router Age Seq# Link ID Ref-lstype Ref-LSID

3.3.3.3 719 0x80000008 2 0x2001 0

OSPF Router with ID (3.3.3.3) (Process ID 1)

Router Link States (Area 0)

ADV Router Age Seq# Fragment ID Link count Bits

1.1.1.1 774 0x80000003 0 1 B

3.3.3.3 699 0x80000002 0 1 B

2.2.2.2 698 0x80000004 0 2

Inter Area Prefix Link States (Area 0)

ADV Router Age Seq# Metric Prefix

1.1.1.1 1516 0x80000005 1 2001:DB8:ACAD::/64

1.1.1.1 1516 0x80000006 1 2001:DB8:ACAD:1::/64

1.1.1.1 1516 0x80000007 1 2001:DB8:ACAD:2::/64

1.1.1.1 1516 0x80000008 1 2001:DB8:ACAD:3::/64

3.3.3.3 693 0x80000001 1 2001:DB8:4::/64

3.3.3.3 693 0x80000002 1 2001:DB8:5::/64

3.3.3.3 693 0x80000003 1 2001:DB8:6::/64

3.3.3.3 693 0x80000004 1 2001:DB8:7::/64

Link (Type-8) Link States (Area 0)

ADV Router Age Seq# Link ID Interface

3.3.3.3 699 0x80000002 4 Se0/0/1

2.2.2.2 701 0x80000006 4 Se0/0/1

Intra Area Prefix Link States (Area 0)

ADV Router Age Seq# Link ID Ref-lstype Ref-LSID

3.3.3.3 701 0x80000001 2 0x2001 0

1.1.1.1 1520 0x80000002 2 0x2001 0

2.2.2.2 698 0x80000005 2 0x2001 0

R3#

R3#show ipv6 router ospf

^

% Invalid input detected at '^' marker.

R3#show ipv6 route ospf

IPv6 Routing Table - 16 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OI 2001:DB8:ACAD::/62 [110/129]

via FE80::2, Serial0/0/1

OI 2001:DB8:ACAD::/64 [110/129]

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:8::/64 [110/65]

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:12::/64 [110/128]

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:23::/64 [110/128]

via FE80::2, Serial0/0/1

R3#ipv6 router ospf 1

^

% Invalid input detected at '^' marker.

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#ipv6 router ospf 1

R3(config-rtr)#area 2 range 2001:db8:acad:4::/62

R3(config-rtr)#end

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#show ipv6 route ospf

IPv6 Routing Table - 16 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OI 2001:DB8:ACAD::/62 [110/129]

via FE80::2, Serial0/0/1

OI 2001:DB8:ACAD::/64 [110/129]

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:8::/64 [110/65]

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:12::/64 [110/128]

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:23::/64 [110/128]

via FE80::2, Serial0/0/1

R3#

**CAPÍTULO 7**

**Características de EIGRP**

EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF, como una RFC informativa. Esto significa que otros proveedores de redes ahora pueden implementar EIGRP en sus equipos para que interoperen con routers que ejecuten EIGRP, ya sean de Cisco o de otros fabricantes. Sin embargo, las características avanzadas de EIGRP, como las rutas internas de EIGRP necesarias para la implementación de la red privada virtual dinámica multipunto (DMVPN), no se cederán al IETF. Como RFC informativa, Cisco mantendrá el control de EIGRP.

EIGRP incluye características de protocolos de routing de estado de enlace y vector distancia. Sin embargo, aún se basa en el principio clave del protocolo de routing vector distancia, según el cual la información acerca del resto de la red se obtiene a partir de vecinos conectados directamente.

EIGRP es un protocolo de routing vector distancia avanzado que incluye características que no se encuentran en otros protocolos de routing vector distancia, como RIP e IGRP.

Las características principales de EIGRP son:

* Es un protocolo de transporte confiable
* Establece adyacencias
* Usa tablas de vecinos y topología
* Utiliza el algoritmo de actualización por difusión (DUAL).
* Usa actualizaciones ilimitadas

EIGRP tiene la capacidad para enrutar varios protocolos diferentes, incluidos IPv4 e IPv6, mediante el uso de módulos dependientes de protocolo (PDM). Si bien ahora son obsoletos, EIGRP también usaba PDM para enrutar los protocolos de capa de red IPX de Novell y Apple Talk de Apple Computer. Los PDM son responsables de tareas específicas de los protocolos de capa de red. Un ejemplo de esto es el módulo de EIGRP, que es responsable de enviar y recibir paquetes EIGRP encapsulados en IPv4. Este módulo también es responsable de analizar los paquetes EIGRP y de informar a DUAL la nueva información recibida. EIGRP pide a DUAL que tome decisiones de routing, pero los resultados se almacenan en la tabla de routing IPv4.

Los PDM son responsables de las tareas específicas de routing de cada protocolo de capa de red, incluido lo siguiente:

* Mantener las tablas de vecinos y de topología de los routers EIGRP que pertenecen a esa suite de protocolos.
* Construir y traducir paquetes específicos del protocolo para DUAL.
* Conectar a DUAL con la tabla de routing específica del protocolo.
* Calcular la métrica y pasar esa información a DUAL.
* Implementar listas de filtrado y de acceso.
* Realizar funciones de redistribución hacia otros protocolos de routing y desde ellos.
* Redistribuir rutas descubiertas por otros protocolos de routing.

Cuando un router descubre a un nuevo vecino, registra su dirección y su interfaz como una entrada en la tabla de vecinos. Existe una tabla de vecinos para cada módulo dependiente de protocolo, como IPv4. EIGRP también mantiene una tabla de topología. La tabla de topología contiene todos los destinos que anuncian los routers vecinos. También existe una tabla de topología separada para cada PDM.

**Actualizaciones y Mecanismos de EIGRP**

EIGRP no envía actualizaciones periódicas y las entradas de ruta no expiran. EIGRP utiliza un protocolo Hello (muy ligero) para comprobar que sigue conectado a sus vecinos.  
Sólo los nuevos cambios (por ejemplo cambios en la topología o la desconexión de una interfaz) producen una actualización de enrutamiento. DUAL nos asegura rutas sin bucles.

EIGRP no utiliza temporizadores de espera. Lo que hace es buscar las rutas por medio de un sistema de cálculos de ruta entre los routers.  
La consecuencia es una convergencia más rápida que la de los protocolos de enrutamiento vector distancia.

Los routers EIGRP descubren vecinos y establecen adyacencias mediante el paquete de saludo.

EIGRP envía actualizaciones parciales y limitadas (sólo propaga actualizaciones parciales de aquellos routers que se ven afectados por un cambio). De esta forma eigrp minimiza el ancho de banda requerido para enviar los paquetes EIGRP.

EIGRP utiliza el protocolo de transporte confiable (RTP) para la entrega y recepción de paquetes EIGRP. EIGRP se diseñó como un protocolo de routing independiente de capa de red y; debido a este diseño, no puede usar los servicios de UDP o TCP. Esto permite que EIGRP se utilice para protocolos distintos de aquellos de la suite de protocolos TCP/IP, como IPX y Apple Talk. En la ilustración se muestra conceptualmente cómo opera RTP. Si bien el término “confiable” forma parte de su nombre, RTP incluye entrega confiable y entrega poco confiable de los paquetes EIGRP, de manera similar a TCP y UDP respectivamente. RTP confiable requiere que el receptor envíe un acuse de recibo al emisor. Los paquetes RTP poco confiables no requieren acuse de recibo. Por ejemplo, un paquete de actualización EIGRP se envía de manera confiable por RTP y requiere un acuse de recibo. Un paquete de saludo EIGRP también se envía por RTP, pero de manera poco confiable. Esto significa que los paquetes de saludo EIGRP no requieren un acuse de recibo.

RTP puede enviar paquetes EIGRP como unidifusión o multidifusión.

* Los paquetes de multidifusión EIGRP para IPv4 utilizan la dirección IPv4 de multidifusión reservada 224.0.0.10.
* Los paquetes de multidifusión EIGRP para IPv6 se envían a la dirección IPv6 de multidifusión reservada FF02: A.

**Tipos de paquetes EIGRP**

EIGRP utiliza cinco tipos de paquetes distintos, algunos en pares. Los paquetes EIGRP se envían mediante entrega RTP confiable o poco confiable y se pueden enviar como unidifusión o multidifusión —o, a veces, de ambas maneras. Los tipos de paquetes EIGRP también reciben el nombre de “formatos de paquetes EIGRP” o “mensajes EIGRP”.

**Paquetes de saludo:** se utilizan para descubrir a los vecinos y para mantener las adyacencias de vecinos.

* Enviados con entrega poco confiable
* Multidifusión (en la mayoría de los tipos de redes)

**Paquetes de actualización:** propagan información de routing a vecinos EIGRP.

* Enviados con entrega confiable
* Unidifusión o multidifusión

**Paquetes de acuse de recibo:** se utilizan para acusar recibo de un mensaje EIGRP que se envió con entrega confiable.

* Enviados con entrega poco confiable
* Unidifusión

**Paquetes de consulta:** se utilizan para consultar rutas de vecinos.

* Enviados con entrega confiable
* Unidifusión o multidifusión

**Paquetes de respuesta:** se envían en respuesta a consultas EIGRP.

* Enviados con entrega poco confiable
* Unidifusión

**Paquetes de EIGRP**

**Paquetes de Saludo**

EIGRP utiliza pequeños paquetes de saludo para descubrir otros routers con EIGRP habilitado en enlaces conectados directamente. Los routers utilizan los paquetes de saludo para formar adyacencias de vecinos EIGRP, también conocidas como “relaciones de vecinos”.

Los paquetes de saludo EIGRP se envían como transmisiones IPv4 o IPv6 de multidifusión y utilizan entrega RTP poco confiable. Esto significa que el receptor no responde con un paquete de acuse de recibo.

* La dirección de multidifusión EIGRP reservada para IPv4 es 224.0.0.10.
* La dirección de multidifusión EIGRP reservada para IPv6 es FF02:vA.

Los routers EIGRP descubren vecinos y establecen adyacencias con los routers vecinos mediante el paquete de saludo. En la mayoría de las redes, los paquetes de saludo EIGRP se envían como paquetes de multidifusión cada cinco segundos. Sin embargo, en redes multipunto multiacceso sin difusión (NBMA), como X.25, Frame Relay, e interfaces de modo de transferencia asíncrona (ATM) con enlaces de acceso de T1 (1,544 Mb/s) o más lentos, los paquetes de saludo se envían como paquetes de unidifusión cada 60 segundos.

EIGRP también usa paquetes de saludo para mantener adyacencias establecidas. Un router EIGRP supone que, mientras reciba paquetes de saludo de un vecino, el vecino y sus rutas siguen siendo viables.

EIGRP utiliza un temporizador de espera para determinar el tiempo máximo que el router debe esperar para recibir el siguiente saludo antes de declarar que el vecino es inalcanzable. De manera predeterminada, el tiempo de espera es tres veces el intervalo de saludo, es decir, 15 segundos en la mayoría de las redes y 180 segundos en redes NBMA de baja velocidad. Si el tiempo de espera expira, EIGRP declara la ruta como inactiva y DUAL busca una nueva ruta mediante el envío de consultas.

**Paquetes de actualización**

EIGRP envía paquetes de actualización para propagar información de routing. Los paquetes de actualización se envían sólo cuando es necesario. Las actualizaciones de EIGRP sólo contienen la información de enrutamiento necesaria y sólo se envían a los routers que la requieren.

A diferencia de RIP, EIGRP (otro protocolo de routing vector distancia) no envía actualizaciones periódicas, y las entradas de ruta no vencen. En cambio, EIGRP envía actualizaciones incrementales solo cuando se modifica el estado de un destino. Esto puede incluir cuando una nueva red está disponible, cuando una red existente deja de estar disponible, o cuando ocurre un cambio en la métrica de routing de una red existente.

En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos *parcial*es y limitados. El término parcial significa que la actualización sólo envía información acerca de los cambios de ruta. El término “limitada” se refiere a la propagación de las actualizaciones parciales que se envían solo a aquellos routers que se ven afectados por el cambio. Al enviar solo la información de routing necesaria únicamente a los routers que la necesitan, EIGRP minimiza el ancho de banda que se requiere para enviar actualizaciones EIGRP.

Los paquetes de actualización EIGRP usan entrega confiable, lo que significa que el router emisor requiere un acuse de recibo. Los paquetes de actualización se envían como multicast cuando son requeridos por múltiples routers, o como unicast cuando son requeridos por sólo un router. En la figura, debido a que los enlaces son punto a punto, las actualizaciones se envían como unicast.

EIGRP envía paquetes de acuse de recibo (ACK) cuando se usa el método de entrega confiable. Un acuse de recibo EIGRP es un paquete de saludo EIGRP sin ningún dato. RTP utiliza una entrega confiable para los paquetes EIGRP de actualización, consulta y respuesta. Los paquetes de acuse de recibo EIGRP se envían siempre como transmisiones de unidifusión poco confiables. El sentido de la entrega poco confiable es que, de otra manera, habría un bucle interminable de acuses de recibo.

**Paquetes de consulta y respuesta**

**\*Paquetes de consulta EIGRP**

DUAL utiliza paquetes de consulta y de respuesta cuando busca redes y cuando realiza otras tareas. Los paquetes de consulta y respuesta utilizan una entrega confiable. Las consultas utilizan multicast o unicast, mientras que las respuestas se envíen siempre como unicast.

En la figura, R2 ha perdido la conectividad con LAN y envía consultas a todos los vecinos EIGRP y busca cualquier ruta posible hacia la LAN. Debido a que las consultas utilizan entrega confiable, el router receptor debe devolver un paquete de acuse de recibo EIGRP. El acuse de recibo informa al emisor de la consulta que se recibió el mensaje de consulta. Para que el ejemplo sea más simple, se omitieron los acuses de recibo en el gráfico.

**\*Paquetes de respuesta EIGRP**

Todos los vecinos deben enviar una respuesta, independientemente de si tienen o no una ruta a la red fuera de servicio. Debido a que las respuestas también usan entrega confiable, los routers como el R2 deben enviar un acuse de recibo.

Quizá no sea obvio por qué el R2 debería enviar una consulta para una red que sabe que está inactiva. En realidad, solo la interfaz del R2 que está conectada a la red está inactiva. Otro router podría estar conectado a la misma LAN y tener una ruta alternativa a la misma red. Por lo tanto, el R2 consulta por un router tal antes de eliminar completamente la red de su tabla de topología.

**Encapsulamiento de mensajes**

La porción de datos de un mensaje EIGRP se encapsula en un paquete. Este campo de datos se llama “tipo, longitud, valor” (TLV). Los tipos de TLV pertinentes a este curso son los parámetros de EIGRP, las rutas IP internas y las rutas IP externas.

El encabezado del paquete EIGRP se incluye con cada paquete EIGRP, independientemente de su tipo. Luego, el encabezado del paquete EIGRP y el TLV se encapsulan en un paquete IPv4. En el encabezado del paquete IPv4, el campo de protocolo se establece en 88 para indicar EIGRP, y la dirección IPv4 de destino se establece en multidifusión 224.0.0.10. Si el paquete EIGRP se encapsula en una trama de Ethernet, la dirección MAC de destino también es una dirección de multidifusión, 01-00-5E-00-00-0A. EIGRP para IPv6 usa un tipo de encapsulación similar. EIGRP para IPv6 se encapsula con un encabezado de IPv6. La dirección IPv6 de destino es la dirección de multidifusión FF02: A, y el campo de encabezado siguiente se establece en 88.

**TLV y encabezado de paquetes**

Todos los paquetes EIGRP incluyen el encabezado, como se muestra en la figura 1. Los campos importantes incluyen el campo de código de operación y el campo de número de sistema autónomo. El código de operación especifica el tipo de paquete EIGRP de la siguiente manera:

* Actualizar
* Consulta
* Respuesta
* Saludo

El número de sistema autónomo especifica el proceso de routing EIGRP. A diferencia de RIP, se pueden ejecutar varias instancias de EIGRP en una red, y el número de sistema autónomo se usa para realizar el seguimiento de cada proceso EIGRP en ejecución.

El mensaje de parámetros de EIGRP incluye las ponderaciones que EIGRP usa para su métrica compuesta. Solo el ancho de banda y el retardo se ponderan de manera predeterminada. Ambos se ponderan de igual manera, por ello, tanto el campo K1 para el ancho de banda como el campo K3 para el retraso se establecen en uno (1). Los demás valores K se establecen en cero (0).

El Tiempo de espera es la cantidad de tiempo que el vecino EIGRP que recibe este mensaje debe esperar antes de considerar que router que realiza la notificación se encuentra desactivada. El mensaje de IP internas se usa para anunciar las rutas EIGRP dentro de un sistema autónomo. Los campos importantes incluyen los campos de métrica (retraso y ancho de banda), el campo de máscara de subred (longitud de prefijo) y el campo de destino.

El retardo se calcula como la suma de retardos desde el origen hacia el destino en unidades de 10 microsegundos. El ancho de banda es el que cuenta con la configuración más baja en todas las interfaces de la ruta.

La máscara de subred se especifica como la duración de prefijo o el número de bits de la red en la máscara de subred. Por ejemplo, la longitud de prefijo para la máscara de subred 255.255.255.0 es 24, porque 24 es el número de bits de red.

El campo Destino almacena la dirección de la red de destino. A pesar de que se muestran sólo 24 bits en esta figura, este campo varía en función del valor de la porción de red de la dirección de red de 32 bits. Por ejemplo, la porción de red de 10.1.0.0/16 es 10.1; por lo tanto, el campo de destino almacena los primeros 16 bits. Como la longitud mínima de este campo es de 24 bits, el resto del campo se rellena con ceros. Si una dirección de red es más larga que 24 bits (192.168.1.32/27, por ejemplo), entonces el campo Destino se extiende otros 32 bits más (con un total de 56 bits) y los bits no utilizados se completan con ceros.

**Funcionamiento de EIGRP**

**Adyacencia de Vecinos**

El objetivo de cualquier protocolo de routing dinámico es descubrir redes remotas de otros routers y lograr la convergencia en el dominio de routing. Antes de que se pueda intercambiar cualquier paquete de actualización EIGRP entre routers, EIGRP debe descubrir a sus vecinos. Los EIGRP vecinos son otros routers que ejecutan EIGRP en redes conectadas directamente.

EIGRP utiliza paquetes de saludo para establecer y mantener las adyacencias de vecinos. Para que dos routers EIGRP se conviertan en vecinos, deben coincidir varios parámetros entre ambos. Por ejemplo, dos routers EIGRP deben usar los mismos parámetros de métrica de EIGRP y ambos deben estar configurados con el mismo número de sistema autónomo.

Cada router EIGRP mantiene una tabla de vecinos, que contiene una lista de los routers en los enlaces compartidos que tienen una adyacencia EIGRP con ese router. La tabla de vecinos se usa para rastrear el estado de estos vecinos EIGRP.

Las actualizaciones de EIGRP contienen redes a las que se puede llegar desde el router que envía la actualización. A medida que se intercambian actualizaciones EIGRP entre vecinos, el router receptor agrega esas entradas a su tabla de topología de EIGRP.

Cada router EIGRP mantiene una tabla de topología para cada protocolo de routing configurado, como IPv4 e IPv6. La tabla de topología incluye las entradas de ruta para cada destino que el router descubre de sus vecinos EIGRP conectados directamente. Cuando un router recibe una actualización de routing EIGRP, agrega la información de routing a su tabla de topología de EIGRP y responde con un acuse de recibo EIGRP.

1. El R1 recibe la actualización de EIGRP del vecino R2 e incluye información acerca de las rutas que anuncia el vecino, incluida la métrica a cada destino. El R1 agrega todas las entradas de actualización a su tabla de topología. La tabla de topología incluye todos los destinos anunciados por los routers vecinos (adyacentes) y el costo (métrica) para llegar a cada red.

2. Los paquetes de actualización EIGRP utilizan entrega confiable; por lo tanto, el R1 responde con un paquete de acuse de recibo EIGRP que informa al R2 que recibió la actualización.

3. El R1 envía una actualización de EIGRP al R2 en la que anuncia las redes que conoce, excepto aquellas descubiertas del R2 (horizonte dividido).

4. El R2 recibe la actualización de EIGRP del vecino R1 y agrega esta información a su propia tabla de topología.

5. El R2 responde al paquete de actualización EIGRP del R1 con un acuse de recibo EIGRP.

**Métricas EIGRP**

**Métrica compuesta de EIGRP**

De manera predeterminada, EIGRP utiliza los siguientes valores en su métrica compuesta para calcular la ruta preferida a una red:

* **Ancho de banda:** el ancho de banda más lento entre todas las interfaces de salida, a lo largo de la ruta de origen a destino.
* **Retraso:** la acumulación (suma) de todos los retrasos de las interfaces a lo largo de la ruta (en decenas de microsegundos).

Se pueden utilizar los valores siguientes, pero no se recomienda, porque generalmente dan como resultado recálculos frecuentes de la tabla de topología:

* **Confiabilidad:** representa la peor confiabilidad entre origen y destino, que se basa en keepalives.
* **Carga:** representa la peor carga en un enlace entre origen y destino, que se calcula sobre la base de la velocidad de paquetes y el ancho de banda configurado de la interfaz.

**La métrica compuesta**

La fórmula consiste en los valores K1 a K5, conocidos como “ponderaciones de la métrica de EIGRP”. K1 y K3 representan el ancho de banda y el retraso, respectivamente. K2 representa carga, y K4 y K5 representan la confiabilidad. De manera predeterminada, K1 y K3 están establecidos en 1, y K2, K4 y K5 están establecidos en 0. Como resultado, solamente se usan los valores de ancho de banda y de retraso en el cómputo de la métrica compuesta predeterminada. En EIGRP para IPv4 y EIGRP para IPv6 se utiliza la misma fórmula para la métrica compuesta. El método para calcular la métrica (valores *k*) y el número de sistema autónomo de EIGRP deben coincidir entre vecinos EIGRP. Si no coinciden, los routers no forman una adyacencia.

Los valores *k* predeterminados se pueden cambiar con el comando **metric weights** del modo de configuración del router:

Router (config-router)# **metric weights** *tos* *k1 k2 k3 k4 k5*

**Verificación de los valores *k***

El comando **show ip protocols** se utiliza para verificar los valores *k*. En la figura 2, se muestra el resultado del comando para el R1. Observe que los valores *k* en el R1 están establecidos en la configuración predeterminada.

**Examen de los valores de la métrica**

El comando **show interfaces** muestra información de las interfaces, incluidos los parámetros utilizados para el cálculo de la métrica de EIGRP. En la ilustración, se muestra el comando **show interfaces** para la interfaz Serial 0/0/0 en el R1.

* **BW:** ancho de banda de la interfaz (en kilobits por segundo).
* **DLY:** retraso de la interfaz (en microsegundos).
* **Reliability:** confiabilidad de la interfaz expresada como una fracción de 255 (255/255 es una confiabilidad del 100%), calculada como un promedio exponencial durante cinco minutos. De manera predeterminada, EIGRP no incluye su valor al calcular la métrica.
* **Txload, Rxload:** carga transmitida y recibida a través de la interfaz expresada como una fracción de 255 (255/255 es completamente saturada), calculada como un promedio exponencial durante cinco minutos. De manera predeterminada, EIGRP no incluye su valor al calcular la métrica.

**Métrica de ancho de banda**

La métrica de ancho de banda es un valor estático que usan algunos protocolos de routing, como EIGRP y OSPF, para calcular la métrica de routing. El ancho de banda se muestra en kilobits por segundo (kb/s). La mayoría de las interfaces seriales usan el valor de ancho de banda predeterminado de 1544 kb/s o 1 544 000 b/s (1,544 Mb/s). Éste es el ancho de banda de una conexión T1. Sin embargo, algunas interfaces seriales utilizan otro valor de ancho de banda predeterminado. En la figura 1, se muestra la topología que se utiliza en esta sección. Es posible que los tipos de interfaces seriales y sus anchos de banda asociados no reflejen necesariamente los tipos de conexiones más frecuentes que se encuentran en las redes en la actualidad.

Verifique siempre el ancho de banda con el comando **show interfaces**.

El valor predeterminado del ancho de banda puede reflejar o no el ancho de banda físico real de la interfaz. Si el ancho de banda real del enlace difiere del valor de ancho de banda predeterminado, se debe modificar el valor de ancho de banda.

**Configuración del parámetro de ancho de banda**

En la mayoría de los enlaces seriales, la métrica de ancho de banda predeterminada es 1544 kb/s. Debido a que EIGRP y OSPF utilizan el ancho de banda en los cálculos métricos predeterminados, un valor correcto para el ancho de banda es muy importante para la precisión de la información de enrutamiento.

Utilice el siguiente comando del modo de configuración de interfaz para modificar la métrica de ancho de banda:

Router (config-if)# **bandwidth** *kilobits-bandwidth-value*

Utilice el comando **no bandwidth** para restaurar el valor predeterminado.

En la figura 2, el enlace entre el R1 y el R2 tiene un ancho de banda de 64 kb/s, y el enlace entre el R2 y el R3 tiene un ancho de banda de 1024 kb/s. La figura muestra la configuración utilizada en los tres routers para modificar el ancho de banda en las interfaces seriales adecuados.

**Verificación del parámetro de ancho de banda**

Utilice el comando **show interfaces** para verificar los nuevos parámetros de ancho de banda, como se muestra en la figura 3. Es importante modificar la métrica del ancho de banda en ambos lados del enlace para garantizar el enrutamiento adecuado en ambas direcciones. La modificación del valor del ancho de banda no cambia el ancho de banda real del enlace. El comando **bandwidth** solo modifica la métrica de ancho de banda que utilizan los protocolos de routing, como EIGRP y OSPF.

**Métrica de retraso**

El retraso es la medida del tiempo que tarda un paquete en atravesar la ruta. La métrica del retardo (DLY) es un valor estático determinado en función del tipo de enlace al cual se encuentra conectada la interfaz y se expresa en microsegundos. El retardo no se mide de manera dinámica. En otras palabras, el router no hace un seguimiento realmente del tiempo que les toma a los paquetes llegar al destino. El valor de retardo, como el valor de ancho de banda, es un valor predeterminado que el administrador de red puede modificar.

Cuando se utiliza para determinar la métrica de EIGRP, el retraso es la acumulación (suma) de todos los retrasos de las interfaces a lo largo de la ruta (medida en decenas de microsegundos).

Utilice el comando **show interfaces** para verificar el valor de retraso en una interfaz. Si bien una interfaz con varios anchos de banda puede tener el mismo valor de retraso predeterminado, Cisco recomienda no modificar el parámetro de retraso, salvo que el administrador de red tenga una razón específica para hacerlo.

**Calculo de la métrica**

**\*Ancho de banda**

EIGRP usa el ancho de banda más lento en el cálculo de su métrica. El ancho de banda más lento se puede determinar por medio de analizar cada interfaz entre el R2 y la red de destino 192.168.1.0. La interfaz Serial 0/0/1en el R2 tiene un ancho de banda de 1024 kb/s. La interfaz GigabitEthernet 0/0 en el R3 tiene un ancho de banda de 1 000 000 kb/s. Por lo tanto, el ancho de banda más lento es de 1024 kb/s y se usa en el cálculo de la métrica.

EIGRP divide un valor de ancho de banda de referencia de 10 000 000 por el valor en kb/s del ancho de banda de la interfaz. Como resultado, los valores más altos de ancho de banda reciben una métrica más baja, y los valores más bajos de ancho de banda reciben una métrica más alta. 10 000 000 se divide por 1024. Si el resultado no es un número entero, el valor se redondea hacia abajo. En este caso, 10 000 000 dividido por 1024 es igual a 9765,625. Los decimales (625) se descartan, y el resultado es 9765 para la porción de ancho de banda de la métrica compuesta.

**\*Retardo**

EIGRP usa la suma de todos los retrasos hasta el destino. La interfaz Serial 0/0/1en el R2 tiene un retraso de 20 000 microsegundos. La interfaz Gigabit 0/0 en el R3 tiene un retraso de 10 microsegundos. La suma de estos retrasos se divide por 10. En el ejemplo, (20 000+10)/10, da como resultado un valor de 2001 para la porción de retraso de la métrica compuesta.

**\*Cálculo de la métrica**

Utilice los valores calculados para el ancho de banda y el retraso en la fórmula de la métrica. El resultado es una métrica de 3 012 096, como se muestra en la figura 4. Este valor coincide con el valor que se muestra en la tabla de routing para el R2.

**Algoritmo DUAL**

EIGRP utiliza el algoritmo de convergencia DUAL. La convergencia es fundamental para las redes para evitar bucles de routing.

Los bucles de routing, incluso los temporarios, pueden ser perjudiciales para el rendimiento de la red. Los protocolos de routing vector distancia, como RIP, evitan los bucles de routing con temporizadores de espera y horizonte dividido. A pesar de que EIGRP utiliza ambas técnicas, las usa de manera un tanto diferentes; la manera principal en la que EIGRP evita los loops de enrutamiento es con el algoritmo DUAL.

El algoritmo DUAL se utiliza para asegurar que no haya bucles en cada instancia a través del cómputo de una ruta. Esto permite que todos los routers involucrados en un cambio de topología se sincronicen al mismo tiempo. Los routers que no se ven afectados por los cambios en la topología no se encuentran involucrados en el recálculo. Este método proporciona a EIGRP mayor tiempo de convergencia que a otros protocolos de enrutamiento vector distancia.

La máquina de estados finitos (FSM) DUAL realiza el proceso de decisión para todos los cómputos de ruta. Una FSM es un modelo de flujo de trabajo, similar a un diagrama de flujo, que está compuesto por lo siguiente:

* Un número finito de etapas (estados)
* Transiciones entre estas etapas
* Operaciones

La FSM DUAL rastrea todas las rutas, utiliza las métricas de EIGRP para elegir rutas eficaces sin bucles e identifica las rutas con el menor costo para insertarlas en la tabla de routing.

El recálculo del algoritmo DUAL puede ser muy exigente para el procesador. EIGRP mantiene una lista de rutas de respaldo que DUAL ya determinó que no tienen bucles para evitar los recálculos siempre que sea posible. Si la ruta principal en la tabla de enrutamiento falla, el mejor camino de respaldo se agrega de inmediato a la tabla de enrutamiento.

DUAL puede converger rápidamente después de un cambio en la topología, debido a que puede usar rutas de respaldo a otras redes sin recalcular DUAL. Estas rutas de respaldo se conocen como “sucesores factibles” (FS).

Un FS es un vecino que tiene una ruta de respaldo sin bucles a la misma red que el sucesor y satisface la condición de factibilidad (FC). El sucesor de R2 para la red 192.168.1.0/24 es el R3, que proporciona la mejor ruta o la métrica más baja a la red de destino. Observe en la figura 1 que el R1 proporciona una ruta alternativa, pero ¿es un FS? Antes de que el R1 pueda ser un FS para el R2, debe cumplir la FC.

La FC se cumple cuando la distancia notificada (RD) desde un vecino hasta una red es menor que la distancia factible desde el router local hasta la misma red de destino. Si la distancia notificada es menor, representa una ruta sin bucles. La distancia notificada es simplemente una distancia factible desde el vecino EIGRP hasta la misma red de destino. La distancia notificada es la métrica que un router informa a un vecino acerca de su propio costo hacia esa red.

**Máquina de estados finitos (FSM) Dual**

El núcleo de EIGRP son DUAL y su motor de cálculos de ruta EIGRP. El nombre real de esta tecnología es Máquina de Estados Finito (FSM) DUAL. Esta FSM contiene toda la lógica que se utiliza para calcular y comparar rutas en una red EIGRP. La figura muestra una versión simplificada de FSM DUAL.

Una FSM es una máquina abstracta, no un dispositivo mecánico con partes móviles. FSM define un conjunto de estados posibles por los que se puede pasar, qué eventos causan estos estados y qué eventos son el resultado de estos estados. Los diseñadores usan las FSM para describir la manera en que un dispositivo, un programa informático o un algoritmo de routing reaccionan ante un conjunto de eventos de entrada.

Las FSM exceden el ámbito de este curso. Sin embargo, el concepto se utiliza para examinar algunos de los resultados de las FSM de EIGRP mediante el uso del comando **debug eigrp fsm**. Utilice este comando para analizar qué hace DUAL cuando se elimina una ruta de la tabla de routing.

**EIGRP para IPv6**

De manera similar a su homólogo para IPv4, EIGRP para IPv6 intercambia información de routing para completar la tabla de routing IPv6 con prefijos remotos. EIGRP para IPv6 está disponible a partir del IOS de Cisco versión 12.4(6)T.

EIGRP para IPv4 se ejecuta a través de la capa de red IPv4, por lo que se comunica con otros peers IPv4 EIGRP y solo anuncia rutas IPv4. EIGRP para IPv6 tiene la misma funcionalidad que EIGRP para IPv4, pero utiliza IPv6 como el protocolo de capa de red, se comunica con peers EIGRP para IPv6 y anuncia rutas IPv6.

EIGRP para IPv6 también usa DUAL como motor de cómputo para garantizar rutas principales y de respaldo sin bucles a través de todo el dominio de routing.

Al igual que con todos los protocolos de routing IPv6, EIGRP para IPv6 tiene procesos separados de los de su homólogo para IPv4. Los procesos y las operaciones son básicamente los mismos que en el protocolo de routing IPv4; no obstante, se ejecutan de manera independiente. EIGRP para IPv4 y EIGRP para IPv6 tienen tablas de vecinos EIGRP, tablas de topología EIGRP y tablas de IP routing separadas, como se muestra en la ilustración. EIGRP para IPv6 es un módulo dependiente de protocolo (PDM) separado.

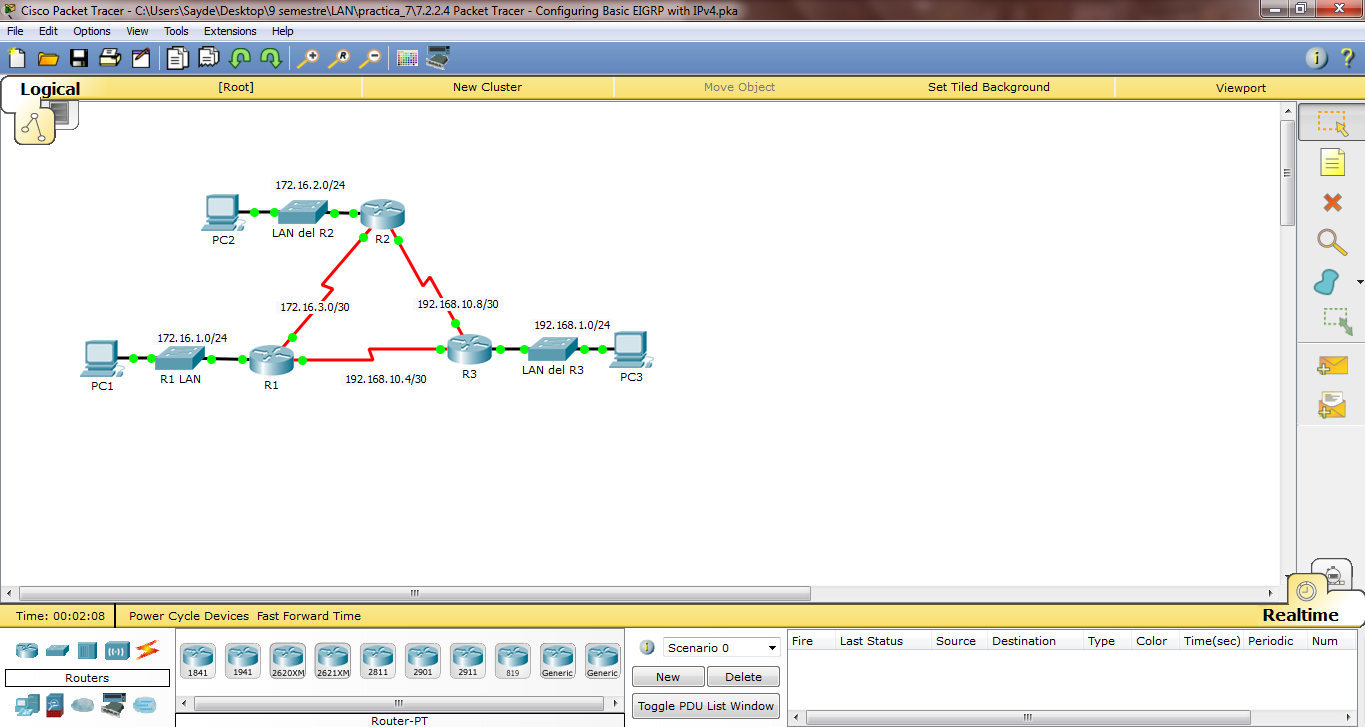
Los comandos de configuración y verificación de EIGRP para IPv6 son muy similares a los que se utilizan en EIGRP para IPv4.

**Comparación entre EIGRP IPv4 e IPv6**

La siguiente es una comparación de las principales características de EIGRP para IPv4 e EIGRP para IPv6:

* **Rutas anunciadas:** EIGRP para IPv4 anuncia redes IPv4, mientras que EIGRP para IPv6 anuncia prefijos IPv6.
* **Vector distancia:** EIGRP para IPv4 y para IPv6 son protocolos de routing vector distancia avanzados. Ambos protocolos usan las mismas distancias administrativas.
* **Tecnología de convergencia:** tanto EIGRP para IPv4 como para IPv6 usan el algoritmo DUAL. Ambos protocolos usan las mismas técnicas y procesos de DUAL, incluidos sucesor, FS, FD y RD.
* **Métrica:** tanto EIGRP para IPv4 como para IPv6 usan ancho de banda, retraso, confiabilidad y carga para su métrica compuesta. Ambos protocolos de routing usan la misma métrica compuesta y, de manera predeterminada, usan solo ancho de banda y retraso.
* **Protocolo de transporte:** el protocolo de transporte confiable (RTP) es responsable de la entrega garantizada de paquetes EIGRP a todos los vecinos para ambos protocolos, EIGRP para IPv4 y para IPv6.
* **Mensajes de actualización:** tanto EIGRP para IPv4 como para IPv6 envían actualizaciones incrementales cuando el estado de un destino cambia. Los términos “parcial” y “limitada” se usan para hacer referencia a las actualizaciones de ambos protocolos.
* **Mecanismo de descubrimiento de vecinos:** tanto EIGRP para IPv4 como EIGRP para IPv6 utilizan un simple mecanismo de saludo para descubrir routers vecinos y formar adyacencias.
* **Direcciones de origen y destino:** EIGRP para IPv4 envía mensajes a la dirección de multidifusión 224.0.0.10. Estos mensajes utilizan la dirección IPv4 de origen de la interfaz de salida. EIGRP para IPv6 envía sus mensajes a la dirección de multidifusión FF02: A. Los mensajes EIGRP para IPv6 se originan en la dirección IPv6 link-local de la interfaz de salida.
* **Autenticación:** EIGRP para IPv4 puede usar autenticación de texto no cifrado o autenticación de síntesis del mensaje 5 (MD5). EIGRP para IPv6 usa MD5.
* **ID del router:** EIGRP para IPv4 y EIGRP para IPv6 usan un número de 32 bits para la ID del router EIGRP. La ID de router de 32 bits se representa con una notación decimal con puntos que comúnmente se considera una dirección IPv4. Si el router EIGRP para IPv6 no está configurado con una dirección IPv4, se debe utilizar el comando **eigrp router-id** para configurar una ID de router de 32 bits. El proceso para determinar la ID del router es el mismo para ambos protocolos EIGRP, para IPv4 y para IPv6.

**#7.2.2.4**



**R1**

R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router eigrp 1

R1(config-router)#network 172.16.1.0 0.0.0.255

R1(config-router)#network 172.16.3.0 0.0.0.3

R1(config-router)#network 192.168.10.4 0.0.0.3

R1(config-router)#passive-interface g0/0

R1(config-router)#no auto-summary

R1(config-router)#end

R1#

**R2**

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router eigrp 1

R2(config-router)#network 172.16.2.0 0.0.0.255

R2(config-router)#network 172.16.3.0 0.0.0.3

R2(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency

R2(config-router)#network 192.168.10.8 0.0.0.3

R2(config-router)#passive-interface g0/0

R2(config-router)#no auto-summary

R2(config-router)#

**R3**

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router eigrp 1

R3(config-router)#network 192.168.1.0 0.0.0.255

R3(config-router)#network 192.168.10.4 0.0.0.3

R3(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up: new adjacency

R3(config-router)#network 192.168.10.8 0.0.0.3

R3(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is up: new adjacency

R3(config-router)#end

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#copy run start

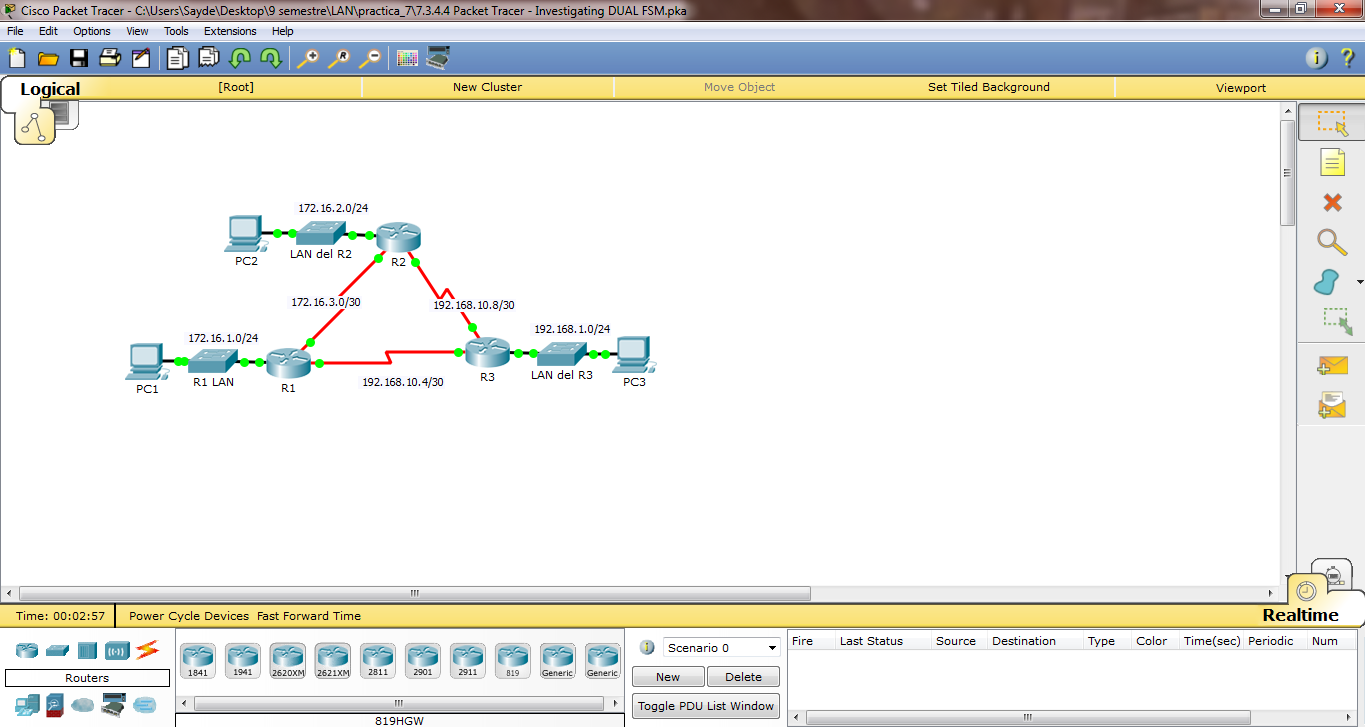
Destination filename [startup-config]?

Building configuration...

[OK]

R3#

**#7.3.4.4**



**R1**

R1>en

R1#show ip eigrp topology

IP-EIGRP Topology Table for AS 1/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 172.16.1.0/24, 1 successors, FD is 2816

via Connected, GigabitEthernet0/0

P 172.16.2.0/24, 1 successors, FD is 2170112

via 172.16.3.2 (2170112/2816), Serial0/0/0

P 172.16.3.0/30, 1 successors, FD is 2169856

via Connected, Serial0/0/0

P 192.168.1.0/24, 1 successors, FD is 2170112

via 192.168.10.6 (2170112/2816), Serial0/0/1

P 192.168.10.4/30, 1 successors, FD is 2169856

via Connected, Serial0/0/1

P 192.168.10.8/30, 2 successors, FD is 2681856

via 172.16.3.2 (2681856/2169856), Serial0/0/0

via 192.168.10.6 (2681856/2169856), Serial0/0/1

R1#debug eigrp fsm

EIGRP FSM Events/Actions debugging is on

R1#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.6 (Serial0/0/1) is down: interface down

DUAL: linkdown: start - 192.168.10.6 via Serial0/0/1

DUAL: Destination 192.168.1.0/24

DUAL: rcvupdate: 192.168.1.0/24 via 192.168.10.6 metric 4294967295/4294967295

DUAL: Find FS for dest: 192.168.1.0/24. FD is 2170112, RD is 2816

DUAL: 0.0.0.0 metric 4294967295/4294967295 not found Dmin is 4294967295

DUAL: Destination 192.168.10.8/30

DUAL: rcvupdate: 192.168.10.8/30 via 192.168.10.6 metric 4294967295/4294967295

DUAL: Find FS for dest: 192.168.10.8/30. FD is 2681856, RD is 2169856

DUAL: linkdown: finish

DUAL: rcvupdate: 192.168.10.4/30 via 0.0.0.0 metric 4294967295/4294967295

DUAL: Find FS for dest: 192.168.10.4/30. FD is 2169856, RD is 0

DUAL: 0.0.0.0 metric 4294967295/4294967295 not found Dmin is 4294967295

DUAL: ifdelete: Serial0/0/1 is being deleted

DUAL: dual\_ifdelete(): finish

DUAL: rcvupdate: 192.168.1.0/24 via 172.16.3.2 metric 2682112/2170112

DUAL: Find FS for dest: 192.168.1.0/24. FD is 4294967295, RD is 4294967295

DUAL: RT installed 192.168.1.0/24 via 172.16.3.2

DUAL: Send update about 192.168.1.0/24. Reason: metric chg

DUAL: rcvupdate: 192.168.10.4/30 via Connected metric 4294967295/0

DUAL: Find FS for dest: 192.168.10.4/30. FD is 4294967295, RD is 4294967295

DUAL: 0.0.0.0 metric 4294967295/4294967295 not found Dmin is 4294967295

DUAL: Dest 192.168.10.4/30 (No peers) not entering active state.

DUAL: Removing dest 192.168.10.4/30, nexthop 0.0.0.0

DUAL: No routes. Flushing dest 192.168.10.4/30

DUAL: Send update about 192.168.10.4/30. Reason: metric chg

R1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

C 172.16.1.0/24 is directly connected, GigabitEthernet0/0

L 172.16.1.254/32 is directly connected, GigabitEthernet0/0

D 172.16.2.0/24 [90/2170112] via 172.16.3.2, 00:18:33, Serial0/0/0

C 172.16.3.0/30 is directly connected, Serial0/0/0

L 172.16.3.1/32 is directly connected, Serial0/0/0

D 192.168.1.0/24 [90/2682112] via 172.16.3.2, 00:01:18, Serial0/0/0

192.168.10.0/30 is subnetted, 1 subnets

D 192.168.10.8/30 [90/2681856] via 172.16.3.2, 00:18:33, Serial0/0/0

R1#show ip eigrp topology

IP-EIGRP Topology Table for AS 1/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 172.16.1.0/24, 1 successors, FD is 2816

via Connected, GigabitEthernet0/0

P 172.16.2.0/24, 1 successors, FD is 2170112

via 172.16.3.2 (2170112/2816), Serial0/0/0

P 172.16.3.0/30, 1 successors, FD is 2169856

via Connected, Serial0/0/0

P 192.168.1.0/24, 1 successors, FD is 2682112

via 172.16.3.2 (2682112/2170112), Serial0/0/0

P 192.168.10.8/30, 1 successors, FD is 2681856

via 172.16.3.2 (2681856/2169856), Serial0/0/0

R1#show ip eigrp neighbors

IP-EIGRP neighbors for process 1

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

0 172.16.3.2 Se0/0/0 13 00:22:35 40 1000 0 15

R1#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

DUAL: rcvupdate: 192.168.10.4/30 via Connected metric 2169856/0

DUAL: Find FS for dest: 192.168.10.4/30. FD is 4294967295, RD is 4294967295

DUAL: RT installed 192.168.10.4/30 via 0.0.0.0

DUAL: Send update about 192.168.10.4/30. Reason: metric chg

DUAL: Send update about 192.168.10.4/30. Reason: new if

DUAL: rcvupdate: 172.16.1.0/24 via Connected metric 2816/0

DUAL: Find FS for dest: 172.16.1.0/24. FD is 2816, RD is 0

DUAL: Send update about 172.16.1.0/24. Reason: new if

DUAL: rcvupdate: 172.16.3.0/30 via Connected metric 2169856/0

DUAL: Find FS for dest: 172.16.3.0/30. FD is 2169856, RD is 0

DUAL: Send update about 172.16.3.0/30. Reason: new if

DUAL: rcvupdate: 192.168.10.4/30 via 172.16.3.2 metric 4294967295/4294967295

DUAL: Find FS for dest: 192.168.10.4/30. FD is 2169856, RD is 0

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.6 (Serial0/0/1) is up: new adjacency

DUAL: rcvupdate: 192.168.10.4/30 via 192.168.10.6 metric 4294967295/4294967295

DUAL: Find FS for dest: 192.168.10.4/30. FD is 2169856, RD is 0

DUAL: rcvupdate: 172.16.1.0/24 via 192.168.10.6 metric 3194112/2682112

DUAL: Find FS for dest: 172.16.1.0/24. FD is 2816, RD is 0

DUAL: rcvupdate: 172.16.2.0/24 via 192.168.10.6 metric 2682112/2170112

DUAL: Find FS for dest: 172.16.2.0/24. FD is 2170112, RD is 2816

DUAL: rcvupdate: 172.16.3.0/30 via 192.168.10.6 metric 3193856/2681856

DUAL: Find FS for dest: 172.16.3.0/30. FD is 2169856, RD is 0

DUAL: rcvupdate: 192.168.1.0/24 via 192.168.10.6 metric 2170112/2816

DUAL: Find FS for dest: 192.168.1.0/24. FD is 2682112, RD is 2170112

DUAL: RT installed 192.168.1.0/24 via 192.168.10.6

DUAL: Send update about 192.168.1.0/24. Reason: metric chg

DUAL: rcvupdate: 192.168.10.8/30 via 192.168.10.6 metric 2681856/2169856

DUAL: Find FS for dest: 192.168.10.8/30. FD is 2681856, RD is 2169856

DUAL: rcvupdate: 172.16.1.0/24 via 192.168.10.6 metric 4294967295/4294967295

DUAL: Find FS for dest: 172.16.1.0/24. FD is 2816, RD is 0

R1#undebug all

All possible debugging has been turned off

R1#

**R2**

R2>EN

R2#conf t

R2#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

D 172.16.1.0/24 [90/2170112] via 172.16.3.1, 00:06:38, Serial0/0/0

C 172.16.2.0/24 is directly connected, GigabitEthernet0/0

L 172.16.2.254/32 is directly connected, GigabitEthernet0/0

C 172.16.3.0/30 is directly connected, Serial0/0/0

L 172.16.3.2/32 is directly connected, Serial0/0/0

D 192.168.1.0/24 [90/2170112] via 192.168.10.10, 00:06:40, Serial0/0/1

192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks

D 192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:06:40, Serial0/0/1

[90/2681856] via 172.16.3.1, 00:06:36, Serial0/0/0

C 192.168.10.8/30 is directly connected, Serial0/0/1

L 192.168.10.9/32 is directly connected, Serial0/0/1

R2#

R2#show ip eigrp topology

IP-EIGRP Topology Table for AS 1/ID(192.168.10.9)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 172.16.1.0/24, 1 successors, FD is 2170112

via 172.16.3.1 (2170112/2816), Serial0/0/0

P 172.16.2.0/24, 1 successors, FD is 2816

via Connected, GigabitEthernet0/0

P 172.16.3.0/30, 1 successors, FD is 2169856

via Connected, Serial0/0/0

P 192.168.1.0/24, 1 successors, FD is 2170112

via 192.168.10.10 (2170112/2816), Serial0/0/1

P 192.168.10.4/30, 2 successors, FD is 2681856

via 192.168.10.10 (2681856/2169856), Serial0/0/1

via 172.16.3.1 (2681856/2169856), Serial0/0/0

P 192.168.10.8/30, 1 successors, FD is 2169856

via Connected, Serial0/0/1

R2#

**R3**

R3>en

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int s0/0/0

R3(config-if)#shutdown

R3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is down: interface down

R3(config-if)#exit

R3(config)#exit

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#exit

R3 con0 is now available

Press RETURN to get started.

R3>en

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int s0/0/0

R3(config-if)#no shutdown

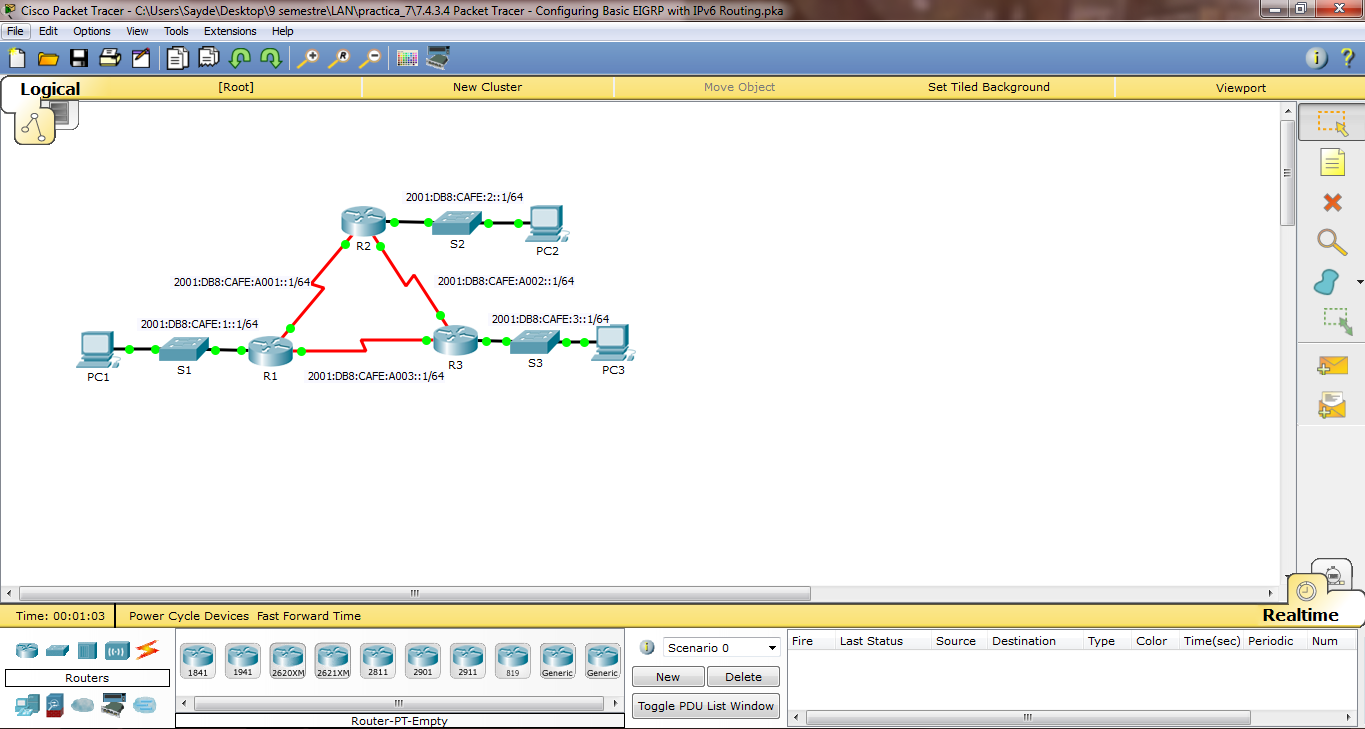
R3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up: new adjacency

**#7.4.3.4**



R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ipv6 unicast-routing

R1(config)#ipv6 router eigrp 1

R1(config-rtr)#no shutdown

R1(config)#int g0/0

R1(config-if)#ipv6 eigrp 1

R1(config-if)#int s0/0/0

R1(config-if)#ipv6 eigrp 1

R1(config-if)#

R1(config-if)#int s0/0/1

R1(config-if)#ipv6 eigrp 1

R1(config-if)#

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ipv6 unicast-routing

R2(config)#ipv6 router eigrp 1

R2(config-rtr)#no shutdown

R2(config)#int g0/0

R2(config-if)#ipv6 eigrp 1

R2(config-if)#int s0/0/0

R2(config-if)#ipv6 eigrp 1

R2(config-if)#

R2(config-if)#int s0/0/1

R2(config-if)#ipv6 eigrp 1

R2(config-if)#

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#ipv6 unicast-routing

R3(config)#ipv6 router eigrp 1

R3(config-rtr)#no shutdown

R3(config)#int g0/0

R3(config-if)#ipv6 eigrp 1

R3(config-if)#int s0/0/0

R3(config-if)#ipv6 eigrp 1

R3(config-if)#

R3(config-if)#int s0/0/1

R3(config-if)#ipv6 eigrp 1

R3(config-if)#

**CAPÍTULO 8**

**Rutas resumidas automáticas**

Uno de los métodos de ajuste más comunes de EIGRP es habilitar y deshabilitar la sumarización automática de rutas. La sumarización de ruta permite que un router agrupe redes y las anuncie como un gran grupo por medio de una única ruta resumida. La capacidad para resumir rutas es necesaria debido al rápido crecimiento de las redes.

Un router de frontera es un router que se ubica en el límite de una red. Este router debe poder anunciar todas las redes conocidas dentro de su tabla de rutas a un router de red o router ISP conector. Potencialmente, esta convergencia puede dar como resultado tablas de rutas muy grandes. Imagine si un solo router tuviera 10 redes diferentes y debiera anunciar las 10 entradas de rutas a un router conector. ¿Qué sucedería si ese router conector también tuviera 10 redes y debiera anunciar las 20 rutas a un router ISP? Si cada router de la empresa siguiera este patrón, la tabla de routing del router ISP sería enorme.

La sumarización disminuye la cantidad de entradas en las actualizaciones de enrutamiento y reduce la cantidad de entradas en las tablas de enrutamiento locales. Reduce, además, el uso del ancho de banda para las actualizaciones de enrutamiento y acelera las búsquedas en las tablas de enrutamiento.

Para limitar la cantidad de anuncios de routing y el tamaño de las tablas de routing, los protocolos de routing, como EIGRP, utilizan la sumarización automática en los límites con clase. Esto significa que EIGRP reconoce las subredes como una única red de clase A, B o C y crea solo una entrada en la tabla de routing para la ruta resumida. Como resultado, todo el tráfico destinado a las subredes viaja por esa ruta.

En la ilustración, se muestra un ejemplo de la manera en que funciona la sumarización automática. Los routers R1 y R2 están configurados con EIGRP para IPv4, con sumarización automática. El R1 tiene tres subredes en la tabla de routing: 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24. En la arquitectura de direccionamiento de redes con clase, todas estas subredes se consideran parte de una red de clase B más grande: 172.16.0.0/16. Debido a que EIGRP en el router R1 está configurado para sumarización automática, cuando envía la actualización de routing al R2, resume las tres subredes /24 como una única red 172.16.0.0/16. Esto reduce la cantidad de actualizaciones de routing que se envían y la cantidad de entradas en la tabla de routing IPv4 del R2.

Todo el tráfico destinado a las tres subredes viaja a través de la única ruta. El R2 no mantiene rutas a subredes individuales y no se descubre información de subredes. En una red empresarial, es posible que la ruta elegida para alcanzar la ruta sumarizada no sea la mejor elección para el tráfico que está intentando alcanzar la subred individual. La única forma en que todos los routers pueden encontrar las mejores rutas para cada subred individual es que los vecinos envíen información sobre las subredes. En esta situación, se debe deshabilitar la sumarización automática. Cuando se deshabilita la sumarización automática, las actualizaciones incluyen información de subredes.

La sumarización automática de EIGRP para IPv4 está deshabilitada de manera predeterminada a partir de las versiones 15.0(1)M y 12.2(33) del IOS de Cisco. Antes de esto, la sumarización automática estaba habilitada de manera predeterminada. Es decir que EIGRP realizaba la sumarización automática cada vez que la topología EIGRP cruzaba un límite entre dos redes principales con clase diferentes.

En la figura 1, el resultado del comando show ip protocols en el R1 indica que la sumarización automática de EIGRP está deshabilitada. Este router ejecuta IOS 15.2; por ende, la sumarización automática de EIGRP está deshabilitada de manera predeterminada. En la figura 2, se muestra la tabla de routing actual del R3. Observe que la tabla de routing IPv4 del R3 contiene todas las redes y subredes dentro del dominio de routing EIGRP.

Para habilitar la sumarización automática de EIGRP, use el comando auto-summary en el modo de configuración del router, como se muestra en la figura 3:

R1(config)# router eigrp *as-number*

R1(config-router)# auto-summary

La forma no de este comando se usa para deshabilitar la sumarización automática.

Utilice el verificador de sintaxis de la figura 4 para habilitar la sumarización automática en el R3

**Rutas resumidas manuales**

EIGRP puede configurarse para que resuma rutas, ya sea que se encuentre habilitado la sumarización automática (auto-summary) o no. Debido a que EIGRP es un protocolo de enrutamiento sin clase e incluye la máscara de subred en las actualizaciones de enrutamiento, la sumarización manual puede incluir rutas de superredes. Para determinar el resumen de estas tres redes, se usa el mismo método que para determinar rutas estáticas resumidas:

Paso 1. Escriba las redes que se resumirán en formato binario.

Paso 2. Para encontrar la máscara de subred para la sumarización, empiece con el bit del extremo izquierdo.

Paso 3. De izquierda a derecha, encuentre todos los bits que coincidan en forma consecutiva.

Paso 4. Cuando haya una columna de bits que no coincidan, deténgase. Este es el límite de resumen.

Paso 5. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo. En el ejemplo, es 22. Este número se usa para determinar la máscara de subred de la ruta resumida: /22 o 255.255.252.0.

Paso 6. Para encontrar la dirección de red para el resumen, copie los 22 bits que coinciden y agregue a todos los bits 0 al final para obtener 32 bits.

El resultado es la dirección de red resumida y la máscara para 192.168.0.0/22.

Configuración de la sumarización manual de EIGRP

Para establecer la sumarización manual EIGRP en una interfaz EIGRP específica, utilice el siguiente comando del modo de configuración de interfaz:

Router(config-if)# ip summary-address eigrp *as-number network-address subnet-mask*

**Rutas manuales resumidas para IPv6**

Si bien la sumarización automática no está disponible para redes IPv6 EIGRP, es posible habilitar la sumarización manual para estas redes.

Para configurar la sumarización manual de EIGRP para IPv6 en una interfaz EIGRP específica, utilice el siguiente comando del modo de configuración de interfaz:

Router(config-if)# ipv6 summary-address eigrp *as-number prefix/prefix-length*

La recepción de la ruta resumida manual se puede verificar mediante la revisión de la tabla de routing de los otros routers en el dominio de routing. En la figura 4, se muestra la ruta 2001:DB8:ACAD:/48 en la tabla de routing IPv6 del R1.

Propagación de una ruta estática predeterminada.

El uso de una ruta estática a 0.0.0.0/0 como ruta predeterminada no constituye routing dependiente de protocolo. La ruta estática predeterminada "quad zero" se puede utilizar con cualquier protocolo de enrutamiento actualmente admitido. En general, la ruta estática predeterminada se configura en el router que tiene una conexión a una red fuera del dominio de routing EIGRP; por ejemplo, a un ISP.

Un método para propagar una ruta estática predeterminada dentro del dominio de routing EIGRP es mediante el comando redistribute static. El comando redistribute static le indica a EIGRP que incluya rutas estáticas en sus actualizaciones de EIGRP a otros routers.

La entrada de la ruta predeterminada que se descubrió mediante EIGRP se identifica por lo siguiente:

* D: esta ruta se descubrió en una actualización de routing EIGRP.
* \*: la ruta es candidata para una ruta predeterminada.
* EX: la ruta es una ruta EIGRP externa, en este caso, una ruta estática fuera del dominio de routing EIGRP.
* 170: distancia administrativa de una ruta EIGRP externa.

Las rutas predeterminadas proporcionan una ruta predeterminada para salir del dominio de enrutamiento y, al igual que las rutas sumarizadas, minimizan el número de entradas en la tabla de enrutamiento.

**Verificación de la propagación de una ruta predeterminada**

La propagación de la ruta estática predeterminada IPv6 se puede verificar mediante la revisión de la tabla de routing IPv6 del R1 con el comando show ipv6 route.

**Ancho de Banda**

**Ancho de banda de EIGRP para IPv4**

De manera predeterminada, EIGRP usa solo hasta el 50% del ancho de banda de una interfaz para la información de EIGRP. Esto impide que el proceso EIGRP utilice en exceso los enlaces y que no permita suficiente ancho de banda para el enrutamiento de tráfico normal.

Use el comando ip bandwidth-percent eigrp para configurar el porcentaje del ancho de banda que EIGRP puede utilizar en una interfaz.

Router(config-if)# ip bandwidth-percent eigrp *as-number percent*

El comando ip bandwidth-percent eigrp usa el ancho de banda configurado (o el ancho de banda predeterminado) para calcular el porcentaje que EIGRP puede usar. En este ejemplo, EIGRP se limita a no más del 40% del ancho de banda del enlace. Por eso, EIGRP nunca usa más de 32 kb/s del ancho de banda del enlace para el tráfico de paquetes EIGRP.Para restaurar el valor predeterminado, utilice la versión no de este comando.

**Ancho de banda de EIGRP para IPv6**

Para configurar el porcentaje del ancho de banda que puede utilizar EIGRP para IPv6 en una interfaz, utilice el comando ipv6 bandwidth-percent eigrp en el modo de configuración de interfaz. Para restaurar el valor predeterminado, utilice la versión no de este comando.

Router(config-if)# ipv6 bandwidth-percent eigrp *as-number percent*

**Temporizadores**

Intervalos de saludo y tiempos de espera en EIGRP para IPv4

EIGRP usa un protocolo de saludo ligero para establecer y controlar el estado de conexión de los vecinos. El tiempo de espera le indica al router la cantidad máxima de tiempo que debe esperar para recibir el siguiente saludo, antes de declarar que el vecino es inalcanzable.

Los intervalos de saludo y los tiempos de espera se pueden configurar por interfaz y no tienen que coincidir con otros routers EIGRP para establecer o mantener adyacencias. El comando para configurar un intervalo de saludo diferente es el siguiente:

Router(config-if)# ip hello-interval eigrp *as-number seconds*

Si cambia el intervalo de saludo, asegúrese de que el valor del tiempo de espera sea igual o superior al intervalo de saludo. De lo contrario, la adyacencia de vecino se desactiva después de que expira el tiempo de espera y antes del siguiente intervalo de saludo. Para configurar un tiempo de espera diferente, use el siguiente comando:

Router(config-if)# ip hold-time eigrp *as-number seconds*

El valor de *segundos* para los intervalos de saludo y de tiempo de espera puede ser de 1 a 65 535.

No es necesario que el tiempo del intervalo de saludo y el tiempo de espera coincidan para que dos routers formen una adyacencia EIGRP.

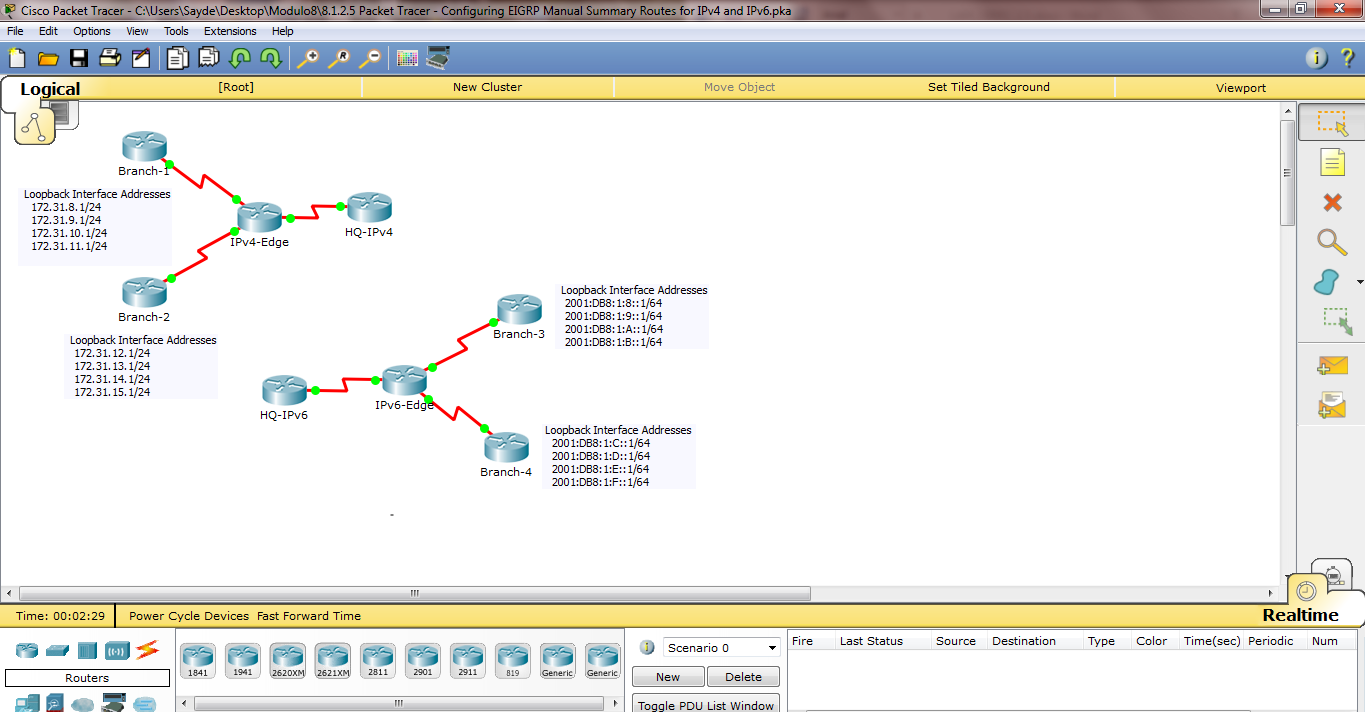
**Intervalos de saludo y tiempos de espera en EIGRP para IPv6**

EIGRP para IPv6 utiliza los mismos tiempos de intervalo de saludo y de espera que EIGRP para IPv4. Los comandos del modo de configuración de interfaz son parecidos a los que se usan para IPv4:

Router (config-if)# ipv6 hello-interval eigrp *as-number seconds*

Router (config-if)# ipv6 hold-time eigrp *as-number seconds*

**#8.1.2.5**



Branch-1>en

Branch-1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Branch-1(config)#int s0/0/0

Branch-1(config-if)#ip summary-address eigrp 1 172.31.8.0 255.255.252.0

Branch-2>en

Branch-2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Branch-2(config)#int s0/0/0

Branch-2(config-if)#int s0/0/1

Branch-2(config-if)#ip summary-address eigrp 1 172.31.12.0 255.255.252.0

Branch-2(config-if)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.7.1 (Serial0/0/1) is up: new adjacency

IPv4-Edge>en

IPv4-Edge#conf t

Enter configuration commands, one per line. End with CNTL/Z.

IPv4-Edge(config)#int s0/1/0

IPv4-Edge(config-if)#ip summary-address eigrp 1 172.31.8.0 255.255.248.0

IPv4-Edge(config-if)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.10.1 (Serial0/1/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.7.2 (Serial0/0/1) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.6.2 (Serial0/0/0) is up: new adjacency

IPv4-Edge(config-if)#

IPV6

Branch-3>en

Branch-3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Branch-3(config)#int s0/0/0

Branch-3(config-if)#ipv6 summary-address eigrp 1 2001:db8:1:a::1/63

Branch-3(config-if)#

Branch-4>en

Branch-4#conf t

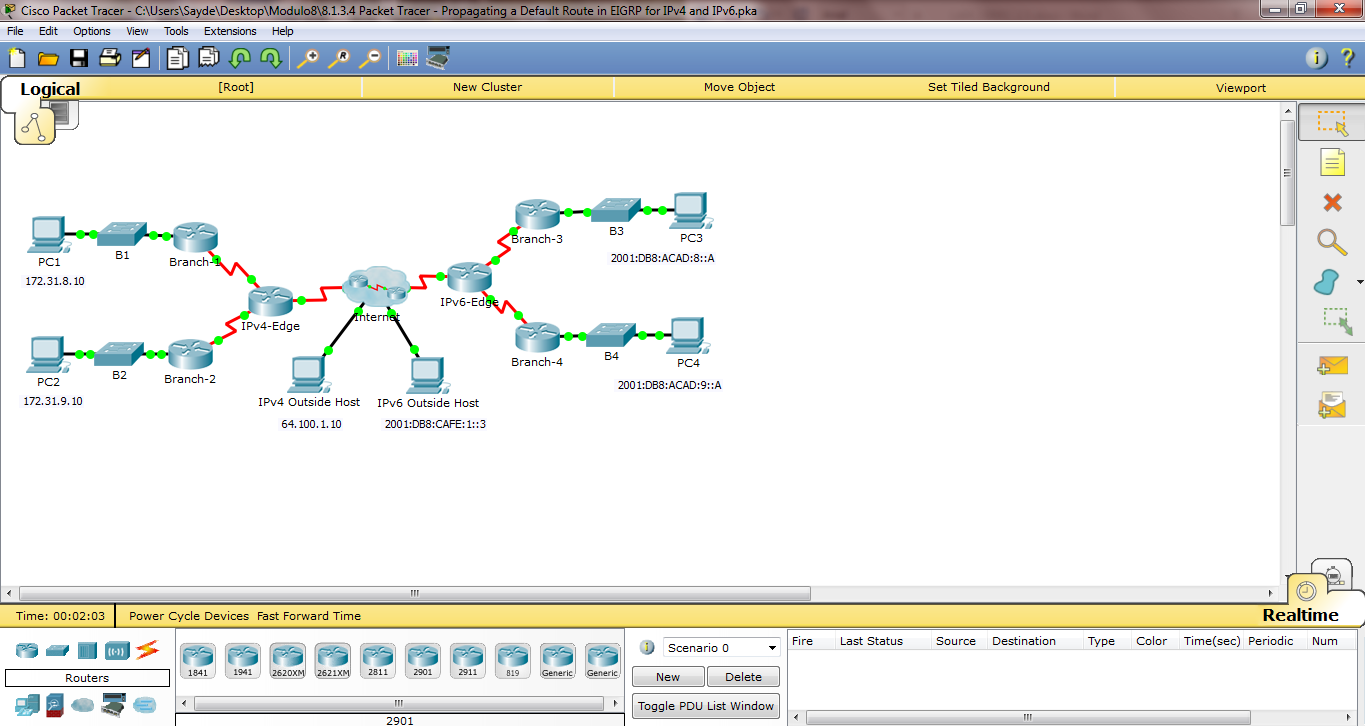
Enter configuration commands, one per line. End with CNTL/Z.

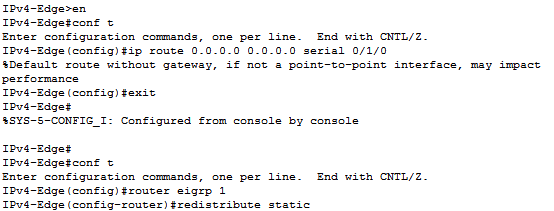
Branch-4(config)#int s0/0/1

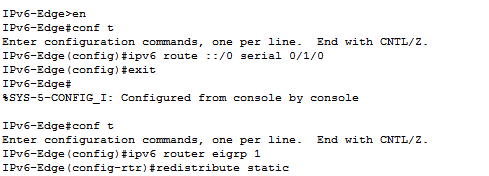
Branch-4(config-if)#ipv6 summary-address eigrp 1 2001:db8:1:f::1/63

Branch-4(config-if)#

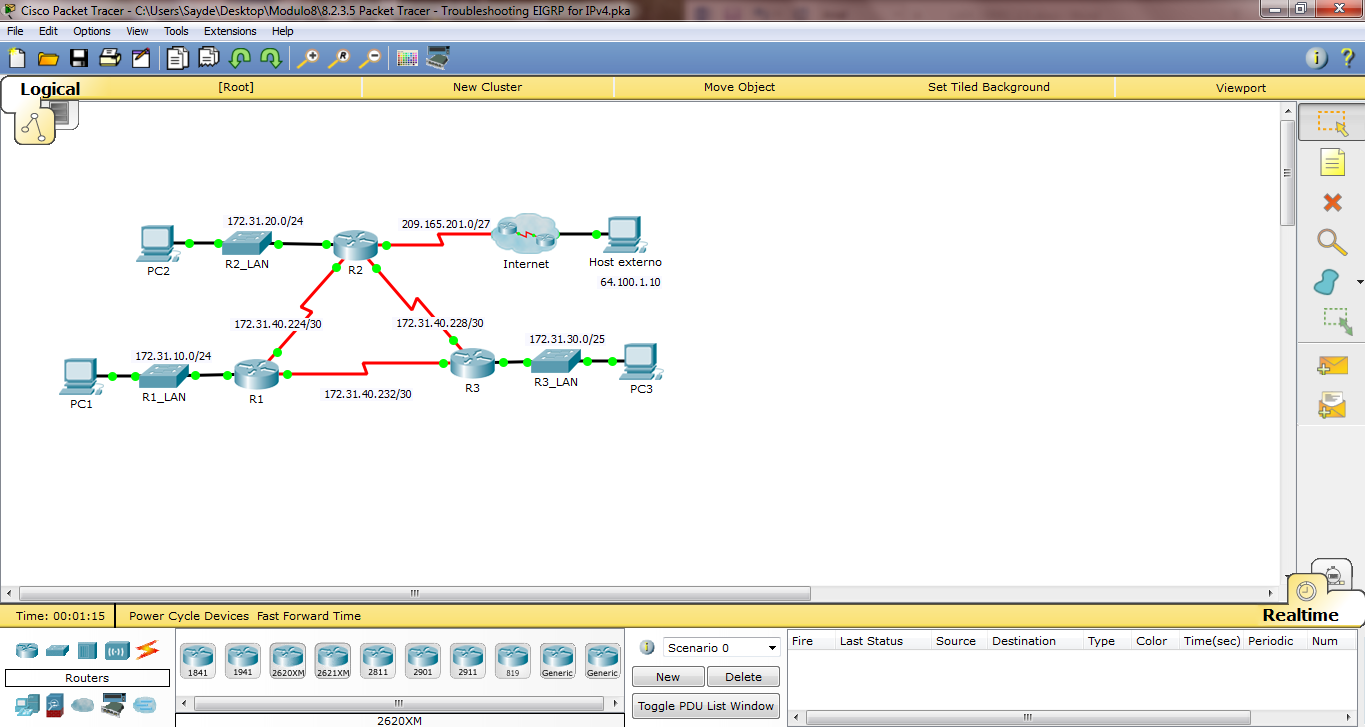
**#8.1.3.4**







**#8.2.3.5**



R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#no router eigrp 11

R1(config)#router eigrp 1

R1(config-router)#passive-interface g0/0

R1(config-router)#network 172.31.10.0 0.0.0.255

R1(config-router)#network 172.31.40.224 0.0.0.3

R1(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.40.226 (Serial0/0/0) is up: new adjacency

R1(config-router)#network 172.31.40.232 0.0.0.3

R1(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.40.234 (Serial0/0/1) is up: new adjacency

R1(config-router)#no auto-summary

R1(config-router)#

R2>ena

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router eigrp 1

R2(config-router)#network 172.31.40.228 0.0.0.3

R2(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.40.230 (Serial0/0/1) is up: new adjacency

R2(config-router)#

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router eigrp 1

R3(config-router)#no network 172.31.30.0 0.0.0.255

R3(config-router)#network 172.31.20.0 0.0.0.127

R3(config-router)#no auto-summary

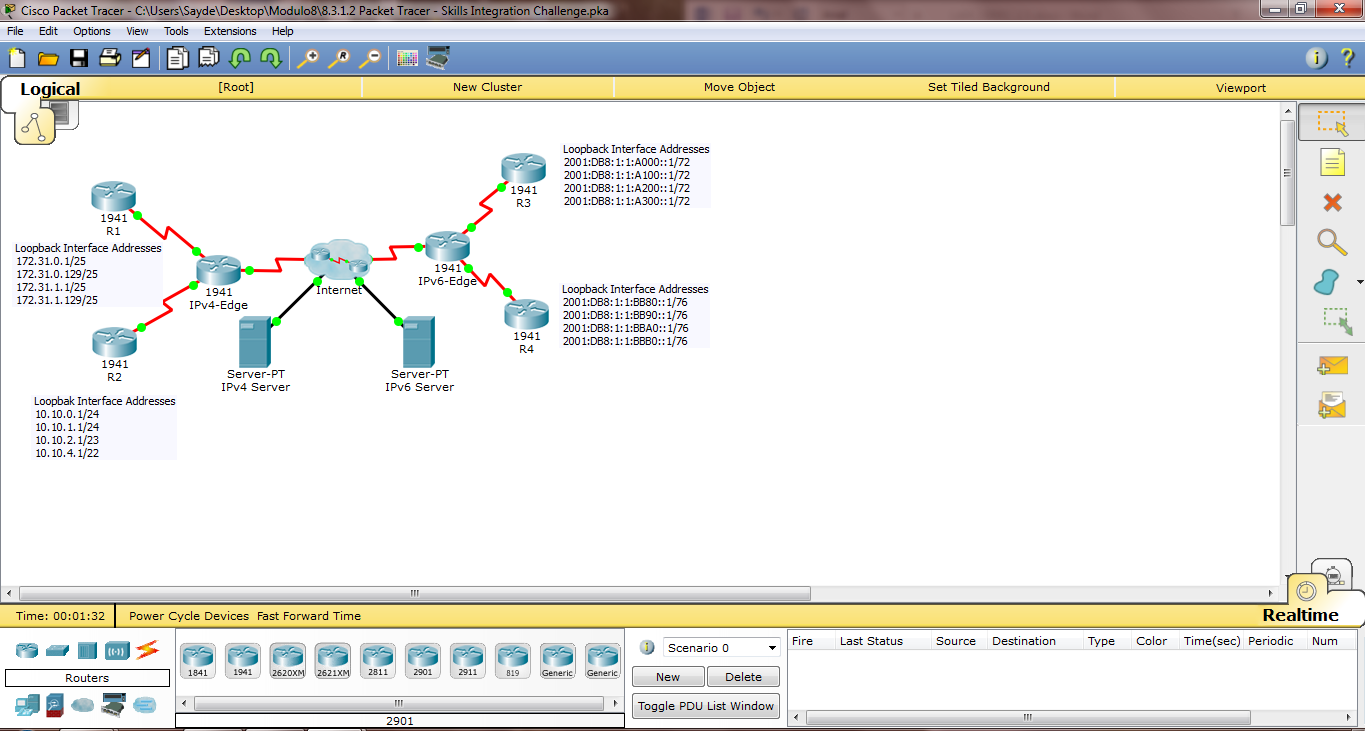
R3(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.40.233 (Serial0/0/0) resync: summary configured

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.40.229 (Serial0/0/1) resync: summary configured

R3(config-router)#

**#8.3.1.2**



R1>ena

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router eigrp 1

R1(config-router)#network 172.31.0.0

R1(config-router)#network 172.31.6.0 0.0.0.3

R1(config-router)#passive-interface default

R1(config-router)#no passive-interface serial 0/0/0

R1(config-router)#

R1(config-router)#no auto-summary

R1(config-router)#int s0/0/0

R1(config-if)#ip hello-interval eigrp 1 10

R1(config-if)#ip summary-address eigrp 1 172.31.0.0 255.255.254.0

R1(config-if)#

R2>en

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router eigrp 1

R2(config-router)#network 10.10.0.0

R2(config-router)#network 10.10.8.0 0.0.0.3

R2(config-router)#passive-interface default

R2(config-router)#no passive-interface s0/0/1

R2(config-router)#no auto-summary

R2(config-router)#int s0/0/1

R2(config-if)#ip hello-interval eigrp 1 10

R2(config-if)#ip summary-address eigrp 1 10.10.0.0 255.255.248.0

R2(config-if)#end

R2#

IPv4-Edge>ena

IPv4-Edge#conf t

Enter configuration commands, one per line. End with CNTL/Z.

IPv4-Edge(config)#router eigrp 1

IPv4-Edge(config-router)#network 172.31.6.0 0.0.0.3

IPv4-Edge(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.6.2 (Serial0/0/0) is up: new adjacency

IPv4-Edge(config-router)#network 10.10.8.0 0.0.0.3

IPv4-Edge(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.8.2 (Serial0/0/1) is up: new adjacency

IPv4-Edge(config-router)#passive-interface default

IPv4-Edge(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.8.2 (Serial0/0/1) is down: holding time expired

IPv4-Edge(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.6.2 (Serial0/0/0) is down: holding time expired

IPv4-Edge(config-router)#no passive-interface s0/0/0

IPv4-Edge(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.6.2 (Serial0/0/0) is up: new adjacency

IPv4-Edge(config-router)#no passive-interface s0/0/1

IPv4-Edge(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.8.2 (Serial0/0/1) is up: new adjacency

IPv4-Edge(config-router)#

IPv4-Edge(config-router)#no auto-summary

IPv4-Edge(config-router)#exit

IPv4-Edge(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0

%Default route without gateway, if not a point-to-point interface, may impact performance

IPv4-Edge(config)#

IPv4-Edge(config)#router eigrp 1

IPv4-Edge(config-router)#redistribute static

IPv4-Edge(config-router)#int s0/0/0

IPv4-Edge(config-if)#ip hello-interval eigrp 1 10

IPv4-Edge(config-if)#end

IPv4-Edge#

%SYS-5-CONFIG\_I: Configured from console by console

IPv4-Edge(config-router)#int s0/0/1

IPv4-Edge(config-if)#ip hello-interval eigrp 1 10

IPv4-Edge(config-if)#

R3>ena

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#ipv6 unicast-routing

R3(config)#ipv6 router eigrp 1

R3(config-rtr)#no sh

R3(config-rtr)#int s0/0/0

R3(config-if)#ipv6 summary-address eigrp 1 2001:db8:1:1:a::/68

R3(config-if)#end

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#int s0/0/0

^

% Invalid input detected at '^' marker.

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int s0/0/0

R3(config-if)#ipv6 eigrp 1

R3(config-if)#int lo0

R3(config-if)#ipv6 eigrp 1

R3(config-if)#int lo1

R3(config-if)#ipv6 eigrp 1

R3(config-if)#int lo2

R3(config-if)#ipv6 eigrp 1

R3(config-if)#int lo3

R3(config-if)#ipv6 eigrp 1

R3(config-if)#end

R3#

%SYS-5-CONFIG\_I: Configured from console by console

R3#

R4>en

R4#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R4(config)#ipv6 inicast-routing

^

% Invalid input detected at '^' marker.

R4(config)#ipv6 unicast-routing

R4(config)#ipv6 router eigrp 1

R4(config-rtr)#no sh

R4(config-rtr)#int s0/0/1

R4(config-if)#ipv6 summary-address eigrp 1 2001:db8:1:1:bb::/72

R4(config-if)#ipv6 eigrp 1

R4(config-if)#

R4(config-if)#int lo8

R4(config-if)#ipv6 eigrp 1

R4(config-if)#int lo9

R4(config-if)#ipv6 eigrp 1

R4(config-if)#int lo10

R4(config-if)#ipv6 eigrp 1

R4(config-if)#int lo11

R4(config-if)#ipv6 eigrp 1

R4(config-if)#end

R4#

IPv6-Edge>en

IPv6-Edge#conf t

Enter configuration commands, one per line. End with CNTL/Z.

IPv6-Edge(config)#ipv6 unicast-routing

IPv6-Edge(config)#ipv6 router eigrp 1

IPv6-Edge(config-rtr)#no sh

IPv6-Edge(config-rtr)#exit

IPv6-Edge(config)#ipv6 route ::/0 serial 0/1/0

IPv6-Edge(config)#ipv6 router eigrp 1

IPv6-Edge(config-rtr)#redistribute static

IPv6-Edge(config-rtr)#int s0/0/0

IPv6-Edge(config-if)#ipv6 eigrp 1

IPv6-Edge(config-if)#int s0/0/1

IPv6-Edge(config-if)#ipv6 eigrp 1

IPv6-Edge(config-if)#

**CAPÍTULO 9**

**Detección del IOS**

Su lugar de estudios o universidad acaba de recibir una donación de routers y switches Cisco. Usted los transporta desde el departamento de envíos y recepción hasta el laboratorio de redes de Cisco y comienza a clasificarlos en grupos de switches y de routers.

El software IOS de Cisco evolucionó de un sistema operativo de plataforma única para routing a un sistema operativo sofisticado que admite una amplia matriz de características y tecnologías, como VoIP, NetFlow e IPsec. Para cumplir mejor con los requisitos de los distintos segmentos del mercado, el software está organizado en familias de versiones de software y trenes de software.

Una familia de versiones del software consta de varias versiones del software IOS que presentan las siguientes características:

* Comparten una base de código.
* Se aplican a plataformas de hardware relacionadas.
* Se superponen en la cobertura de la compatibilidad (cuando concluye la vida útil de un OS, se introduce y admite otro OS).
* El tren del software IOS de Cisco 12.4 se considera el tren de línea principal. El tren de línea principal recibe mayormente correcciones de software (errores) con el objetivo de mejorar la calidad de este. Las versiones del tren de línea principal también se denominan “versiones de Implementación de mantenimiento (MD)”.
* Un tren de línea principal siempre está asociado a un tren de tecnología (tren T). Un tren T, como 12.4T, recibe las mismas correcciones de errores de software que el tren de línea principal. El tren T también recibe nuevas características de compatibilidad de hardware y software. Las versiones en el tren 12.4T del software IOS de Cisco se consideran versiones de Implementación temprana (ED).
* Puede haber otros trenes, según la familia de la versión del software. Por ejemplo, otro tren disponible es el tren de proveedor de servicios (tren S). Un tren S contiene características específicas diseñadas para cumplir con los requisitos de los proveedores de servicios.
* Todos los trenes secundarios del tren de línea principal (T, S, etc.) suelen tener una letra mayúscula que designa el tipo de tren.
* Tren de línea principal = 12.4
* Tren T: 12.4T (12.4 + nuevas características de compatibilidad de hardware y software)
* Hasta la familia de la versión 12.4 del software IOS de Cisco inclusive, los trenes de línea principal y los trenes T estaban separados. En otras palabras, desde el tren de línea principal, un tren T se ramificaba y se convertía en una base de código independiente que recibía nuevas características y compatibilidad de hardware. Con el tiempo, un nuevo tren de línea principal evolucionaba de un tren T establecido, y el ciclo comenzaba nuevamente. El uso de varios trenes se modificó con la versión 15 del software IOS de Cisco.

La convención de numeración de versiones del IOS de Cisco se utiliza para identificar la versión del software IOS, incluso correcciones de errores y nuevas características de software. En la ilustración, se muestra un ejemplo del esquema de numeración para los trenes de línea principal y para los trenes T:

* El esquema de numeración de versiones del software para un tren de línea principal consta de un número de tren, un identificador de mantenimiento y un identificador de recopilación. Por ejemplo, la versión 12.4(21a) del software IOS de Cisco es un tren de línea principal. La versión para un tren T consta de un número de tren, un identificador de mantenimiento, un identificador de tren y un identificador de recopilación. Por ejemplo, la versión 12.4(20)T1 del software IOS de Cisco pertenece al tren 12.4T del software IOS de Cisco.
* Cada identificador de mantenimiento de la línea principal del software IOS de Cisco 12.4, como 12.4(7), incluye correcciones de mantenimiento y de software adicionales. Este cambio se indica con el número entre paréntesis. Cada versión de mantenimiento del software IOS de Cisco 12.4T, como 12.4(20)T, incluye estas mismas correcciones de software, junto con características de software adicionales y compatibilidad de hardware.
* Cisco utiliza recopilaciones de una versión individual para integrar correcciones de problemas importantes. Esto reduce el posible impacto en los clientes que ya implementaron y certificaron una versión individual. Una recopilación típicamente incluye correcciones para una cantidad limitada de defectos de software, conocidos como advertencias. Se indica con una letra minúscula dentro del paréntesis de los trenes de línea principal o con un número final en otros trenes. Por ejemplo, la versión 12.4(21) del software IOS de Cisco recibió algunas correcciones de advertencias, y la recopilación resultante se denominó 12.4(21a). De manera similar, 12.4(15)T8 es la octava recopilación de 12.4(15)T. Cada nueva recopilación aumenta el identificador de recopilación y entrega correcciones de software adicionales en un programa acelerado, antes de la siguiente versión individual planeada. Los criterios para realizar cambios en una recopilación son estrictos.

Se utiliza un conjunto único de números de versión individual para todos los trenes 12.4 del software IOS de Cisco. La versión de mantenimiento 12.4 y la versión 12.4T del software IOS de Cisco utilizan un pool de números de versión individual que se comparten en toda la familia de la versión 12.4 de dicho software. A la versión 12.4(6)T del software IOS de Cisco le siguió la versión 12.4(7)T y la versión 12.4(8)T. Esto permite que el administrador rastree cambios introducidos en el código.

Antes de la versión 15.0 del software IOS de Cisco, dicho software contaba con ocho paquetes para los routers Cisco, como se muestra en la ilustración. El esquema de paquetes se introdujo con el tren de línea principal 12.3 del software IOS de Cisco, y posteriormente se utilizó en otros trenes. Los paquetes de imágenes constan de ocho imágenes del IOS, tres de las cuales se consideran paquetes superiores.

**Los cinco paquetes no superiores son los siguientes:**

* **IP Base:** es la imagen básica del software IOS de Cisco.
* **Voz sobre IP:** voz y datos convergentes, VoIP, VoFR y telefonía IP.
* **Advanced Security:** características de VPN y de seguridad, incluido el firewall del IOS de Cisco, IDS/IPS, IPsec, 3DES y VPN.
* **Servicios de proveedor de servicios (SP):**agrega SSH/SSL, ATM, VoATM y MPLS a Voz sobre IP.
* **Base para empresas:** protocolos para empresas (Appletalk, IPX e IBM Support).

Después de la versión 12.4(24)T del IOS de Cisco, la siguiente versión del software IOS de Cisco fue 15.0.

IOS 15.0 proporciona varias mejoras al sistema operativo, por ejemplo:

* Nueva compatibilidad de hardware y de características
* Mayor coherencia de características con otras versiones principales del IOS
* Versión de nuevas características y programas de recopilación más predecibles
* Políticas de compatibilidad de versiones individuales proactivas
* Numeración de versión simplificada
* Pautas de migración e implementación de software más claras

. En lugar de dividirse en trenes independientes, los trenes T y de línea principal del software IOS de Cisco 15 tendrán versión de mantenimiento extendido (versión de EM) y versión de mantenimiento estándar (versión T). Con el nuevo modelo de versión del IOS, las versiones de línea principal del IOS de Cisco 15 se denominan “trenes M”.

Comenzando por 15.0, las nuevas versiones en la forma de un tren T se encuentran disponibles aproximadamente de dos a tres veces por año. Las versiones de EM están disponibles aproximadamente cada 16 a 20 meses. Las versiones T permiten recibir la característica de Cisco más rápidamente, antes de que la siguiente versión de EM esté disponible.

Una versión de EM incorpora la compatibilidad de características y de hardware de todas las versiones T anteriores. Esto hace que las últimas versiones de EM contengan la funcionalidad total del tren en el momento del lanzamiento.

En resumen, entre los beneficios del nuevo modelo de versión del IOS de Cisco se incluyen los siguientes:

* Legado de características de las versiones 12.4T y 12.4 de línea principal del software IOS de Cisco
* Nuevas versiones de características aproximadamente cada dos a tres veces por año que se entregan en forma secuencial desde un único tren
* Versiones de EM aproximadamente cada 16 a 20 meses e inclusión de nuevas características
* Versiones T para las características más recientes y compatibilidad de hardware antes de que la siguiente versión de EM se encuentre disponible en Cisco.com
* Las recopilaciones de mantenimiento de versiones T y M solo contienen correcciones de errores.
* **Versión de mantenimiento extendido**
* La versión de EM es ideal para el mantenimiento a largo plazo, y permite a los clientes cumplir con los requisitos, implementar la versión y mantenerla durante un período extendido. El tren de línea principal incorpora características proporcionadas en versiones anteriores y nuevas mejoras de características incrementales y compatibilidad de hardware.
* La primera recopilación de mantenimiento (para correcciones de errores solamente, sin nuevas características ni nueva compatibilidad de hardware) de la versión 15.0(1)M lleva el número 15.0(1)M1. Las versiones de mantenimiento posteriores se definen por un incremento del número de recopilación de mantenimiento (p. ej., M2, M3, etc.).
* **Versión de mantenimiento estándar**
* La versión T se utiliza para versiones de implementación cortas ideales para las características más recientes y la compatibilidad de hardware antes de que la siguiente versión de EM se encuentre disponible. La versión T proporciona recopilaciones de mantenimiento de corrección de errores regulares y soporte de errores crítico para errores que afectan la red, como problemas del Equipo de informes de incidentes de seguridad del producto (PSIRT).
* La primera versión de nuevas características 15 T planeada lleva el número de versión 15.1(1)T. La primera recopilación de mantenimiento (para correcciones de errores solamente, sin nuevas características o nueva compatibilidad de hardware) de la versión 15.1(1)T llevará el número 15.1(1)T1. Las versiones posteriores se definen por un incremento del número de recopilación de mantenimiento (p. ej., T2, T3, etc.).

**Paquetes de imagen de sistema del IOS 15**

Las series de routers de servicios integrados Cisco de segunda generación (ISR G2) 1900, 2900 y 3900 admiten servicios a petición mediante el uso de licencias de software. El proceso de Servicios a petición permite que los clientes logren ahorros operativos mediante la facilidad de pedido y administración del software. Cuando se realiza un pedido de una nueva plataforma de ISR G2 de Cisco, el router se envía con una imagen única y universal del software IOS de Cisco, y se utiliza una licencia para habilitar los paquetes de conjuntos de características específicos.

Existen dos tipos de imágenes universales admitidas en ISR G2:

* **Imágenes universales con la designación “universalk9” en el nombre de la imagen:**esta imagen universal ofrece todas las características del software IOS de Cisco, incluso características de criptografía del contenido seguras, como IPsec VPN, SSL VPN y comunicaciones unificadas seguras.
* **Imágenes universales con la designación “universalk9\_npe” en el nombre de la imagen:** el cumplimiento seguro de las capacidades de cifrado que proporciona Cisco Software Activation satisface los requisitos para la exportación de capacidades de cifrado. Sin embargo, algunos países tienen requisitos de importación que exigen que la plataforma no admita ninguna funcionalidad de criptografía segura, como la criptografía del contenido. Para satisfacer los requisitos de importación de dichos países, la imagen universal npe no admite ningún cifrado del contenido seguro.

Con los dispositivos ISR G2, se facilitó la selección de la imagen del IOS, debido a que se incluyen todas las características dentro de la imagen universal. Las características se activan mediante licencias. Cada dispositivo se envía con imagen universal. Los paquetes de tecnología IP Base, Datos, UC (Comunicaciones unificadas) y SEC (Seguridad) se habilitan en la imagen universal mediante las claves de licencia de Cisco Software Activation. Cada clave de licencia es exclusiva de un dispositivo en particular y se obtiene de Cisco al proporcionar la ID del producto, el número de serie del router y una clave de activación del producto (PAK). Cisco proporciona la PAK en el momento de la compra del software. IP Base se instala de manera predeterminada.

Al seleccionar o actualizar un router con IOS de Cisco, es importante elegir la imagen del IOS adecuada con el conjunto de características y la versión correctos. El archivo de imagen del IOS de Cisco está basado en una convención de nomenclatura especial. El nombre del archivo de imagen del IOS de Cisco contiene varias partes, cada una con un significado específico. Es importante comprender esta convención de nomenclatura al actualizar y seleccionar un software IOS de Cisco.

Como se muestra en la figura 1, el comando**show flash** muestra los archivos almacenados en la memoria flash, incluso los archivos de imagen de sistema.

* **Nombre de la imagen (c2800nm):** identifica la plataforma en la que se ejecuta la imagen. En este ejemplo, la plataforma es un router Cisco 2800 con un módulo de red.
* **advipservicesk9:** especifica el conjunto de características. En este ejemplo, advipservicesk9 se refiere al conjunto de características de Advanced IP Services, que incluye los paquetes de proveedor de servicios y de seguridad avanzada junto con IPv6.
* **mz:** indica dónde se ejecuta la imagen y si el archivo está comprimido. En este ejemplo, “mz” indica que el archivo se ejecuta desde la RAM y está comprimido.
* **124-6.T:** indica el formato del nombre del archivo para la imagen 12.4(6)T. Este es el número de tren, el número de versión de mantenimiento y el identificador de tren.
* **bin:** la extensión de archivo. Esta extensión indica que este es un archivo binario ejecutable.

Estas son las distintas partes de un archivo de imagen de sistema del IOS 15 en un dispositivo ISR G2:

* **Nombre de la imagen (c1900):** identifica la plataforma en la que se ejecuta la imagen. En este ejemplo, la plataforma es un router Cisco 1900.
* **universalk9:** especifica la designación de la imagen. Las dos designaciones para un ISR G2 son universalk9 y universalk9\_npe. Universalk9\_npe no contiene cifrado seguro y está pensado para países con restricciones de cifrado. Las características se controlan mediante licencias y pueden dividirse en cuatro paquetes de tecnología. Estos son IP Base, Seguridad, Comunicaciones unificadas y Datos.
* **mz:** indica dónde se ejecuta la imagen y si el archivo está comprimido. En este ejemplo, “mz” indica que el archivo se ejecuta desde la RAM y está comprimido.
* **SPA:** indica que el archivo está firmado digitalmente por Cisco.
* **152-4.M3:** especifica el formato del nombre del archivo para la imagen 15.2(4)M3. Esta es la versión del IOS, que incluye los números de la versión principal, de la versión secundaria, de la versión de mantenimiento y de la recopilación de mantenimiento. La M indica que se trata de una versión de mantenimiento extendido.
* **bin:** la extensión de archivo. Esta extensión indica que este es un archivo binario ejecutable.

La designación más común para ubicación de memoria y formato de compresión es mz. La primera letra indica la ubicación donde se ejecuta la imagen en el router. Las ubicaciones pueden incluir las siguientes:

* **f:** flash
* **m:** RAM
* **r:** ROM
* **l:** reubicable

El formato de compresión puede ser z para zip o x para mzip. La compresión de archivos es un método que utiliza Cisco para comprimir algunas imágenes ejecutadas desde la RAM que es eficaz para reducir el tamaño de la imagen. Se autodescomprime, de modo que cuando la imagen se carga en la RAM para ejecutarse, la primera acción es la descompresión.

**Nota:** las convenciones de nomenclatura, el significado de los campos, el contenido de la imagen y otros detalles del software IOS de Cisco están sujetos a cambios.

**Requisitos de memoria**

En la mayoría de los routers Cisco, incluso en los routers de servicios integrados, el IOS se almacena en la memoria CompactFlash como una imagen comprimida y se carga en la DRAM durante el arranque. Las imágenes de la versión 15.0 del software IOS de Cisco disponibles para los ISR Cisco 1900 y 2900 requieren 256 MB de memoria flash y 512 MB de memoria RAM. El ISR 3900 requiere 256 MB de memoria flash y 1 GB de RAM. Esto no incluye herramientas de administración adicionales, como Cisco Configuration Professional (Cisco CP). Para obtener detalles completos, consulte la ficha técnica del producto para el router específico.

# Servidores TFTP como ubicación de copia de seguridad

A medida que una red crece, las imágenes y los archivos de configuración del software IOS de Cisco pueden almacenarse en un servidor TFTP central. Esto ayuda a controlar la cantidad de imágenes del IOS y las revisiones a dichas imágenes del IOS, así como los archivos de configuración que deben mantenerse.

Las internetworks de producción suelen abarcar áreas extensas y contienen varios routers. Para cualquier red, es aconsejable tener una copia de seguridad de la imagen del software IOS de Cisco en caso de que la imagen de sistema en el router se dañe o se elimine accidentalmente.

Los routers distribuidos ampliamente necesitan una ubicación de origen o de copia de seguridad para las imágenes del software IOS de Cisco. El uso de un servidor TFTP de red permite las cargas y descargas de la imagen y la configuración a través de la red. El servidor TFTP de red puede ser otro router, una estación de trabajo o un sistema host.

# Creación de copias de seguridad de la imagen del IOS de Cisco

Para mantener las operaciones de red con el mínimo tiempo de inactividad, es necesario implementar procedimientos para realizar copias de seguridad de las imágenes del IOS de Cisco. Esto permite que el administrador de red copie rápidamente una imagen a un router en caso de que la imagen esté dañada o borrada.

Para realizar una copia de seguridad de la imagen del IOS de Cisco en un servidor TFTP, siga estos tres pasos:

**Paso 1.**Asegúrese de que haya acceso al servidor TFTP de red. Haga ping en el servidor TFTP para probar la conectividad.

**Paso 2.**Verifique que el servidor TFTP tenga suficiente espacio en disco para admitir la imagen del software IOS de Cisco. Utilice el comando **show flash0:** en el router para determinar el tamaño del archivo de imagen del IOS de Cisco. El archivo del ejemplo tiene 68831808 bytes de longitud.

**Paso 3.**Copie la imagen en el servidor TFTP mediante el comando**copy***source-url destination-url*.

Después de emitir el comando utilizando los URL de origen y de destino especificados, se solicita al usuario que introduzca el nombre del archivo de origen, la dirección IP del host remoto y el nombre del archivo de destino. A continuación, se inicia la transferencia.

**Comando boot system**

Para actualizar a la imagen del IOS copiada una vez que esa imagen se guarda en la memoria flash del router, configure este último para que cargue a nueva imagen durante el arranque mediante el comando **boot system**. Guarde la configuración. Vuelva a cargar el router para que arranque con la nueva imagen. Una vez que arranque el router, utilice el comando **show version** para verificar que se cargó la nueva imagen.

Durante el arranque, el código bootstrap analiza el archivo de configuración de inicio en la NVRAM para detectar los comandos **boot system** que especifican el nombre y la ubicación de la imagen del software IOS de Cisco que se debe cargar. Se pueden introducir varios comandos **boot system** de manera secuencial para proporcionar un plan de arranque que tenga tolerancia a fallas.

Como se muestra en la figura 1, el comando**boot system** es un comando de configuración global que permite que el usuario especifique el origen para que se cargue la imagen del software IOS de Cisco. Entre las opciones de sintaxis disponibles se encuentran las siguientes:

* Especificar el dispositivo flash como el origen de la imagen del IOS de Cisco.

Router(config)# **boot system flash0://c1900-universalk9-mz.SPA.152-4.M3.bin**

* Especificar el servidor TFTP como el origen de la imagen del IOS de Cisco, con ROMmon como copia de seguridad.

Router(config)# **boot system tftp://c1900-universalk9-mz.SPA.152-4.M3.bin**

Si no hay comandos **boot system** en la configuración, de manera predeterminada, el router carga y ejecuta la primera imagen válida del IOS de Cisco en la memoria flash.

Descripción general de licencias

A partir de la versión 15.0 del software IOS de Cisco, Cisco modificó el proceso para habilitar las nuevas tecnologías dentro de los conjuntos de características del IOS. La versión 15.0 del software IOS de Cisco incorpora conjuntos de características interplataforma para simplificar el proceso de selección de imágenes. Lo hace proporcionando funciones similares a través de los límites de las plataformas. Cada dispositivo se envía con la misma imagen universal. Los paquetes de tecnología se habilitan en la imagen universal mediante claves de licencia de Cisco Software Activation. La característica Cisco IOS Software Activation permite que el usuario habilite características con licencia y registre licencias. La característica Cisco IOS Software Activation es un conjunto de procesos y componentes que se utilizan para activar los conjuntos de características del software IOS de Cisco mediante la obtención y validación de licencias del software de Cisco.

Paquetes de tecnología disponibles:

* IP Base
* Datos
* Comunicaciones unificadas (UC)
* Seguridad (SEC)

**Licencias de paquetes de tecnología**

Las licencias de paquetes de tecnología se admiten en plataformas ISR G2 de Cisco (routers Cisco de las series 1900, 2900 y 3900). La imagen universal del IOS de Cisco contiene todos los paquetes y características en una imagen. Cada paquete es un conjunto de características específicas de la tecnología. Se pueden activar varias licencias de paquetes de tecnología en las plataformas ISR Cisco de las series 1900, 2900 y 3900.

# Proceso de obtención de licencias

Cuando se envía un router nuevo, vienen preinstaladas la imagen del software y las licencias permanentes correspondientes para los paquetes y características especificadas por el cliente.

El router también viene con la licencia de evaluación, conocida como licencia temporal, para la mayoría de los paquetes y características admitidas en el router especificado. Esto permite que los clientes prueben una nueva característica o un nuevo paquete de software mediante la activación de una licencia de evaluación específica. Si los clientes desean activar de forma permanente una característica o un paquete de software en el router, deben obtener una licencia de software nueva.

**Activación de una licencia de Right-to-Use de evaluación**

El proceso de licencia de evaluación pasó por tres revisiones en los dispositivos ISR G2. En la revisión más reciente, comenzando con las versiones del IOS de Cisco 15.0(1)M6, 15.1(1)T4, 15.1(2)T4, 15.1(3)T2 y 15.1(4)M, las licencias de evaluación se reemplazan por licencias de Right-to-Use (RTU) de evaluación después de 60 días. Una licencia de evaluación es válida durante un período de evaluación de 60 días. Después de 60 días, se lleva a cabo la transición de esta licencia a una licencia de RTU de forma automática. Estas licencias se encuentran disponibles en el sistema de honor y requieren que el cliente acepte el EULA. El EULA se aplica automáticamente a todas las licencias del software IOS de Cisco.

El comando del modo de configuración global**license accept end user agreement** se utiliza para configurar una aceptación única del EULA para todas las características y paquetes del software IOS de Cisco. Una vez que se emite el comando y que se acepta el EULA, este último se aplica automáticamente a todas las licencias del software IOS de Cisco, y no se le solicita al usuario que acepte el EULA durante la instalación de la licencia.

Configurar una aceptación única del EULA:

Router(config)# **license accept end user agreement**

Además, en la figura 1 se muestra el comando para activar una licencia de RTU de evaluación:

Router# **license boot module***module-name* **technology-package***package-name*

Use **?**en lugar de los argumentos para determinar qué nombres de módulos y paquetes de software admitidos se encuentran disponibles en el router. Los nombres de los paquetes de tecnología para las plataformas de ISR G2 de Cisco son los siguientes:

* ipbasek9:paquete de tecnología IP Base
* securityk9:paquete de tecnología de Seguridad
* datak9: paquete de tecnología de Datos
* uck9: paquete de tecnología de Comunicaciones unificadas (no disponible en la serie 1900)

**P**ara activar el paquete de software, se requiere volver a cargar mediante el comando**reload**.

Las licencias de evaluación son temporales, y se utilizan para evaluar un conjunto de características en hardware nuevo. Las licencias temporales se limitan a un período de uso específico (por ejemplo, 60 días).

Una vez que se instala correctamente una licencia, vuelva a cargar el router mediante el comando **reload**. El comando **show license**de la figura 2 verifica si se instaló la licencia.

# Realización de copias de seguridad de la licencia

El comando **license save** se utiliza para copiar todas las licencias en un dispositivo y almacenarlas en un formato requerido por la ubicación de almacenamiento especificada. Las licencias guardadas se restablecen mediante el comando **license install**.

El comando para realizar una copia de seguridad de las licencias en un dispositivo es el siguiente:

Router# **license save***file-sys://lic-location*

Utilice el comando **show flash0:** para verificar que las licencias se hayan guardad.

La ubicación de almacenamiento de licencias puede ser un directorio o un URL que corresponda a un sistema de archivos. Utilice el comando **?**para ver las ubicaciones de almacenamiento que admite un dispositivo.

**Bibliografías:**

<http://es.slideshare.net/WilfredoMatheu/protocolos-de-cada-capa-del-modelo-osi>

<http://protocolotcpip.galeon.com>

<https://claudiooq2.wordpress.com/switch-hub-router-bridge/>

<https://msdn.microsoft.com/es-es/library/cc786900(v=ws.10).aspx>

http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

http://ctecnologicou.blogspot.mx/2015/03/broadcast-storm-control-y-spanning-tree.html

<http://es.ccm.net/contents/258-vpn-redes-privadas-virtuales>

<http://elastixtech.com/fundamentos-de-telefonia/interconexion-a-la-pstn/>

<http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-net.html>

<http://es.ccm.net/contents/163-sistema-de-prevencion-de-intrusiones-ips>

<http://www.interoute.es/hosting/servicios-gestionados/seguridad-gestionada/prevencion-de-intrusiones>

<http://domosolutions.co/switches-capa-2-capa-3-y-capa-4/>

<https://esemanal.mx/2013/11/guia-de-switches-capa-2-y-3/>

<http://aprenderedes.com/2006/11/protocolo-de-arbol-de-extensionstp/>

<http://www.ecured.cu/Est%C3%A1ndares_IEEE_802.3>

<http://www.sos-info.es/preguntasfrecuentes/97-cables-y-adaptadores/322-ique-es-y-como-funciona-un-poe>

<http://www.textoscientificos.com/redes/redes-virtuales>