UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO INTERIOR IP PARA EL SISTEMA OPERATIVO IOS 12.2

T E S I S

P A R A O B T E N E R E L T I T U L O D E

INGENIERO MECÁNICO ELÉCTRICO

P R E S E N T A :

M A N Z A N O R I O S R A Ú L

ASESOR: ING. BENITO BARRANCO CASTELLANOS

San Juan de Aragón, Estado de México, Noviembre de 2011

AGRADECIMIENTOS

A MIS PADRES: Gracias, por su invaluable apoyo y el gran trabajo que hicieron para guiarme y llegar ser una persona responsable y de bien, lo cual hoy me lleva a cumplir una de las metas más importantes en mi vida.

A MI ESPOSA: Gracias por ser una persona de vital importancia en mi vida, por tu infinita paciencia, comprensión, cariño y apoyo incondicional para la culminación de esta meta.

A MIS HIJOS: Porque los maravillosos momentos a su lado, su inocencia y amor son el aliciente perfecto que me permite poder lograr lo que me proponga.

A MIS HERMANOS: Por también ser parte fundamental de mi vida, mi formación como persona y porque sé que cuento con su invaluable apoyo.

A MIS AMIGOS: Que en gran parte de mi vida han estado conmigo y que hemos compartido tantas buenas y malas experiencias que nos han enseñado el valor de la amistad.

A MI ASESOR EL ING. BENITO BARRANCO CASTELLANOS: Porque siempre estuvo al pendiente y apoyándome en la elaboración de este trabajo.

En especial a la memoria de mi hermano RENÉ MANZANO RIOS quien debería estar cumpliendo esta meta conmigo, pero sé que desde donde se encuentre me acompañara.

ÍNDICE

OBJETIVO

Diseñar un material inteligible de consulta para quienes deseen obtener en forma específica conocimientos teóricos de enrutamiento y poder realizar tareas prácticas, referente a las configuraciones básicas del router, de enrutamiento estático y de los diferentes protocolos de enrutamiento interior IP en el Sistema Operativo de Internetwork cisco IOS 12.2.

INTRODUCCIÓN

Al tomar en cuenta las necesidades y los avances actuales producidos en una sociedad que cada día se vuelve más dependiente de los sistemas de comunicación, resulta de gran importancia destacar tanto la transmisión de información, como la necesidad de que ésta llegué a su destino en el momento preciso mediante el uso de las redes.

Es a través de la Internet que queda probado y todos los días se muestra con mejor detalle, que la transmision de información ha sido y será revolucionaria en las áreas de los servicios financieros, de entretenimiento, salud, educación y gobierno.

El proceso de digitalización de todas las técnicas de comunicación, transmisión y recepción, producen nuevas convergencias entre diferentes sectores (cultura, comunicación, lengua, educación, telecomunicaciones, etc.), pero muy especialmente lo que producen es la transformación de los “espacios de comunicación”, los límites y las fronteras y, como consecuencia, la transformación de los espacios de intercambios culturales. Los principales cambios estructurales de la sociedad se producen ahora entorno del tratamiento y de la transmisión de la información.

Uno de los dispositivos que hacen posible que la información llegué al destino deseado, son los routers o enrutadores, estos realizan el proceso de enrutamiento y son la columna vertebral de las grandes redes internas y de la Internet, es por eso que estos dispositivos son de trascendental importancia para el proceso de transmisión de información.

El enrutamiento es el proceso de enviar paquetes de una ubicación a otra. Un protocolo de enrutamiento es un protocolo de capa de red que interpreta la información de una dirección de capa de red para permitir el envío de un paquete a la dirección de destino. Los routers trabajan en la capa de red, esta capa dentro de una arquitectura de red de datos, es la que se encarga de llevar los paquetes de datos desde el origen (estación transmisora) hasta el destino (estación receptora).

Llegar al destino, en tiempo y forma, puede requerir que el protocolo de enrutamiento o ruteo, que es el encargado de escoger las rutas más eficientes y mantener las tablas de enrutamiento, cumpla con ciertas propiedades que aseguren la eficiencia de su trabajo, ya que debe estar preparado para manejar cambios de topología y tráfico sin requerir el aborto de las actividades o el reinicio de la red.

Este trabajo está enfocado al estudio del proceso de enrutamiento y del funcionamiento, características, ventajas y desventajas de los diferentes protocolos de enrutamiento; así como sus respectivas configuraciones dentro del Cisco IOS.

El software Cisco IOS puede ejecutarse en la mayor parte del backbone de Internet y es ampliamente implementado por las empresas y proveedores de servicios en todo el mundo.

En el capítulo 1 de este trabajo se mencionan conceptos básicos en la transmisión de datos. Se habla del modelo de referencia OSI en comparativa con el modelo de referencia TCP/IP, se identifican las diferencias y analogías. Posteriormente, se analiza el funcionamiento de la capa de red, que es donde se definen las direcciones lógicas que son las que se utilizan en el proceso de enrutamiento, después se estudia todo lo referente al direccionamiento IP y las técnicas que se han desarrollado ante el agotamiento de las direcciones IPv4 como lo es VLSM y CIDR. También se muestra el papel de los routers dentro de las WAN y por último, se hace una descripción de los componentes y la secuencia de inicio del router.

El capítulo 2 inicia con los requerimientos necesarios para conectarse al router y realizar configuraciones en él, se empieza con configuraciones generales que se hacen en los routers como nombre, contraseñas, mensajes, interfaces, respaldos y comandos de verificación. Después se trata el enrutamiento estático en donde de manera práctica se configuran rutas estáticas y estáticas por defecto, también se describe la importancia del parámetro llamado distancia administrativa. Al final de este capítulo se describe el funcionamiento en general de los protocolos de enrutamiento dinámico y la clasificación de estos en protocolos vector-distancia y estado de enlace.

En el capítulo 3 se describe toda la información teórica necesaria, como lo es la forma en que se anuncian las rutas, la configuración de temporizadores, métricas, interfaces pasivas, redistribución de rutas, filtrado de rutas y autenticación en las actualizaciones de enrutamiento; para que se desarrollen ejemplos prácticos en donde se configura y se analiza el funcionamiento, en el Cisco IOS de los protocolos de enrutamiento interior IP. Los protocolos que se ejemplifican son **RIPv2** (Routing Information Protocol versión 2), **EIGRP** (Enhanced Interior Gateway Routing Protocol) y **OSPF** (Open Shortest Path First). Los protocolos **RIP** e **IGRP** (Interior Gateway Routing Protocol) solo se mencionan como referencia ya que prácticamente están en desuso.

Es preciso mencionar que los ejemplos desarrollados son meramente con fines didácticos. Para llevar a cabo las prácticas se puede utilizar el simulador *Cisco Packet Tracer 5.2*, ya que en el ámbito de la educación pública es difícil contar con un laboratorio de redes en donde puedan efectuarse y los lugares donde imparten la capacitación referente a los temas que se exponen en este trabajo son, por lo general, caros.

CAPÍTULO 1 . GENERALIDADES

1.1. CAPACIDAD DEL CANAL EN LA TRANSMISIÓN DE DATOS

Cuando se realiza una transmisión de datos hay una gran variedad de efectos nocivos que distorsionan o corrompen la señal que contiene la información. Para los datos digitales, la cuestión a resolver es en qué medida estos efectos limitan la velocidad con la que se pueden transmitir. Se denomina capacidad del canal a la velocidad máxima a la que se pueden transmitir los datos en un canal, o ruta de comunicación de datos, bajo unas condiciones dadas.

Hay cuatro conceptos en juego relacionados entre sí, que son:

- **La velocidad de transmisión de los datos:** es expresada en bits por segundo (bps).
- **El ancho de banda:** éste estará limitado por el transmisor y por la naturaleza del medio de transmisión; se mide en ciclos por segundo o hertz.
- **El ruido:** nivel medio de ruido a través del camino de transmisión.
- **La tasa de errores:** tasa a la que ocurren los errores. Se considera que ha habido un error cuando se recibe un 1 habiendo transmitido un 0, o se recibe un 0 habiendo transmitido un 1.

El problema considerado es el siguiente: los servicios de comunicaciones son por lo general caros y, normalmente, cuanto mayor es el ancho de banda requerido por el servicio, mayor es el coste. Es más, todos los canales de transmisión de interés práctico están limitados en banda. Las limitaciones surgen de las propiedades físicas de los medios de transmisión o por limitaciones que se imponen deliberadamente en el transmisor para prevenir interferencias con otras fuentes. Por - consiguiente, es deseable hacer un uso tan eficiente como sea posible del ancho de

banda limitado. En el caso de los datos digitales, esto significa que dado un ancho de banda sería deseable conseguir la mayor velocidad de datos posible no superando la tasa de errores permitida. El mayor inconveniente para conseguir este objetivo es la existencia de ruido.

1.1.1. RUIDO

Para cualquier dato transmitido, la señal recibida consistirá en la señal transmitida modificada por las distorsiones introducidas en la transmisión, además de señales no deseadas que se insertaran en algún punto entre el transmisor y el receptor. A estas últimas señales no deseadas se les denomina ruido. El ruido es el factor de mayor importancia de entre los que limitan las prestaciones de un sistema de comunicación.

La señal de ruido se puede clasificar en cuatro categorías:

- Ruido térmico.
- Ruido de intermodulación.
- Diafonía.
- Ruido impulsivo.

El **ruido térmico** se debe a la agitación térmica de los electrones. Está presente en todos los dispositivos electrónicos y medios de transmisión; como su nombre indica, es función de la temperatura. El ruido térmico está uniformemente distribuido en el espectro de frecuencias usado en los sistemas de comunicación, es por esto por lo que a veces se denomina ruido blanco. El ruido térmico no se puede eliminar y, por tanto, impone un límite superior en las prestaciones de los sistemas de comunicación. Es especialmente dañino en las comunicaciones satelitales, ya que en estos sistemas, la señal recibida por las estaciones terrestres es muy débil. En cualquier dispositivo o conductor, la cantidad de ruido térmico presente en un ancho de banda de 1 Hz es

$$N_0 = kT(\text{W/Hz})$$

Donde:

N_0 = densidad de potencia del ruido, en watts por 1Hz de ancho de banda

k = constante de Boltzmann = 1.38×10^{-23} J/K.

T = temperatura absoluta, en grados Kelvin.

A temperatura ambiente, es decir a T= 17°C, o 290 K, la densidad de potencia del ruido térmico será:

$$N_0 = (1.38 \times 10^{-23}) \times 290 = 4 \times 10^{-21} \text{ W/Hz} = -204\text{dBW/Hz}$$

donde dBW corresponde a decibeles-watts.

Se supone que el ruido es independiente de la frecuencia. Así pues, el ruido térmico presente en un ancho de banda de B hertz se puede expresar como:

$$N = kTB$$

o, expresado en decibeles-watts

$$N = 10\log k + 10\log T + 10\log B$$
$$= -228.6 \text{ dBW} + 10\log T + 10\log B \qquad (1.1)$$

Dado a un receptor con una temperatura efectiva de ruido de 294 K y un ancho de banda de 10 MHz, el ruido térmico a la salida del receptor será

$$N = -228.6 \text{ dBW} + 10\log(294) + 10\log 10^7$$

$$N = -228.6 + 24.7 + 70$$

$$N = -133.9 \text{ dBW}$$

Cuando señales de distintas frecuencias comparten el mismo medio de transmisión puede producirse **ruido de intermodulación**. El efecto del ruido de intermodulación es la aparición de señales a frecuencias que sean suma o diferencia de las dos frecuencias originales o múltiplos de éstas. Por ejemplo, la mezcla de las señales de frecuencias f_1 y f_2 puede producir energía a frecuencia $f_1 + f_2$. Estas componentes espúreas podrían interferir con otras componentes a frecuencia $f_1 + f_2$.

El ruido de intermodulación se produce cuando hay alguna no linealidad en el transmisor, en el receptor o en el sistema de transmisión. Idealmente, estos sistemas se comportan como lineales; es decir, la salida es igual a la entrada multiplicada por una constante. Sin embargo, en cualquier sistema real, la salida es una función más compleja de la entrada. El comportamiento no lineal puede aparecer debido al funcionamiento incorrecto de los sistemas o por sobrecargas producidas al utilizar señales con mucha energía. Bajo estas circunstancias es cuando aparecen los términos suma o diferencia no deseados.

La diafonía la ha podido experimentar todo aquel que al usar un teléfono haya oído otra conversación; se trata, en realidad, de un acoplamiento no deseado entre las líneas que transportan las señales. Esto puede ocurrir por el acoplamiento eléctrico entre cables de pares cercanos o, en raras ocasiones, en líneas de cable coaxial que transporten varias señales. La diafonía también aparece cuando las señales no deseadas se captan en las antenas de microondas; aunque estas se caracterizan por ser altamente direccionales, la energía de las microondas se dispersa durante la transmisión. Generalmente, la diafonía es del mismo orden de magnitud (o inferior) que el ruido térmico.

Los ruidos antes descritos son de magnitud constante y razonablemente predecibles. Así pues es posible idear un sistema de transmisión que les haga frente. Por el contrario, el **ruido impulsivo** es no continuo y está constituido por pulsos o picos irregulares de corta duración y de amplitud relativamente grande. Se generan por una gran diversidad de causas, por ejemplo, por perturbaciones electromagnéticas exteriores producidas por tormentas atmosféricas o por fallos y defectos en los sistemas de comunicación.

Generalmente, el ruido impulsivo no tiene mucha transcendencia para los datos analógicos. Por ejemplo, la transmisión de voz se puede perturbar mediante chasquidos o crujidos cortos, sin que ello implique pérdida significativa de inteligibilidad. Sin embargo, el ruido impulsivo es una de las fuentes principales de error en la comunicación digital de datos. Por ejemplo, un pico de energía con

duración de 0.01 seg. no inutilizaría datos de voz, pero podría corromper aproximadamente 560 bits si se transmitieran a 56 kbps. La Figura 1.1 muestra un ejemplo del efecto del ruido sobre una señal digital. Aquí el ruido consiste en un nivel relativamente pequeño de ruido térmico más picos ocasionales de ruido impulsivo. Los datos digitales se recuperan muestreando la señal recibida una vez por cada intervalo de duración del bit. Como se puede observar, el ruido es a veces suficiente para convertir un 1 en un 0, o un 0 en un 1.

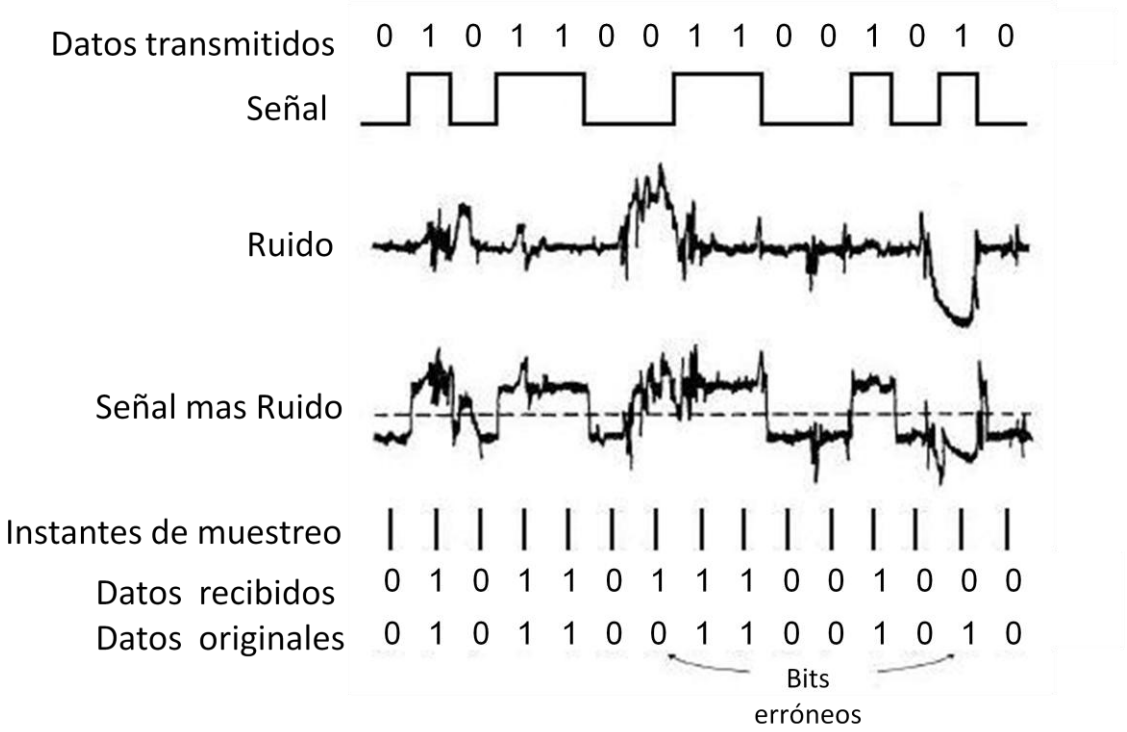


Figura 1.1 Efecto del ruido en una señal digital[1].

1.1.2. TEOREMA DE MUESTREO

El teorema de muestreo de Nyquist-Shannon, es fundamental en la teoría de la información y de especial interés en las telecomunicaciones.Este teorema fue formulado en forma de conjetura por primera vez por Harry Nyquist en 1928 (*Certain topics in telegraph transmission theory*), y fue demostrado formalmente por Claude E. Shannon en 1949 (*Communication in the presence of noise*).

[1] Stallings William, *Data and computer communications,* p.60.

Teorema de muestreo. *Cualquier forma de onda física puede estar representada en el intervalo -∞ < t < ∞ por*

$$w(t) = \sum_{n=-\infty}^{n=\infty} a_n \frac{\text{sen}\{\pi f_s[t-(n/f_s)]\}}{\pi f_s[t-(n/f_s)]} \tag{1.2}$$

donde:

$$a_n = f_s \int_{-\infty}^{\infty} w(t) \frac{\text{sen}\{\pi f_s[t-(n/f_s)]\}}{\pi f_s[t-(n/f_s)]}\, dt \tag{1.3}$$

y f_s es un parámetro al que se le asigna un valor conveniente mayor que cero. Además si w(t) es de banda limitada a B hertz y $f_s \geq 2B$, entonces la ecuación (1.2) se convierte en la representación de la función de muestreo donde,

$$a_n = w(n/f_s) \tag{1.4}$$

Es decir, cuando $f_s \geq 2B$ los coeficientes de la serie son simplemente los valores de la forma de onda obtenidos cuando se muestrea cada $1/f_s$ segundos.

A continuación se examina el problema de reproducir una forma de onda de banda limitada con *N* valores de muestreo. Supóngase que se desea reproducir la forma de onda en el intervalo $T_0 s$ como se muestra en la figura 1.2a. En tal caso se puede truncar la serie de la función de muestreo de (1.2) para incluir solo *N* de las funciones $\varphi_n(t)$ cuyos picos queden dentro del intervalo de interés. Es decir, la forma de onda se puede reconstruir de una manera aproximada con *N* muestras:

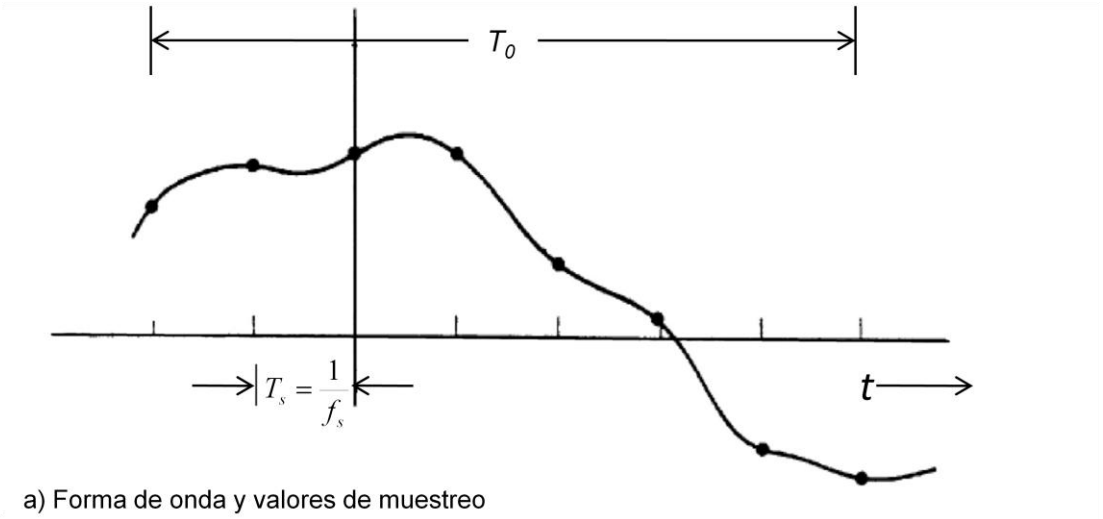
$$w(t) \approx \sum_{n=n_1}^{n=n_1+N} a_n \varphi_n(t) \tag{1.5}$$

donde las funciones $\varphi_n(t)$

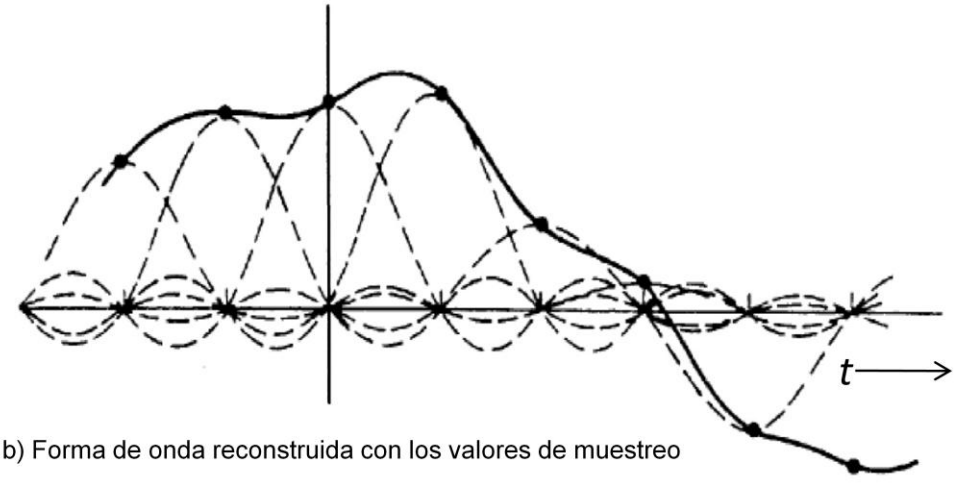
$$\varphi_n(t) = \frac{\text{sen}\{\pi f_s[t-(n/f_s)]\}}{\pi f_s[t-(n/f_s)]}$$

La figura 1.2b muestra la forma de onda reconstruida (línea llena) obtenida con la suma ponderada de formas de onda (sen x)/x retardadas (líneas de trazos),

donde los pesos son los valores de muestreo, $a_n = w(n/f_s)$, denotados por los puntos. La forma de onda es de banda limitada a B hertz con la frecuencia de muestreo fs ≥ 2B.



a) Forma de onda y valores de muestreo



b) Forma de onda reconstruida con los valores de muestreo

Figura 1.2 Teorema de muestreo.

El número mínimo de valores de muestreo para la reconstrucción de la forma de onda es:

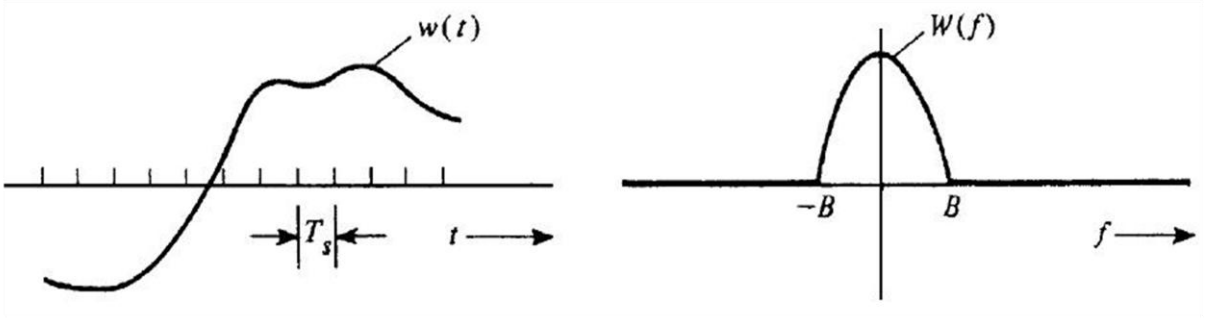
$$N = \frac{T_0}{1/f_s} = f_s T_0 \geq 2BT_0 \tag{1.6}$$

y existen *N* funciones ortogonales en el algoritmo de reconstrucción. Se puede decir que *N* es el número de dimensiones necesario para reconstruir la aproximación de la forma de onda en el intervalo T_0 segundos.

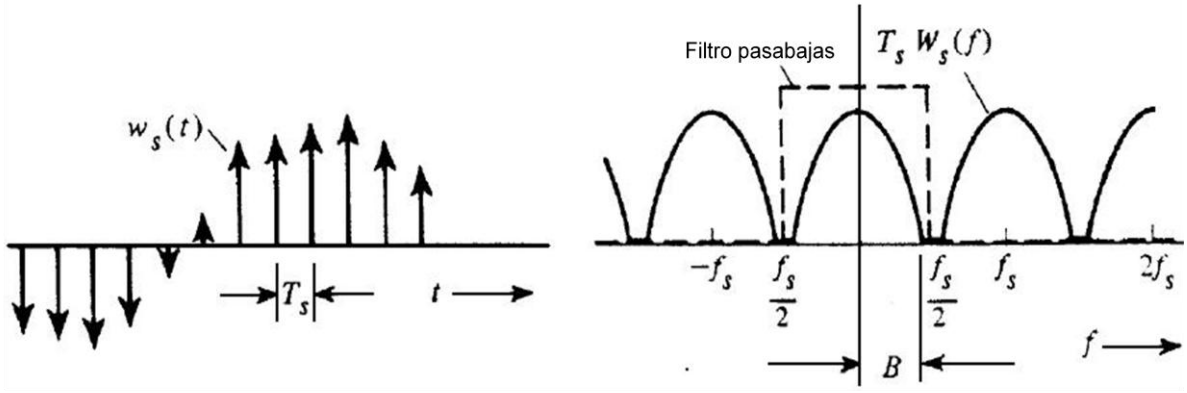
Si se desea reconstruir una forma de onda en tiempo real, con frecuencia se utiliza un procedimiento alternativo llamado **muestreo de impulsos.** La forma de onda se muestrea con un tren de impulsos de peso unitario. Esto se logra multiplicando la forma de onda con un tren de impulsos de peso unitario. La forma de onda muestreada resultante es

$$w_s(t) = w(t) \sum_{n=-\infty}^{n=\infty} \delta(t - nT_s) = \sum_{n=-\infty}^{n=\infty} w(nT_s)\, \delta(t - nT_s) \tag{1.7}$$

donde $T_s = 1/f_s$. Esta situación se ilustra en la figura 1.3, suponiendo que *W(f)* es real.



a) Forma de onda y su espectro



b) Forma de onda muestreada por impulsos y su espectro ($f_s > 2B$)

Figura 1.3 Muestreo por impulsos.

En la figura 1.3 el peso (área) de cada impulso, $w(nT_s)$, está indicado por la altura. El espectro de la forma de onda $w_s(t)$ muestreada por impulsos se evalúa sustituyendo la serie de Fourier del tren de impulsos (periódicos) en la ecuación (1.7).

$$w_s(t) = w(t) \sum_{n=-\infty}^{\infty} \frac{1}{T_s} e^{jnw_s t} \tag{1.8}$$

Considerando la transformada de Fourier de ambos lados de esta ecuación, se obtiene

$$W_s(f) = \frac{1}{T_s} W(f) * \mathcal{F}\left[\sum_{n=-\infty}^{\infty} e^{jnw_s t}\right] = \frac{1}{T_s} W(f) * \sum_{n=-\infty}^{\infty} \mathcal{F}\left[e^{jnw_s t}\right]$$

$$= \frac{1}{T_s} W(f) * \sum_{n=-\infty}^{\infty} \delta(f - nf_s)$$

ó

$$W_s(f) = \frac{1}{T_s} \sum_{n=-\infty}^{\infty} W(f - nf_s) \tag{1.9}$$

El espectro de la forma de onda muestreada por impulsos se compone del espectro de la forma de onda no muestreada replicada cada f_s Hz. Esto se muestra en la figura 1.3 b. Obsérvese que la técnica de muestreo por impulsos se puede usar para transformar el espectro de una señal en otra banda de frecuencia centrada en un armónico de la frecuencia de muestreo.

Si $f_s \geq 2B$, tal como se ilustra en la figura 1.3, los espectros replicados no se sobreponen y se puede regenerar el espectro original recortando $W_s(f)$ por encima de $f_s/2$. De este modo $w(t)$ se puede reproducir a partir de $w_s(t)$ simplemente con pasar $w_s(t)$ a traves de un filtro pasabajas ideal cuya frecuencia de corte sea $f_c = f_s/2$ donde $f_s \geq 2B$. Si $f_s < 2B$ (es decir, la forma de onda esta submuestreada), el espectro de $w_s(t)$ se compondrá de espectros replicados de $w_s(t)$ sobrepuestos.[2]

[2] Couch II Leon W., *Digital and analog communications systems,* pp.86-91.

1.1.3. ANCHO DE BANDA DE NYQUIST

Para comenzar, considérese el caso de un canal exento de ruido. En este entorno, la limitación en la velocidad de los datos está impuesta simplemente por el ancho de banda de la señal. Nyquist formalizó esta limitación, afirmando que si la velocidad de transmisión de la señal es *2B,* en una señal con frecuencias no superiores a *B* es suficiente para transportar esta velocidad de transmisión de la señal. Y viceversa: dado un ancho de banda *B,* la mayor velocidad de transmisión de la señal que se puede conseguir es *2B.* Esta limitación está provocada por la interferencia entre símbolos que se produce por la distorsión de retardo.

Obsérvese que en el último párrafo nos hemos referido a la velocidad de la señal. Si las señales a transmitir son binarias (dos niveles de tensión), la velocidad de transmisión de datos que se puede conseguir con *B* Hz es igual a *2B* bps. Por ejemplo, considérese un canal de voz que se utiliza mediante un módem para transmitir datos digitales. Supóngase un ancho de banda de 3100 Hz. Entonces, la capacidad c del canal es *2B* = 6,200 bps. No obstante, se pueden usar señales con más de dos niveles; es decir, cada elemento de señal puede representar a más de dos bits. Por ejemplo, si se usa una señal con cuatro niveles de tensión, cada elemento de dicha señal podrá representar dos bits. La formulación de Nyquist para el caso de señales multinivel es:

$$\boldsymbol{C} = 2B\log_2 M \tag{1.10}$$

donde *M* es el número de señales discretas o niveles de tensión. Así pues, para *M*=8, valor típico que se usa en algunos módem, la capacidad resulta ser 18,600 bps, siendo el ancho de banda igual a 3,100 Hz.

Por tanto, para un ancho de banda dado, la velocidad de transmisión de datos se puede incrementar considerando un número mayor de señales diferentes. Sin embargo, esto supone una dificultad mayor en el receptor: en lugar de tener que distinguir una de entre dos señales, deberá distinguir una de entre *M* posibles

señales. El ruido y otras dificultades en la línea de transmisión limitarán el valor de *M.*

1.1.3. FÓRMULA PARA LA CAPACIDAD DE SHANNON

La fórmula de Nyquist implica que al duplicar el ancho de banda se duplica la velocidad de transmisión, si todo lo demás se mantiene inalterado. Ahora establezcamos una relación entre la velocidad de transmisión, el ruido y la tasa de errores. La presencia de ruido puede corromper uno o más bits. Si se aumenta la velocidad de transmisión, el bit se hace más «corto», de tal manera que dado un patrón de ruido, éste afectará a un mayor número de bits. Así pues, dado un nivel de ruido, cuanto mayor es la velocidad de transmisión, mayor es la tasa de errores.

La Figura 1.1 ilustra esta relación. Si se incrementa la velocidad de transmisión de los datos, entonces habrá más bits durante el intervalo de duración del ruido y, por tanto, habrá un mayor número de errores.

Todos estos conceptos se han relacionado en la fórmula desarrollada por el matemático Claude Shannon. Como se ha comentado, cuanto mayor es la velocidad de transmisión, mayor es el daño que puede ocasionar el ruido. Dado un nivel de ruido, es de esperar que incrementando la energía señal se mejoraría la recepción de datos en presencia de ruido. Un parámetro fundamental en el desarrollo de este razonamiento es la relación señal-ruido (SNR, o S/N), que se define como el cociente de la potencia de la señal entre la potencia del ruido presente en un punto determinado en el medio de transmisión. Generalmente, este cociente se mide en el receptor, ya que es aquí donde se realiza el procesado de la señal y la eliminación del ruido no deseado. Por cuestiones de comodidad SNR se expresa en decibeles:

$$SNR_{dB}=10\ log\ (\text{potencia de señal/potencia de ruido})$$

Esta expresión muestra, en decibeles, cuanto excede la señal al nivel de ruido. Una SNR alta significará una señal de alta calidad y, por tanto, la necesidad de un número reducido de repetidores.

La relación señal-ruido es importante en la transmisión de datos digitales, ya que ésta determina la máxima velocidad de transmisión que se puede conseguir. Una conclusión de Shannon es que la capacidad máxima del canal, en bits por segundo, verifica la ecuación

$$\boldsymbol{C} = B\log_2 (1 + \text{SNR}) \tag{1.11}$$

donde C es la capacidad del canal en bits por segundo y B es el ancho de banda del canal en hertz. La fórmula de Shannon representa el máximo límite teórico que se puede conseguir. Sin embargo, en la práctica, se consiguen velocidades mucho menores. Una razón para esto reside en el hecho de que la fórmula anterior supone ruido blanco (ruido térmico). Además, no se han tenido en cuenta el ruido impulsivo, la distorsión de atenuación o la distorsión de retardo.

La capacidad, tal y como se ha calculado en la fórmula precedente, se denomina capacidad libre de errores. Shannon probó que si la velocidad de información real en el canal es menor que la capacidad libre de errores, entonces es teóricamente posible encontrar una codificación de la señal que consiga una transmisión exenta de errores a través del canal. Desafortunadamente, el teorema de Shannon no sugiere la manera de encontrar dicho código, pero proporciona un criterio de referencia con el que se pueden comparar las prestaciones de los esquemas de comunicación reales.

Pueden ser instructivas otras consideraciones adicionales que se deducen a partir de la ecuación anterior. Para un nivel de ruido dado, podría parecer que la velocidad de transmisión se puede aumentar incrementando tanto la energía de la señal como el ancho de banda. Sin embargo, al aumentar la energía de la señal, también lo hacen las no linealidades del sistema, dando lugar a un aumento del ruido

de intermodulación. Obsérvese igualmente que, como el ruido se ha supuesto blanco, cuanto mayor sea el ancho de banda, más ruido se introducirá en el sistema. Por tanto, cuando B aumenta, la SNR disminuye.

En el siguiente ejemplo se relacionan las formulaciones de Shanon y Nyquist. Supóngase que el espectro de un canal está situado entre 3 MHz y 4 MHz y que la SNR_{dB}=24 dB. En este caso:

$$B=4\text{MHz} - 3\text{MHz} = 1\text{MHz}$$

$$SNR_{dB}= 24 \text{ dB} = 10log(SNR)$$

$$SNR = 10^{2.4} = 251$$

Usando la formula de Shannon (1.11) se tiene que:

$$\boldsymbol{C} = 10^6 \text{ x } log_2 (1+251) \approx 10^6 \text{ x } 8 = 8 \text{ Mbps}$$

Este es, como ya se ha mencionado, un límite teórico difícil de alcanzar. No obstante supóngase que este límite se puede alcanzar. Según la fórmula de Nyquist, (1.10) ¿Cuántos niveles de señalización se necesitarán? Se tiene que:

$$\boldsymbol{C} = 2B\ log_2 M$$

$$8 \text{ x } 10^6 = 2 \text{ x } 10^6 \text{ x } log_2 M$$

$$4 = log_2 M$$

$$M = 2^4 = 16$$

1.1.4. EL COCIENTE E_b / N_0

Ahora se presenta un parámetro relacionado con la SNR que es más adecuado para determinar las tasas de error y la velocidad de transmisión. Además, se usa habitualmente para medir la calidad de las prestaciones de los sistemas de comunicación digital. Este parámetro es el cociente de la energía de la señal por bit

entre la densidad de potencia del ruido por hercio E_b/N_0. Sea una señal, digital o analógica, que contenga datos digitales binarios transmitidos a una determinada velocidad R. Teniendo en cuenta que 1 W = 1 J/s, la energía por bit de la señal será $E_b = ST_b$, donde S es la potencia de la señal y T_b es el tiempo necesario para transmitir un bit. La velocidad de transmisión es $R = 1/T_b$. Por tanto,

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}$$

o, expresado en decibelios,

$$\left(\frac{E_b}{N_0}\right)_{dB} = S_{dBW} - 10logR - 10logk - 10logT$$

$$= S_{dBW} - 10logR + 228.6\,dBW - 10logT$$

El cociente E_b/N_0 es importante, ya que para los datos digitales la tasa de error por bit es una función (decreciente) de este cociente. Dado un valor de E_b/N_0 necesario para conseguir una tasa de errores deseada, los parámetros se pueden seleccionar de acuerdo con la fórmula anterior. Nótese que cuando se aumenta la velocidad de transmisión R, la potencia de la señal transmitida, relativa al ruido, debe aumentarse para mantener el cociente E_b/N_0 requerido.

Intentemos inferir intuitivamente este resultado a partir de la Figura 1.1, la señal aquí considerada es digital, pero el mismo razonamiento podría extenderse para el caso de una señal analógica. En algunos casos, el ruido es suficiente como para alterar el valor de un bit. Ahora, si la velocidad de transmisión se duplicase, los bits tendrían asociada una duración menor, con lo que el ruido podría destruir dos bits. Por tanto, para una señal y ruido de energías constantes, un incremento en la velocidad de transmisión aumentaría la tasa de error.

La ventaja del cociente E_b/N_0 sobre la SNR es que esta última depende del ancho de banda.

En la modulación digital binaria PSK *(Phase Shift Keying)*, para obtener una tasa de error por bit igual 10^{-4} (un bit erróneo cada 10 000) se necesita un cociente E_b/N_0 = 8.4 dB. Si la temperatura efectiva es 290^0K (temperatura ambiente) y la velocidad de transmisión es 2 400 bps, ¿Qué nivel de señal recibida se necesita? En este caso se tiene que:

$$8.4 = S(dBW) - 10\log 2400 + 228.6\ dBW - 10\log 290$$

$$8.4 = S(dBW) - 10(3.38) + 228.6 - 10(2.46)$$

$$S = -161.8\ dBW$$

Se puede establecer la relación entre E_b/N_0 y la SNR de la siguiente manera. Se tiene que:

$$\frac{E_b}{N_0} = \frac{S}{N_0 R}$$

El parámetro N_0 es la densidad de potencia del ruido en watts/hercio. Por tanto, el ruido en una señal con ancho de banda B_T es $N = N_0 B_T$. Sustituyendo, se tiene que:

$$\frac{E_b}{N_0} = \frac{S}{N}\frac{B_T}{R} \tag{1.12}$$

Otra formulación de interés es la relación entre la eficiencia espectral y E_b/N_0. La fórmula de Shannon (ecuación 1.11) se puede reescribir como:

$$\frac{S}{N} = 2^{C/B} - 1$$

Usando la ecuación (1.11), igualando B_T con B y R con C, tenemos que

$$\frac{E_b}{N_0} = \frac{B}{C}\left(2^{C/B} - 1\right)$$

Esta es una formula útil que relaciona la eficiencia espectral alcanzable C/B con E_b/N_0.

Supóngase que se quiere encontrar el máximo E_b/N_0 necesario para conseguir una eficiencia espectral de 6 bps/Hz. Entonces

$$\frac{E_b}{N_0} = \frac{1}{6}(2^6 - 1) = 10.5$$

$$\left(\frac{E_b}{N_0}\right)_{dB} = 10\log(10.5) = 10.21\ dB$$

1.1.5. DECIBELES Y ENERGÍA DE LA SEÑAL

Un parámetro importante en cualquier sistema de transmisión es la energía de la señal transmitida. Al propagarse la señal en el medio habrá una pérdida, o atenuación, de energía de la señal. Para compensar este hecho es necesario introducir amplificadores cada cierta distancia que restituyan la energía de la señal.

Los valores de ganancias, pérdidas y, en general, de todas las magnitudes relativas se suelen expresar en decibeles, ya que:

- La energía de la señal decae, por lo general, exponencialmente. Por tanto, las pérdidas se pueden expresar cómodamente en decibeles, ya que es una unidad logarítmica.
- En un sistema de transmisión, las ganancias y pérdidas en cascada se pueden calcular fácilmente mediante sumas o restas, respectivamente.

El decibel es una medida del cociente o proporción entre dos niveles de la señal:

$$G_{dB} = 10log\ \frac{P_{salida}}{P_{entrada}} \tag{1.13}$$

La siguiente tabla muestra varias potencias de 10 expresadas en decibeles:

Cociente de potencias	dB	Cociente de potencias	dB
10^1	10	10^{-1}	-10

Cociente de potencias	dB	Cociente de potencias	dB
10^2	20	10^{-2}	-20
10^3	30	10^{-3}	-30
10^4	40	10^{-4}	-40
10^5	50	10^{-5}	-50

Tabla 1.1 Potencias expresadas en decibeles

A menudo existe confusión al utilizar los términos ganancia y perdida. Si un valor G_{dB} es positivo, corresponde en realidad a una ganancia en potencia. Por ejemplo una ganancia de 3 dB significa que la potencia se ha doblado. Si el valor de G_{dB} es negativo, en realidad implica una pérdida de potencia. Por ejemplo, una ganancia de - 3 dB, significa que la potencia se ha dividido por la mitad, es decir, es una pérdida de potencia. Normalmente eso se expresa diciendo que ha habido una pérdida de 3 dB. Sin embargo, algunas referencias dirian que ha habido una pérdida de -3dB. Tiene más sentido decir que una ganancia negativa corresponde a una pérdida positiva. Por tanto, se define la pérdida en decibelios L_{dB}, como

$$L_{dB} = -10log\ \frac{P_{salida}}{P_{entrada}} = 10log\ \frac{P_{entrada}}{P_{salida}} \tag{1.14}$$

Si en una línea de transmisión se transmite una señal con una potencia de 10mW y a cierta distancia se miden 5 mW, la pérdida se puede expresar como

L_{dB}=10 *log* (10/5)=10(0.3)=3 dB

Obsérvese que el decibel es una medida de una diferencia relativa, es decir, no es absoluta. Una pérdida de 1000 W a 500 W es igualmente una pérdida de 3 dB.

El decibel también se usa para medir diferencias de tensión, ya que la potencia es proporcional al cuadrado de la tensión:

$$P = \frac{V^2}{R}$$

donde

P = potencia disipada en una resistencia *R.*

V = caída de tensión en la resistencia *R.*

Por tanto,

$$L_{dB} = 10log\ \frac{P_{entrada}}{P_{salida}} = 10log\ \frac{V_{entrada}^2/R}{V_{salida}^2/R} = 20log\ \frac{V_{entrada}}{V_{salida}}$$

Los decibelios son útiles para determinar la ganancia o pérdida acumulada por una serie de elementos de transmisión. Sea un conjunto de elementos atacados por una potencia de entrada igual a 4mW. Sea el primer elemento una línea de transmisión con 12 dB de atenuación (-12 de ganancia), el segundo elemento un amplificador con una ganancia igual a 35 dB y, por último, una línea de transmisión con 10 dB de pérdida. La ganancia o atenuación neta será (-12+35-10)=13 dB. El cálculo de la potencia de salida P_{salida} es,

$$G_{dB}=13=10\ log\ (P_{salida}/4mW)$$

$$P_{salida}= 4 \times 10^{1.3}\ mW = 79.8\ mW$$

Los valores en decibeles se refieren a magnitudes relativas a cambios en magnitud, no a valores absolutos. A veces es conveniente expresar un nivel absoluto de potencia o tensión en decibeles para facilitar así el cálculo de la pérdida o ganancia con respecto a un valor inicial de la señal el **dBW (decibel-watt)** se usa frecuentemente en aplicaciones de microondas. Se elige como referencia el valor de 1 W y se define como 0 dBW. Se define por tanto, el nivel absoluto de potencia en dBW como:

$$Potencia_{dBW} = 10\log\frac{Potencia_W}{1\ W}$$

Una potencia de 1000 W corresponde a 30 dBW y una potencia de 1mW corresponde a -30 dBW.

Otra unidad es el **dBm (decibel-miliwatt)**, en la que se usa 1mW como referencia. Así 0 dBm = 1mW. La fórmula es:

$$Potencia_{dBm} = 10 \log \frac{Potencia_{mW}}{1\ mW}$$

Obsérvese las siguientes relaciones:

+ 30 dBm = 0 dBW

0 dBm = - 30 dBW

Otra unidad frecuente en los sistemas de televisión por cable y en las aplicaciones LAN de banda ancha es el **dBmV (decibel-milivolt)**. Esta es una medida absoluta, donde 0 dBmV equivale a 1mV. Por tanto,:

$$Tensión_{dBmV} = 20 \log \frac{Tensión_{mV}}{1\ mW}$$

En este caso se ha supuesto que la caída de tensión se realiza en una resistencia de 75 ohms [3].

[3] Stallings William, *Comunicaciones y Redes de computadores,* pp. 80-93.

1.2. MODULACIÓN DIGITAL

La modulación implica la modificación de uno o varios de los tres parámetros fundamentales que caracterizan la señal portadora, la amplitud, la frecuencia o la fase. Consecuentemente hay tres técnicas básicas de modulación que transforman los datos digitales en señales analógicas como se muestra en la figura 1.4, modulación por desplazamiento de amplitud **ASK** (Amplitud Shift Keying), modulación por desplazamiento de frecuencia **FSK** (Frequency Shift Keying) y modulación por desplazamiento de fase **PSK** (Phase Shift Keying). En todos los casos, la señal resultante ocupa un ancho de banda centrado en torno a la frecuencia de la portadora.

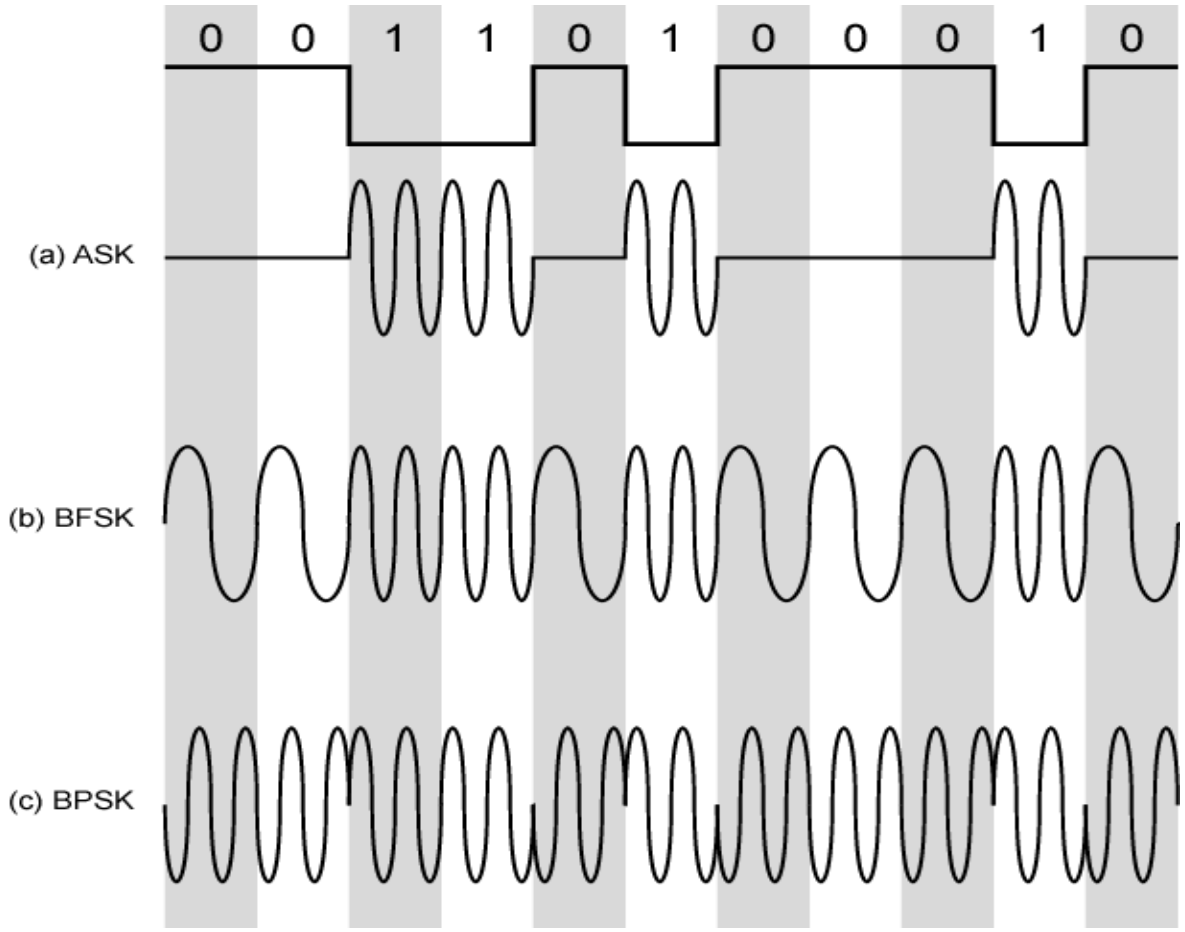


Figura 1.4 Técnicas básicas de modulación digital.[4]

[4] Ibidem, p.147

Se tiene que para:

ASK
$$s(t)=\begin{cases} A\cos(2\pi f_c t) & \text{1 binario} \\ 0 & \text{0 binario} \end{cases} \tag{1.15}$$

BFSK
$$s(t)=\begin{cases} A\cos(2\pi f_1 t) & \text{1 binario} \\ A\cos(2\pi f_2 t) & \text{0 binario} \end{cases} \tag{1.16}$$

BPSK
$$s(t)=\begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t+\pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t) & \text{1 binario} \\ -A\cos(2\pi f_c t) & \text{0 binario} \end{cases} \tag{1.17}$$

Se puede conseguir un uso más eficaz del ancho de banda si cada elemento de señalización representa más de un bit. Por ejemplo, en lugar de un desplazamiento de fase de 180º, como se hace en BPSK, una técnica habitual de codificación, conocida como modulación por desplazamiento de fase en cuadratura (QPSK, Quadrature Phase Shift Keying), considera desplazamientos múltiplos de 90º ($\pi/2$).

QPSK
$$s(t)=\begin{cases} A\cos\left(2\pi f_c t+\frac{\pi}{4}\right) & 11 \\ A\cos\left(2\pi f_c t+\frac{3\pi}{4}\right) & 01 \\ A\cos\left(2\pi f_c t-\frac{3\pi}{4}\right) & 00 \\ A\cos\left(2\pi f_c t-\frac{\pi}{4}\right) & 10 \end{cases} \tag{1.18}$$

Por tanto, cada elemento de señalización representa dos bits en lugar de uno.

La utilización de varios niveles se puede extender para transmitir más de dos bits de una vez. Por ejemplo, usando ocho ángulos de fase diferentes es posible transmitir 3 bits. Es más cada ángulo puede tener más de una amplitud. Por

ejemplo, un modem estándar a 9600 bps utiliza 12 ángulos de fase, cuatro de los cuales tienen dos valores de amplitud, dando lugar a 16 elementos de señalización diferentes.

Lo anterior pone de manifiesto la diferencia entre velocidad de transmisión ***R*** (en bps) y velocidad de modulación ***D*** (en baudios) de la señal. Supongamos que este sistema se empleara sobre una señal digital en la que cada bit se representara por un pulso constante de tensión, tomando un nivel para el uno binario y otro nivel distinto para el cero. La velocidad de transmisión sería $R= 1/T_b$. Sin embargo, la señal codificada contendrá $L=4$ bits por cada elemento de señalización, utilizando $M=16$ combinaciones distintas de amplitud y fase. La velocidad de modulación, en este caso, es *R/4,* ya que cada elemento de señal transporta 4 bits. Por tanto, la velocidad de señalización es 2400 baudios, pero la velocidad de transmisión es igual a 9600 bps. Esta misma aproximación posibilita mayores velocidades de transmisión en líneas de calidad telefónica mediante utilización de esquemas de modulación más complejos.

En general, se tiene que:

$$D = \frac{R}{L} = \frac{R}{\log_2 M} \tag{1.19}$$

donde:

D= velocidad de modulación en baudios.
R= velocidad de transmisión en bps.
M= número de elementos de señalización diferentes = 2^L.
L= número de bits por elemento de señal.

En la figura 1.5 se resumen algunos resultados relevantes basados en ciertas suposiciones relativas a los sistemas de transmisión. Aquí se representa la tasa de errores por bit en función del cociente E_b/N_0, cuando este cociente aumenta, la tasa de errores disminuye.

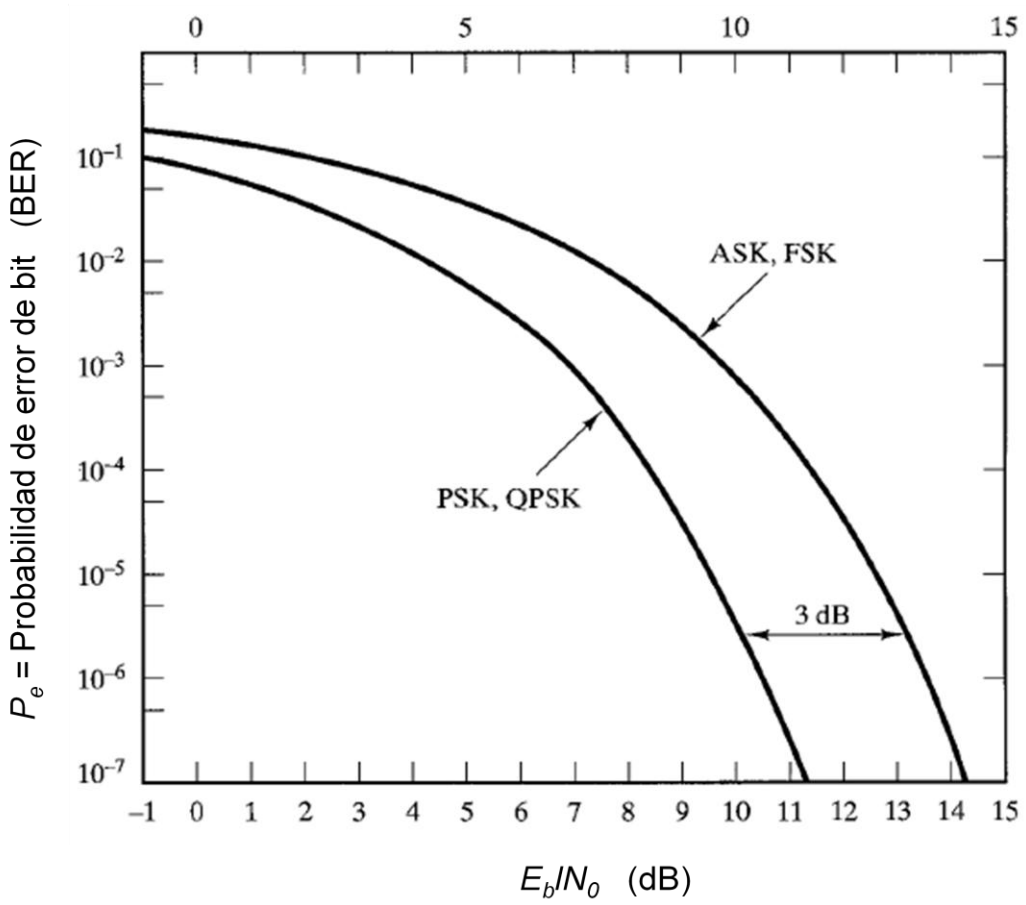


Figura 1.5 BER (Bit Error Rate) teóricas para varios esquemas de señalización digital[5].

¿Cuál es la eficiencia del ancho de banda en FSK, ASK, PSK, y QPSK, siendo la tasa de errores por bit igual a 10^{-7} en un canal con una SNR de 12 dB?

Utilizando la ecuación (1.12), se tiene que

$$\frac{E_b}{N_0} = 12dB - \left(\frac{R}{B_T}\right)_{dB}$$

Para FSK y ASK, a partir de la figura 1.5:

$$\frac{E_b}{N_0} = 14.2dB$$

$$\left(\frac{R}{B_T}\right)_{dB} = -2.2\ dB$$

[5] Couch II Leon W., *Digital and analog communications systems,* p.468.

$$\frac{R}{B_T} = 0.6$$

Para PSK, a partir de la figura 1.5:

$$\frac{E_b}{N_0} = 11.2\ dB$$

$$\left(\frac{R}{B_T}\right)_{dB} = 0.8\ dB$$

$$\frac{R}{B_T} = 1.2$$

En QPSK se debe tener en cuenta que la velocidad de modulación debe verificar que *D=R/2*. Por tanto,

$$\frac{R}{B_T} = 2.4$$

Como se muestra en el ejemplo anterior, los esquemas ASK y FSK proporcionan la misma eficiencia del ancho de banda; PSK es mejor y se consigue todavía mayor eficiencia si se utiliza una señalización multinivel.[6]

[6] Stallings William, *Comunicaciones y Redes de computadores,* pp. 146-155.

1.3. EL MODELO OSI Y TCP/IP

1.3.1. MODELO DE REFERENCIA OSI

Durante las últimas décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas; sin embargo, se desarrollaron utilizando implementaciones de hardware y software diferentes. Como resultado, muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas, poderse comunicar entre sí. Para solucionar este problema, la Organización Internacional para la Normalización (ISO) reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI (Open System Interconnection) en 1984[7].

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

[7] *Cisco Certified Network Associate Curriculum, Semestre 1*, V2.1.2.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking (sistema de redes) se denomina división en capas. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo de referencia OSI son:

Capa 7: Capa de aplicación
Capa 6: Capa de presentación
Capa 5: Capa de sesión
Capa 4: Capa de transporte
Capa 3: Capa de red
Capa 2: Capa de enlace de datos
Capa 1: Capa física

El modelo OSI se ilustra en la figura 1.6.

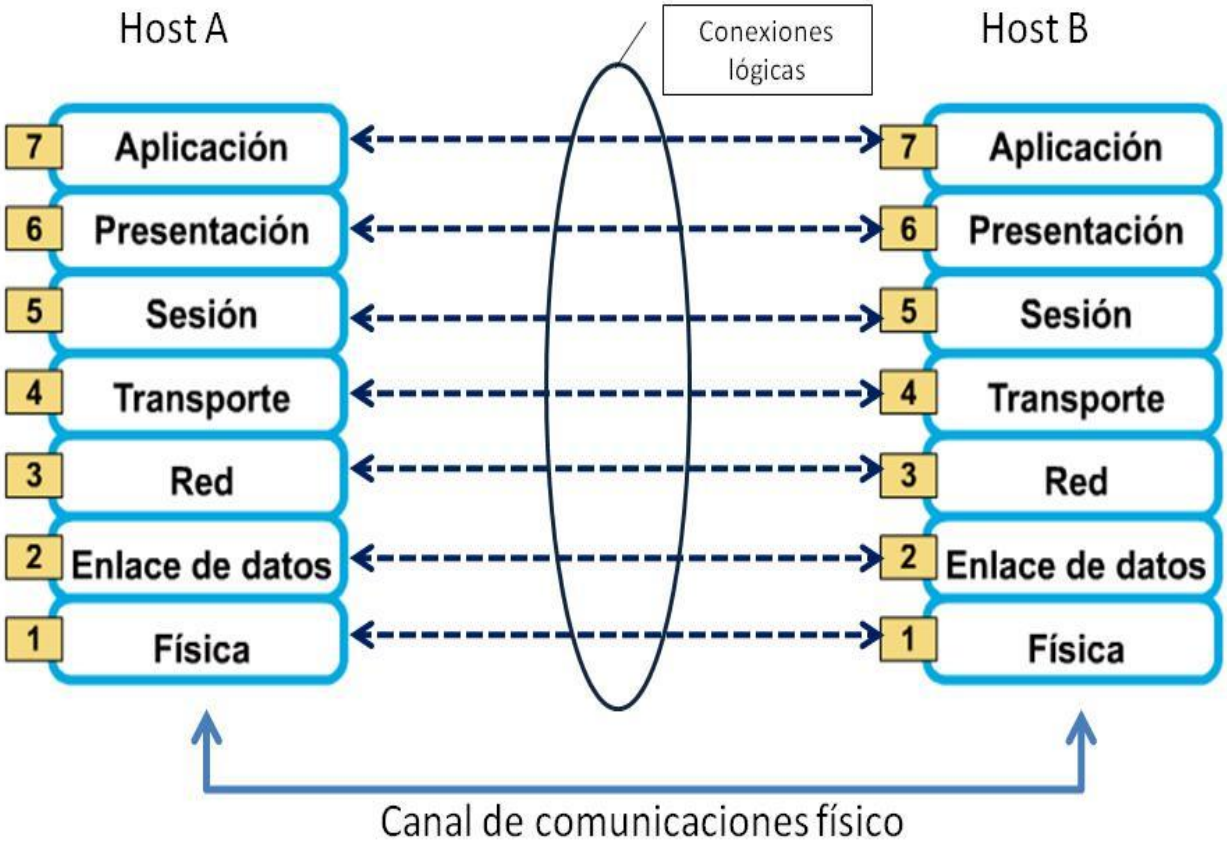


Figura 1.6 Modelo de referencia OSI de las conexiones físicas y lógicas[8].

A continuación, se presenta una breve descripción de cada capa del modelo de referencia OSI.

Capa 7: La capa de aplicación

Esta es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto, etc.. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

[8] Couch II Leon W., *Digital and analog communications systems,* p.689.

Capa 6: La capa de presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa 5: La capa de sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Capa 4: La capa de transporte

La capa de transporte segmenta los datos originados en el host emisor y los re ensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

Capa 3: La capa de red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Capa 2: La capa de enlace de datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Capa 1: La capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física.

1.3.2. MODELO DE REFERENCIA TCP/IP

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el *Protocolo de control de transmisión/Protocolo Internet* (TCP/IP). El modelo de referencia TCP/IP y la pila de protocolos TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, de manera casi inmediata[9].

El Departamento de Defensa de EE.UU. (*DoD*) creó el modelo TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. El DoD deseaba que sus paquetes llegaran al destino siempre, bajo cualquier condición, desde un punto determinado hasta cualquier otro. Este problema fue lo que llevó a la creación del modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló Internet.

El modelo TCP/IP, como se observa en la figura 1.7, tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. No se debe confundir las capas de los dos modelos, porque la capa de aplicación tiene diferentes funciones en cada modelo.

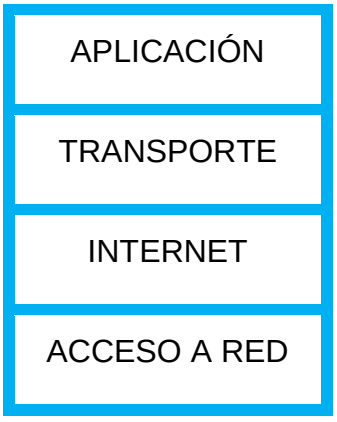


Figura 1.7 MODELO TCP/IP

[9] *Cisco Certified Network Associate Curriculum, Semestre 1*, V2.1.

Capa de aplicación

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.

Capa de transporte

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a la conexión no significa que el circuito exista entre los computadores que se están comunicando (esto sería una conmutación de circuito). Significa que los segmentos de Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.

Capa de Internet

El propósito de la capa de Internet es enviar paquetes origen desde cualquier red en la internetwork (interconexión de redes) y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando se envía una carta por correo, no se sabe cómo llega a destino (existen varias rutas posibles); lo que interesa es que la carta llegue.

Capa de acceso de red

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas, física y de enlace de datos del modelo OSI.

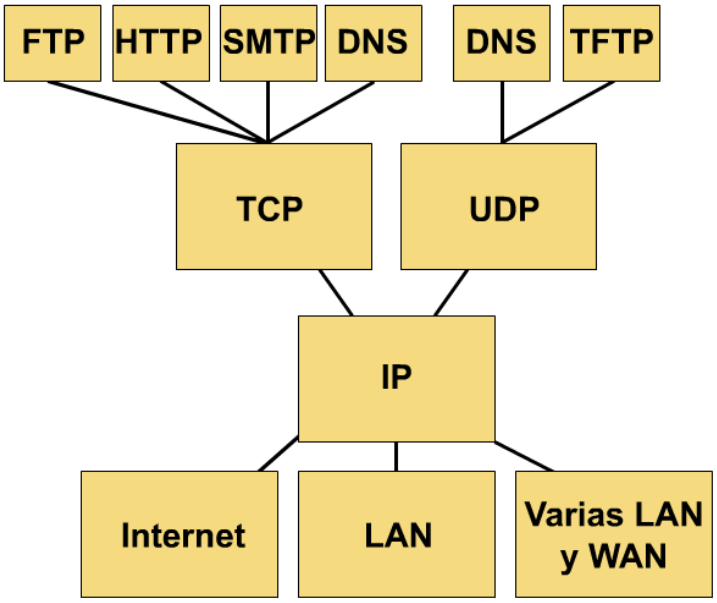


Figura 1.8 Grafico de protocolo TCP/IP[10]

El diagrama que aparece en la figura 1.8 ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP. En la capa de aplicación, aparecen distintas tareas de red, que probablemente cualquier usuario de la Internet utilice a diario. Estas aplicaciones incluyen las siguientes:

- *FTP*: File Transfer Protocol (Protocolo de transferencia de archivos)
- *HTTP*: Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)
- *SMTP*: Simple Mail Transfer Protocol (Protocolo de transferencia de correo simple)
- *DNS*: Domain Name System (Sistema de nombres de dominio)

[10] Ibídem.

- *TFTP*: Trivial File Transfer Protocol (Protocolo de transferencia de archivo trivial)

El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los creadores de software. La capa de transporte involucra dos protocolos: el protocolo de control de transmisión (TCP) y el protocolo de datagrama de usuario (UDP). La capa inferior, la capa de acceso de red, se relaciona con la tecnología específica de LAN o WAN que se utiliza.

En el modelo TCP/IP existe solamente un protocolo de red: el protocolo Internet, o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

1.3.3. COMPARACIÓN ENTRE TCP/IP Y OSI

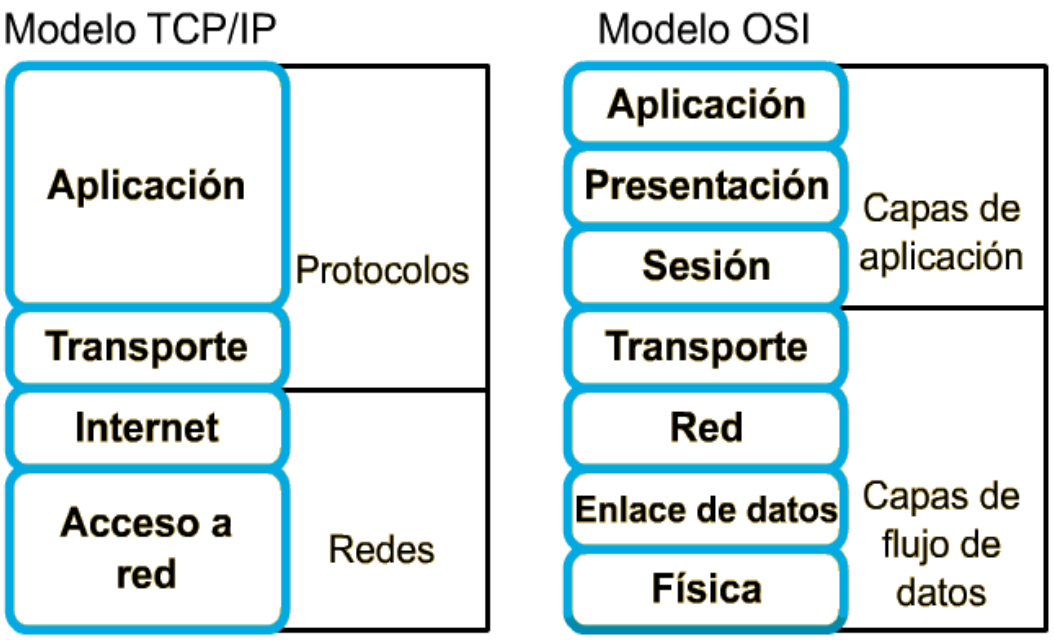


Figura 1.9 Modelo TCP/IP y OSI

En la figura 1.9 se compara el modelo OSI con el modelo TCP/IP y se observa que ambos presentan similitudes y diferencias las cuales se enlistan a continuación:

Similitudes

- Ambos se dividen en capas
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos
- Ambos tienen capas de transporte y de red similares
- Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito)

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación

- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Mucha gente dedicada al área de redes, tienen distintas opiniones con respecto al modelo que se debe usar, lo cierto es que se deben conocer ambos modelos para entender los distintos procesos que se llevan a cabo cuando se realiza cualquier comunicación entre dos computadoras.

1.4. FUNCIONES DE LA CAPA DE RED

La capa de red define cómo se efectúa el transporte de tráfico entre dispositivos que no están conectados localmente en el mismo dominio de difusión. Para conseguir esto se necesitan dos elementos de información:

- Una dirección lógica asociada a cada puesto de origen y de destino.
- Una ruta a través de la red para alcanzar el destino deseado.

La figura 1.10 muestra la ubicación de la capa de red en relación con la capa de enlace de datos. La capa de red es independiente de la capa de enlace de datos y, por tanto, puede ser utilizada para conectividad, usando la estructura lógica de direccionamiento.

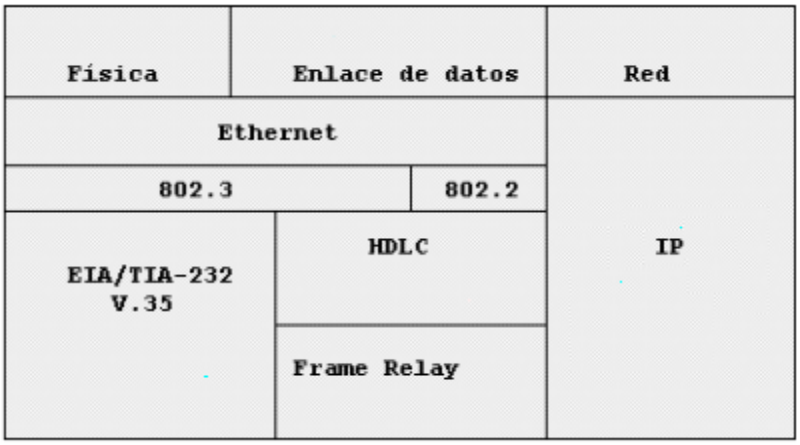


Figura 1.10 Ubicación de la capa de red

Los esquemas de direccionamiento lógico se utilizan para identificar redes en una interconexión de redes y la ubicación de los dispositivos dentro del contexto de dichas redes. Estos esquemas varían en función del protocolo de capa de red que se utilice. En esta sección se describe cómo opera la capa de red para las pilas de los protocolos TCP/IP.

Las direcciones de la capa de red denominadas direcciones lógicas se sitúan en la capa 3 del modelo de referencia OSI. A diferencia de las direcciones de la capa

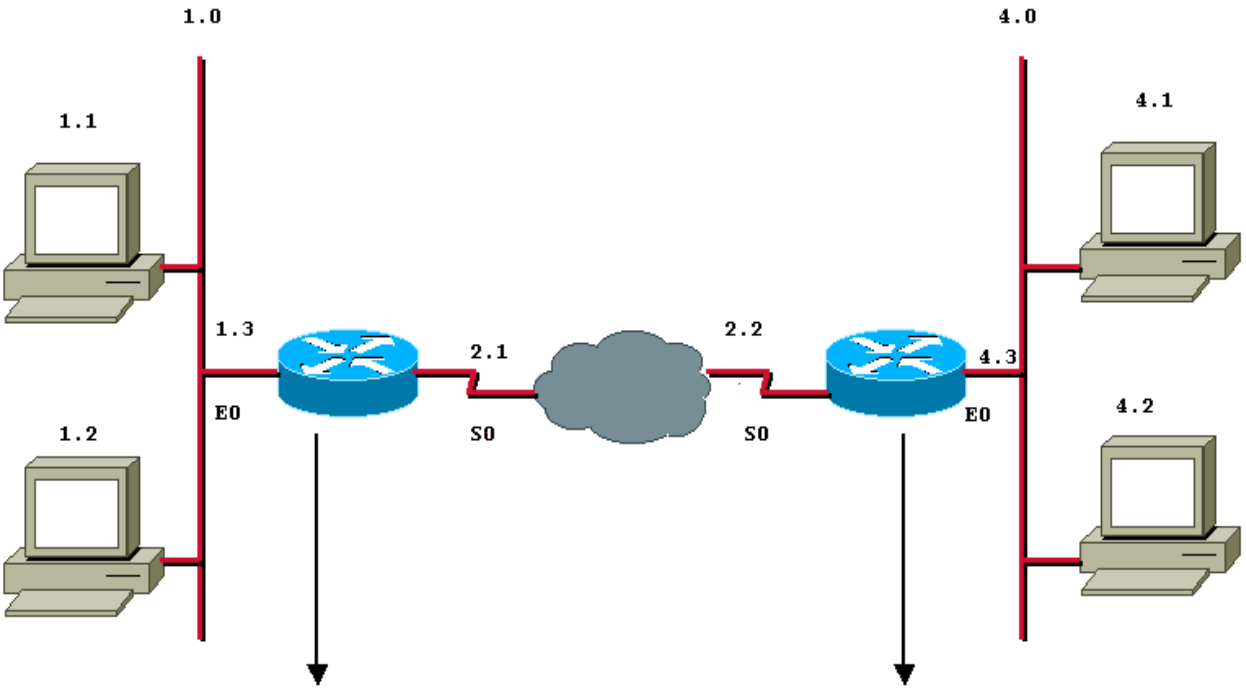
de enlace de datos, que suelen residir en un espacio de direcciones plano, las direcciones de la capa de red poseen habitualmente una estructura jerárquica en la cual se definen primero las redes y después los dispositivos o nodos de cada red. En otras palabras, las direcciones de la capa de red son como direcciones postales, que describen el lugar de residencia de un individuo por medio de un código postal y una dirección (calle). El código postal define la ciudad, provincia o estado, mientras que la dirección representa una ubicación específica dentro de esa ciudad. Esto contrasta con las direcciones de la capa MAC, de naturaleza plana. Un buen ejemplo de dirección plana podría ser el sistema de numeración de la seguridad social o del Documento nacional de identidad, donde cada persona posee un número único que lo identifica.

Los routers operan en la capa de red registrando y grabando las diferentes redes y eligiendo la mejor ruta para las mismas. Los routers colocan esta información en una tabla de enrutamiento, que incluye los siguientes elementos (véase figura 1.11):

- **Dirección de red**. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.

- **Interfaz**. Se refiere a la interfaz usada por el router para llegar a una red dada. Esta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.

- **Métrica**. Se refiere al coste o distancia para llegar a la red de destino. Se trata de un valor que facilita el router la elección de la mejor ruta para alcanzar una red dada. Esta métrica cambia en función de la forma en que el router elige las rutas. Entre las métricas más habituales figuran el número de redes que han de ser cruzadas para llegar al destino(conocido también como **saltos**), el tiempo que se tarda en atravesar todas las interfaces hasta una red dada(conocido también como **retraso**), o un valor asociado con la velocidad de un enlace(conocido también como **ancho de banda**).



T. Enrutamiento		
RED	INT	Métrica
1	E0	0
2	S0	0
4	S0	1

T. Enrutamiento		
RED	INT	Métrica
1	S0	1
2	S0	0
4	E0	0

Figura 1.11 Tablas de enrutamiento

Debido a que los routers funcionan en la capa de red del modelo OSI, se utilizan para separar segmentos en dominios de colisión y de difusión únicos. Cada segmento se conoce como una red y debe estar identificado por una dirección de red para que pueda ser alcanzado por un puesto final. Además de identificar cada segmento como una red, cada puesto de la red debe ser identificado también de forma unívoca mediante direcciones lógicas. Esta estructura de direccionamiento permite una configuración jerárquica de la red, ya que está definida por la red en la que se encuentra, así como por un identificador de host.

1.5. DIRECCIONAMIENTO IP

En Internet se utilizan diversos protocolos, que son parte de una serie de protocolos denominados TCP/IP. TCP/IP se basa en la identificación de cada equipo con una dirección denominada dirección IP, que posibilita la transmisión de datos a la dirección correcta.

Para que los routers puedan operar en una red, es necesario que cada tarjeta de interfaz de red (NIC), que es la parte del equipo que permite la conexión a una red a través de líneas especialmente proporcionadas para el envío de información digital, esté configurada en la red única que ésta representa. El router debe tener también una dirección de host en esa red. El router utiliza la información de configuración de la tarjeta para determinar la parte de la dirección correspondiente a la red, a fin de construir una tabla de enrutamiento.

Una dirección IP es un identificador numérico asignado a cada máquina en una red IP y se dice que es una dirección de software, lo que significa que es configurable. El direccionamiento IP fue diseñado para permitir que un host en una red pueda comunicarse con otro host en una red diferente, sin importar el tipo de LAN en la que se encuentren. Una dirección IP es una secuencia compuesta por 32 bits que se dividen en 4 octetos o bytes y se puede escribir de las siguientes maneras:

- 172.16.30.57 → en decimal
- 10101100.00010000.00011110.00111001 → en binario

Tanto los números binarios como los decimales representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada y también evita que se produzca una gran cantidad de errores por transposición, que se producirían si sólo se utilizaran números binarios.

Estas direcciones se tratan con una estructura jerárquica. La ventaja de usar esta estructura es que se facilita manipular el gran número de direcciones que se pueden obtener con los 32 bits que las conforman, ya que son aproximadamente 32.4 billones de direcciones. Un ejemplo de esquema jerárquico es un número telefónico, la primera sección es el código de área y designa un área muy extensa, después se tiene un prefijo que limita una zona más específica llamada central local y por último se tiene el segmento que identifica al destino individual dentro del área local indicada. Las direcciones IP tienen casi la misma estructura de capas, en lugar de que los 32 bits sean tratados como un identificador único, como sucedería en un esquema de direccionamiento plano, una parte de la dirección es designada como la dirección de red y la otra parte puede ser designada como dirección de subred o de host. La dirección de red ayuda al router a identificar una ruta dentro de la nube de red. El router utiliza la dirección de red para identificar la red destino de un paquete dentro de la internetwork. La porción host le comunica al router hacia qué dispositivo específico deberá entregar el paquete.[11]

Como las direcciones IP están formadas por cuatro octetos separados por puntos, se pueden utilizar uno, dos o tres de estos octetos para identificar el número de red. De modo similar, se pueden utilizar hasta tres de estos octetos para identificar la parte de host de una dirección IP. Las dos partes que componen una dirección IP se establecen claramente a partir de la máscara de red o subred. El siguiente ejemplo muestra una típica dirección IP con su respectiva máscara, donde se aprecia la parte de red y la parte de host.

Dirección IP 172.16.1.3
Mascara 255.255.0.0

172	16	1	3
10101100	00010000	00000001	00000011
255	255	0	0
11111111	11111111	00000000	00000000
Porción de red		Porción de Host	

Tabla 1.2 Dirección IP

[11] Lammle Todd, Odom Sean y Wallace Kevin, *CCNP Routing Study Guide,* p.66.

1.5.1. CLASES DE DIRECCIONAMIENTO IP

Para adaptar redes grandes y pequeñas, el Centro de Información de Red (NIC), segregó la dirección IP de 32 bits en clases de la A a la E. Los primeros bits del primer octeto determinan la clase de una dirección; esto, a su vez, determina cuantos bits de red y bits de host se encuentran en la dirección[12].

Esto se ilustra en la siguiente tabla:

Clase de dirección IP	Bits mas significativos	Intervalo de dirección	Bits en la dirección de red	Cantidad de Redes	Cantidad de hosts por red
A	0	1.0.0.0 126.0.0.0	8	126	16777216
B	10	128.0.0.0 191.255.255.255	16	16384	65534
C	110	192.0.0.0 223.255.255.0	24	2097152	254
D	1110	224.0.0.0 239.255.255.254	28	No es aplicable	No es aplicable
E	1111	240.0.0.0 254.255.255.255	No es aplicable	No es aplicable	No es aplicable

Tabla 1.3 Clases de direccionamiento IP

La red 127.0.0.0 se reserva para las pruebas de loopback. Los routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red[13].

La clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

[12] Habraken Joseph, *Routers Cisco*, p536
[13] Lammle Todd, Odom Sean y Wallace Kevin, *CCNP Routing Study Guide,* p.68.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de Tareas de Ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. El rango del primer octeto para las direcciones Clase E es 240 a 255.

1.5.2. DIRECCIONES IP RESERVADAS

Ciertas direcciones IP son reservadas, ya que no pueden asignarse a dispositivos de la red (hosts). Estas direcciones reservadas incluyen:

Dirección de red: Utilizada para identificar la red en sí.

La dirección IP que tiene ceros binarios en todas las posiciones de bits de host queda reservada para la dirección de red. Tomando como ejemplo una red Clase A, 112.0.0.0 es la dirección IP de la red, conocida como el ID (identificador) de la red. Un router usa la dirección IP de red al enviar datos por Internet. Los números del host sólo tienen importancia cuando los datos se encuentran en una red de área local.

Dirección de broadcast: Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red.

Para enviar información a todos los dispositivos de la red, se necesita una dirección de broadcast. Un broadcast se produce cuando una fuente envía datos a todos los dispositivos de una red. Para asegurar que todos los demás dispositivos de una red procesen el broadcast, el transmisor debe utilizar una dirección IP destino que ellos puedan reconocer y procesar. Las direcciones IP de broadcast terminan con unos binarios en toda la parte de la dirección que corresponde al host. Como ejemplo, de la red, 176.10.0.0, los últimos 16 bits componen el campo del host o la parte de la dirección del host. El broadcast que se envía a todos los dispositivos de la red incluye una dirección destino de 176.10.255.255. Esto se produce porque 255 es el valor decimal de un octeto que contiene 11111111.

1.5.3. DIRECCIONES IP PÚBLICAS Y PRIVADAS

La estabilidad de la Internet depende de forma directa de la exclusividad de las direcciones de red utilizadas públicamente. En un principio, una organización conocida como el Centro de información de la red Internet (InterNIC) manejaba un procedimiento para asegurar que las direcciones fueran, de hecho, exclusivas. InterNIC ya no existe y la Agencia de asignación de números de Internet (lANA) la ha sucedido. lANA administra, cuidadosamente, la provisión restante de las direcciones IP para garantizar que no se genere una repetición de direcciones utilizadas de forma pública. La repetición suele causar inestabilidad en la Internet y compromete su capacidad para entregar datagramas a las redes.

Las direcciones IP públicas son exclusivas. Dos máquinas que se conectan a una red pública nunca pueden tener la misma dirección IP porque las direcciones IP públicas son globales y están estandarizadas. Todas las máquinas que se conectan a la Internet acuerdan adaptarse al sistema. Hay que obtener las direcciones IP públicas de un proveedor de servicios de Internet (ISP) o un registro, a un costo. Con el rápido crecimiento de Internet, las direcciones IP públicas comenzaron a escasear. Se desarrollaron nuevos esquemas de direccionamiento, tales como el enrutamiento entre dominios sin clase (CIDR) y el IPv6, para ayudar a resolver este problema.

Las direcciones IP privadas son otra solución al problema del inminente agotamiento de las direcciones IP públicas. Como ya se ha mencionado, las redes públicas requieren que los hosts tengan direcciones IP únicas. Sin embargo, las redes privadas que no están conectadas a la Internet pueden utilizar cualquier dirección de host, siempre que cada host dentro de la red privada sea exclusivo. Existen muchas redes privadas junto con las redes públicas. No obstante, no es recomendable que una red privada utilice una dirección cualquiera debido a que, con el tiempo, dicha red podría conectarse a Internet. El RFC 1918 asigna tres bloques de direcciones IP para uso interno y privado. Estos tres bloques consisten en un rango de Clase A, un rango de direcciones de Clase B y un rango de direcciones de Clase C. Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los routers de Internet descartan inmediatamente las

direcciones privadas. Si se produce un direccionamiento hacia una intranet que no es pública, como por ejemplo un laboratorio de prueba o una red domestica, es posible utilizar direcciones privadas en lugar de direcciones exclusivas a nivel global.

Clase	Intervalo de dirección
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Tabla 1.4 Direcciones privadas

La conexión de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se conoce como Traducción de Direcciones de Red (NAT - Network Address Translation). En general, un router es el dispositivo que realiza NAT.

1.5.4. COMPARACIÓN ENTRE EL DIRECCIONAMIENTO IPv4 E IPv6

Cuando se adoptó TCP/IP en los años 80, la Versión 4 del IP (IPv4) ofrecía una estrategia de direccionamiento que, aunque resultó escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones. A mediados de los años 90 se comenzaron a detectar las siguientes dificultades sobre IPv4:

- Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de Clase B estaba a punto de agotarse.
- Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4.Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits como VLSM y CIDR[14].

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la Versión 6 del IP (IPv6). IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 340 sextillones de direcciones[15]. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación.

Las direcciones IPv6 miden 128 bits y son identificadores de interfaces - individuales y conjuntos de interfaces. Las direcciones IPv6 se asignan a interfaces no a nodos. Como cada interfaz pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.Las direcciones IPv6 se escriben en hexadecimal separados por dos puntos. Los campos IPv6 tienen una longitud de 16 bits.

Dirección IPv6:

24AE:0002:F2F3:B542:0001:5687:A2FF:6184

Para que las direcciones sean mas fáciles de leer, es posible omitir los ceros iniciales de cada campo. El campo :0002: se escribe :2: el campo :0001: se escribe :1:

24AE:2:F2F3:B542:1:5687:A2FF:6184

[14] Ariganello Ernesto, *Técnicas de configuración de routers Cisco*, p.178.
[15] Beijnum Iljitsch van, *Running IPv6,* p.2.

También se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000"). Por ejemplo:

2001:0DB8:85A3:0000:1319:8A2E:0370:7344

2001:0DB8:85A3::1319:8A2E:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

2001:0DB8:0000:0000:0000:0000:1428:57AB

2001:0DB8:0000:0000:0000::1428:57AB

2001:0DB8:0:0:0:0:1428:57 AB

2001:0DB8:0::0:1428:57AB

2001:0DB8::1428:57AB

son todas válidas y significan lo mismo, pero

2001::25DE::CADE

no es válida porque no queda claro cuántos grupos nulos hay en cada lado[16].

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

::	**La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.**
::1	La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.
fe80::	El prefijo de *enlace local* (en inglés *link local*) específica que la dirección sólo es válida en el enlace físico local.
ff00::	El prefijo de multicast. Se usa para las direcciones multicast.

[16] Ibídem, pp. 13-15.

Hay que resaltar que no existen las direcciones de difusión (en inglés broadcast) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast **FF01::1**, denominada todos los nodos (en inglés all nodes).

1.5.5. MÁSCARAS DE SUBRED

En la RFC 950 se propone un procedimiento, llamado enmáscaramiento de subred, para dividir las direcciones de Clase A, B y C en partes más pequeñas, incrementando así el número de redes posibles. Una máscara de subred es un valor de 32 bits que identifica qué bits de una dirección representan los bits de red y cuáles representan los bits de host.

En otras palabras, el router no determina la parte de red de la dirección examinando el valor del primer octeto; examina la máscara de subred asociada a la dirección. De esta forma, las máscaras de subred permiten ampliar el uso de una dirección IP. Ésta es una forma de hacer de una dirección IP una jerarquía de tres niveles, corno se ve en la Figura 1.12.

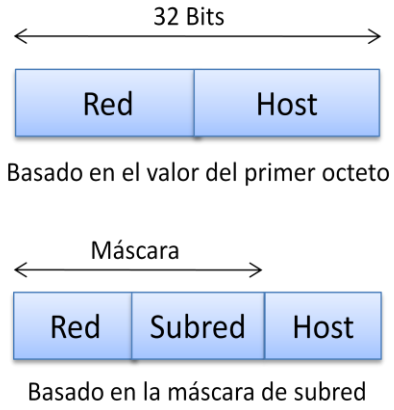


Figura 1.12 Una máscara de subred determina como se interpreta una dirección IP.

Para crear una máscara de subred en una dirección, utilice un 1 en cada bit que quiera representar una parte de red o subred de la dirección, y utilice un 0 en cada bit que quiera representar la parte de nodo de la dirección. Observe que los unos de la máscara son contiguos. Las máscaras de subred predeterminadas de las Clases A, B y C se muestran en la siguiente tabla

Clase	Máscara predeterminada en binario	Máscara predeterminada en decimal
Clase A	11111111.00000000.00000000.00000000	255.0.0.0
Clase B	11111111.11111111.00000000.00000000	255.255.0.0
Clase C	11111111.11111111.11111111.00000000	255.255.255.0

Tabla 1.5 Máscaras de subred predeterminadas

Dado que las máscaras de subred amplían el número de direcciones de red empleando bits de la parte de *host,* no conviene decidir al azar el número adicional de bits que se van a usar en la parte de red. En su lugar, conviene investigar un poco antes de determinar cuántas direcciones de red se necesitan derivar de la dirección IP disponible. Por ejemplo, si se tiene la dirección IP 172.16.0.0 y que se quiere configurar la red de la figura 1.13[17].

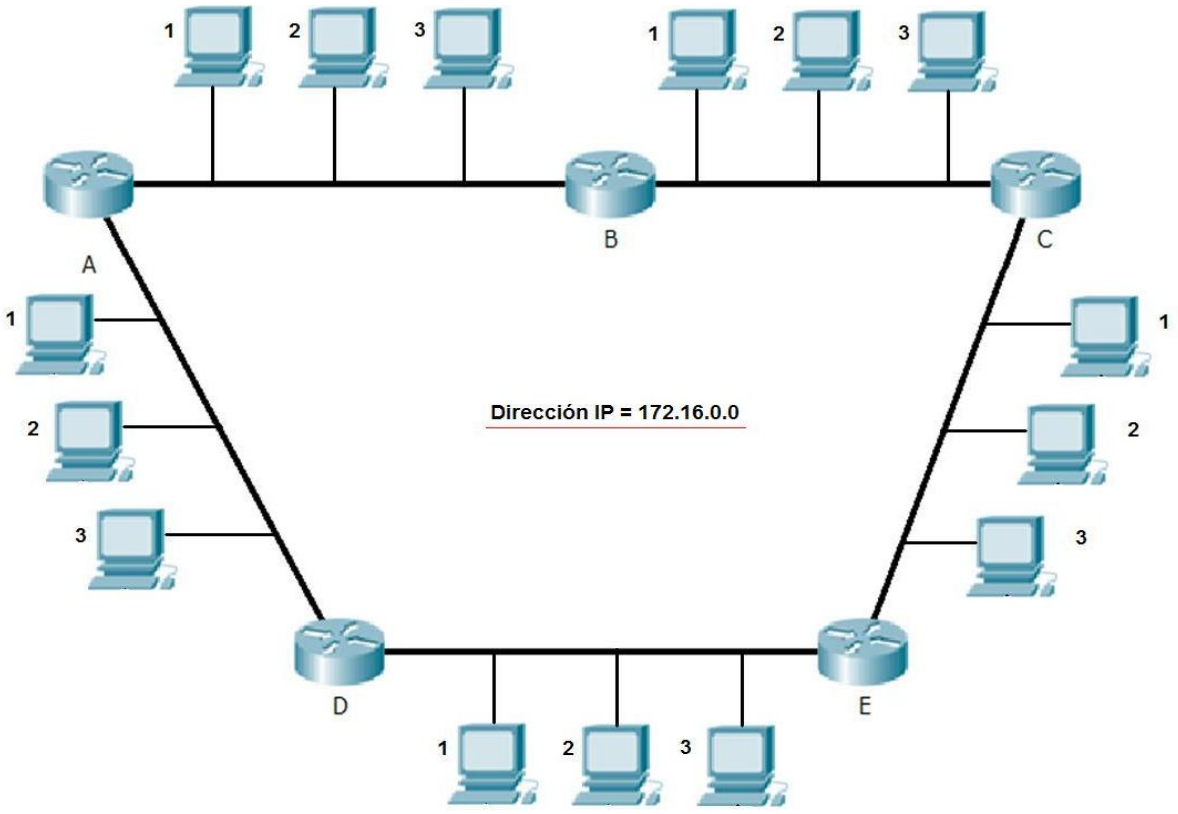


Figura 1.13 Red utilizada en el ejemplo de máscara de subred

Para establecer la máscara de subred, se hace lo siguiente:

[17] Habraken Joseph, *Routers Cisco*, pp.538-540

1. Determinar el número de subredes necesarias. En la figura 1.9 hay 5 redes
2. Determinar el número de nodos por subred que hay que definir. En el ejemplo hay cinco nodos por cada subred, dos routers y tres estaciones de trabajo.
3. Determinar los futuros requisitos de la red. En el ejemplo supondremos un crecimiento del cien por cien.
4. Con base en la información reunida, se determina el numero total de subredes requerido para seleccionar la máscara de subred apropiada; en este ejemplo se requieren 10 subredes.

La siguiente tabla es aplicable a todos los tipos de redes adecuándola al octeto correspondiente:

Bits prestados	Cantidad de Subredes	Mascara de Subred en binario	Mascara de Subred en decimal
1	2	10000000	128
2	4	11000000	192
3	8	11100000	224
4	16	11110000	240
5	32	11111000	248
6	64	11111100	252
7	128	11111110	254
8	256	11111111	256

Tabla 1.6 Cantidad de subredes por bits prestados

Como ninguna máscara adapta exactamente 10 subredes, ya que si se utilizan 3 bits de subred se tendrán 2^3 = 8 subredes, entonces se deben utilizar 4 bits de red y se tendrán 2^4 = 16 subredes, por lo tanto la máscara de subred será:

- 255.255.240.0 → en decimal
- 11111111.11111111.11110000.00000000 → en binario

Otra forma de identificar el número de bits de una dirección que representa las partes de red, de subred y de host, consiste en utilizar un prefijo el cual es una

barra inclinada (***/***) y un valor numérico que es la suma de los bits que representan la red y la parte de subred de una dirección. Si la máscara de subred es 255.255.240.0 el prefijo seria ***/***20.

Una vez que se identificó la máscara de subred, se deben calcular las direcciones de las subredes, para lo cual se hace lo siguiente:

1. Se escribe la dirección con subredes en formato binario e identificamos los bits prestados para crear las subredes, como se muestra a continuación.

Dirección asignada 172.16.0.0/16
En binario 10101100.00010000.00000000.00000000
Dirección con subredes 172.16.0.0/20
En binario 10101100.00010000.XXXX0000.00000000

2. Enfocándose en los bits de subred y para calcular la dirección de subred, todos los bits de host se establecen a cero. Para volverlo a convertir a notación decimal, es importante recalcar que siempre debe convertir un octeto completo, es decir, 8 bits. En la primera subred, los bits de subred son 0000, mientras que el resto del octeto (todos los bits de host) es 0000; el primer número de subred seria 00000000, o el decimal 0. El segundo número más bajo de la subred, sería 0001 y al combinarse con los bits de host resultaría el binario 00010000, o un decimal 16, al realizar esto consecutivamente se obtiene lo siguiente.

No. De Subred	Dirección IP en binario (Red / Subred / Host)	Dirección IP en decimal
0	10101100.00010000.**0000**0000.00000000	172.16.0.0
1	10101100.00010000.**0001**0000.00000000	172.16.16.0
2	10101100.00010000.**0010**0000.00000000	172.16.32.0
3	10101100.00010000.**0011**0000.00000000	172.16.48.0
4	10101100.00010000.**0100**0000.00000000	172.16.64.0
5	10101100.00010000.**0101**0000.00000000	172.16.80.0
6	10101100.00010000.**0110**0000.00000000	172.16.96.0
7	10101100.00010000.**0111**0000.00000000	172.16.112.0
8	10101100.00010000.**1000**0000.00000000	172.16.128.0
9	10101100.00010000.**1001**0000.00000000	172.16.144.0
10	10101100.00010000.**1010**0000.00000000	172.16.160.0
11	10101100.00010000.**1011**0000.00000000	172.16.176.0
12	10101100.00010000.**1100**0000.00000000	172.16.192.0

No. De Subred	Dirección IP en binario Red Subred Host	Dirección IP en decimal
13	10101100.00010000.11010000.00000000	172.16.208.0
14	10101100.00010000.11100000.00000000	172.16.224.0
15	10101100.00010000.11110000.00000000	172.16.240.0

Tabla 1.7 Direcciones de subredes

Es importante tener claro que, al realizar una división en subredes, todas las subredes que se obtengan a partir de esa división van a tener la misma máscara de subred. Por otro lado, la primera dirección de cada red y/o subred está reservada (identificador de la red/subred); además, la ultima dirección de cada red/subred también está reservada (broadcast).

Otras reglas aplicadas en la división en subredes:

- Para conocer la cantidad de hosts utilizables debemos elevar al cuadrado la cantidad de bits que restan para hosts y restarle 2. En el ejemplo anterior se tendrían $2^{12} - 2 = 4094$ host disponibles por subred.
- El número mínimo de bits que deben quedar para hosts es 2.

La máscara de subred es utilizada por un router para determinar la dirección de la red o subred a la cual pertenece una dirección de host. Esto se realiza efectuando la operación AND entre los bits de la dirección IP de host y la máscara de subred. Por ejemplo si se tiene la dirección IP de un host que es 145.50.119.223 y la máscara de subred es 255.255.248.0; para determinar la dirección de la subred a la que pertenece el host:

Host	10010001.00110010.01110111.11011111	AND
Máscara	11111111.11111111.11111000.00000000	
Red	10010001.00110010.01110000.00000000	→145.50.112.0

1.5.6. MÁSCARAS DE SUBRED DE LONGITUD VARIABLE (VLSM)

El crecimiento exponencial de las redes ha hecho que el direccionamiento IPv4 no permita un desarrollo y una escalabilidad acorde a lo deseado por los administradores de red. IPv4 pronto será reemplazado por IP versión 6 (IPv6) como protocolo dominante de Internet. IPv6 posee un espacio de direccionamiento prácticamente ilimitado y algunos administradores ya han empezado a implementarlo en sus redes.

Para dar soporte al direccionamiento IPv4 se ha creado VLSM (máscara de subred de longitud variable) que permite incluir más de una máscara de subred dentro de la misma dirección de red y con frecuencia se le conoce como división de subredes en subredes (véase figura 1.14). VLSM es soportado únicamente por protocolos sin clase tales como OSPF, RIPv2 y EIGRP[18].

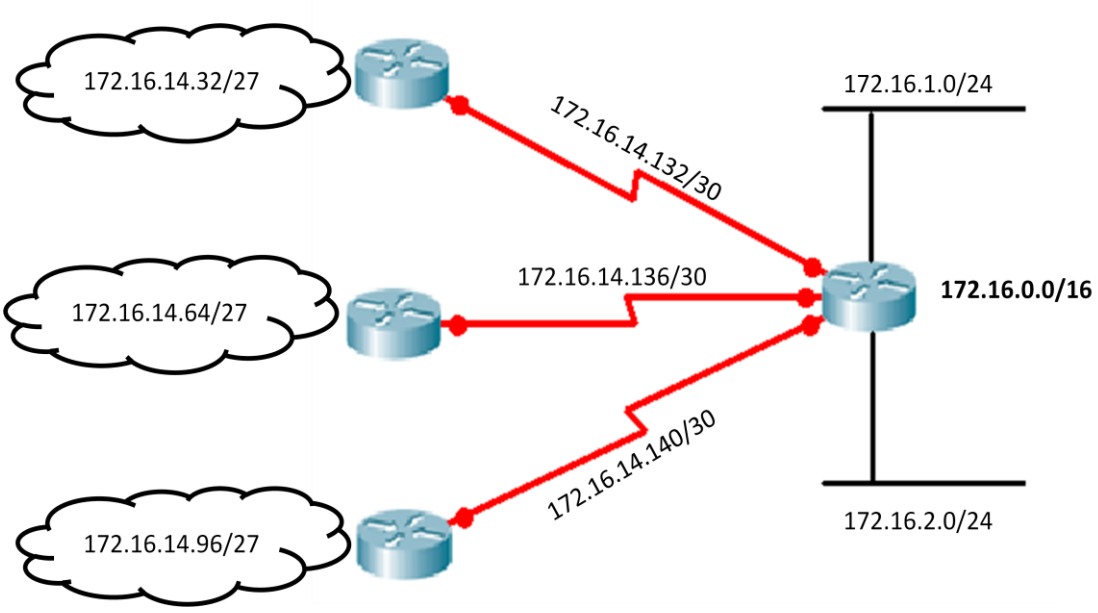


Figura 1.14. La subred 172.16.14.0/24 se divide en subredes más pequeñas

El uso de las máscaras de subred de longitud variable permite el uso más eficaz del direccionamiento IP. Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos hosts, y una máscara corta en las subredes

[18] Ariganello Ernesto, *Técnicas de configuración de routers Cisco*, p.179.

con muchos hosts. Al permitir niveles de jerarquía se pueden resumir diferentes direcciones en una sola, evitando gran cantidad de actualizaciones de ruta.

VLSM se desarrolló por la crisis de direccionamiento (el inminente agotamiento de direcciones de red Clase B) y por el rápido aumento de las tablas de enrutamiento de los routers de la Internet.

En el pasado, se suponía que la primera y la última subred no debían utilizarse. El uso de la primera subred, conocida como la subred cero, no se recomendaba debido a la confusión que podría producirse si una red y una subred tuvieran la misma dirección. Este concepto también se aplicaba al uso de la última subred, conocida como la subred de unos. Con la evolución de las tecnologías de red y el agotamiento de las direcciones IP, el uso de la primera y la última subred se ha convertido en una práctica aceptable si se utilizan junto con VLSM.

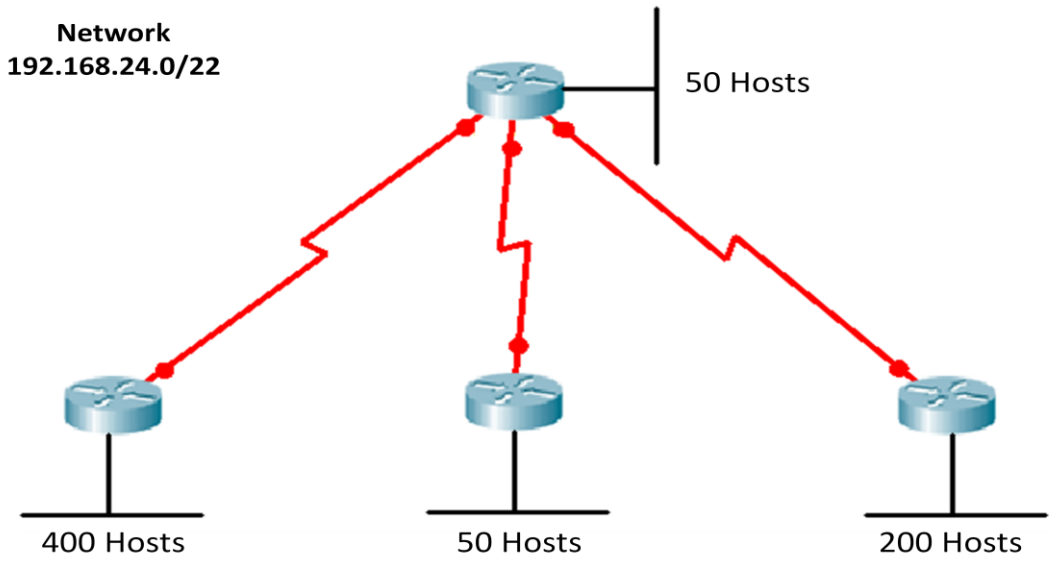


Figura 1.15. Los segmentos LAN usualmente poseen diferentes cantidades de host

El ejemplo de la figura 1.15 muestra una red que necesita un esquema de direccionamiento. El ejemplo incluye cuatro LAN que requieren diferentes cantidades de hosts cada una. Los enlaces WAN sólo necesitan dos direcciones, una para cada router.

Utilizando VLSM, se puede aplicar una máscara de 23 bits en el segmento LAN de 400 hosts, una máscara de 24 bits en el de 200 hosts, una máscara de 26 bits en los de 50 hosts y una máscara de 30 bits para los enlaces WAN, dado que sólo se necesitan dos direcciones de host. Es importante señalar que se pueden seguir subdividiendo las subredes no utilizadas.

Aplicando VLSM, las direcciones IP, con sus respectivas máscaras, quedarían como se muestra en la siguiente figura:

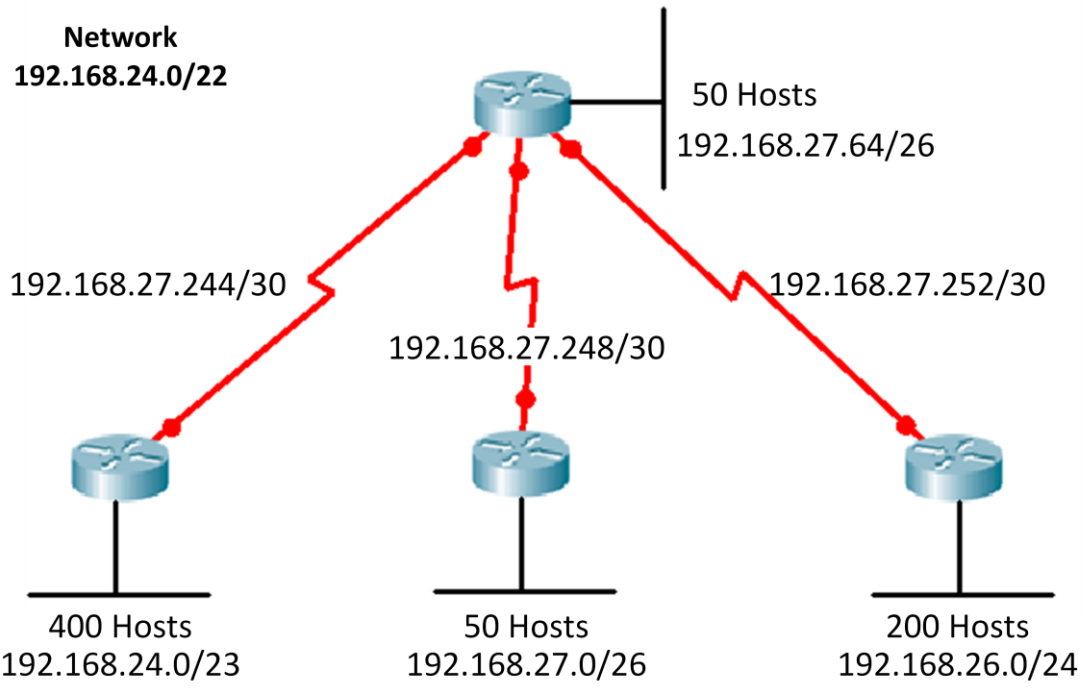


Figura 1.16. Asignación de direcciones IP utilizando mascaras de subred de longitud variable (VLSM).

1.5.7. RESUMEN DE RUTA CON VLSM

El uso de enrutamiento entre dominios sin clase (CIDR) y VLSM evita el desperdicio de direcciones y reduce la cantidad de rutas que un router debe mantener en sus tablas anunciando y manteniendo una sola dirección que contenga a las demás. Sin el resumen de rutas o supernetting, es probable que el enrutamiento por el backbone de Internet se hubiese desplomado antes de 1997.

Cuando se utiliza VLSM, es importante mantener la cantidad de subredes agrupadas en la red para permitir la unificación. Por ejemplo, redes como 172.16.14.0/24 y 172.16.15.0/24 deberían estar cerca de manera que los routers sólo tengan que poseer una ruta para 172.16.14.0/23.

La figura 1.17 muestra cómo el resumen de rutas reduce la carga de los routers corriente arriba. Esta compleja jerarquía de redes y subredes de varios tamaños se resume en diferentes puntos con una dirección prefijo, hasta que la red completa se publica como sola ruta unificada de 200.199.48.0/22.

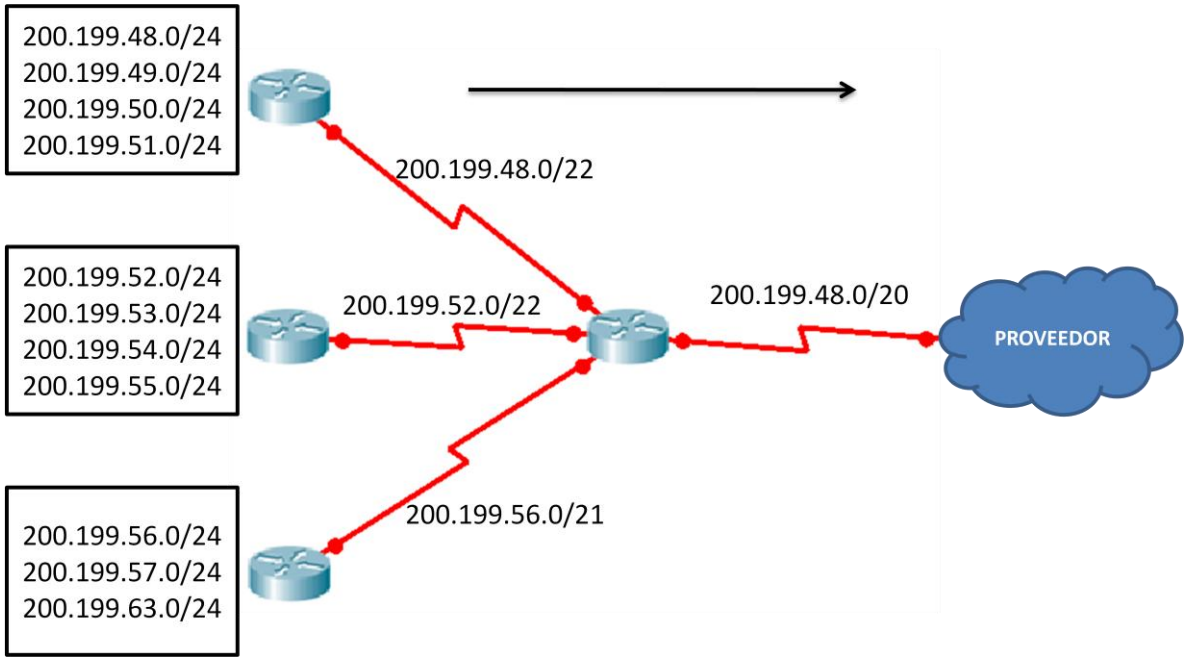


Figura 1.17. Resumen de rutas

DIRECCIÓN	PRIMER OCTETO	SEGUNDO OCTETO	TERCER OCTETO	CUARTO OCTETO
200.199.48.0/24	11001000	11000111	0011 0000	00000000
200.199.49.0/24	11001000	11000111	0011 0001	00000000
200.199.50.0/24	11001000	11000111	0011 0010	00000000
200.199.51.0/24	11001000	11000111	0011 0011	00000000
200.199.52.0/24	11001000	11000111	0011 0100	00000000
200.199.53.0/24	11001000	11000111	0011 0101	00000000
200.199.54.0/24	11001000	11000111	0011 0110	00000000
200.199.55.0/24	11001000	11000111	0011 0111	00000000
200.199.56.0/24	11001000	11000111	0011 1000	00000000
200.199.57.0/24	11001000	11000111	0011 1001	00000000
200.199.63.0/24	11001000	11000111	0011 1111	00000000
	Bits comunes=20 Resumen 200.199.48.0/20			Bits no comunes o de Host

Tabla 1.8 Dirección de resumen

El resumen de ruta o la superred, sólo es posible si los routers de una red utilizan un protocolo de enrutamiento sin clase, como por ejemplo OSPF o EIGRP. En la figura 1.17, el resumen de rutas que finalmente llega al proveedor contiene un prefijo de 20 bits común a todas las direcciones de la organización. Para que el resumen funcione, las direcciones se deben asignar cuidadosamente de manera jerárquica para que las direcciones resumidas compartan la misma cantidad de bits de mayor peso.

Es importante recordar lo siguiente:

- Un router debe conocer con detalle los números de las subredes conectadas a él.
- No es necesario que un router informe a los demás routers de cada subred si el router puede enviar una ruta unificada que represente un conjunto de routers.
- Un router que usa rutas unificadas tiene menos entradas en su tabla de enrutamiento.
- VLSM aumenta la flexibilidad del resumen de ruta porque utiliza los bits de mayor peso compartidos a la izquierda, aun cuando las redes no sean contiguas.

1.5.8. MÁSCARA WILDCARD

Las listas de acceso y algunos protocolos de enrutamiento hacen uso del concepto conocido como máscara comodín o wildcard. Aunque parece similar a la máscara de red, la máscara wildcard parece la inversa de la máscara de red. Las posiciones de bit establecidas a 1 en la máscara wildcard que coinciden con el bit correspondiente de la máscara de red serán ignorados, mientras que los que posean el valor 0 serán tomados en cuenta por el router. Una máscara wildcard de 0.0.0.255 coincide con cualquier dirección número en el rango 0 a 255 que aparezca en el cuarto octeto de una dirección IP. Una máscara wildcard de 0.0.3.255 coincide con cualquier dirección IP que tenga un 0, 1 ó 3 en el tercer octeto y cualquier número en

el cuarto octeto. Las máscaras wildcard permiten que el administrador de red especifique, por ejemplo, rangos de direcciones[19].

Por ejemplo la subred 172.16.32.0/19 posee una máscara que identifica a los primeros 19 bits como pertenecientes a la red y los últimos 13 al rango de host, por lo tanto estos deberán ser ignorados por el router poniendo los bits en 1 en la máscara wildcard.

DIRECCIÓN IP	172	16	32	0
EN BINARIO	10101100	00010000	00100000	00000000
MASCARA DE RED	11111111	11111111	111**00000**	**00000000**
WILDCARD	00000000	00000000	000**11111**	**11111111**
RESULTADO	Se toman en cuenta 8 bits	Se toman en cuenta 8 bits	Se toman en cuenta 3 bits se ignoran 5	Ignorados

Tabla 1.9 Máscara *wildcard*

[19] Ibídem p.183

1.6.WAN Y ROUTERS

Una WAN (red de área amplia) opera en la capa física y la capa de enlace de datos del modelo de referencia OSI (véase figuras 1.18 y 1.19). Esto no significa que las otras 5 capas del modelo OSI no se encuentren en una WAN; simplemente significa que las características que distinguen una red WAN de una LAN, en general, se encuentran en la capa física y en la capa de enlace de datos. Una WAN interconecta las LAN (redes de área local) que normalmente se encuentran separadas por grandes áreas geográficas. Las WAN llevan a cabo el intercambio de paquetes y tramas de datos entre routers y puentes y las LAN que soportan.

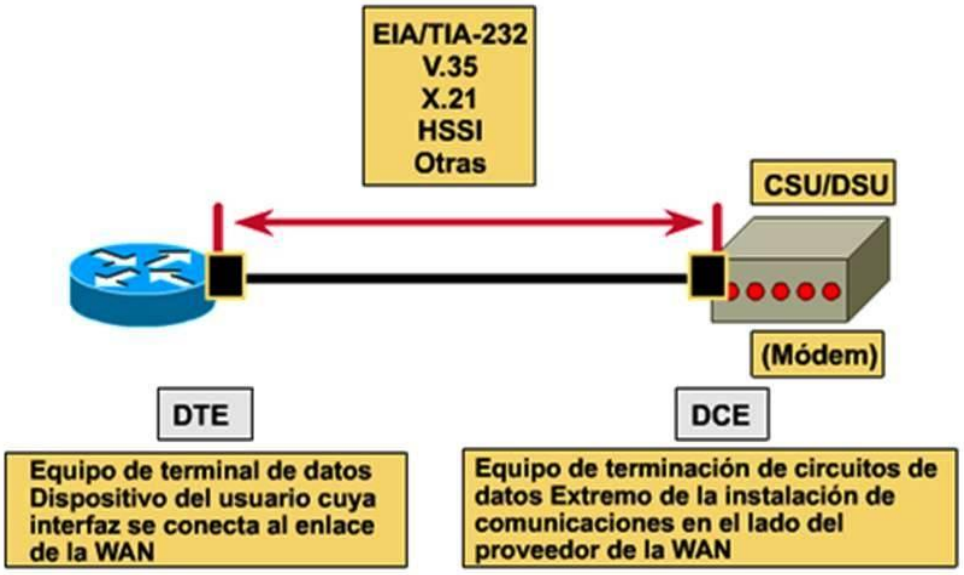
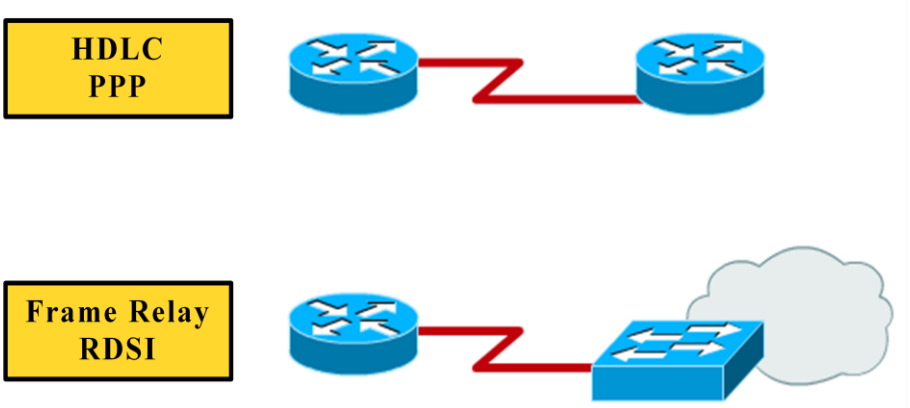


Figura 1.18. Capa física WAN

Las características principales de las WAN son las siguientes:

- Operan dentro de un área geográfica mayor que el área en la que operan las redes LAN locales y utilizan los servicios de proveedores de servicios de telecomunicaciones.
- Usan conexiones seriales de diversos tipos para acceder al ancho de banda dentro de áreas geográficas extensas.
- Por definición, las WAN conectan dispositivos separados por áreas geográficas extensas. Entre estos dispositivos se incluyen:

- Routers: ofrecen varios servicios, entre ellos internetworking y puertos de interfaz WAN
- Switches: utilizan al ancho de banda de las WAN para la comunicación de voz, datos y video
- Módems: servicios de interfaz con calidad de voz; unidades de servicio de canal y unidades de servicio de datos (CSU/DSU) que realizan interfaz con servicios T1/E1; y Adaptadores de Terminal y Terminación de red 1 (TA/NT1) que realizan interfaz con los servicios de la Red digital de servicios integrados (RDSI)
- Servidores de comunicaciones: concentran la comunicación de usuarios de servicios de acceso telefónico



HDLC: Control de enlace de datos de alto nivel.

PPP: Protocolo punto a punto.

Frame Relay: Forma simplificada de tecnología de conmutación de paquetes.

RDSI: Red digital de servicios integrados (señal de enlace de datos).

Figura 1.19. Protocolos de capa de enlace de datos WAN

Los routers, cuentan con interfaces LAN y WAN y aunque se utilizan para segmentar LANs, su función principal esta en las WAN. De hecho, las tecnologías WAN con frecuencia se usan para conectar routers (véase fig. 1.20). Se comunican entre sí mediante conexiones WAN y constituyen sistemas autónomos, y el backbone de Internet.

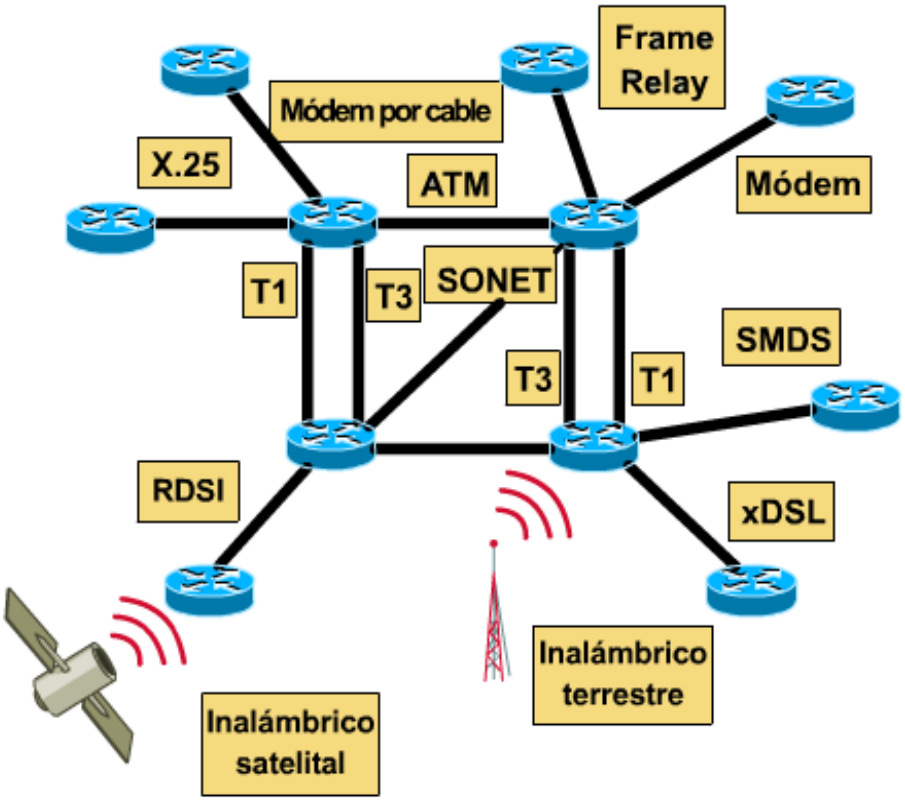


Figura 1.20. Routers conectados con tecnologías WAN[20].

Debido a que los routers son los dispositivos de backbone de las redes internas extensas y de Internet, operan en la Capa 3 del modelo OSI, tomando decisiones basadas en direcciones de red (en Internet, utilizando el Protocolo Internet, o IP).

Las dos funciones principales de los routers son la selección de mejores rutas para los paquetes de datos entrantes, y la conmutación de paquetes a la interfaz de salida correspondiente. Los routers hacen esto creando tablas de enrutamiento e intercambiando la información de red de estas tablas con otros routers. Se pueden configurar las tablas de enrutamiento, pero por lo general se mantienen de forma dinámica mediante un protocolo de enrutamiento que intercambia información de topología (ruta) de red con otros routers.

[20] *Cisco Certified Network Associate Curriculum, Semestre 1*, V2.1.2.

1.6.1. SISTEMAS AUTÓNOMOS

Un Sistema Autónomo (en inglés, *Autonomous System*: **AS**) es un conjunto de redes y dispositivos IP que se encuentran administrados por una sola entidad (o en algunas ocasiones varias) que cuentan con una política común de definición de trayectorias para Internet.

Los Sistemas Autónomos se comunican entre sí mediante routers BGP y se intercambian el tráfico de Internet que va de una red a la otra (véase fig. 1.21). A su vez cada Sistema Autónomo es como una Internet en pequeño, ya que su rol se llevara a cabo por una sola entidad, típicamente un Proveedor de Servicio de Internet (ISP) o una gran organización con conexiones independientes a múltiples redes, las cuales se apegaban a una sola y clara política de definición de trayectorias definida.

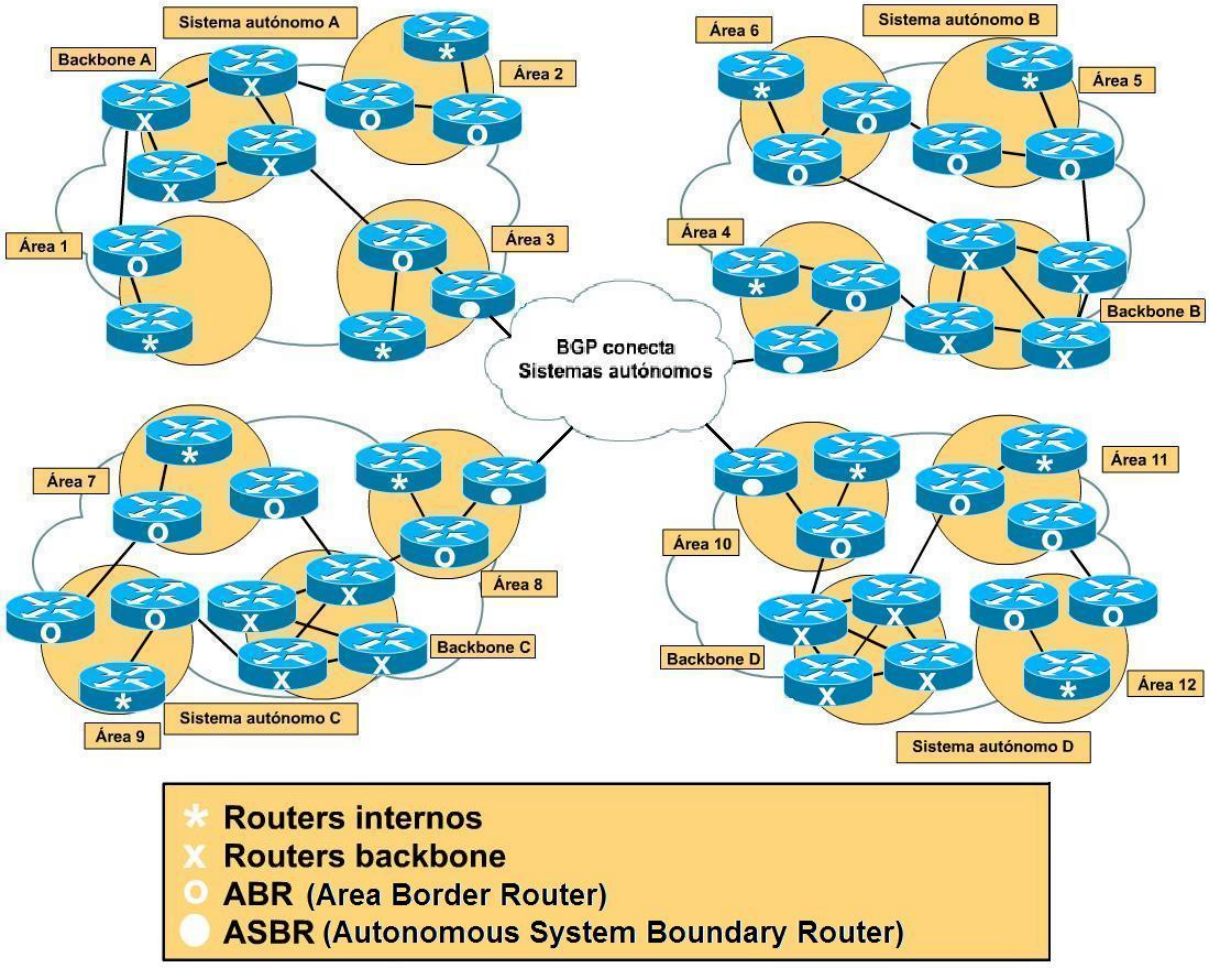


Figura 1.21. Routers en Sistemas Autónomos

Internet es una red de sistemas autónomos, cada uno de los cuales tiene routers que normalmente cumplen uno de cuatro roles.

- Routers internos: internos de un área
- Routers fronterizos: conectan dos o más áreas
- Routers backbone: rutas primarias para el tráfico que se origina o tiene como destino otras redes
- Routers fronterizos de un sistema autónomo (AS): se comunican con los routers en otros sistemas autónomos

El protocolo enrutado casi universalmente es IP. El protocolo de enrutamiento es el Protocolo de Gateway Fronterizo (BGP) usado ampliamente entre los routers de Internet.

1.7. INTRODUCCIÓN A LOS ROUTERS

Los routers tienen cuatro componentes básicos: una CPU, memoria, interfaces y un bus por lo tanto se puede considerar como una computadora. Sin embargo, se trata de una computadora de propósito específico. El router es una computadora que selecciona las mejores rutas y maneja la conmutación de paquetes entre dos redes diferentes. Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software denominado Sistema Operativo de Internetworking (IOS) para ejecutar archivos de configuración. Estos archivos de configuración controlan el flujo de tráfico a los routers.

Los componentes de la configuración interna de un router son los siguientes y se ilustran en la figura 1.22:

- RAM/DRAM: Almacena tablas de enrutamiento, caché ARP, caché de conmutación rápida, búfering de paquetes (RAM compartida) y colas de espera de paquetes. La RAM también proporciona memoria temporal y/o de ejecución para el archivo de configuración del router, mientras el router se enciende. El contenido de la RAM se pierde cuando se apaga o se reinicia el router.
- NVRAM: RAM no volátil. Almacena el archivo de configuración de inicio/copia de respaldo del archivo de configuración de un router. El contenido no se elimina cuando se apaga o se reinicia el router.
- Flash: ROM borrable y reprogramable. Contiene la imagen y microcódigo del sistema operativo. Permite actualizar el software sin eliminar y reemplazar chips en el procesador. El contenido se conserva cuando se apaga o reinicia el router. Se pueden almacenar múltiples versiones del software IOS en la memoria Flash
- ROM: Contiene diagnósticos de encendido, un programa bootstrap y software del sistema operativo. Las actualizaciones de software en ROM requieren el reemplazo de chips enchufables en el CPU
- Interfaz: Conexión de red a través de la cual los paquetes entran y salen de un router. Puede estar en un motherboard o en un módulo de interfaz separado

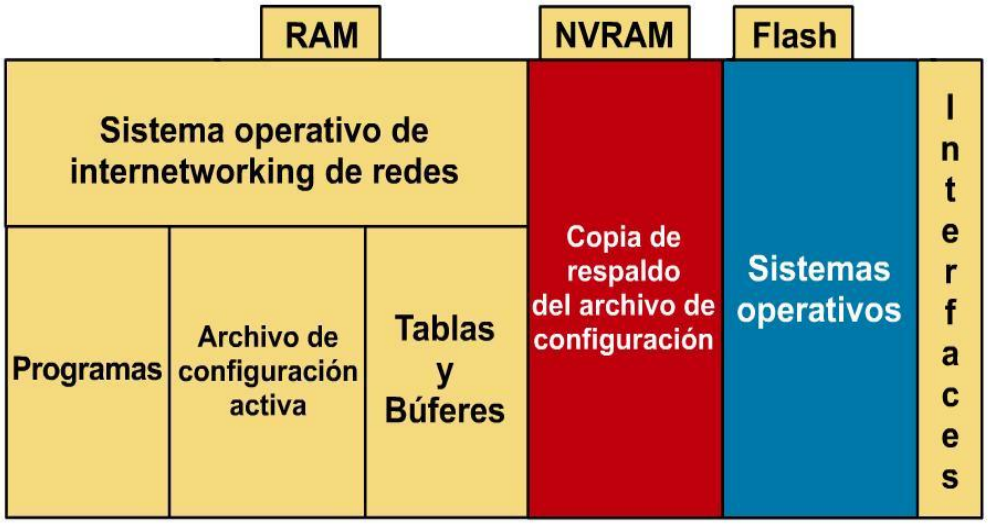


Figura 1.22. Componentes de configuración interna

Cuando se enciende un router Cisco, realiza una prueba automática de encendido (POST). Durante esta prueba automática, el router ejecuta diagnósticos desde la ROM para todos los módulos de hardware. Estos diagnósticos verifican la operación básica de la CPU, memoria y puertos de interfaz de red. Después de verificar las funciones de hardware, el router procede a inicializar el software.

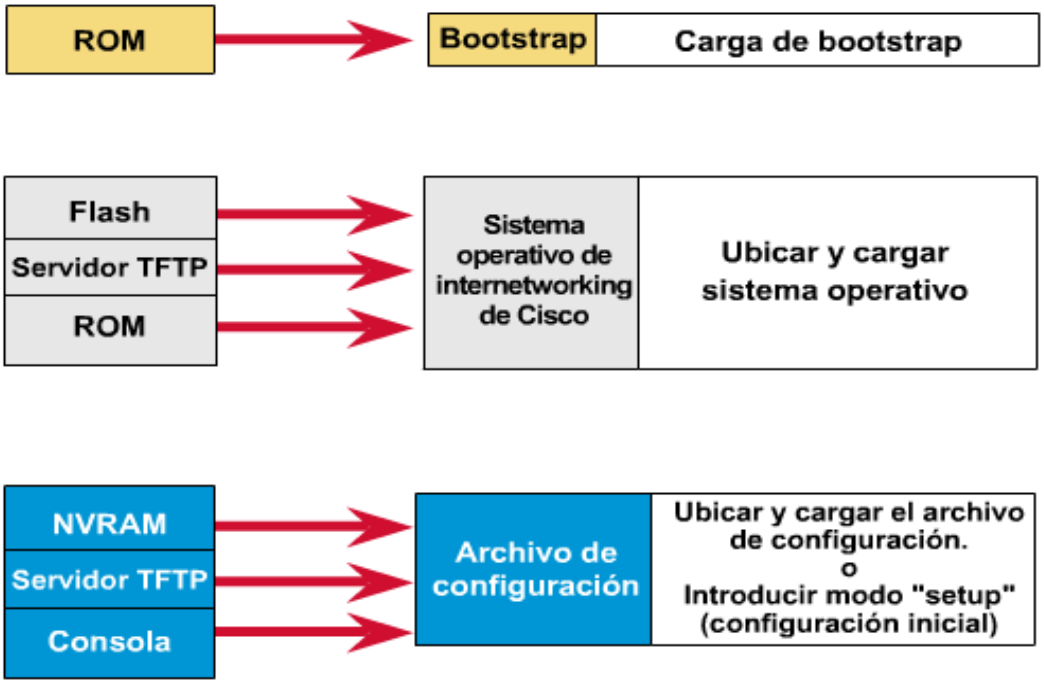


Figura 1.23. Secuencia de inicio[21]

[21] Ibídem.

Al inicializar el software, como se ilustra en la figura1.23, se producen los siguientes eventos:

- **Paso 1**: El cargador genérico de bootstrap, que se encuentra en la ROM, se ejecuta en la tarjeta de la CPU. Un bootstrap es una operación simple por defecto para cargar instrucciones que a su vez hacen que se carguen otras instrucciones en la memoria, o provocan la entrada a otros modos de configuración.
- **Paso 2**: El sistema operativo (Cisco IOS) se puede encontrar en uno de varios lugares. Se revela la ubicación en el campo de arranque del registro de configuración. Si el campo de arranque indica un Flash, o carga de red, comandos del **sistema de arranque** en el archivo de configuración indican la ubicación exacta de la imagen.
- **Paso 3**: Se carga la imagen del sistema operativo. Cuando está cargado y funcionando, el sistema operativo ubica los componentes del hardware y software y muestra los resultados en la terminal de consola.
- **Paso 4**: El archivo de configuración guardado en la NVRAM se carga en la memoria principal y se ejecuta línea por línea. Estos comandos de configuración inician procesos de enrutamiento, brindan direcciones para las interfaces, establecen las características de los medios, etc.
- **Paso 5**: Si no existe ningún archivo de configuración válido en la NVRAM, el sistema operativo ejecuta una rutina de configuración inicial con preguntas denominada *diálogo de configuración del sistema*, también denominado *diálogo de configuración inicial,* el cual no debe ser utilizado para introducir funciones complejas.

CAPÍTULO 2 . CONFIGURACIÓN DE ROUTERS CISCO SERIE 2800

2.1. CONFIGURACIONES INÍCIALES

2.1.1. CONECTÁNDOSE POR PRIMERA VEZ AL ROUTER

Para la configuración inicial del router se utiliza el puerto de consola conectado a un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al puerto **COM1** de la computadora; la cual debe tener instalado un software de emulación de terminal, como el Hyper Terminal. Los parámetros de configuración son:

- El Puerto COM adecuado
- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada
- Sin control de flujo

Desde la línea de comandos el router inicia en el modo EXEC usuario; las tareas que se pueden ejecutar en este modo son solo de verificación, ya que no se permiten cambios de configuración. En el modo EXEC privilegiado es en donde se pueden realizar las tareas comunes de configuración. Para pasar del modo usuario al privilegiado se debe ejecutar el comando **`enable,`** y **`disable`** para regresar al modo usuario. Esto es posible porque no se ha configurado contraseña, de lo contrario seria requerida cada vez que se pasara al modo privilegiado.

```
Router>              ←Modo EXEC usuario
Router>enable
Router#              ←Modo EXEC privilegiado
Router#disable
Router>
```

Modo global y de interfaz:

```
Router>enable
Router#configure terminal
Router(config)#interface [tipo de interfaz] [número-slot/numero-interfaz]
Router(config-if)#exit
Router(config)#exit
Router#
```

Para pasar del modo privilegiado al global se debe de introducir el comando **`configure terminal`**, y del modo global al de interfaz ejecute **`interface FastEthernet 0/0`**, en este caso se ha elegido la FastEthernet 0. Para regresar un modo mas atrás utilice **`exit`** o **Control+Z** que lo llevará directamente al modo privilegiado.

Los routers ofrecen información detallada a través de las ayudas pues resulta difícil memorizar todos los comandos disponibles; el signo de interrogación (**?**) y el tabulador del teclado nos brindan la ayuda necesaria a ese efecto. El tabulador completa los comandos que no recordamos completos o que no queremos escribir en su totalidad. El signo **?** colocado inmediatamente después de un comando muestra todos los que comienzan con esas letras; colocado después de un espacio (**barra espaciadora+?**) nos lista todos los comandos que se pueden ejecutar en posición. La ayuda se puede ejecutar desde cualquier modo:

```
Router#?
Exec commands:
  <1-99>      Session number to resume
  auto        Exec level Automation
  clear       Reset functions
```

```
  clock       Manage the system clock
  configure   Enter configuration mode
     .
     .
     .
```

Inmediatamente o después de un espacio según la ayuda solicitada:

```
Router#sh?
Show

Router#show ?
  aaa              Show AAA values
  access-lists     List access lists
  arp              Arp table
  cdp              CDP information
  class-map        Show QoS Class Map
  clock            Display the system clock
  controllers      Interface controllers status
  crypto           Encryption module
  debugging        State of each debugging option
  dhcp             Dynamic Host Configuration Protocol status
  --More--
```

La indicación **--More--** significa que existe más información disponible. La barra espaciadora pasará de página en página, mientras que el INTRO lo hará línea por línea. El acento circunflejo '**^**' indicará un fallo de escritura en un comando:

```
Router#configure terninal
                     ^
% Invalid input detected at '^' marker.
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

El uso de Control+P (también flecha hacia arriba) permite ver los últimos comandos ejecutados, el Control-N (también flecha hacia abajo) la inversa del anterior. Estos comandos quedan registrados en un búfer llamado historial y pueden verse con el comando **show history**. Por defecto la cantidad de comandos que se guardan en memoria es de 10, pero puede ser modificado por el administrador utilizando el **history size**:

```
Router#terminal history size ?
  <0-256>  Size of history buffer
Router#terminal history size 15
```

2.1.2. ASIGNACIÓN DE NOMBRE Y CONTRASEÑA

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante el siguiente comando:

```
Router(config)#hostname [nombre]
nombre(config)#
```

Para garantizar la seguridad del sistema se pueden utilizar contraseñas y restringir el acceso. Las contraseñas se pueden establecer tanto en líneas individuales como en el modo EXEC privilegiado.

- **`enable password`** y **`enable secret:`** se utilizan para restringir el acceso al modo EXEC privilegiado. El comando **`enable password`** se utiliza sólo si no se ha configurado previamente **`enable secret.`**El comando **`enable secret`** utilza un proceso de cifrado propietario de Cisco para modificar la cadena de caracteres de la contraseña.

```
Router(config)#enable password [contraseña]
Router(config)#enable secret [contraseña]
```

- **`line console 0:`**establece una contraseña en la terminal de consola.

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password [contraseña]
```

- **`line vty 0 4:`**establece una contraseña en las sesiones Telnet entrantes, en este caso se permiten cinco conexiones múltiples, según le versión del sistema operativo el numero de sesiones soportadas puede variar. En todos los casos el comando **`login`** suele estar configurado por defecto, este permite que el router pregunte la contraseña al intentar conectarse.

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password [contraseña]
```

- **service password-encryption:** evita que las contraseñas se visualicen. Este algoritmo de cifrado no coincide con el Estándar Cifrado de Datos (DES).Una vez cifradas las contraseñas no se podrán volver a leer en texto plano.

```
Router(config)# service password-encryption
```

Durante el proceso de configuración de contraseñas el comando login local le permitirá al router preguntar qué usuario intenta ingresar y su respectiva contraseña. Para que esto funcione se deben crear uno o más nombres de usuario y contraseña con el siguiente comando:

```
Router(config)#username [nombre usuario] password [contraseña]
nombre(config)# line vty 0 4
Router(config-line)#login local
```

2.1.3. CONFIGURACIÓN DE MENSAJES

Con el fin de brindar información ante posibles averías o advertencias e intrusos existen Varios tipos de banners o mensajes. Los mensajes más utilizados son el **banner motd** que ofrece la posibilidad de un mensaje diario, el **banner login** que será visto al establecer una sesión de telnet y el **banner exec** que se mostrara al pasar al modo privilegiado utilizando la contraseña.

En la configuración de un banner, el texto que se mostrara debe ponerse entre caracteres similares al comenzar y al terminar.

```
SERVIDOR(config)#banner motd
SERVIDOR(config)#banner motd *ESTE ES UN SISTEMA PROTEGIDO*
SERVIDOR(config)#exit
SERVIDOR#exit


SERVIDOR con0 is now available
```

```
Press RETURN to get started.


ESTE ES UN SISTEMA PROTEGIDO

SERVIDOR>
```

2.1.4. CONFIGURACIÓN DE INTERFACES

Las interfaces de un router forman parte de las redes que están directamente conectadas al dispositivo. Estas interfaces activas deben llevar una dirección IP y su correspondiente máscara, como un host perteneciente a esa red.

Como todas las interfaces de un router se inician automáticamente en el modo administrativamente desactivado, muchas funciones se activan por interface. Los comandos de configuración de interface modifican la operación de un puerto Ethernet, Loopback o Serial. Las interfaces ethernet, fastethernet o gigabitethernet se refieren a las velocidades 10, 100, y 1000 Mbps respectivamente; en este trabajo nos referiremos a cualquiera de ellas como Ethernet. Los subcomandos de interface siempre se colocan a continuación de un comando de interface porque el comando de interface sólo define el tipo de interface.

- **interface *[tipo de interfaz] [0/ranura/puerto]*:** con este comando se inicia el proceso de configuración de una interfaz, "0" indica las ranuras que están incorporadas en el chasis del router, dependiendo del modelo del router esta numeración puede cambiar[22]. Para obtener información detallada de las interfaces con las que cuenta un router, se utiliza el comando **show interfaces** el cual se describe más adelante.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#
```

```
Router(config)#interface serial 0/0/0
Router(config-if)#
```

[22] Guía rápida para routers de la serie Cisco 2800 de servicios integrados.

- **ip address *[dirección IP] [máscara]*:** establece la dirección IP de la interfaz.

```
Router(config-if)#ip address 192.68.1.1 255.255.255.0
```

- **no shutdown:** activa la interfaz administrativamente.

```
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
up
```

- **shutdown:** desactiva la interfaz administrativamente.

```
Router(config-if)#shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
```

En los enlaces seriales, se debe tener especial cuidado para determinar quién es el DCE (equipo de comunicaciones) y quien el DTE (equipo terminal del abonado) debido a que el DCE lleva el sincronismo de la comunicación. Por defecto los routers Cisco son dispositivos DTE, pero en algunos casos se pueden utilizar como dispositivos DCE. Para la interfaz que sea determinada como DCE se debe especificar una velocidad mediante el comando **clock rate,** la cual debe ser especificada en bps. El comando **banwidth** configura el ancho de banda, que el router utilizara para el cálculo de costes y métricas para los protocolos de enrutamiento, mientras que el **clock rate** brinda la verdadera velocidad del enlace. El ancho de banda debe ser especificado en Kbps. A continuación se observa la configuración de un enlace serial como DCE:

```
Router(config-if)#interface Serial 0/1/0
Router(config-if)#ip address 192.168.27.253 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#bandwidth 128
Router(config-if)#no shutdown
```

2.1.5. SUB-INTERFACES

Las subinterfaces permiten utilizar varios enlaces a través de una interfaz física. Las interfaces Fastethernet y las interfaces seriales permiten la creación de gran cantidad de subinterfaces. Una vez establecida la interfaz física, el número de subinterfaz se configura seguidamente separada por un punto.

interface [tipo] [número-slot/numero-interfaz.numero-subinterfaz]

Las subinterfaces normalmente se utilizan como enlaces troncales. Para que las VLAN puedan establecer comunicación entre ellas deben ser necesarios los servicios de un router. Para esto se deben establecer subinterfaces Fastethernet, encapsulación y dirección IP correspondiente de manera que cada una de estas pertenezca a una VLAN determinada.

A continuación se describe la sintaxis de una interfaz Fastethernet a la que se le han creado dos subinterfaces con encapsulación 802.1Q para un enrutamiento de VLAN (véase figura 2.1).

```
Router(config)#interface fastethernet 0/0.1
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#description CONEXION TRONCAL VLAN 2
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.2
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#description CONEXION TRONCAL VLAN 3
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to
up
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to
up
```

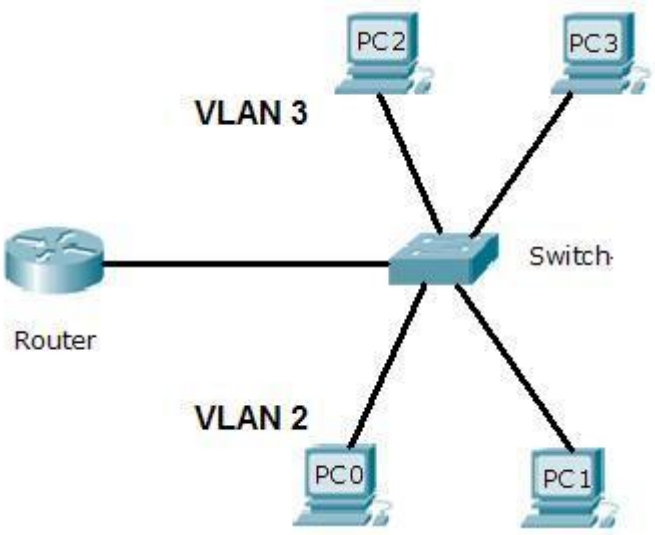


Figura 2.1. Router para comunicar VLANs

2.1.6. COPIAS DE RESPALDO DEL ARCHIVO DE CONFIGURACIÓN

Las configuraciones actuales del router como las tablas de enrutamiento son almacenadas en la memoria **RAM** (**`running-config`**), este tipo de memoria pierde el contenido al apagarse el router. Para que esto no ocurra es necesario hacer una copia de respaldo a la **NVRAM** (**`startup-config`**).

El comando **`copy`** se utiliza con esta finalidad, identificando un origen con datos a guardar y un destino donde se almacenarán esos datos. A continuación se muestra como se guarda la configuración.

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

En caso necesario de hacer lo contrario y traer la configuración de la **NVRAM** a la **RAM**.

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

Los datos de configuración almacenados en la memoria no volátil no son afectados por la falta de alimentación, el contenido permanecerá en la NVRAM hasta que se ejecute el comando apropiado para su eliminación.

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

Por el contrario no existe comando para borrar el contenido de la **RAM**. Si se pretende dejar sin ningún dato de configuración debe reiniciar o apagar el router. La **RAM** se borra únicamente ante la falta de alimentación eléctrica.

```
Router#reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
```

Se debe de responder no a la pregunta para que se borre la configuración que se encuentra en la **RAM**.

El contenido de la **RAM** puede almacenarse en un servidor **TFTP**, en este caso el router solicitará el nombre de archivo con el que se guardará la configuración y la dirección IP del servidor. Por defecto el router asigna un nombre de archivos entre corchetes, en este caso se ha utilizado la dirección IP 204.200.10.56 como dirección del servidor TFTP.

```
Router_2811#copy running-config tftp
Address or name of remote host []? 204.200.10.56
Destination filename [Router_2811-confg]?
```

```
.!!
[OK - 659 bytes]

659 bytes copied in 6.328 secs (0 bytes/sec)
Router_2811#
```

Para ejecutar el proceso inverso el router debe tener como mínimo una conexión de red activa hacia el servidor **tftp**.

```
Router_2811#ping 204.200.10.56

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 204.200.10.56, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
141/153/157 ms

Router_2811#copy tftp running-config
Address or name of remote host []? 204.200.10.56
Source filename []? Router_2811-confg
Destination filename [running-config]?
Accessing tftp://204.200.10.56/Router_2811-confg...
Loading Router_2811-confg from 204.200.10.56: !
[OK - 659 bytes]

659 bytes copied in 0.141 secs (4673 bytes/sec)
Router_2811#
%SYS-5-CONFIG_I: Configured from console by console
Router_2811#
```

El router también permite copiar la configuración en texto plano para almacenarla en cualquier procesador de texto, ésta puede copiarse y pegarse directamente al router haciendo posible que se configure de manera rápida y sencilla.

2.1.7. COPIA DEL CISCO IOS

En ocasiones es necesario restaurar el IOS del router o actualizarlo se debe hacer desde un servidor TFTP. El sistema operativo se almacena en la memoria **flash**. Es importante que se guarden copias de seguridad de todas las IOS en un

servidor central. El comando **copy flash tftp** ejecuta la copia sobre el servidor TFTP.

```
Router_2811#copy flash tftp
Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 204.200.10.56
Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 50938004 bytes]

50938004 bytes copied in 144.453 secs (352000 bytes/sec)
Router_2811#
```

Cuando se introduce el comando se debe especificar el nombre del archivo que se desea copiar, la dirección del servidor TFTP y el nombre que tendrá al guardarse en el servidor, si no se especifica ninguno se guardará con el nombre original. En el proceso inverso al anterior o para actualizar el IOS se debe verificar el espacio en la memoria flash con el comando **show flash** y luego ejecutar el comando **copy tftp flash.**

```
Router_2811#show flash

System flash directory:
File  Length   Name/status
  3   50938004 c2800nm-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

Una vez que se verificó que hay suficiente espacio para el IOS que se desea copiar desde el servidor TFTP.

```
Router_2811#copy tftp flash
Address or name of remote host []? 204.200.10.56
Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin
Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing  tftp://204.200.10.56/c2800nm-advipservicesk9-mz.124-
15.T1.bin...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing  device...  eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: completeAccessing tftp://204.200.10.56/c2800nm-
advipservicesk9-mz.124-15.T1.bin...
Loading      c2800nm-advipservicesk9-mz.124-15.T1.bin      from
204.200.10.56:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 50938004 bytes]

50938004 bytes copied in 143.19 secs (25793 bytes/sec)
Router_2811#
```

2.1.8. COMANDOS SHOW Y DE VERIFICACIÓN DEL ROUTER

Es importante que se pueda monitorear la salud y estado del router en cualquier momento. Los comandos show son la herramienta más eficaz para la lectura y análisis del funcionamiento del router. De una buena interpretación de la

sintaxis expresada en un comando show dependerá la resolución de una incidencia o un fallo. Un comando show puede ejecutarse en el modo usuario con grandes limitaciones y en el privilegiado, done se expone la información completa.

A continuación se suministran los comandos show más usados:

- **show version:** Muestra la configuración de hardware del sistema, la versión de IOS, los nombres y orígenes de los archivos de configuración y la imagen de arranque.

```
Router_2811#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on
System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes
of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
3 FastEthernet/IEEE 802.3 interface(s)
```

```
1 Low-speed serial(sync/async) network interface(s)
239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Router_2811#
```

- **show processes:** Muestra información acerca de los procesos activos.
- **show protocols:** Muestra el estado de los protocolos configurados de capa 3.

```
Router_2811#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
FastEthernet0/1 is up, line protocol is up
  Internet address is 204.200.9.1/24
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.27.250/30
Serial0/1/0 is down, line protocol is down
FastEthernet1/0 is up, line protocol is down
Vlan1 is administratively down, line protocol is down
Router_2811#
```

- **show memory:** Muestra estadísticas acerca de la memoria del router, incluyendo estadísticas de memoria disponible.
- **show stacks:** Monitorea el uso de la pila de procesos y rutinas de interrupción y muestra la causa del último reinicio del sistema.
- **show buffers:** Suministra estadísticas sobre los grupos de búfer en el router.
- **show flash:** Muestra la información contenida en la memoria flash.
- **show running-config:** Muestra la información contenida en la memoria RAM, es decir el archivo de configuración activo.
- **show startup-config:** Muestra la información contenida en la NVRAM, es decir el respaldo del archivo de configuración.
- **show interfaces:** Muestra estadísticas para todas las interfaces instaladas en el router.

```
Router_2811#show interfaces
FastEthernet0/0 is administratively down, line protocol is down
(disabled)
  Hardware is Lance, address is 0003.e417.6801 (bia 0003.e417.6801)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.27.250/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 22 bits/sec, 0 packets/sec
  5 minute output rate 1 bits/sec, 0 packets/sec
     9 packets input, 828 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 52 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

```
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0001.9602.27d8 (bia
0001.9602.27d8)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
Router_2811#
```

- **`show ip interfaces`:** Muestra información generalizada de las interfaces IP.
- **`show ip interface brief`:** Muestra una tabla con información básica de todas las interfaces.

```
Router_2811#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES manual administratively down down

FastEthernet0/1        204.200.9.1     YES manual up                    up

Serial0/0/0            192.168.27.250  YES manual up                    up

Serial0/1/0            unassigned      YES manual down                  down

FastEthernet1/0        unassigned      YES manual up                    down

Vlan1                  unassigned      YES manual administratively down down
Router_2811#
```

- **`show tech-support:`** Muestra información muy completa sobre el funcionamiento del router.
- **`show cdp neighbors:`** Muestra información de los vecinos Cisco.

```
Router_2811#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Router       Ser 0/0/0         122           R       PT1000      Ser 3/0
Switch       Fas 0/1           154           S       2960        Fas 0/1
```

Uno de los problemas más comunes que se producen en redes IP es el de direccionamiento, y es de suma importancia verificar la configuración de direcciones antes de seguir con la configuración. Hay tres comandos que permiten verificar la configuración de direcciones en la internetwork (véase figura 2.2):

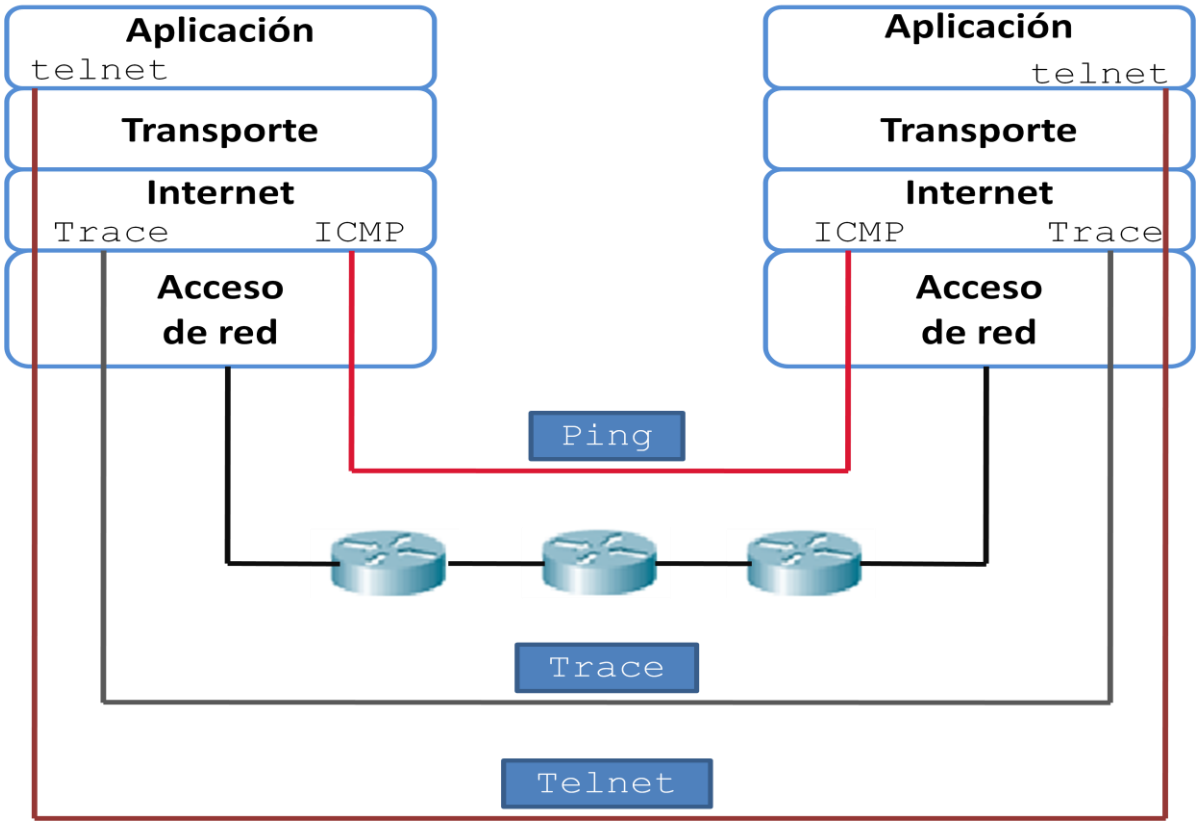


Figura 2.2. Comandos de verificación.

- **`telnet:`** verifica el software de la capa de aplicación entre las estaciones origen y destino. Es el mecanismo de verificación mas completo disponible.

```
cliente#telnet 10.0.0.1
Trying 10.0.0.1 ...OpenEste es un sistema protegido

User Access Verification

Password:
SERVIDOR>
```

- **`ping:`** utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet. Es un mecanismo de verificación sumamente básico.

```
Router1#ping 204.200.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 204.200.10.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
40/48/60 ms
```

- **`trace:`** utiliza valores TTL para generar mensajes desde cada router que se utiliza a lo largo de la ruta. Es sumamente poderoso en cuanto a su capacidad para ubicar fallas en la ruta desde el origen hasta el destino.

```
Router1#trace 192.68.1.2
Type escape sequence to abort.
Tracing the route to 192.68.1.2

  1   204.200.10.2    80 msec   30 msec   40 msec
  2   192.168.27.253  60 msec   60 msec   60 msec
  3   192.68.1.2      70 msec   80 msec   90 msec
```

2.2. ENRUTAMIENTO ESTÁTICO

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas. Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios. En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

La información de enrutamiento que el router aprende desde sus fuentes de enrutamiento se coloca en su propia tabla de enrutamiento. El router se vale de ésta para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino. La tabla de enrutamiento es la fuente principal de información del router acerca de las redes. Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar paquetes. Si las redes de destino no están conectadas directamente, el router debe aprender y calcular la ruta

más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se construye mediante uno de estos dos métodos o ambos[23]:

- Manualmente, por el administrador de la red.
- A través de procesos dinámicos que se ejecutan en la red.

El enrutamiento estático posee varias aplicaciones útiles. Mientras que el enrutamiento dinámico tiende a revelar todo lo que se conoce acerca de la internetwork, es posible que por razones de seguridad se desee ocultar parte de una internetwork. El enrutamiento estático le permite especificar la información que desea revelar acerca de redes restringidas.

2.2.1. RUTAS ESTÁTICAS

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador. Estas rutas, se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única (stub) (véase fig.2.3), ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento.

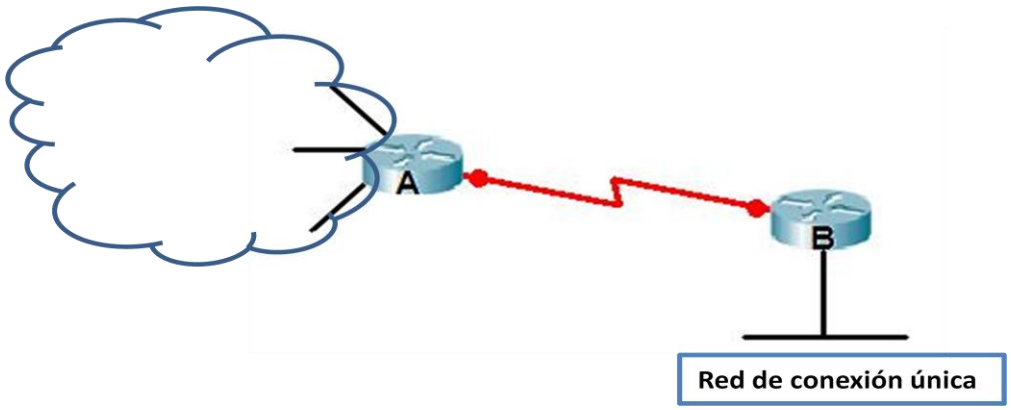


Figura 2.3. Red de conexión única (stub).

[23]Ariganello Ernesto, *Técnicas de configuración de routers Cisco*, p.25.

La ruta estática se configura para conseguir conectividad con un enlace de datos, que no esté directamente conectado al router. Para conectividad de extremo a extremo, es decir, para una comunicación en ambas direcciones, es necesario configurar la ruta en ambas direcciones.

El comando **`ip route`** inicia el proceso de configuración de una ruta estática, los parámetros del comando definen la ruta estática. La sintaxis de configuración del comando es la siguiente, se puede utilizar la interfaz de salida o la IP del próximo salto, como se obseva en la figura 2.4:

```
Router(config)#ip route [red] [máscara] [dirección IP/interfaz]
                        [distancia] [permanent]
```

PARÁMETRO	DESCRIPCIÓN
`Red`	Red o subred de destino
`Mascara`	Mascara de subred de la red de destino
`dirección IP/interfaz`	Dirección IP del router del próximo salto o la interfaz local que debe usarse para llegar a la red de destino
`Distancia`	Parámetro opcional, que define la distancia administrativa
`Permanent`	Parámetro opcional que especifica que la ruta no debe ser eliminada, aunque la interfaz deje de estar activa

Tabla 2.1 Parámetros del comando ip route

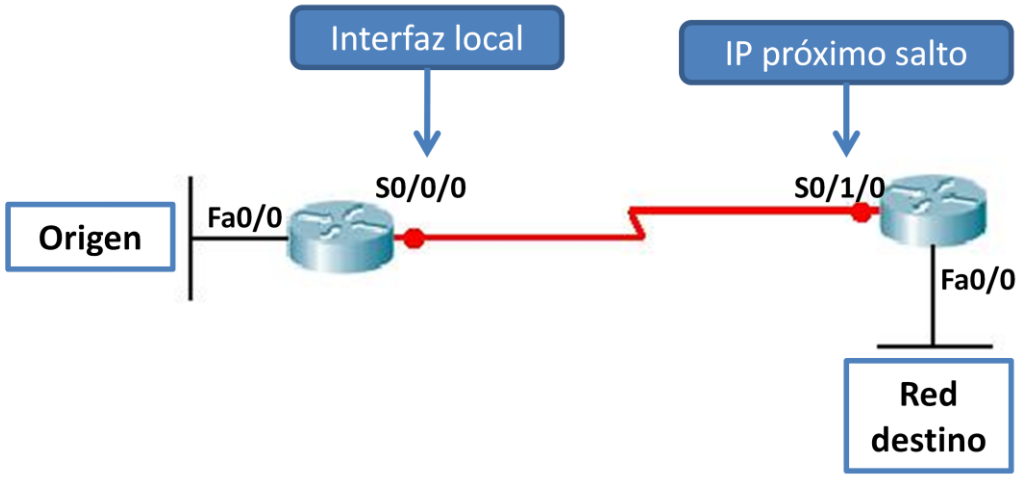


Figura 2.4. Opciones en una ruta estática.

Cuando se configuran las rutas estáticas en enlaces punto a punto, como se ilustra en la figura 2.5, es mejor utilizar el parámetro de la interfaz local de salida para llegar a la red destino y no la dirección IP del próximo salto.

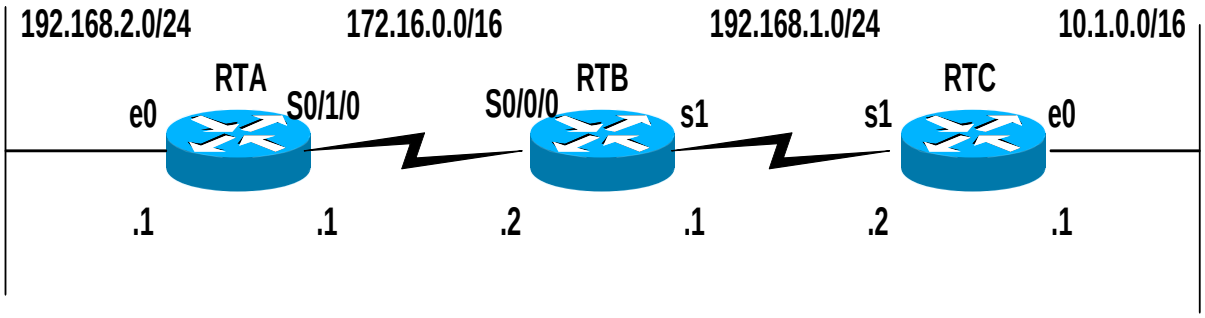


Figura 2.5.Routers con enlace punto a punto

```
RTA(config)#ip route 192.168.1.0 255.255.255.0 serial 0/1/0
```

Cuando se trata de un enlace vía broadcast como Ethernet (véase fig. 2.6), es mejor utilizar ambos parámetros, el de la interfaz de salida y la IP del próximo salto.

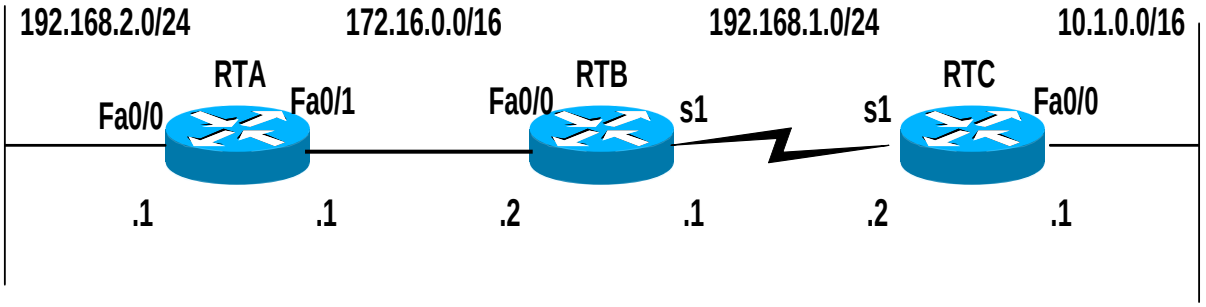


Figura 2.6. Routers con enlace broadcast

```
RTA(config)#ip route 192.168.1.0 255.255.255.0 fa 0/1 172.16.0.2
```

Estas son recomendaciones importantes que se deben tomar en cuenta cuando se configuran las rutas estáticas ya que pueden disminuir procesos en el router[24].

[24] Graziani Rick, *CCNA 1* v 3.0, Ch.3 – Routing Overview.

2.2.2. DISTANCIA ADMINISTRATIVA

La distancia administrativa es una medida del nivel de confiabilidad de la ruta, un valor menor de distancia administrativa indica una ruta más confiable. Como los routers pueden utilizar al mismo tiempo diferentes protocolos incluidas rutas estáticas, de estos se puede obtener la misma información de enrutamiento, por lo tanto se debe de otorgar un valor administrativo a la información que se obtiene, es decir, la distancia administrativa permite que un protocolo tenga mayor prioridad sobre otro si su distancia administrativa es menor. Este valor viene por defecto, sin embargo el administrador puede configurar un valor diferente. El rango de las distancias administrativas varia de 0 a 255, a continuación se especifican los valores predeterminados de la distancia administrativa[25]:

INFORMACIÓN DE:	DISTANCIA ADMINISTRATIVA
INTERFAZ	**0**
RUTA ESTÁTICA	**1**
EIGRP INTERNO	**90**
IGRP	**100**
OSPF	**110**
IS-IS	**115**
RIP	**120**
EIGRP EXTERNO	**170**
INALCANZABLE	**255**

Tabla 2.2 Valores por defecto de la distancia administrativa

En ocasiones, las rutas estáticas se utilizan como rutas de respaldo o también llamadas rutas flotantes. Es posible configurar una ruta estática en un router, la cual solo se usara en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente se fija la distancia administrativa

[25] Lammle Todd, Odom Sean y Wallace Kevin, *CCNP Routing Study Guide,* p.33.

en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

2.2.3. RUTAS ESTÁTICAS POR DEFECTO

Una ruta por defecto o predeterminada es una entrada en la tabla de enrutamiento que dirige los paquetes hacia el salto siguiente, cuando este salto no se encuentra explícitamente determinado en la tabla de enrutamiento, o cuando no es posible almacenar en la tabla cada una de las redes accesibles a través de la nube de Internet.

La sintaxis de configuración de una ruta estática por defecto o de último recurso, es la siguiente:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [dirección IP/interfaz]
                [distancia]
```

Con la máscara 0.0.0.0, cuando el router ejecuta el AND lógico con la dirección IP de destino del paquete, siempre obtiene la red 0.0.0.0. Si el paquete no coincide con una ruta más especifica en la tabla de enrutamiento, será enviado hacia la red 0.0.0.0.

La configuración manual de rutas estáticas por defecto en cada router es sencillo en una red pequeña, pero en situaciones más complejas, los routers pueden intercambiar dinámicamente rutas por defecto. Este intercambio trabaja de forma diferente, dependiendo del protocolo de enrutamiento empleado y podría crear serios problemas si se configura inapropiadamente. Generalmente, las rutas por defecto apuntan hacia fuera de la red, por consecuencia estas son visibles cuando fallan.

En la figura 2.7 se muestra un ejemplo de utilización de una ruta estática por defecto, el router **“Y”** tiene configurada la ruta por defecto hacia el exterior como

única salida/entrada del sistema autónomo 65000, los demás routers aprenderán ese camino gracias a la redistribución que el protocolo hará dentro del sistema autónomo.

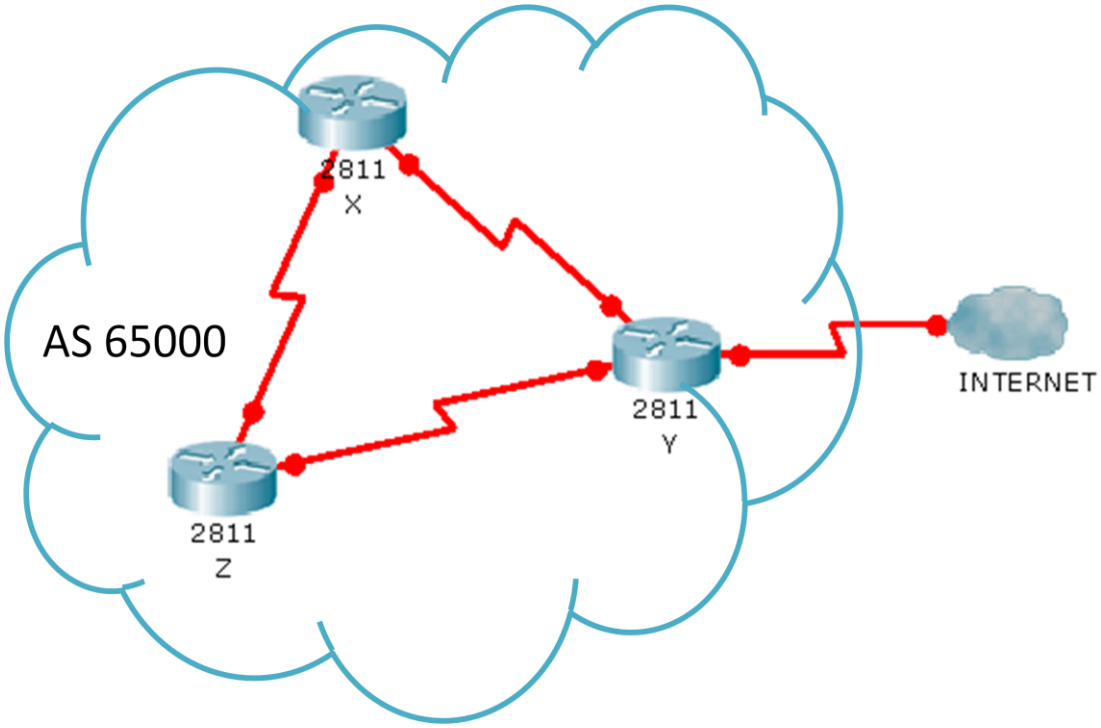


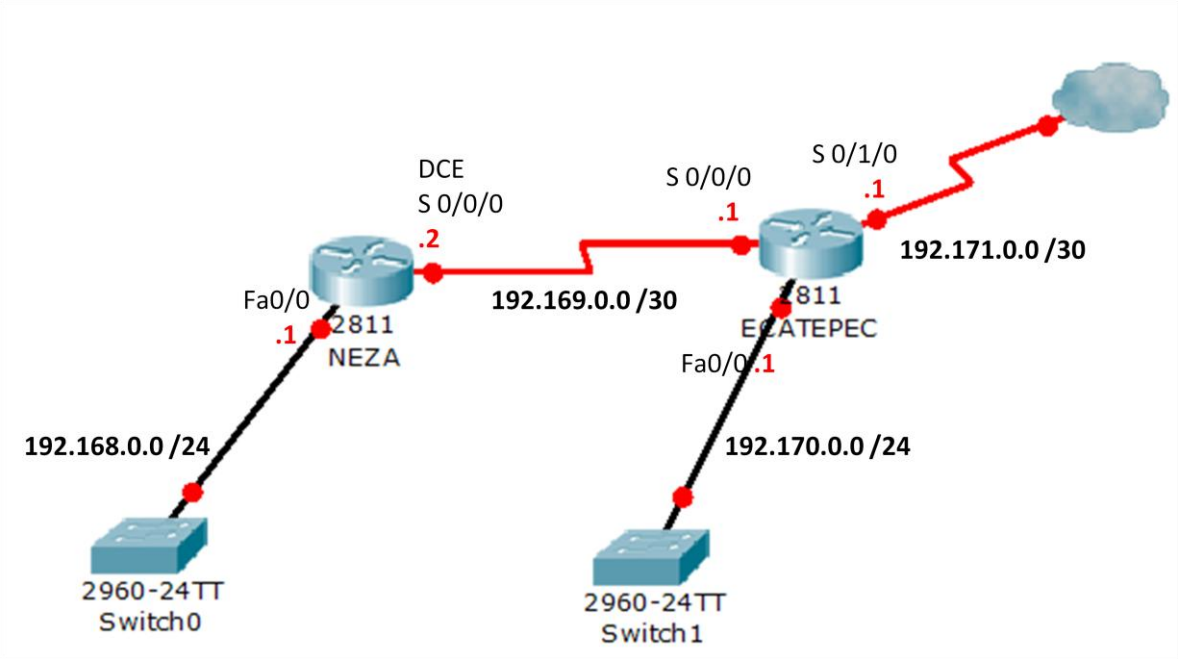
Figura 2.7. Ruta por defecto hacia el exterior.

Cuando se han configurado las rutas estáticas y estáticas por defecto se debe verificar que estas se encuentren en la tabla de enrutamiento, para esto se utilizan los siguientes comandos:

- **`show ip route:`** Muestra toda la tabla de enrutamiento.
- **`show ip route static:`** Muestra las tablas de rutas estáticas.

EJEMPLO PRÁCTICO 2.1

En este ejemplo se realiza la configuración de rutas estáticas y rutas estáticas por defecto.



A continuación se muestra la configuración completa para el router NEZA :

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname neza
neza(config)#enable secret fes
neza(config)#line vty 0 4
neza(config-line)#password unam
neza(config-line)#login
neza(config-line)#line con 0
neza(config-line)#password unam
neza(config-line)#login
neza(config-line)#exit
neza(config)#interface fastethernet 0/0
neza(config-if)#ip address 192.168.0.1 255.255.255.0
neza(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
neza(config-if)#exit
neza(config)#interface serial 0/0/0
```

```
neza(config-if)#ip address 192.169.0.2 255.255.255.252
neza(config-if)#clock rate 250000
neza(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
neza(config-if)#exit
neza(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 100
```

La interfaz **Serial 0/0/0** cambiara a estado activo cuando se configure apropiadamente la interfaz **Serial 0/0/0** en el router ECATEPEC. A continuación se muestra la configuración completa para el router ECATEPEC:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ecatepec
ecatepec(config)#enable secret fes
ecatepec(config)#line vty 0 4
ecatepec(config-line)#password unam
ecatepec(config-line)#login
ecatepec(config-line)#line con 0
ecatepec(config-line)#password unam
ecatepec(config-line)#login
ecatepec(config-line)#exit
ecatepec(config)#interface fastethernet 0/0
ecatepec(config-if)#ip address 192.170.0.1 255.255.255.0
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
ecatepec(config-if)#interface serial 0/0/0
ecatepec(config-if)#ip address 192.169.0.1 255.255.255.252
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ecatepec(config-if)#interface serial 0/1/0
ecatepec(config-if)#ip address 192.171.0.1 255.255.255.252
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
ecatepec(config-if)#exit
ecatepec(config)#ip route 192.168.0.0 255.255.255.0 serial 0/0/0
ecatepec(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0 100
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```

A continuación se verifican las rutas configuradas con los commandos **`show ip route`** y **`show ip route static`.** Para el router NEZA:

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    192.168.0.0/24 is directly connected, FastEthernet0/0
     192.169.0.0/30 is subnetted, 1 subnets
C       192.169.0.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

```
neza#show ip route static
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

Para el router ECATEPEC:

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S    192.168.0.0/24 is directly connected, Serial0/0/0
     192.169.0.0/30 is subnetted, 1 subnets
C       192.169.0.0 is directly connected, Serial0/0/0
C    192.170.0.0/24 is directly connected, FastEthernet0/0
     192.171.0.0/30 is subnetted, 1 subnets
C       192.171.0.0 is directly connected, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

```
ecatepec#show ip route static
S    192.168.0.0/24 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

2.3. ENRUTAMIENTO DINÁMICO

Los protocolos de enrutamiento soportan un protocolo enrutado (en este trabajo el protocolo enrutado es el Internet Protocol) proporcionando mecanismos para compartir la información de enrutamiento. Los mensajes de protocolo de enrutamiento se desplazan entre los routers. Un protocolo de enrutamiento permite que los routers se comuniquen con otros routers para actualizar y mantener las tablas. Los siguientes son ejemplos de protocolos de enrutamiento TCP/IP[26]:

- RIP (Routing Information Protocolo o Protocolo de información de enrutamiento)
- IGRP (Interior Gateway Routing Protocolo Protocolo de enrutamiento de gateway interior)
- EIGRP (Enhanced Interior Gateway Routing Protocol o Protocolo de enrutamiento de gateway interior extendido)
- OSPF (Open Shortest Path First o Primero la ruta libre más corta)

El conocimiento de las rutas estáticas es gestionado manualmente por el administrador de red, en cambio el conocimiento de las rutas dinámicas funciona de manera diferente. Después de que un administrador de red introduce comandos de configuración para empezar el enrutamiento dinámico, el conocimiento de la ruta se actualiza automáticamente a través de un proceso de enrutamiento siempre que se reciba nueva información de la internetwork. Los cambios en el conocimiento dinámico se intercambian entre routers como parte del proceso de actualización.

[26] *Cisco Certified Network Associate Curriculum, Semestre 2*, V2.1.

El éxito del enrutamiento dinámico depende de dos funciones básicas del router, el mantenimiento de un tabla de enrutamiento y la distribución oportuna del conocimiento, bajo la forma de actualizaciones de enrutamiento, hacia otros routers.

Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un router cuando se comunica con los routers vecinos, es decir un protocolo de enrutamiento describe[27]:

- Como enviar actualizaciones
- Que información llevan esas actualizaciones
- Cuando enviar esa información
- Como ubicar a los receptores de las actualizaciones

2.3.1. MÉTRICAS

Cuando un algoritmo de enrutamiento actualiza una tabla de enrutamiento, su objetivo principal es determinar cuál es la mejor información que debe incluir en la tabla. Cada algoritmo de enrutamiento interpreta lo que es mejor a su manera. El algoritmo genera un número, denominado métrica, para cada ruta a través de la red. Normalmente, cuanto menor sea la métrica, mejor será la ruta. Se pueden calcular las métricas tomando como base una sola característica de la ruta. Se pueden calcular métricas más complejas combinando varias características. Las métricas utilizadas con mayor frecuencia por los routers son:

- **Ancho de banda:** Capacidad de transmisión de datos de un enlace.
- **Retardo:** Tiempo requerido para mover un paquete desde el origen hasta el destino en una ruta dada.
- **Carga:** Cantidad de actividad de un recurso de la red, como por ejemplo un router o un enlace.
- **Confiabilidad:** Comúnmente se refiere al índice de error de cada enlace de red.

[27] Ibídem.

- **Número de saltos:** Cantidad de routers que un paquete debe atravesar antes de llegar a su destino.
- **Costo:** Valor arbitrario, basado normalmente, en el numero de saltos, ancho de banda del medio u otras medidas, que es asignado por un administrador de red y utilizado para comparar diversas rutas a través de un entorno de internetwork de redes.
- **MTU(unidad máxima de transmisión):** Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

2.3.2. PROTOCOLOS DE ENRUTAMIENTO POR VECTOR-DISTANCIA Y ESTADO-ENLACE

El enrutamiento por vector-distancia determina la dirección (vector) y la distancia hacia cualquier enlace en la internetwork. Los algoritmos de enrutamiento basados en vector distancia envían copias periódicas de una tabla de enrutamiento de un router a otro. Estas actualizaciones regulares entre routers comunican los cambios de de topología. Cada router recibe una tabla de enrutamiento de los routers vecinos directamente conectados, como se observa en la fiura 2.8.

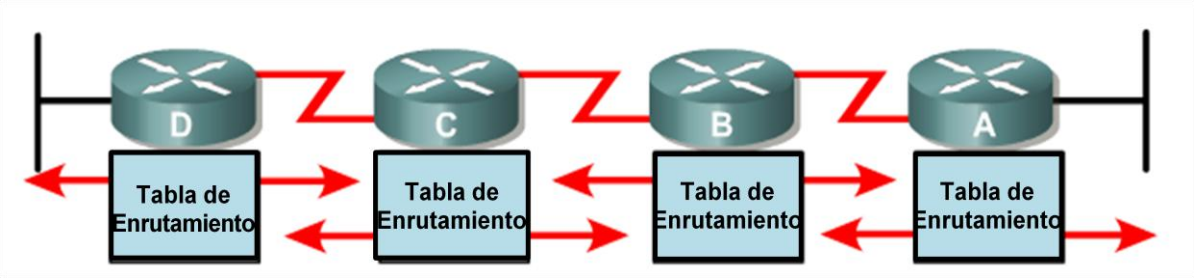


Figura 2.8.Envio de tablas en enrutamiento por vector distancia[28].

Cada router que utiliza el enrutamiento vector-distancia empieza identificando sus propios vecinos. En la figura 2.9, la interfaz que lleva a cada red directamente conectada tiene una distancia de 0. A medida que el proceso de descubrimiento de

[28]Graziani Rick, *CCNA 1* v 3.0, Ch.3 – Routing Overview.

red vector-distancia continúa, los routers descubren la mejor ruta hacia las redes destino basándose en la información que reciben de cada vecino. Por ejemplo, el router A obtiene conocimiento acerca de otras redes tomando como base la información que recibe del router B. Cada una de las demás entradas de red en la tabla de enrutamiento posee un vector-distancia acumulado para demostrar la distancia a la que se encuentra esta red en una dirección determinada.

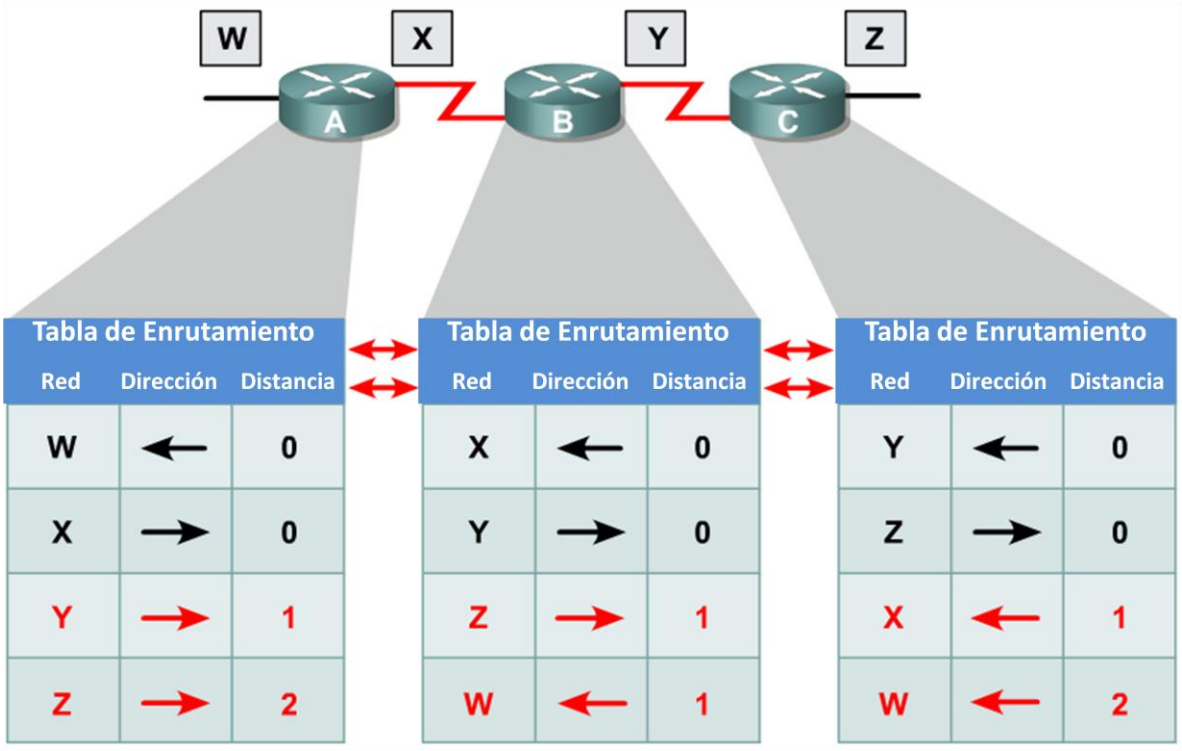


Figura 2.9 Enrutamiento por vector distancia[29].

Cuando cambia la topología de una red que utiliza un protocolo vector-distancia, deben producirse actualizaciones de la tabla de enrutamiento y estas como en el proceso de descubrimiento de red, continúan paso a paso de un router a otro.

Los algoritmos vector-distancia requieren que cada router envié la tabla de enrutamiento completa a cada uno de sus vecinos adyacentes, estas tablas incluyen información acerca del costo de ruta total (definido por su métrica) y la dirección lógica del primer router en la ruta para cada red contenida en la tabla.

[29] Ibidem.

Por otro lado el enrutamiento por estado-enlace recrea la topología exacta de toda la internetwork o al menos la de la porción en que está ubicado el router.

Los algoritmos de enrutamiento de estado de enlace, también conocidos como algoritmos SPF (primero la ruta libre más corta), mantienen una compleja base de datos de información de topología, es decir, un algoritmo de estado de enlace conoce perfectamente los routers distantes y como se interconectan (véase fig. 2.10).

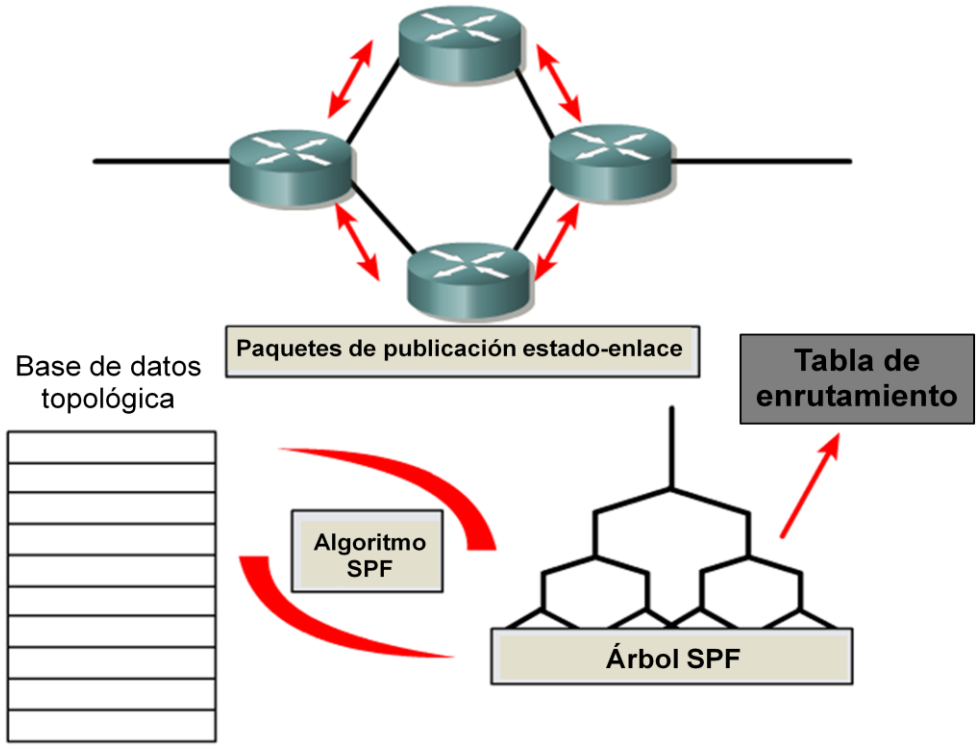


Figura 2.10 Enrutamiento por estado de enlace [30].

El enrutamiento por estado-enlace utiliza:

- Publicaciones estado de enlace (LSA, Link State Advertisement).
- Una base de datos topológica.
- El algoritmo SPF y el árbol resultante.
- Una tabla de enrutamiento de rutas y puertos hacia cada red.

[30] Ibidem.

Los protocolos de enrutamiento del estado de enlace se diseñaron para superar las limitaciones de los protocolos de enrutamiento por vector-distancia. Por ejemplo, los protocolos de vector-distancia sólo intercambian actualizaciones de enrutamiento con sus vecinos inmediatos mientras que los protocolos de enrutamiento del estado de enlace intercambian información de enrutamiento a través de un área mucho más amplia.

Cuando se produce una falla en la red, como por ejemplo que un vecino se vuelve inalcanzable, los protocolos del estado de enlace inundan el área con LSA mediante una dirección multicast especial. La inundación es un proceso que envía información por todos los puertos, salvo el puerto donde se recibió la información. Cada router de estado de enlace toma una copia de la LSA y actualiza su base de datos del estado de enlace o topológica. Luego, el router de estado de enlace envía la LSA a todos los dispositivos vecinos. Las LSA hacen que cada router que se encuentra dentro del área vuelva a calcular las rutas. Por esta razón, es necesario limitar la cantidad de routers de estado de enlace dentro de un área.

Un enlace es igual a una interface en un router. El estado de enlace es la descripción de una interface y de su relación con los routers vecinos. Por ejemplo, una descripción de interface incluiría la dirección IP de la interface, la máscara de subred, el tipo de red a la cual está conectada, los routers conectados a esa red, etc. La recopilación de estados de enlace forma una base de datos del estado de enlace que con frecuencia se denomina base de datos topológica. La base de datos del estado de enlace se utiliza para calcular las mejores rutas por la red. Los routers de estado de enlace aplican el algoritmo de Dijkstra a la base de datos del estado de enlace. Esto permite crear el árbol SPF utilizando el router local como raíz. Luego se seleccionan las mejores rutas del árbol SPF y se colocan en la tabla de enrutamiento.

Los algoritmos de enrutamiento del estado de enlace mantienen una base de datos compleja de la topología de red intercambiando publicaciones del estado de

enlace (LSAs) con otros routers de una red. El intercambio de LSA se desencadena por medio de un evento en la red en lugar de actualizaciones periódicas Esto acelera el proceso de convergencia porque no hay necesidad de esperar que un conjunto de temporizadores expire antes de que los routers puedan convergir.

A continuación se muestra una tabla comparativa entre protocolos basados en vector-distancia y estado-enlace.

VECTOR-DISTANCIA	ESTADO-ENLACE
➢ Visualiza la topología de red desde la perspectiva de un router vecino.	➢ Obtiene una visión común de la topología de toda la red.
➢ Incrementa el vector distancia de router a router.	➢ Calcula la ruta mas corta a otros los routers.
➢ Realiza actualizaciones periódicas con frecuencia y su convergencia es lenta.	➢ Ofrece actualizaciones desencadenadas por eventos con una convergencia más rápida.
➢ Envía copia de la tabla de enrutamiento a sus vecinos	➢ Envía actualizaciones de enrutamiento de estado enlace a otros routers
➢ Fácil de configurar y administrar.	➢ Es más difícil de configurar.
➢ Consume mayor ancho de banda.	➢ Consume menor ancho de banda.
➢ Requiere menor memoria y potencia de procesamiento.	➢ Requiere más memoria y potencia de procesamiento.

Tabla 2.3 Características de algoritmos vector-distancia y estado de enlace

2.3.3. ENRUTAMIENTO HIBRIDO BALANCEADO

El enrutamiento hibrido balanceado combina aspectos de los algoritmos de estado-enlace y vector-distancia, como se observa en figura 2.11. Un protocolo de enrutamiento hibrido utiliza vectores de distancia con métricas más precisas para determinar las mejores rutas hacia las redes destino. Sin embargo, difieren de la mayoría de los protocolos por vector-distancia porque utilizan cambios de topología para provocar actualizaciones en las bases de datos de enrutamiento

El protocolo de enrutamiento hibrido balanceado converge rápidamente, como los protocolos de estado de enlace. Sin embargo, difiere de los protocolos por vector-distancia y de estado de enlace en el sentido de que utiliza menos recursos de ancho de banda, memoria y potencia de procesamiento.

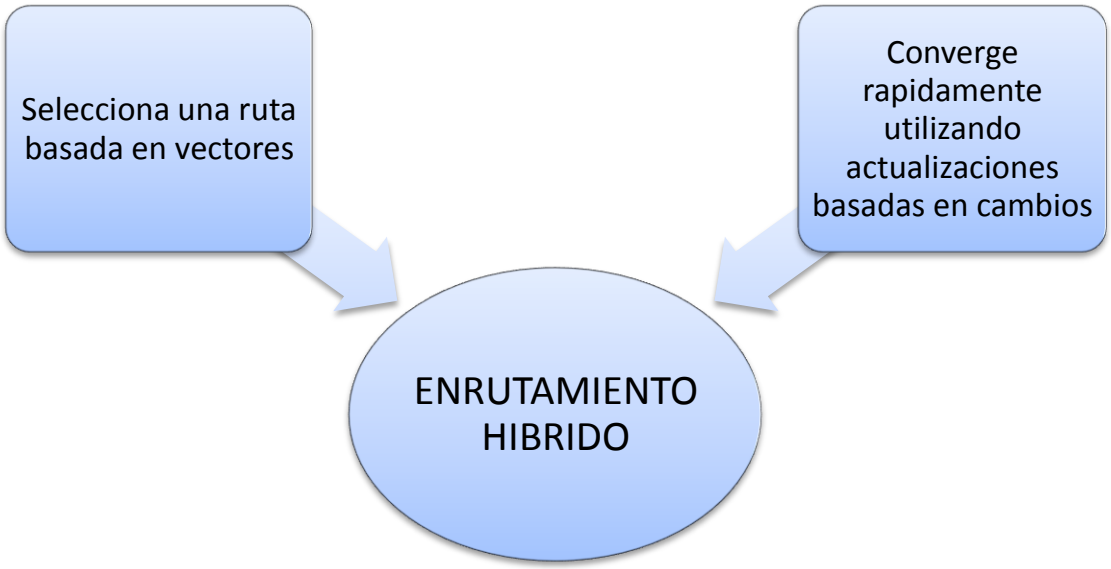


Figura 2.11 Enrutamiento hibrido.

Ejemplos de protocolos de enrutamiento híbridos son IS-IS (Sistema intermedio a Sistema intermedio) de OSI y el protocolo EIGRP (Protocolo de enrutamiento de Gateway interior mejorado) de Cisco.

CAPÍTULO 3 . PROTOCOLOS DE ENRUTAMIENTO INTERIOR IP DENTRO DEL CISCO IOS (Internetwork Operating System)

3.1. RIP (ROUTING INFORMATION PROTOCOL)

El Protocolo de Información de Enrutamiento RIP es uno de los protocolos de enrutamiento más antiguos utilizado por dispositivos basados en IP. El hecho que RIP se base en estándares abiertos y que sea de fácil implementación hace que resulte atractivo para algunos administradores de redes, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados. Su Implementación original fue para el protocolo Xerox a principios de los 80, ganó popularidad cuando se distribuyó con UNIX como protocolo de enrutamiento para esa implementación TCP/IP. RIP es un protocolo de vector de distancia que utiliza la cuenta de saltos del router como métrica[31].

RIP evita que los bucles de enrutamiento se prolonguen en forma indefinida, mediante la fijación de un límite en el número de saltos permitido en una ruta, desde su origen hasta su destino, la cuenta dé saltos máxima de RIP es 15. Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y se etiqueta como inalcanzable al establecerse la cuenta de saltos en 16. En RIP la información de enrutamiento se propaga de un router a los otros vecinos por medio de una difusión de IP usando el protocolo UDP y el puerto 520.

[31]Ariganello Ernesto, *Técnicas de configuración de routers Cisco*, p.31.

RIP incluye características que están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea.

El protocolo RIP ha evolucionado y mientras que, la versión 1 es un protocolo de enrutamiento con clase que no admite la publicación de la información de la máscara de red, el protocolo RIP versión 2 es un protocolo sin clase que admite **CIDR**, **VLSM** y resumen de rutas.

También RIP versión 2 ofrece autenticación en sus actualizaciones, se puede utilizar un conjunto de claves en una interfaz como verificación de autenticación. RIP v2 permite elegir el tipo de autenticación que se utilizará en los paquetes RIP v2. Se puede elegir texto no cifrado o cifrado con Message-Digest 5 (MD5), el texto no cifrado es la opción por defecto. MD5 se puede usar para autenticar el origen de una actualización de enrutamiento.

RIP versión 2 envía sus actualizaciones de enrutamiento en multicast con la dirección Clase D 224.0.0.9, mientras que RIP versión 1 lo hace por broadcast.

El comando **`router rip`** habilita el protocolo de enrutamiento RIP. Luego se ejecuta el comando **`network`** para informar al router acerca de las interfaces donde RIP estará activo. A continuación, el proceso de enrutamiento asocia las interfaces específicas con las direcciones de red y comienza a enviar y a recibir actualizaciones RIP en estas interfaces.

A continuación se muestra la sintaxis de la configuración de RIP:

```
Router(config)#router rip
Router(config-router)#version [tipo de versión]
Router(config-router)#distance [1-255]
Router(config-router)#network [dirección de red]
```

Si no se especifica lo contrario los routers ejecutan por defecto RIP versión 1.

La distancia administrativa permite que el protocolo tenga mayor prioridad sobre otro si su distancia administrativa es menor. El valor por defecto en RIP es 120, sin embrago el administrador puede configurar un valor diferente si así lo determina. El rango de las distancias administrativas varía de 1 a 255, donde 255 es inalcanzable[32].

Los routers RIP conservan solo la mejor ruta hacia un destino pero pueden conservar más de una ruta al mismo destino si el costo de todas es igual. RIP es capaz de balancear las cargas hasta en seis rutas de igual costo, cuatro de ellas por defecto. **RIP** realiza lo que se conoce como balanceo de cargas "por turnos" o "en cadena" (round robin). Significa que **RIP,** envía paquetes por turnos a través de las rutas paralelas[33].

La figura 3.1 muestra un ejemplo de rutas RIP con tres rutas de igual costo. El router comenzará con un apuntador hacia la interfaz conectada al router 1. Luego el apuntador iniciará un ciclo a través de las interfaces y rutas en un orden pre configurado, por ejemplo: 1-2-3-1-2-3-1-2 y así sucesivamente. Como la métrica del protocolo RIP es el número de saltos, no se toma en cuenta la velocidad de los enlaces. Por lo tanto, esto es muy importante considerarlo al configurar RIP ya que **la ruta de 128 Kbps tendrá la misma preferencia que la ruta de 2 Mbps**.

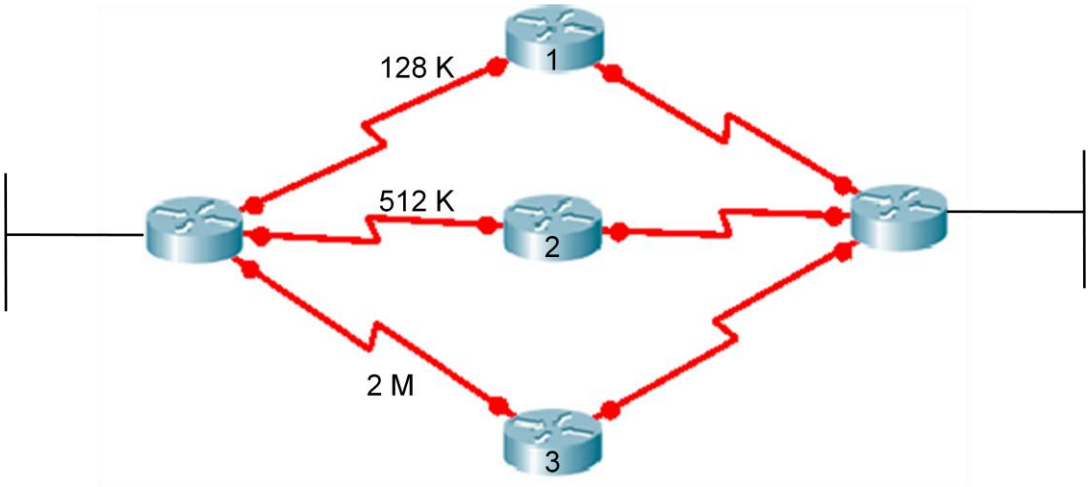


Figura 3.1. Rutas indistintas para RIP.

[32] Ibídem p.32.
[33] Lammle Todd, Odom Sean y Wallace Kevin, *CCNP Routing Study Guide,* p.41.

El software Cisco lOS soporta dos métodos de balanceo de carga de paquetes IP. Estos son balanceo de carga por paquete o balanceo de carga por destino. Si está habilitado el método de conmutación conocido como process switching, el router alternará los caminos paquete a paquete. Si el método de conmutación conocido como fast switching está habilitado, solamente una de las rutas se guardará en la memoria cache para la red de destino. Todos los paquetes dirigidos a un host específico tomarán el mismo camino. Los paquetes dirigidos a hosts distintos en la misma red pueden usar una ruta alternativa. El tráfico se balancea de acuerdo al destino.

Por defecto, el router usa balanceo de cargo por destino también llamado fast switching. El cache de las rutas permite que los paquetes salientes sean balanceados por destino y no por paquete. Para deshabilitar fast switching, use el comando **`no ip route-cache`**. El usar este comando permitirá que los paquetes sean balanceados por paquete.

3.1.1. TEMPORIZADORES

De acuerdo al tipo de topología implementada los valores predeterminados de los temporizadores pueden variarse para optimizar el funcionamiento del protocolo. En RIP los parámetros configurables son los períodos entre las actualizaciones, el período de espera antes que el router declare inválida una red, el período para evitar publicaciones y el tiempo en el que el router guardará la información de una ruta antes de descartarla.

```
Router(config)#router rip
Router(config-router)#timers basic [Updates Invalid Holddown Flush]
```

UPDATES: Define cada cuanto tiempo se deben enviar actualizaciones a un vecino. Viene establecido de forma predeterminada en 30 segundos. Este puede

configurarse para intervalos más prolongados, a fin de ahorrar ancho de banda, o más cortos para disminuir el tiempo de convergencia.

INVALID: Por defecto es de 180 segundos y corresponde al tiempo en el cual una ruta se almacenará en la tabla de enrutamiento hasta que se considere inválida. Este contador se resetea cada vez que el router recibe una actualización.

FLUSH: Define el tiempo que toma el router en eliminar una ruta desde que se declaró como inválida. Por defecto son 240 segundos.

HOLDDOWN: Este temporizador es uno de los mecanismos de RIP para prevenir bucles (loops), junto con el horizonte dividido y el envenenamiento de ruta, evitando que el router tome decisiones de enrutamiento erróneas cuando ha habido un cambio o una falla dentro de algún lugar de la red. De manera predeterminada el tiempo de holddown es de 180 segs. Si un router detecta una red como inalcanzable, este temporizador se inicia y entonces esperará 180 segundos hasta que la red se declare como "estable". Cuando el contador llega a 0 entonces el router aceptará actualizaciones desde sus vecinos[34].

Los temporizadores de espera ayudan a prevenir la cuenta al infinito, pero también aumentan el tiempo de convergencia. Esto evita que una ruta menos conveniente ingrese en la tabla de enrutamiento pero también puede evitar que se instale una ruta alternativa válida. Es posible reducir el lapso del temporizador de espera, para agilizar la convergencia pero esto se debe hacer con cautela. El ajuste ideal es el que fije el temporizador con una duración apenas mayor al lapso máximo de actualización posible de la red. En la figura 3.2, el bucle consta de cuatro routers. Si cada router tiene un lapso de actualización de 30 segundos, el bucle más largo posible es de 120 segundos. Por lo tanto, el temporizador de espera debe ser apenas mayor a 120 segundos.

[34] http://www.redescisco.net/node/28

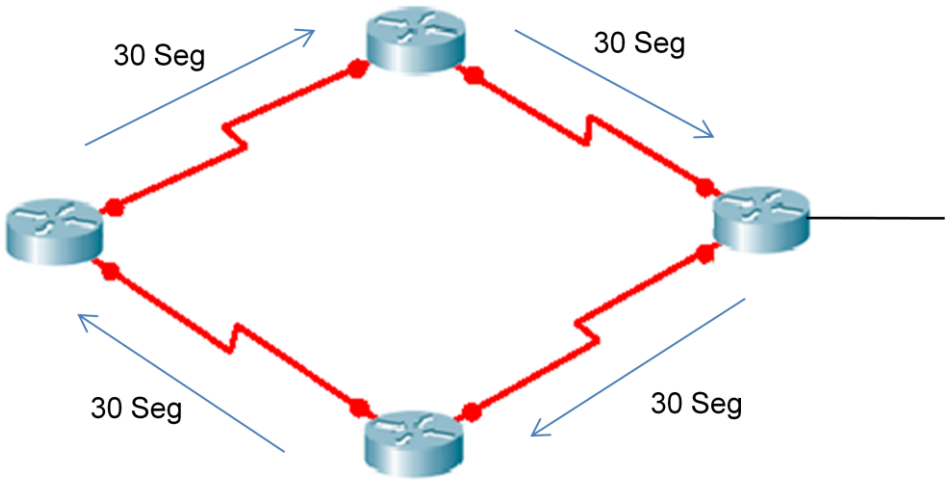


Figura 3.2. Establecer temporizador de espera > 120 segundos.

Para verificar los valores de temporizadores se utiliza el comando **`show ip protocols`**.

```
Router_2811#sh ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 11 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/1       2     2
  Serial0/0/0           2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
     192.168.27.0
     204.200.9.0
Passive Interface(s):
Routing Information Sources:
     Gateway         Distance      Last Update
     192.168.27.249        120      00:00:10
Distance: (default is 120)
```

Para volver a los valores predeterminados de los temporizadores de RIP se ejecuta el comando **`no timers basic`**.

```
Router(config-router)#no timers basic
```

La mayoría de los protocolos de enrutamiento usan una combinación de actualizaciones causadas por eventos (event-driven) o por tiempo (time-driven). RIP es time-driven, pero la implementación Cisco de RIP envía actualizaciones tan pronto se detectan cambios. Cambios en la topología también originan actualizaciones inmediatas en routers IGRP, independientes del valor del temporizador de la actualización; sin actualizaciones event-driven RIP e IGRP no funcionarían adecuadamente. Una vez que se haya actualizado la tabla de enrutamiento por cambios, el router comienza inmediatamente a transmitir las actualizaciones de enrutamiento, a fin de informar estos cambios a los otros routers. Estas actualizaciones, denominadas actualizaciones generadas por eventos, se envían independientemente de las actualizaciones periódicas que envían los routers RIP a intervalos regulares.

3.1.2. INTERFACES PASIVAS

En algunas ocasiones se requiere que los protocolos de enrutamiento no publiquen actualizaciones de enrutamiento desde una interfaz en particular. Cuando se ejecuta un comando **`network`** para una red dada, RIP comenzará inmediatamente a enviar publicaciones hacia todas las interfaces dentro del ámbito de direcciones de red especificado. Para controlar cuáles serán las interfaces que harán intercambio de actualizaciones de enrutamiento el administrador de redes puede inhabilitar el envío de actualizaciones desde las interfaces que desee utilizando el comando **`passive-interface`**.

En RIP cuando se configura una interfaz pasiva esta no puede enviar actualizaciones pero si las puede recibir.

```
RTA(config)#router rip
RTA(config-router)#passive-interface [Default] [Tipo de interfaz numero]
```

Cuando se utiliza el argumento `Default` todas las interfaces se vuelven pasivas. En la figura 3.3 se observa que en el router RTA no es necesario enviar

actualizaciones por la interfaz E0 y que por la interfaz Bri0 no resulta conveniente enviar actualizaciones si se trata de un enlace dial-on-demand[35].

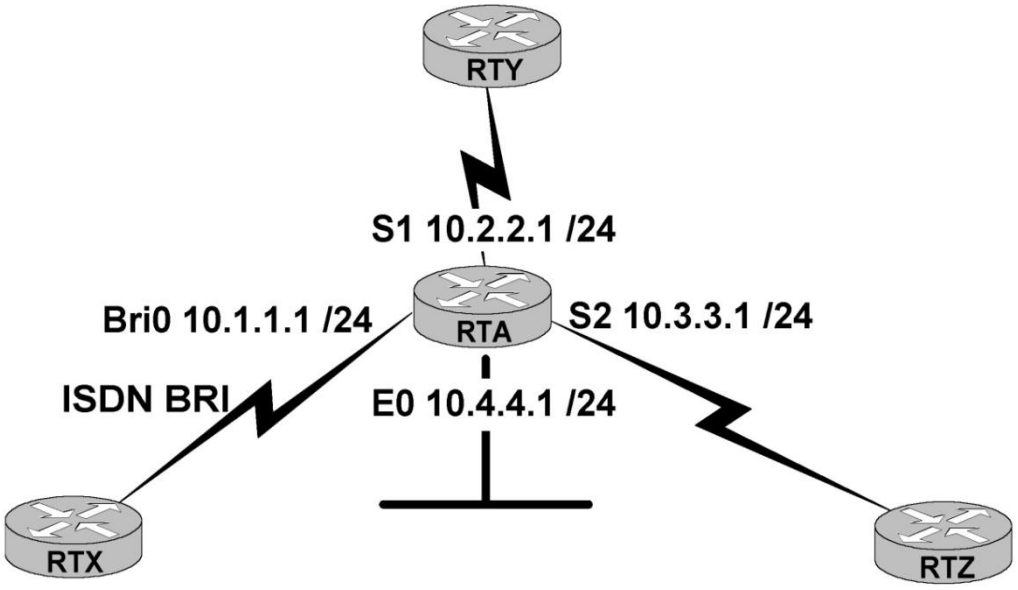


Figura 3.3. Interfaces pasivas en RTA

Otro caso en el que se necesita una interfaz pasiva se observa en la figura 3.4 en donde no tiene ningún caso enviar actualizaciones de enrutamiento hacia el exterior por la interfaz **s 0/0/0** del router **Y**.

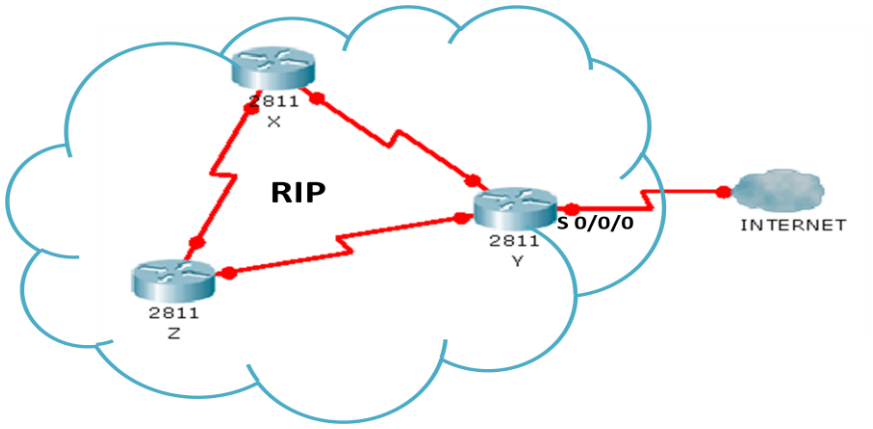


Figura 3.4. Interfaz pasiva al exterior.

[35] Graziani Rick, *CCNP 1 version 3.0*, Ch.8 – Route Optimization.

3.1.3. FILTRADO DE RUTAS

Cuando se configura una interfaz pasiva se evita enviar actualizaciones de enrutamiento por completo, pero hay ocasiones en que se necesita eliminar solo ciertas rutas en las actualizaciones enviadas o recibidas. RIP permite el filtrado de rutas en las interfaces de manera entrante o saliente asociando listas de acceso al protocolo (ACL).

Las ACL son listas de instrucciones que se aplican a una interfaz del router, estas listas indican al router que tipos de paquetes se deben aceptar y cuales se deben denegar. La aceptación y rechazo se pueden basar en ciertas especificaciones, como dirección origen, dirección destino y numero de puerto. Cualquier tráfico que pasa por la interfaz debe cumplir con ciertas condiciones que forman parte de la ACL.

En el siguiente ejemplo (fig. 3.5) la ACL 24 denegara cualquier información de la subred 10.1.1.0 /24, de manera que los routers RTZ y RTY no tendrán información de esta subred, ya que la ACL 24 se aplicara a las actualizaciones de salida del router RTA[36].

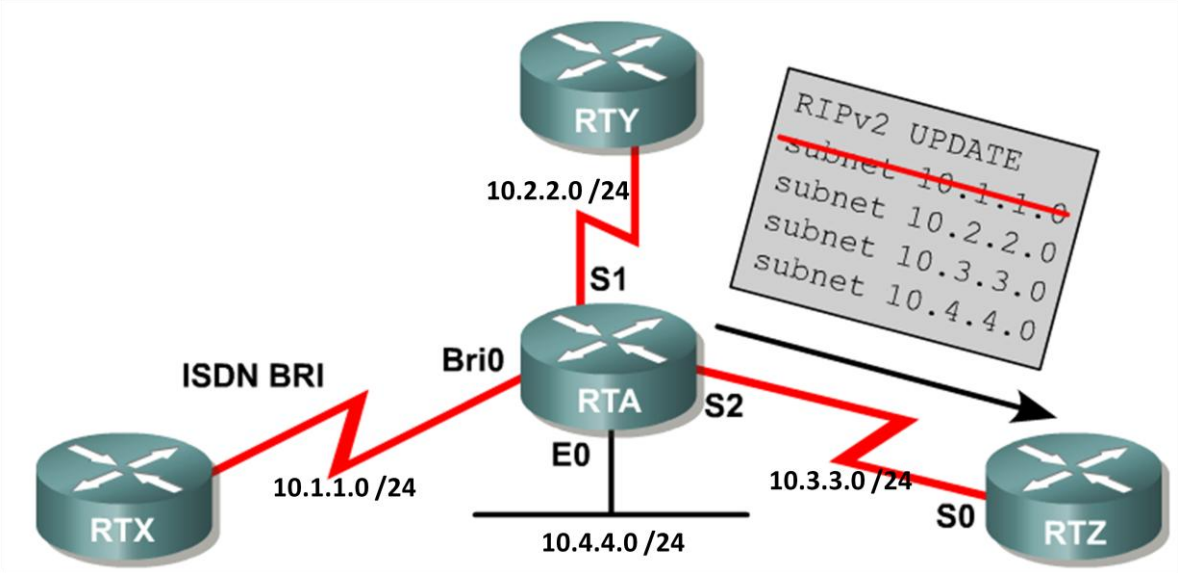


Figura 3.5.Filtro para actualizaciones salientes en RTA.

[36] Ibidem.

```
RTA(config)#router rip
RTA(config-router)#network 10.0.0.0
RTA(config-router)#distribute-list  24 out
RTA(config-router)#exit
RTA(config)#access-list 24 deny 10.1.1.0 0.0.0.255
RTA(config)#access-list 24 permit any
```

La especificación de las interfaces es opcional, si no se detalla dicha información la distribución se aplicará directamente a todas las interfaces, es decir por ninguna interfaz del router se enviaran actualizaciones que contengan rutas filtradas. Cuando este es el caso se dice que es una lista global.

Por otro lado también se puede configurar un router para que no reciba información de ciertas rutas. En la figura 3.6 si se pone la ACL 24 en el router RTZ para las actualizaciones de entrada, el router RTZ no recibirá información de la subred 10.1.1.0/24 por ninguna de sus interfaces.

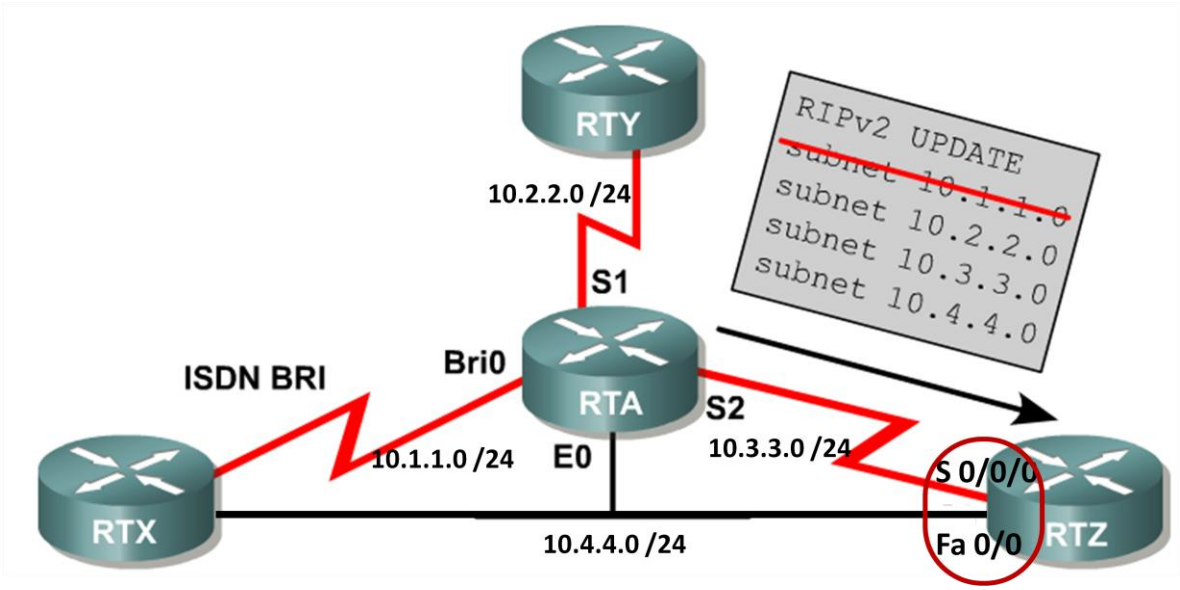


Figura 3.6. Filtro en actualizaciones de entrada en RTZ.

```
RTZ(config)#router rip
RTZ(config-router)#network 10.0.0.0
RTZ(config-router)#distribute-list  24 in
RTZ(config-router)#exit
RTZ(config)#access-list 24 deny 10.1.1.0 0.0.0.255
RTZ(config)#access-list 24 permit any
```

Para que un router filtre información de rutas solo por cierta interfaz, se tiene el siguiente ejemplo (fig. 3.7), en donde el router RTZ solo recibe información de la subred 10.1.1.0/24 por la interfaz Fa 0/0, ya que la ACL 16 deniega la información por la interfaz S 0/0/0.

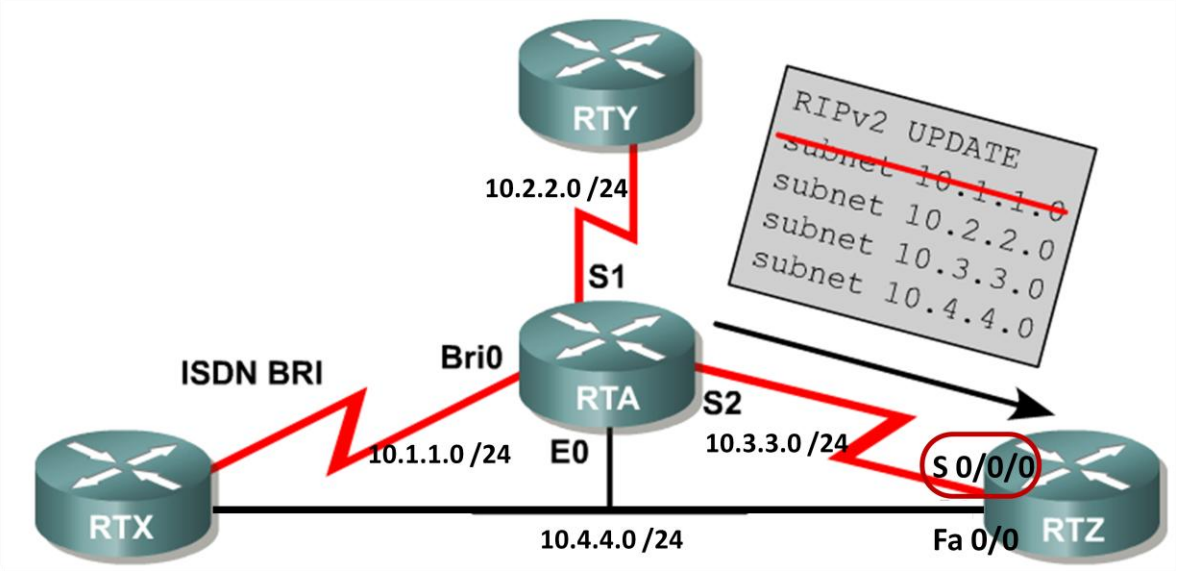


Figura 3.7. Filtro en actualizaciones de entrada para S0/0/0 en RTZ

```
RTZ(config)#router rip
RTZ(config-router)#network 10.0.0.0
RTZ(config-router)#distribute-list  16 in s 0/0/0
RTZ(config-router)#exit
RTZ(config)#access-list 16 deny 10.1.1.0 0.0.0.255
RTZ(config)#access-list 16 permit any
```

En el ejemplo de la figura 3.8 se han creado dos listas de acceso estándar, la ACL 10 denegará cualquier información de enrutamiento de la red 192.168.20.0, mientras que la ACL 20 no enviará información de enrutamiento RIP de la red 10.1.1.0/24 por la interfaz S 0/1/0.

```
RTA#configure terminal
RTA(config)#access-list 10 deny 192.168.20.0 0.0.0.255
RTA(config)#access-list 10 permit any
RTA(config)#access-list 20 deny 10.1.1.0 0.0.0.255
RTA(config)#access-list 20 permit any
```

```
RTA(config)#router rip
RTA(config-router)#distribute-list 10 in Serial 0/0/0
RTA(config-router)#distribute-list 20 out Serial 0/1/0
RTA(config-router)#network 172.16.0.0
RTA(config-router)#network 192.168.10.0
RTA(config-router)#network 10.1.1.0
```

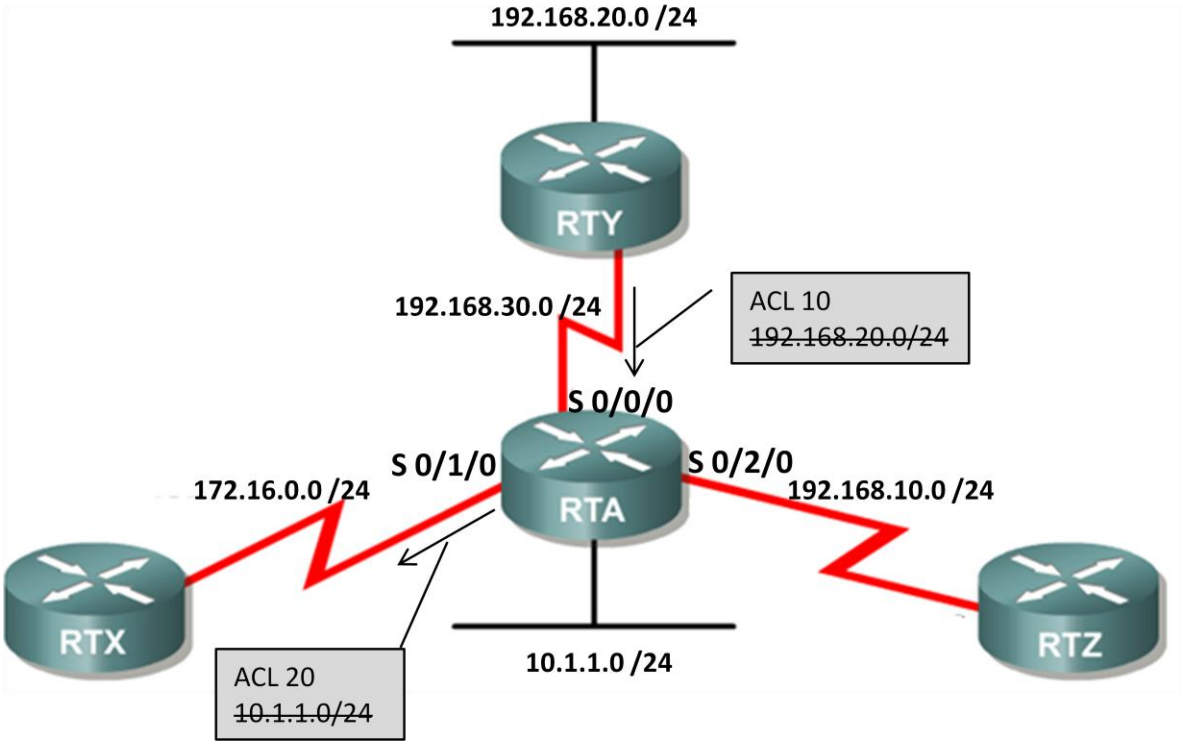


Figura 3.8. Filtros específicos en RTA.

Para cada interface y proceso de enrutamiento el cisco IOS permite:

- Asignar una lista global entrante.
- Asignar una lista global saliente.
- Asignar una lista entrante para interfaz.
- Asignar una lista saliente para interfaz.

```
RTZ(config)#router rip
RTZ(config-router)#distribute-list 1 in
RTZ(config-router)#distribute-list 2 out
RTZ(config-router)#distribute-list 3 in fa0/0
RTZ(config-router)#distribute-list 4 out s0/0/0
```

3.1.4. REDISTRIBUCIÓN ESTÁTICA EN RIP

Cuando un sistema autónomo posee una sola puerta de entrada/salida se puede configurar una ruta estática o una ruta estática por defecto de manera que todos los paquetes que quieran llegar a múltiples redes externas lo hagan por medio de esta ruta preestablecida.

Para que todos los routers contenidos dentro del mismo sistema autónomo tengan conocimiento de la existencia de esa ruta es necesario redistribuirla dentro del protocolo. Esto se hace con el comando **`redistribute static metric`** ***`[metrica]`*** o con **`default-information originate`** si la ruta es estática por defecto. En el ejemplo de la figura 3.9 se ha configurado una ruta estática por defecto, que sale a través de la interfaz S0/0/0 del router Y, además se ha desactivado esta interfaz para que no transmita información del protocolo hacia el exterior.

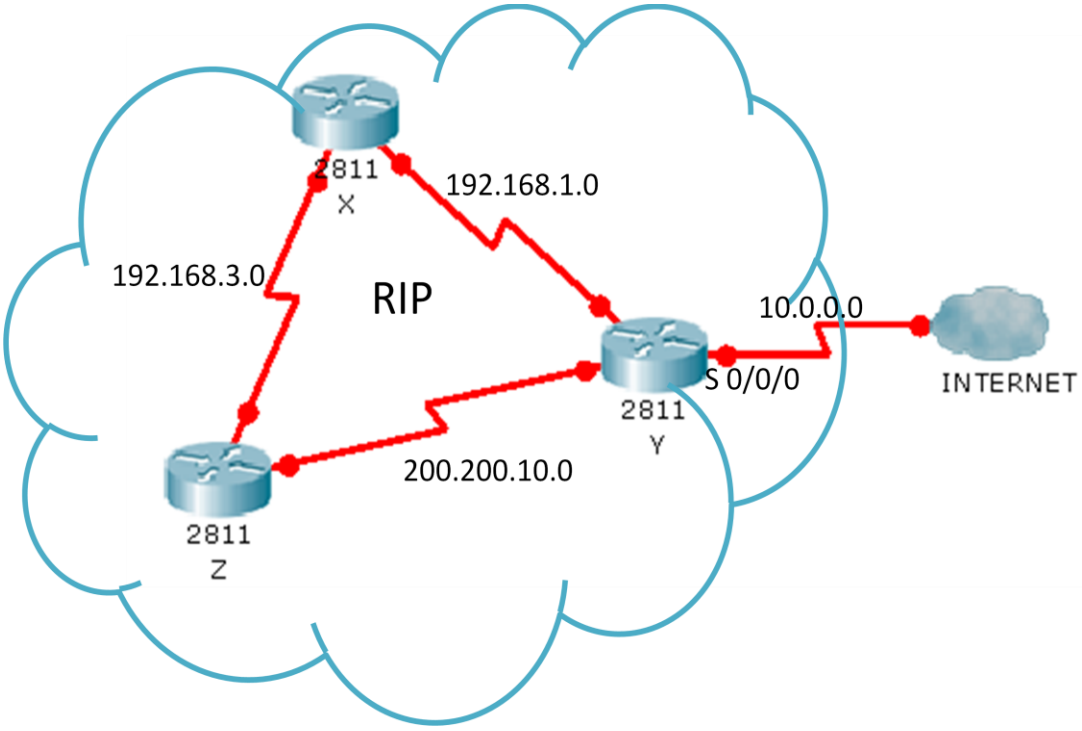


Figura 3.9. Ruta estática por defecto e interfaz pasiva al exterior.

```
RTY(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

```
RTY(config)#router rip
RTY(config-router)#version 2
RTY(config-router)#network 192.168.1.0
RTY(config-router)#network 200.200.10.0
RTZ(config-router)#default-information originate
RTZ(config-router)#passive-interface serial 0/0/0
```

3.1.5. AUTENTICACIÓN EN RIP

RIP versión 2 permite la autenticación entre routers para no incluir actualizaciones no autorizadas, tanto en texto plano como en encriptación MD5.

Autenticación en texto simple:

```
Router(config)#interface [tipo] [numero]
Router(config-if)#ip rip authentication key-chain [nombre]
Router(config-if)#ip rip authentication mode text
```

Autenticación en md5:

```
Router(config)#interface [tipo] [numero]
Router(config-if)#ip rip authentication key-chain [nombre]
Router(config-if)#ip rip authentication mode md5
```

3.1.6. VERIFICACIÓN DE LA CONFIGURACIÓN DE RIP

Existen diversos comandos que se pueden utilizar para verificar que RIP este correctamente configurado. El comando **`show ip protocols`** muestra los protocolos que se están ejecutando en el router. En el caso de RIP se observa la configuración de los temporizadores, los filtros aplicados a las interfaces, redistribuciones, la versión que se está utilizando, sumarizaciones, redes asociadas, las puertas de enlace y la distancia administrativa.

```
Router_2811#sh ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
```

```
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/1        2     2
  Serial0/0/0            2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
     192.168.27.0
     204.200.9.0
Passive Interface(s):
Routing Information Sources:
     Gateway         Distance      Last Update
     192.168.27.249       120      00:00:13
Distance: (default is 120)
```

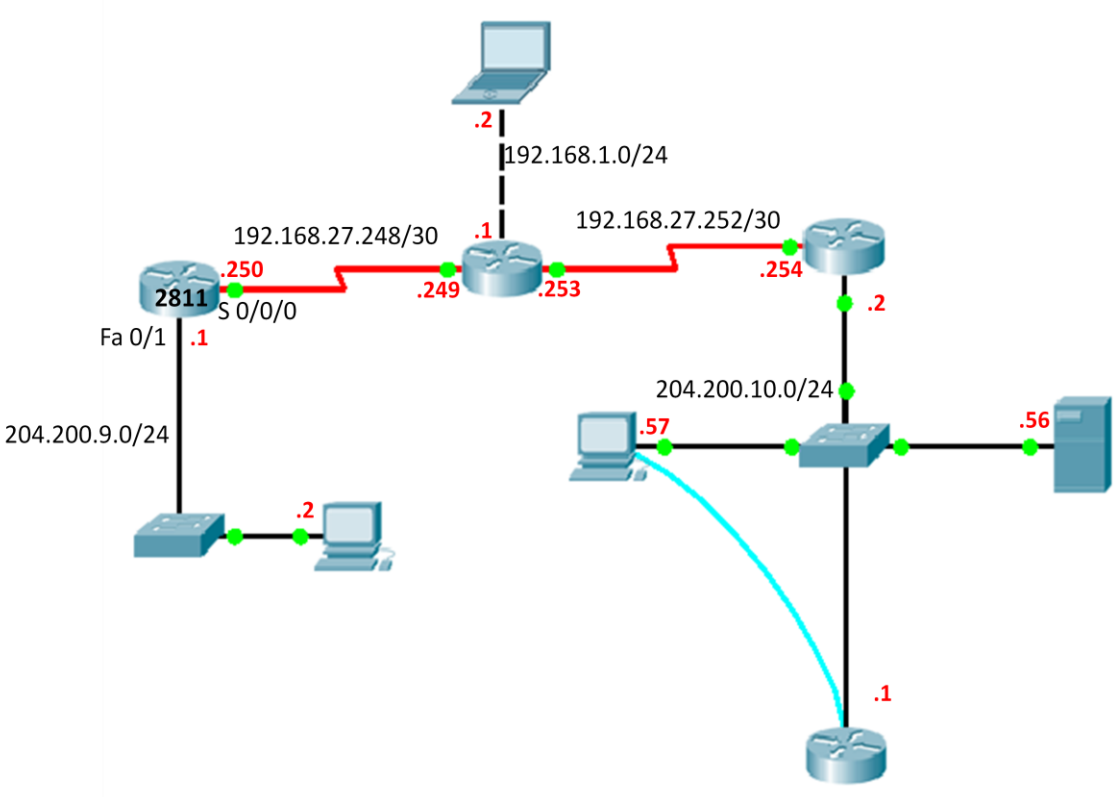


Figura 3.10. Escenario para comandos de verificación RIP.

El comando **`show ip route rip`** muestra la tabla de enrutamiento RIP en la que se pueden observar las redes que son aprendidas por el protocolo, entre

corchetes la distancia administrativa y la métrica, la dirección IP por la cual conoce a dicha red, tiempo de actualización y la interfaz por donde recibió la información.

```
Router_2811#show ip route rip
R    192.68.1.0/24 [120/1] via 192.168.27.249, 00:00:17, Serial0/0/0
     192.168.27.0/30 is subnetted, 2 subnets
R       192.168.27.252 [120/1] via 192.168.27.249, 00:00:17, Serial0/0/0
R    204.200.10.0/24 [120/2] via 192.168.27.249, 00:00:17, Serial0/0/0
```

El comando **debug ip rip** muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe. Existen varios indicadores clave a inspeccionar en el resultado de este comando, problemas tales como subredes discontinuas o redes duplicadas pueden ser diagnosticadas. Un síntoma de estos problemas sería que un router publicara una ruta con una métrica más baja que la métrica que recibió de la red.

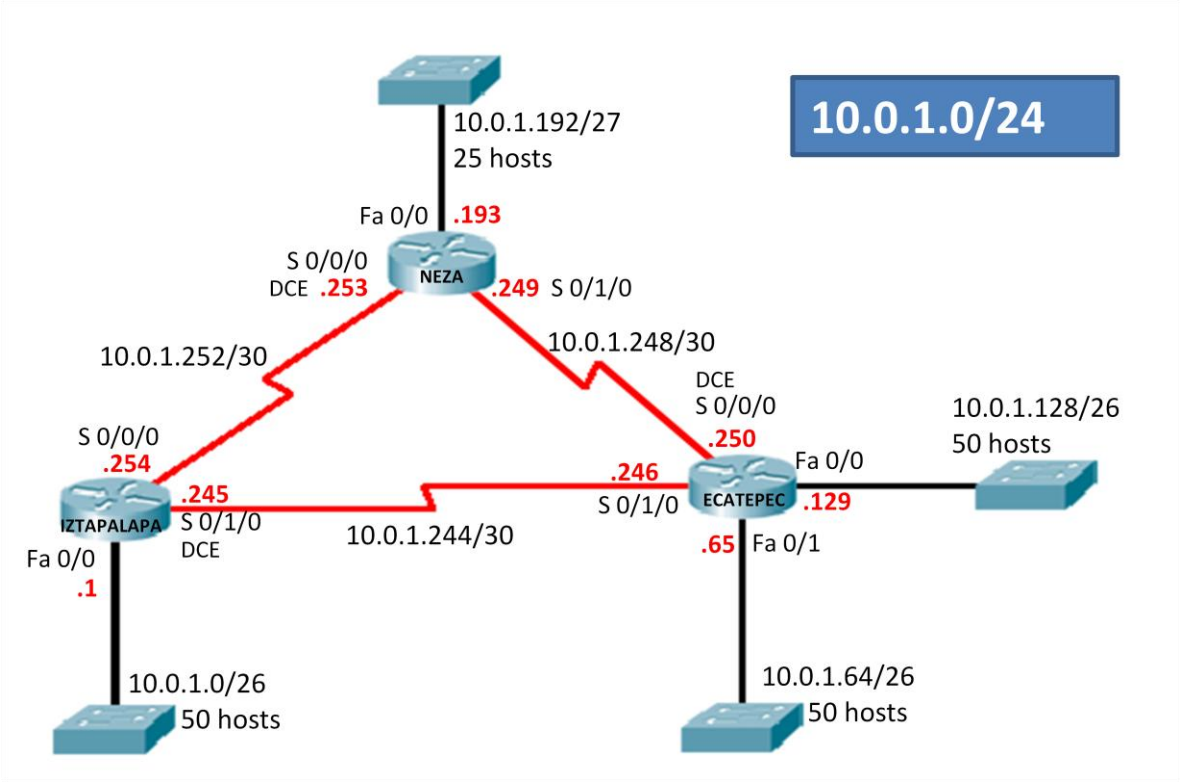
```
Router_2811#debug ip rip
RIP protocol debugging is on
Router_2811#RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/1
(204.200.9.1)
RIP: build update entries
      192.68.1.0/24 via 0.0.0.0, metric 2, tag 0
      192.168.27.0/24 via 0.0.0.0, metric 1, tag 0
      204.200.10.0/24 via 0.0.0.0, metric 3, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (192.168.27.250)
RIP: build update entries
      204.200.9.0/24 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 192.168.27.249 on Serial0/0/0
      192.68.1.0/24 via 0.0.0.0 in 1 hops
      192.168.27.252/30 via 0.0.0.0 in 1 hops
      204.200.10.0/24 via 0.0.0.0 in 2 hops
RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/1 (204.200.9.1)
RIP: build update entries
      192.68.1.0/24 via 0.0.0.0, metric 2, tag 0
      192.168.27.0/24 via 0.0.0.0, metric 1, tag 0
      204.200.10.0/24 via 0.0.0.0, metric 3, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (192.168.27.250)
```

Cuando se utiliza algún comando **debug** el router muestra en tiempo real los procesos que se están ejecutando, este tipo de comandos es útil para verificar el funcionamiento del router, pero, además de que utiliza recursos del router, los

resultados que constantemente muestra pueden resultar incómodos si se continua realizando otras configuraciones. Para desactivar un comando **debug** se antepone la palabra **no** al comando **debug** que se quiera desactivar y para desactivar todos los comandos **debug** que se estén ejecutando se utiliza el comando **undebug all.**

```
Router_2811#no debug ip rip
Router_2811#undebug all
```

EJEMPLO PRÁCTICO 3.1



- **Paso 1.**Se deben realizar las configuraciones básicas en los routers, es decir, la asignación de nombre, contraseñas y direcciones IP de las interfaces.

Para el router neza:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname neza
neza(config)#enable secret fes
neza(config)#line vty 0 4
neza(config-line)#password unam
neza(config-line)#login
neza(config-line)#line con 0
neza(config-line)#password unam
neza(config-line)#login
neza(config-line)#exit
neza(config)#interface fastethernet 0/0
neza(config-if)#ip address 10.0.1.193 255.255.255.224
neza(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
neza(config-if)#interface serial 0/0/0
neza(config-if)#ip address 10.0.1.253 255.255.255.252
neza(config-if)#clock rate 250000
neza(config-if)#bandwidth 250
neza(config-if)#no shutdown

neza(config-if)#interface serial 0/1/0

%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
%LINK-5-CHANGED:  Interface  Serial0/0/0,  changed  state  to
upneza(config-if)#ip address 10.0.1.249 255.255.255.252
neza(config-if)#bandwidth 250
neza(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
neza(config-if)#exit
neza(config)#
```

Para el router iztapalapa:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname iztapalapa
iztapalapa(config)#enable secret fes
iztapalapa(config)#line vty 0 4
iztapalapa(config-line)#password unam
iztapalapa(config-line)#login
iztapalapa(config-line)#line con 0
iztapalapa(config-line)#password unam
iztapalapa(config-line)#login
iztapalapa(config-line)#exit
iztapalapa(config)#interface fastethernet 0/0
iztapalapa(config-if)#ip address 10.0.1.1 255.255.255.192
iztapalapa(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
iztapalapa(config-if)#interface serial 0/0/0
iztapalapa(config-if)#ip address 10.0.1.254 255.255.255.252
iztapalapa(config-if)#bandwidth 250
iztapalapa(config-if)#no shutdown

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

```
iztapalapa(config-if)#interface serial 0/1/0
iztapalapa(config-if)#ip address 10.0.1.245 255.255.255.252
iztapalapa(config-if)#clock rate 250000
iztapalapa(config-if)#bandwidth 250
iztapalapa(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
iztapalapa(config-if)#exit
iztapalapa(config)#
```

Para el router ecatepec:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ecatepec
ecatepec(config)#enable secret fes
ecatepec(config)#line vty 0 4
ecatepec(config-line)#password unam
ecatepec(config-line)#login
ecatepec(config-line)#line con 0
ecatepec(config-line)#password unam
ecatepec(config-line)#login
ecatepec(config-line)#exit
ecatepec(config)#interface fastethernet 0/0
ecatepec(config-if)#ip address 10.0.1.129 255.255.255.192
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
ecatepec(config-if)#interface fastethernet 0/1
ecatepec(config-if)#ip address 10.0.1.65 255.255.255.192
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/1, changed state to up
ecatepec(config-if)#interface serial 0/1/0
ecatepec(config-if)#ip address 10.0.1.246 255.255.255.252
ecatepec(config-if)#bandwidth 250
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
ecatepec(config-if)#interface serial 0/0/0
ecatepec(config-if)#ip address 10.0.1.250 255.255.255.252
ecatepec(config-if)#clock rate 250000
ecatepec(config-if)#bandwidth 250
```

```
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ecatepec(config-if)#exit
ecatepec(config)#
```

- **Paso 2.** Se debe verificar que las interfaces utilizadas de cada router estén activas.

Para el router neza:

```
neza#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.0.1.193      YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/0/0            10.0.1.253      YES manual up                    up

Serial0/1/0            10.0.1.249      YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
neza#
```

Para el router iztapalapa:

```
iztapalapa#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.0.1.1        YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/0/0            10.0.1.254      YES manual up                    up

Serial0/1/0            10.0.1.245      YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
iztapalapa#
```

Para el router ecatepec:

```
ecatepec#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.0.1.129      YES manual up                    up

FastEthernet0/1        10.0.1.65       YES manual up                    up

Serial0/0/0            10.0.1.250      YES manual up                    up

Serial0/1/0            10.0.1.246      YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
ecatepec#
```

- **Paso 3.** Se configura el protocolo RIP versión 2 y se anuncian las redes que se encuentran conectadas a cada router. Como RIP v2 soporta VLSM y en este ejemplo utilizamos la red 10.0.0.0 subneteada basta con anunciar esta red en cada router.

Para el router neza:

```
neza(config)#router rip
neza(config-router)#version 2
neza(config-router)#network 10.0.0.0
neza(config-router)#
```

Para el router iztapalapa:

```
iztapalapa(config)#router rip
iztapalapa(config-router)#version 2
iztapalapa(config-router)#network 10.0.0.0
iztapalapa(config-router)#
```

Para el router ecatepec:

```
ecatepec(config)#router rip
ecatepec(config-router)#version 2
ecatepec(config-router)#network 10.0.0.0
ecatepec(config-router)#
```

- **Paso 4.** Se checan las tablas de enrutamiento que se crean en cada router.

Para el router neza:

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
R       10.0.1.0/26 [120/1] via 10.0.1.254, 00:00:00, Serial0/0/0
R       10.0.1.64/26 [120/1] via 10.0.1.250, 00:00:02, Serial0/1/0
R       10.0.1.128/26 [120/1] via 10.0.1.250, 00:00:02, Serial0/1/0
C       10.0.1.192/27 is directly connected, FastEthernet0/0
R       10.0.1.244/30 [120/1] via 10.0.1.250, 00:00:02, Serial0/1/0
                      [120/1] via 10.0.1.254, 00:00:00, Serial0/0/0
C       10.0.1.248/30 is directly connected, Serial0/1/0
C       10.0.1.252/30 is directly connected, Serial0/0/0
```

En esta tabla de enrutamiento se observa que RIP establece dos rutas para la red 10.0.1.244/30 ya que tienen la misma métrica.

Para el router iztapalapa:

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
C       10.0.1.0/26 is directly connected, FastEthernet0/0
R       10.0.1.64/26 [120/1] via 10.0.1.246, 00:00:15, Serial0/1/0
R       10.0.1.128/26 [120/1] via 10.0.1.246, 00:00:15, Serial0/1/0
R       10.0.1.192/27 [120/1] via 10.0.1.253, 00:00:24, Serial0/0/0
```

```
C       10.0.1.244/30 is directly connected, Serial0/1/0
R       10.0.1.248/30 [120/1] via 10.0.1.253, 00:00:24, Serial0/0/0
                      [120/1] via 10.0.1.246, 00:00:15, Serial0/1/0
C       10.0.1.252/30 is directly connected, Serial0/0/0
```

Para el router ecatepec:

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
R       10.0.1.0/26 [120/1] via 10.0.1.245, 00:00:20, Serial0/1/0
C       10.0.1.64/26 is directly connected, FastEthernet0/1
C       10.0.1.128/26 is directly connected, FastEthernet0/0
R       10.0.1.192/27 [120/1] via 10.0.1.249, 00:00:04, Serial0/0/0
C       10.0.1.244/30 is directly connected, Serial0/1/0
C       10.0.1.248/30 is directly connected, Serial0/0/0
R       10.0.1.252/30 [120/1] via 10.0.1.245, 00:00:20, Serial0/1/0
                      [120/1] via 10.0.1.249, 00:00:04, Serial0/0/0
```

- **Paso 5.** Se activa el **`debug ip rip`** en el router Ecatepec para observar los procesos que están sucediendo.

```
ecatepec#debug ip rip
RIP protocol debugging is on
ecatepec#RIP: received v2 update from 10.0.1.245 on Serial0/1/0
      10.0.1.0/26 via 0.0.0.0 in 1 hops
      10.0.1.192/27 via 0.0.0.0 in 2 hops
      10.0.1.252/30 via 0.0.0.0 in 1 hops
RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/0 (10.0.1.129)
RIP: build update entries
      10.0.1.0/26 via 0.0.0.0, metric 2, tag 0
      10.0.1.64/26 via 0.0.0.0, metric 1, tag 0
      10.0.1.192/27 via 0.0.0.0, metric 2, tag 0
      10.0.1.244/30 via 0.0.0.0, metric 1, tag 0
      10.0.1.248/30 via 0.0.0.0, metric 1, tag 0
      10.0.1.252/30 via 0.0.0.0, metric 2, tag 0
```

```
RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/1 (10.0.1.65)
RIP: build update entries
      10.0.1.0/26 via 0.0.0.0, metric 2, tag 0
      10.0.1.128/26 via 0.0.0.0, metric 1, tag 0
      10.0.1.192/27 via 0.0.0.0, metric 2, tag 0
      10.0.1.244/30 via 0.0.0.0, metric 1, tag 0
      10.0.1.248/30 via 0.0.0.0, metric 1, tag 0
      10.0.1.252/30 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.0.1.250)
RIP: build update entries
      10.0.1.0/26 via 0.0.0.0, metric 2, tag 0
      10.0.1.64/26 via 0.0.0.0, metric 1, tag 0
      10.0.1.128/26 via 0.0.0.0, metric 1, tag 0
      10.0.1.244/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/1/0 (10.0.1.246)
RIP: build update entries
      10.0.1.64/26 via 0.0.0.0, metric 1, tag 0
      10.0.1.128/26 via 0.0.0.0, metric 1, tag 0
      10.0.1.192/27 via 0.0.0.0, metric 2, tag 0
      10.0.1.248/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.0.1.249 on Serial0/0/0
      10.0.1.0/26 via 0.0.0.0 in 2 hops
      10.0.1.192/27 via 0.0.0.0 in 1 hops
      10.0.1.252/30 via 0.0.0.0 in 1 hops
```

De las actualizaciones de enrutamiento que envía y recibe se observa que:

- RIP versión 2 envía sus actualizaciones de enrutamiento en multicast con la dirección Clase D 224.0.0.9 y que también se envían actualizaciones por las interfaces Fastethernet, aunque en este caso no sea necesario.
- El router Iztapalapa anuncia una ruta para la subred 10.0.1.192/27 con una métrica de 2.
- El router Neza anuncia una ruta para la subred 10.0.1.192/27 con una métrica de 1.

➢ **Paso 6.** Se desactivara el enlace entre el router Ecatepec y el router Neza y se observara como quedan las tablas de enrutamiento.

Para desactivar el enlace, se desactiva la interfaz S 0/0/0 del router Ecatepec:

```
ecatepec(config)#interface s 0/0/0
ecatepec(config-if)#shutdown

%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
ecatepec(config-if)#
```

La tabla de enrutamiento para el router Ecatepec queda:

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
R       10.0.1.0/26 [120/1] via 10.0.1.245, 00:00:20, Serial0/1/0
C       10.0.1.64/26 is directly connected, FastEthernet0/1
C       10.0.1.128/26 is directly connected, FastEthernet0/0
R       10.0.1.192/27 [120/2] via 10.0.1.245, 00:00:20, Serial0/1/0
C       10.0.1.244/30 is directly connected, Serial0/1/0
R       10.0.1.252/30 [120/1] via 10.0.1.245, 00:00:20, Serial0/1/0
```

Se observa que ahora se instala una ruta para la subred 10.0.1.192/27 con una métrica de 2 y que ahora solo hay una ruta para la subred 10.0.1.252/30.

La tabla de enrutamiento para el router Iztapalapa queda:

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

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C       10.0.1.0/26 is directly connected, FastEthernet0/0
R       10.0.1.64/26 [120/1] via 10.0.1.246, 00:00:20, Serial0/1/0
R       10.0.1.128/26 [120/1] via 10.0.1.246, 00:00:20, Serial0/1/0
R       10.0.1.192/27 [120/1] via 10.0.1.253, 00:00:26, Serial0/0/0
C       10.0.1.244/30 is directly connected, Serial0/1/0
C       10.0.1.252/30 is directly connected, Serial0/0/0
```

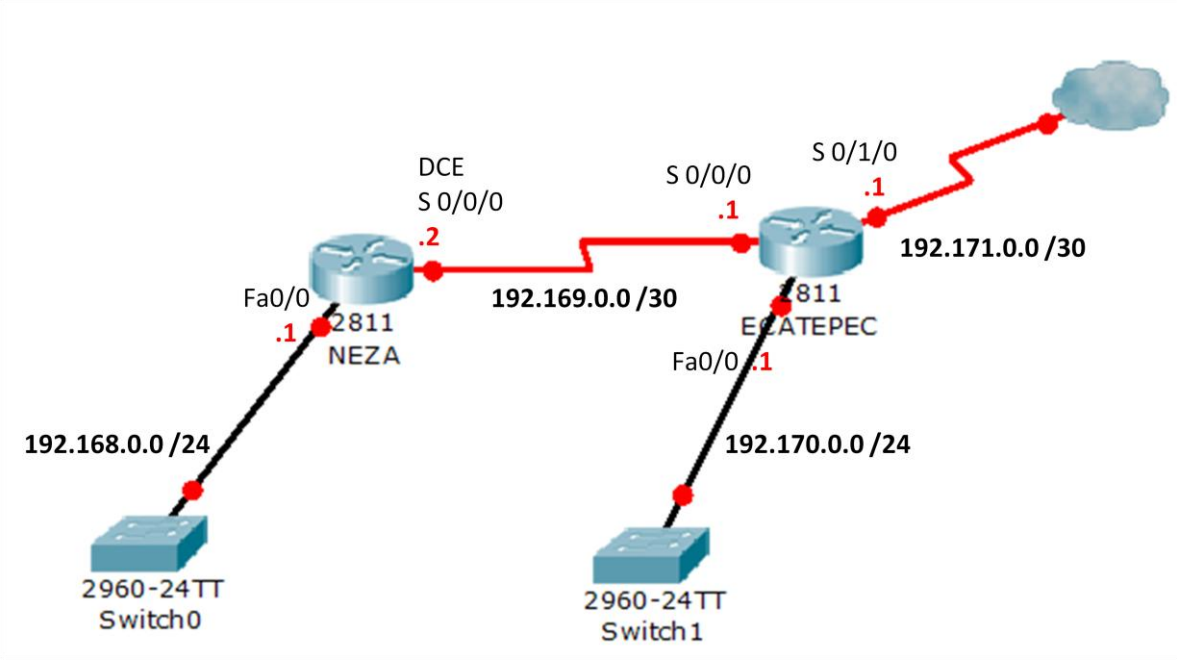
En esta tabla se observa que ya no se tiene ninguna ruta para la subred 10.0.1.248/30.

La tabla de enrutamiento para el router Neza queda:

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
R       10.0.1.0/26 [120/1] via 10.0.1.254, 00:00:09, Serial0/0/0
R       10.0.1.64/26 [120/2] via 10.0.1.254, 00:00:09, Serial0/0/0
R       10.0.1.128/26 [120/2] via 10.0.1.254, 00:00:09, Serial0/0/0
C       10.0.1.192/27 is directly connected, FastEthernet0/0
R       10.0.1.244/30 [120/1] via 10.0.1.254, 00:00:09, Serial0/0/0
C       10.0.1.252/30 is directly connected, Serial0/0/0
```

Se observa que ahora se instalan rutas para las subredes 10.0.1.64/26 y 10.0.1.128/26 con una métrica de 2 y que ahora solo hay una ruta para la subred 10.0.1.244/30.

EJEMPLO PRÁCTICO 3.2



- **Paso 1.** Se realizan las configuraciones básicas en los routers, es decir, la asignación de nombre, contraseñas y direcciones IP de las interfaces.

Para el router Neza:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname neza
neza(config)#enable secret fes
neza(config)#line vty 0 4
neza(config-line)#password unam
neza(config-line)#login
neza(config-line)#line con 0
neza(config-line)#password unam
neza(config-line)#login
neza(config-line)#exit
neza(config)#interface fastethernet 0/0
neza(config-if)#ip address 192.168.0.1 255.255.255.0
neza(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
neza(config-if)#interface serial 0/0/0
neza(config-if)#ip address 192.169.0.2 255.255.255.252
neza(config-if)#clock rate 250000
neza(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
neza(config-if)#exit
```

Para el router Ecatepec:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ecatepec
ecatepec(config)#enable secret fes
ecatepec(config)#line vty 0 4
ecatepec(config-line)#password unam
ecatepec(config-line)#login
ecatepec(config-line)#line con 0
ecatepec(config-line)#password unam
ecatepec(config-line)#login
ecatepec(config-line)#exit
ecatepec(config)#interface fastethernet 0/0
ecatepec(config-if)#ip address 192.170.0.1 255.255.255.0
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
ecatepec(config-if)#interface serial 0/0/0
ecatepec(config-if)#ip address 192.169.0.1 255.255.255.252
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ecatepec(config-if)#interface serial 0/1/0
ecatepec(config-if)#ip address 192.171.0.1 255.255.255.252
ecatepec(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
ecatepec(config-if)#exit
```

- **Paso 2.** Se debe verificar que las interfaces utilizadas de cada router estén activas.

Para el router Neza:

```
neza#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.0.1     YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/0/0            192.169.0.2     YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
```

Para el router Ecatepec:

```
ecatepec#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.170.0.1     YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/0/0            192.169.0.1     YES manual up                    up

Serial0/1/0            192.171.0.1     YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
```

- **Paso 3.** Se configura el protocolo RIP versión 2 y se anuncian las redes que se encuentran conectadas a cada router. En el router Ecatepec no será anunciada la subred 192.171.0.0/30.

Para el router Neza:

```
neza(config)#router rip
neza(config-router)#v 2
neza(config-router)#network 192.168.0.0
neza(config-router)#network 192.169.0.0
neza(config-router)#exit
neza(config)#
```

Para el router Ecatepec:

```
ecatepec(config)#router rip
ecatepec(config-router)#v 2
ecatepec(config-router)#network 192.169.0.0
ecatepec(config-router)#network 192.170.0.0
ecatepec(config-router)#exit
ecatepec(config)#
```

- **Paso 4.** Se configura una ruta estática por defecto que salga por la interfaz s0/1/0 del router Ecatepec y se redistribuye dentro de RIP. También se configura esta interfaz como pasiva para no enviar actualizaciones al exterior.

```
ecatepec(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0
ecatepec(config)#router rip
ecatepec(config-router)#default-information originate
ecatepec(config-router)#passive-interface serial 0/1/0
ecatepec(config-router)#exit
```

- **Paso 5.** Se checan las tablas de enrutamiento.

Para el router Neza:

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

Gateway of last resort is 192.169.0.1 to network 0.0.0.0

C    192.168.0.0/24 is directly connected, FastEthernet0/0
     192.169.0.0/30 is subnetted, 1 subnets
C       192.169.0.0 is directly connected, Serial0/0/0
R    192.170.0.0/24 [120/1] via 192.169.0.1, 00:00:22, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 192.169.0.1, 00:37:44, Serial0/0/0
```

En esta tabla se observa que la ruta estática por defecto fue aprendida por RIP.

Para el router Ecatepec:

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R    192.168.0.0/24 [120/1] via 192.169.0.2, 00:00:26, Serial0/0/0
     192.169.0.0/30 is subnetted, 1 subnets
C       192.169.0.0 is directly connected, Serial0/0/0
C    192.170.0.0/24 is directly connected, FastEthernet0/0
     192.171.0.0/30 is subnetted, 1 subnets
C       192.171.0.0 is directly connected, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

- **Paso 6.** Se configura la autenticación.

```
neza(config)#key chain privado
neza(config-keychain)#key 1
neza(config-keychain-key)#key string 214
neza(config-keychain-key)#exit
neza(config-keychain)#exit
neza(config)#interface s 0/0/0
neza(config-if)#ip rip authentication key-chain privado
neza(config-if)#ip rip authentication mode md5
```

```
ecatepec(config)#key chain privado
ecatepec(config-keychain)#key 1
ecatepec(config-keychain-key)#key string 214
ecatepec(config-keychain-key)#exit
ecatepec(config-keychain)#exit
ecatepec(config)#interface s 0/0/0
ecatepec(config-if)#ip rip authentication key-chain privado
ecatepec(config-if)#ip rip authentication mode md5
```

Se utiliza autenticación md5 que proporciona un nivel más alto de seguridad que el texto plano. El key number y el key string deben ser iguales en ambos lados, en caso contrario la autenticación fallara.

3.2. EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL)

El protocolo de enrutamiento de gateway interior mejorado (Enchaced Interior Gateway Routing Protocol, EIGRP) es una versión mejorada del protocolo IGRP orginal desarrollado por Cisco Systems y fue lanzado en 1994.

EIGRP admite CIDR y VLSM, lo que permite que los diseñadores de red maximicen el espacio de direccionamiento. En comparación con IGRP, que es un protocolo de enrutamiento con clase, EIGRP ofrece tiempos de convergencia más rápidos, mejor escalabilidad y gestión superior de los bucles de enrutamiento. EIGRP funciona en las redes IPX y AppleTalk con potente eficiencia.

EIGRP se considera como un protocolo de enrutamiento híbrido que ofrece lo mejor de los algoritmos de vector-distancia y de estado de enlace. EIGRP es un protocolo de enrutamiento avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones incrementales parciales y la detección de vecinos, se usan de forma similar con EIGRP. Sin embargo, EIGRP es más fácil de configurar que OSPF. EIGRP es una opción ideal para las grandes redes multiprotocolo construidas con routers Cisco[37].

Las comparaciones entre EIGRP e IGRP se pueden dividir en las siguientes categorías principales:

- Modo de compatibilidad
- Cálculo de métrica
- Número de saltos
- Redistribución automática de protocolos
- Etiquetado de rutas

[37] Clare Gough, *CCNP BSCI Exam Certification Guide*, p445.

IGRP y EIGRP son compatibles entre sí. Esta compatibilidad ofrece una interoperabilidad transparente con los routers IGRP, esto es importante, dado que los usuarios, pueden aprovechar los beneficios de ambos protocolos. EIGRP ofrece compatibilidad multiprotocolo, mientras que IGRP no lo hace.

EIGRP e IGRP usan cálculos de métrica diferentes, EIGRP multiplica la métrica de IGRP por un factor de 256. Esto ocurre porque EIGRP usa una métrica que tiene 32 bits de largo, e IGRP usa una métrica de 24 bits. La información EIGRP puede multiplicarse o dividirse por 256 para un intercambio fácil con IGRP.

IGRP tiene un número de saltos máximo de 255. El límite máximo para el número de saltos en EIGRP es 224. Esto es más que suficiente para admitir grandes redes.

IGRP	EIGRP
Protocolo de enrutamiento con clase	Protocolo de enrutamiento sin clase • VLSM, CIDR
bandwidth = (10,000,000/*bandwidth kbps*) delay = *delay*/10 24 bits utilizados para la métrica y el retardo	bandwidth = (10,000,000/*bandwidth kbps*) * 256 delay = (*delay*/10) * 256 32 bits utilizados para la métrica y el retardo
Máximo número de saltos= 255	Máximo número de saltos = 224
No puede diferenciar entre rutas internas y externas.	Las rutas que no se originan en los routers EIGRP son etiquetadas como externas.
Redistribución automática entre IGRP y EIGRP siempre que el número de "AS" sea el mismo.	

Tabla 3.1 Características de IGRP y EIGRP

Se requiere una configuración avanzada para permitir que protocolos de enrutamiento diferentes como OSPF y RIP compartan información. La redistribución o la capacidad para compartir rutas, es automática entre EIGRP e IGRP siempre y cuando ambos procesos usen el mismo número AS. En este caso, EIGRP rotula como externas las rutas aprendidas de IGRP (o cualquier otra fuente externa porque

no se originan en los routers EIGRP), en cambio IGRP no puede diferenciar entre rutas internas y externas.

Como en el caso del protocolo IGRP, EIGRP publica la información de la tabla de enrutamiento sólo a los routers vecinos. EIGRP mantiene las siguientes tres tablas[38]:

- Tabla de vecinos
- Tabla de topología
- Tabla de enrutamiento

La tabla de vecinos es la más importante de EIGRP, cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

La tabla de topología se compone de todas las tablas de enrutamiento EIGRP en el sistema autónomo. DUAL (algoritmo de actualización difusa) toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino.

Los routers vecinos se descubren por medio de un protocolo Hello sencillo intercambiado por los routers que pertenecen a la misma red física estableciendo adyacencias. Hello se utiliza para intercambiar paquetes de saludo una dirección multicast 224.0.0.10. Los hellos se envían por defecto cada cinco segundos. Una vez descubiertos los routers vecinos, EIGRP utiliza un protocolo de transporte fiable para garantizar la entrega correcta y ordenada de la información y las actualizaciones de la tabla de enrutamiento.

Un router hace el seguimiento de sus propias rutas conectadas y, además, de todas las rutas públicas de los routers vecinos. Basándose en esta información,

[38] Ibidem, p.452.

EIGRP puede seleccionar eficaz y rápidamente la ruta de menor coste hasta un destino y garantizar que la ruta no forma parte de un bucle de enrutamiento. Esta ruta elegida como principal será la llamada Sucesor. Al almacenar la información de enrutamiento de los routers vecinos, el algoritmo puede determinar con mayor rapidez una ruta de sustitución o un Sucesor factible en caso de que haya un fallo de enlace o cualquier otro evento de modificación de la topología.

El Protocolo de Transporte Confiable (RTP) es un protocolo de capa de transporte que garantiza la entrega ordenada de paquetes EIGRP a todos los vecinos. En una red IP, los hosts usan TCP para secuenciar los paquetes y asegurarse de que se entreguen de manera oportuna. Sin embargo, EIGRP es independiente de los protocolos. Esto significa que no se basa en TCP/IP para intercambiar información de enrutamiento de la forma en que lo hacen RIP, IGRP y OSPF. Para mantenerse independiente de IP, EIGRP usa RTP como su protocolo de capa de transporte propietario para garantizar la entrega de información de enrutamiento. EIGRP puede hacer una llamada a RTP para que proporcione un servicio confiable o no confiable, según lo requiera la situación. Por ejemplo, los paquetes hello no requieren el gasto de la entrega confiable porque se envían con frecuencia y se deben mantener pequeños. La entrega confiable de otra información de enrutamiento puede realmente acelerar la convergencia porque entonces los routers EIGRP no tienen que esperar a que un temporizador expire antes de retransmitir.

Cuando existen cambios de topologías EIGRP recurre a DUAL (algoritmo de actualización difusa) para conseguir una rápida convergencia entre los routers, estos almacenan sus propias tablas de enrutamiento con rutas alternativas (Sucesor factible); si no existiera alguna ruta alternativa, EIGRP recurre a sus routers vecinos para conseguir información acerca de ese camino alternativo.

3.2.1. MÉTRICAS EIGRP

EIGRP e IGRP utilizan una métrica de enrutamiento compuesta. La ruta que posea la métrica más baja será considerada la ruta óptima. Las métricas de EIGRP e IGRP están asociadas mediante constantes desde K1 hasta K5 que convierten los vectores de métrica EIGRP en cantidades escalables.

La métrica utilizada por EIGRP e IGRP se compone de:

- **K1→Ancho de banda:** valor mínimo de ancho de banda en Kbps en la ruta hacia el destino.
- **K2→Fiabilidad:** fiabilidad entre el origen y el destino, determinado por el intercambio de mensajes de actividad expresado en porcentajes.
- **K3→Retraso:** retraso de interfaz acumulado a lo largo de la ruta en microsegundos.
- **K4→Carga:** carga de un enlace entre el origen y el destino. Medido en bits por segundo es el ancho de banda real de la ruta.
- **K5→MTU:** valor de la unidad máxima de transmisión de la ruta expresado en bytes.

EIGRP e IGRP usan el siguiente cálculo de métrica:

$$Métrica = \left[K1 * AnchodeBanda + \frac{K2 * AnchodeBanda}{256 - carga} + K3 * Retardo \right] * \left[\frac{K5}{Confiabilidad + K4} \right]$$

Los valores por default de las constantes son:

```
K1=1, K2=0, K3=1, K4=0, K5=0
```

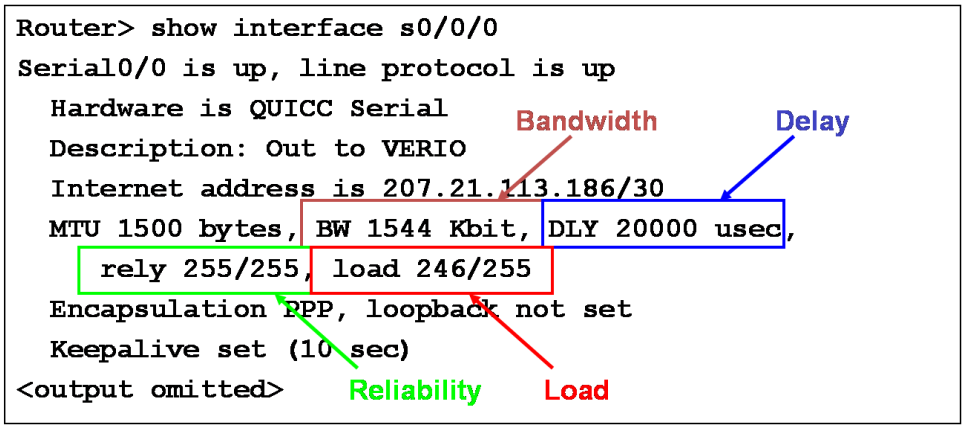
Si estas constantes mantienen sus valores por default, el cálculo para obtener la métrica queda:

$$Métrica = AnchodeBanda + Retardo$$

La métrica EIGRP se calcula en base a las variables resultantes de las constantes Kl y K3. El valor mínimo de ancho de banda se divide por 10^7 multiplicado por 256, mientras que el retraso es la sumatoria de todos los retrasos de la ruta en microsegundos multiplicado por 256.

Ancho de Banda para IGRP=10000000/AnchodeBandakbps
*Ancho de Banda para EIGRP=(10000000/AnchodeBandakbps)*256*
Retraso para IGRP=delay/10
*Retraso para EIGRP= delay/10*256*

Los valores que son utilizados para calcular la métrica pueden observarse al ejecutar el comando `show interface`.



La confiabilidad (reliability) se muestra como una fracción de 255 y entre más grande es mejor:

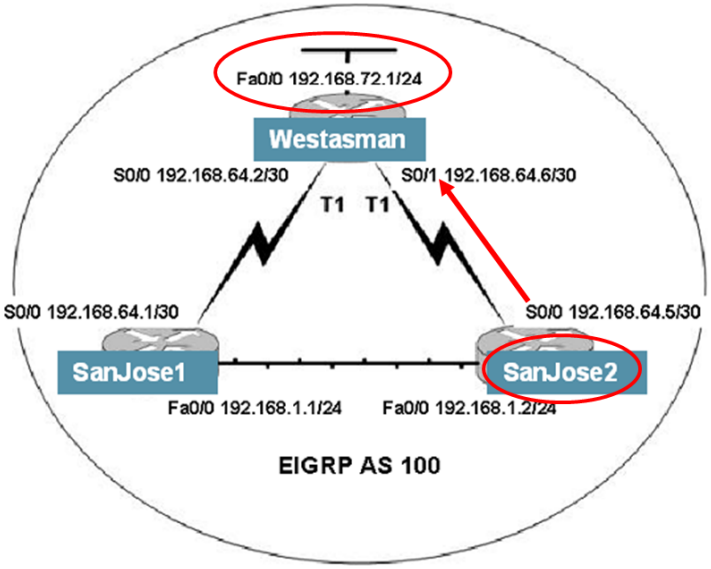
rely 190/255= 74% confiabilidad
rely 255/255= 100% confiabilidad

La carga (load) también se muestra como una fracción de 255 y entre más pequeña es mejor:

load 10/255 = 3% de carga

load 255/255 = 100% de carga

A continuación se muestra un ejemplo para calcular la métrica EIGRP para una ruta determinada. Lo que se muestra es como el router San José 2 calcula la métrica para la ruta mostrada[39].



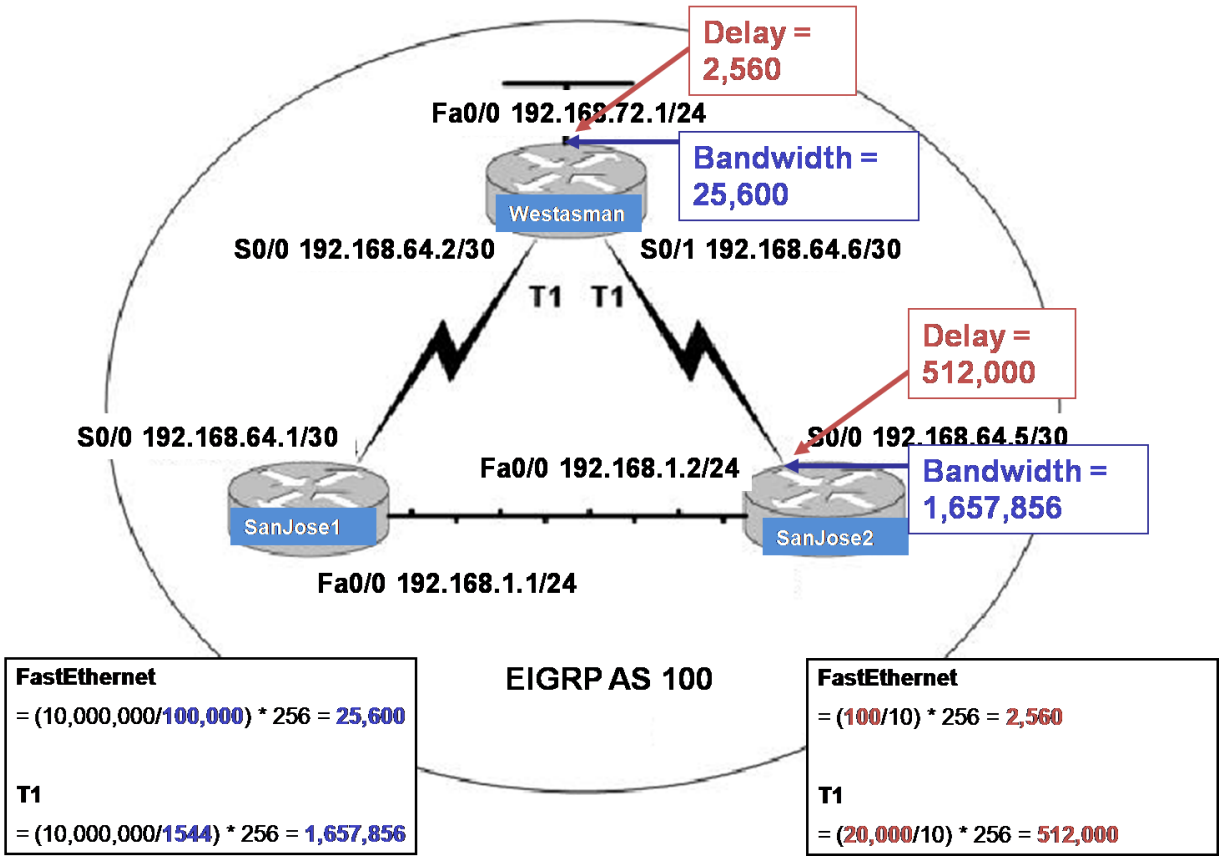

```
SanJose2#show ip route                    Administrative Distance / Metric
D    192.168.72.0/24 [90/2172416]
           via 192.168.64.6, 00:28:26, Serial0/0
```

```
Westasman> show interface fa0/0
Ethernet0 is up, line protocol is up
  Hardware   is   Lance,   address   is   0010.7b3a.cf84   (bia
0010.7b3a.cf84)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     rely 255/255, load 1/255
<output omitted>
```

```
SanJose2> show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is QUICC Serial
  Description: Out to Westasman
```

[39] Graziani Rick, *CCNP 1 version 3.0*, Ch.5 – EIGRP.

```
  Internet address is 192.168.64.5/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     rely 255/255, load 246/255
<output omitted>
```



Como se vio anteriormente, para hacer el cálculo de la métrica se toma el valor obtenido con el menor ancho de banda y se le suman todos los retardos a lo largo de la ruta:

Métrica= 1657856 + 512000 + 2560 = 2172416

```
SanJose2#show ip route
D    192.168.72.0/24 [90/2172416]
           via 192.168.64.6, 00:28:26, Serial0
```

Los valores de las constantes **K** pueden ser modificados con el siguiente comando:

```
Router(config-router)#metric weights tos k1 k2 k3 k4 k5
```

El argumento **tos** (type of service) debe ser siempre cero. Si se desea restablecer los valores por default se utiliza el siguiente comando:

```
Router(config-router)#no metric weights
```

3.2.2. CONFIGURACIÓN DE EIGRP

En el proceso de configuración de EIGRP se debe especificar el número de Sistema Autónomo (AS) que identificará al conjunto de routers que participan de ese mismo protocolo, posteriormente asociar las redes o subredes directamente conectadas, y los parámetros opcionales si así se requiriera.

```
router(config)#router eigrp [sistema autónomo]
router(config-router)#network [dirección de red]
router(config-router)#eigrp log-neighbor-changes
```

El comando **eigrp log-neighbor-changes** habilita el registro de los cambios de adyacencia de vecinos para monitorear la estabilidad del sistema de enrutamiento y para ayudar a detectar problemas.

Al configurar los enlaces seriales mediante EIGRP, es importante configurar el valor del ancho de banda en la interfaz. Si el ancho de banda de estas interfaces no se modifica, EIGRP supone el ancho de banda por defecto en el enlace en lugar del verdadero ancho de banda, si el enlace es más lento, es posible que el router no pueda convergir, que se pierdan las actualizaciones de enrutamiento o se produzca una selección de rutas por debajo de la óptima. Para establecer el ancho de banda para la interfaz, se aplica la siguiente sintaxis:

```
router(config)#interface [tipo] [número]
router(config-if)#bandwidth [kilobits]
```

En versiones actuales de IOS se puede especificar una wildcard de tal manera que identifique si se trata de una red o subred la que deba anunciarse.

```
router(config)#router eigrp [sistema autónomo]
router(config-router)#network [dirección de red] [wildcard]
```

3.2.3. RESUMEN DE RUTA EIGRP

EIGRP resume automáticamente las rutas en el límite con clase. Este es el límite donde termina la dirección de red, de acuerdo con la definición del direccionamiento basado en clase. Esto significa que, en la figura 3.11, aunque el RouterC esté conectado a la subred 2.1.1.0 solamente, publicará que está conectada a toda la red Clase A, 2.0.0.0. En la mayoría de los casos, el resumen automático es beneficioso porque mantiene las tablas de enrutamiento lo más compactas posible.

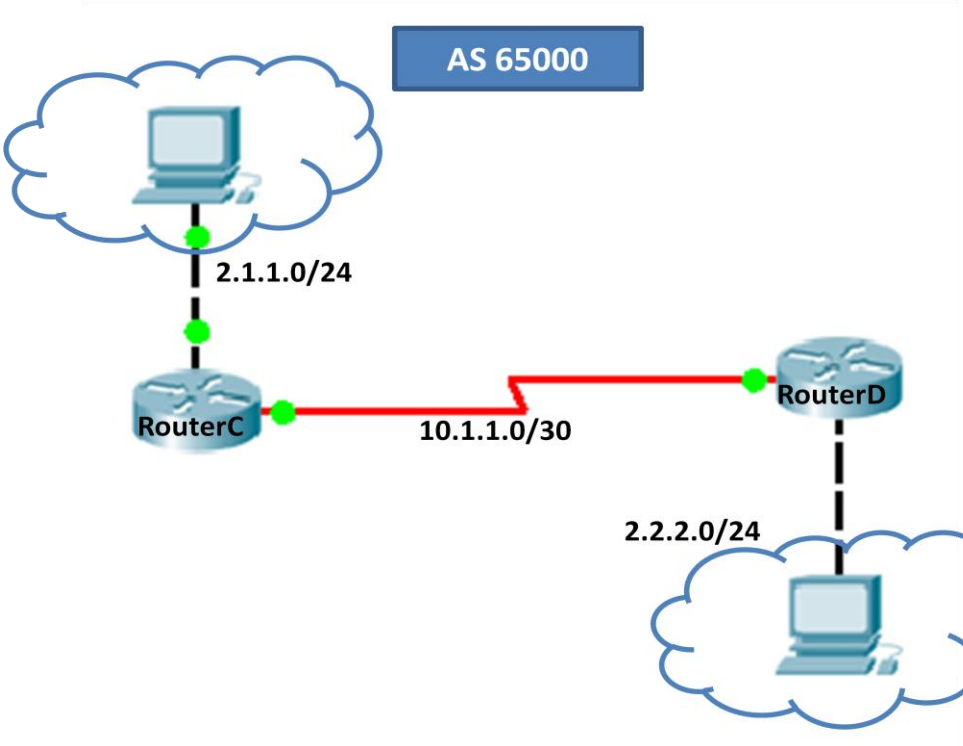


Figura 3.11. El router C publicará que está conectada a toda la red Clase A, 2.0.0.0.

Sin embargo, es posible que el resumen automático no sea la mejor opción en ciertos casos. Por ejemplo, si existen subredes no contiguas el resumen automático, debe deshabilitarse para que el enrutamiento funcione correctamente. Para deshabilitar el resumen automático, use el siguiente comando:

```
router(config-router)#no auto-summary
```

Con EIGRP, una dirección de resumen se puede configurar manualmente al configurar una red prefijo. Las rutas de resumen manuales se configuran por interfaz, de manera que la interfaz que propagará el resumen de ruta se debe seleccionar primero. Entonces, la dirección de resumen se puede definir con el siguiente comando:

```
router(config-if)#ip summary-address eigrp [sistema autónomo]
[dirección de red – mascara] [distancia administrativa]
```

Las rutas de resumen EIGRP tienen una distancia administrativa por defecto de 5. De manera opcional, se pueden configurar con un valor entre 1 y 255.

En la figura 3.11, RouterC se puede configurar mediante los comandos que aparecen a continuación:

```
RouterC(config)#router eigrp 65000
RouterC(config-router)#no auto-summary
RouterC(config-router)#exit
RouterC(config)#interface serial 0/0/0
RouterC(config-if)#ip summary-address eigrp 65000 2.1.0.0 255.255.0.0
```

Con esto el RouterC agrega una ruta a esta tabla de la siguiente manera:

```
RouterC#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
D       2.0.0.0/8 [90/20514560] via 10.1.1.2, 00:00:42, Serial0/0/0
D       2.1.0.0/16 is a summary, 00:00:42, Null0
C       2.1.1.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
```

Se observa que la ruta de resumen se obtiene a partir de **Null0** y no de una interfaz real. Esto ocurre porque esta ruta se usa para fines de publicación y no representa una ruta que el RouterC puede tomar para alcanzar esa red. En el RouterC, esta ruta tiene una distancia administrativa de 5.

El RouterD no es consciente del resumen pero acepta la ruta. A la ruta se le asigna la distancia administrativa de una ruta EIGRP normal que es 90 por defecto.

En la configuración del RouterC, el resumen automático se desactiva con el comando **no auto-summary**. Si no se desactivara el resumen automático, RTD recibiría dos rutas, la dirección de resumen manual, que es 2.1.0.0 /16, y la dirección de resumen automática con clase, que es 2.0.0.0/8.

En la mayoría de los casos, cuando se hace el resumen manual, se debe ejecutar el comando **no auto-summary**.

3.2.4. EQUILIBRADO DE CARGA

El equilibrado de carga en los routers con rutas de coste equivalente suele ser por defecto de un máximo de cuatro. El equilibrado puede modificarse hasta un máximo de seis rutas. EIGRP puede a su vez equilibrar tráfico por múltiples rutas con diferentes métricas utilizando un multiplicador de varianza, por defecto el valor de la

varianza es uno equilibrando la carga por costes equivalentes, este multiplicador puede tomar valores desde 1 hasta 128.

```
Router(config)#router eigrp [sistema autónomo]
Router(config-router)#network [dirección de red]
Router(config-router}#maximum-paths [número maximo]
Router(config-Router}#variance [métrica] [multiplicador]
```

Si el multiplicador es mayor que 1, el proceso EIGRP lo multiplica por el valor de la mejor métrica a un destino y las rutas hacia ese destino que tengan un valor inferior al obtenido son incluidas en la tabla de enrutamiento para el balanceo de carga. La cantidad de tráfico enviado por cada ruta es proporcional al valor de la métrica de la ruta[40].

3.2.5. TEMPORIZADORES

Los intervalos de hello y hold por defecto mantienen los valores de 5 y 15 segundos respectivamente. Estos valores pueden modificarse dentro de las respectivas interfaces tomando en cuenta que deben ser iguales para todos los routers del sistema autónomo.

```
Router(config-if}#ip hello-interval eigrp [sistema autónomo] [segundos]
Router(config-if}#ip hold-time eigrp [sistema autónomo] [segundos]
```

3.2.6. INTERFACES PASIVAS

Para impedir que una interfaz envíe publicaciones de enrutamiento EIGRP se puede desactivar la interfaz dentro del protocolo especificando el tipo y número de dicha interfaz.

```
Router(config)#router eigrp [sistema autónomo]
Router(config-router}#passive-interface [tipo] [número]
```

[40] Clare Gough, *CCNP BSCI Exam Certification Guide*, p485.

Cuando se configura una interfaz pasiva en EIGRP, esta deja de enviar mensajes Hello, cuando esto ocurre el router no puede formar adyacencias con los routers vecinos por dicha interfaz, por lo tanto la interfaz pasiva no puede enviar ni recibir actualizaciones de enrutamiento[41].

3.2.7. FILTRADOS DE RUTAS

EIGRP permite el filtrado de rutas en las interfaces de manera entrante o saliente asociando Listas de acceso al protocolo.

```
Router(config}#router eigrp [sistema autónomo]
Router(config-router)#distribute-list [número de lista][in/out][interfaz]
```

En el siguiente ejemplo de la figura 3.12 el router RTZ solo recibe información de la subred 10.1.1.0/24 por la interfaz Fa 0/0, ya que la ACL 16 deniega la información por la interfaz S 0/0/0.

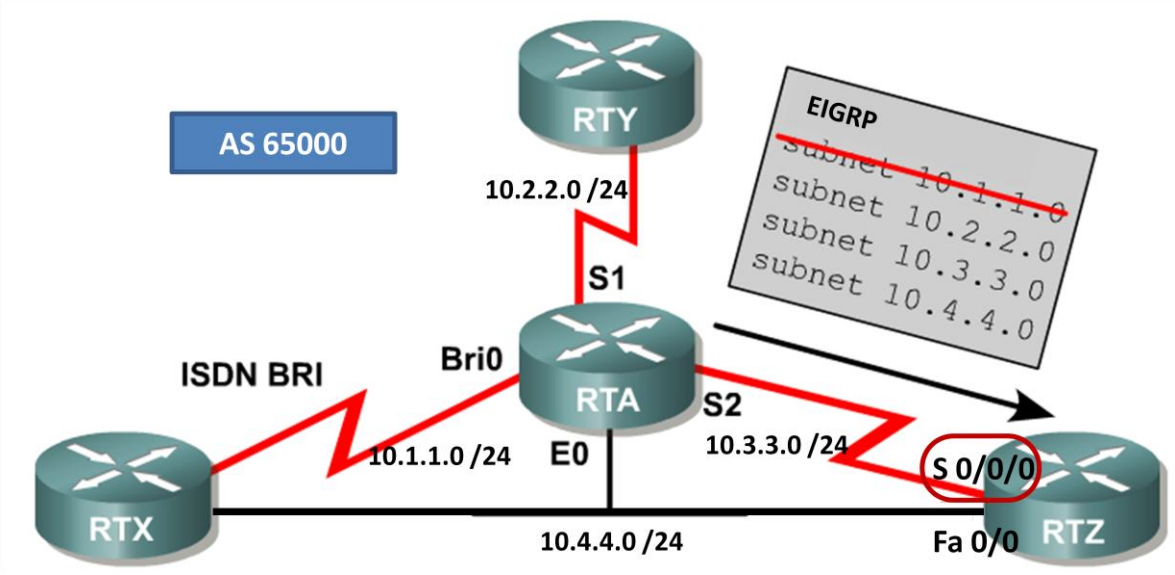


Figura 3.12. Filtro en actualizaciones de entrada para S0/0/0 en RTZ.

[41] Graziani Rick, *CCNP 1 version 3.0*, Ch.8 – Route Optimization.

```
RTZ(config)#router eigrp 65000
RTZ(config-router)#network 10.0.0.0
RTZ(config-router)#distribute-list  16 in s 0/0/0
RTZ(config-router)#exit
RTZ(config)#access-list 16 deny 10.1.1.0 0.0.0.255
RTZ(config)#access-list 16 permit any
```

3.2.8. REDISTRIBUCIÓN ESTÁTICA EN EIGRP

EIGRP redistribuye rutas aprendidas estáticamente dirigidas hacia un destino particular o por defecto.

```
Router(config)#ip route [red mascara] [dirección IP/interfaz] [distancia]
Router(config)#router eigrp [sistema autónomo]
Router(config-router)#redistribute static
```

En el comando **ip route**, se puede utilizar la interfaz de salida o la IP del próximo salto. En el ejemplo de la figura 3.13 se ha configurado una ruta estática por defecto, que sale a través de la interfaz S0/0/0 del router Y, además se ha desactivado esta interfaz para que no transmita información del protocolo hacia el exterior.

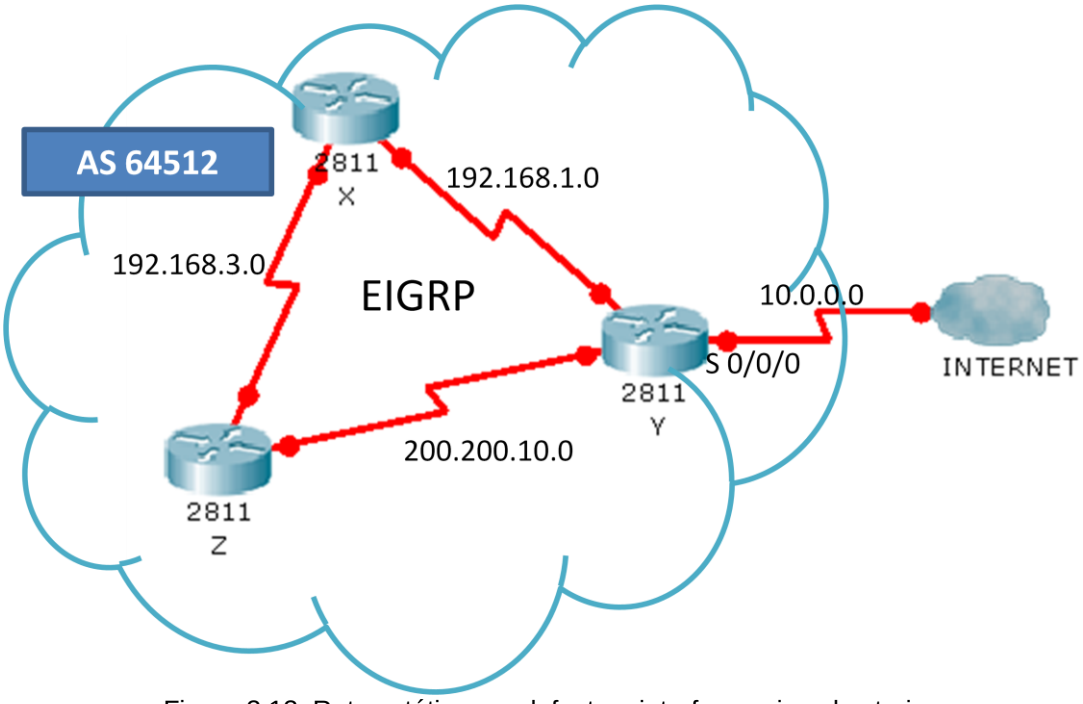


Figura 3.13. Ruta estática por defecto e interfaz pasiva al exterior.

```
RTY(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
RTY(config)#router eigrp 64512
RTY(config-router)#network 192.168.1.0
RTY(config-router)#network 200.200.10.0
RTZ(config-router)#redistribute static
RTZ(config-router)#passive-interface serial 0/0/0
```

Anteriormente se vio que cuando no se especifica una distancia administrativa en el comando **`ip route`**, esta por default es 1 para una ruta estática.

3.2.9. AUTENTICACIÓN EIGRP

La autenticación EIGRP comienza creando una cadena de claves, numerarla y asociarla con la clave correspondiente. Posteriormente se puede configurar un sistema seguro de encriptación como MD5 dentro de la interfaz y habilitar la autenticación dentro de la misma interfaz.

```
Router(config)#key chain [nombre]
Router(config-keychain)#key [número]
Router(config-keychain-key)#key-string [nombre]
Router(config-keychain-key)#exit
Router(config-keychain)#exit
Router(config)#interface [tipo] [número]
Router(config-if)#ip authentication mode eigrp [sistema autónomo] md5
Router(config-if)#ip authentication key-chain eigrp [sistema autónomo]
[nombre de la cadena]
```

3.2.10. VERIFICACIÓN EIGRP

- **`show ip eigrp neighbors [intefaz|numero de AS|static|detail]`**: Muestra la tabla de vecinos EIGRP. Los argumentos son opcionales y sirven para mostrar los vecinos por una interfaz y de un sistema autónomo en específico. La palabra clave **`static`** muestra rutas estáticas y la palabra **`detail`** expande el resultado.

```
RouterC#show ip eigrp neighbors
IP-EIGRP neighbors for process 65000
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   2.3.3.1         Fa0/1           10   00:00:27  40     1000  0   13
1   10.1.1.2        Se0/0/0         11   00:00:21  40     1000  0   5
```

- **show ip eigrp interfaces *[intefaz] [numero de AS]*:** Muestra información de las interfaces EIGRP. Los argumentos son opcionales y sirven para mostrar una interfaz y/o un sistema autónomo en específico.

```
RouterC#show ip eigrp interfaces
IP-EIGRP interfaces for process 65000

                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface       Peers Un/Reliable SRTT   Un/Reliable  Flow Timer   Routes
Fa0/0             0       0/0     1236       0/10          0          0
Fa0/1             1       0/0     1236       0/10          0          0
Se0/0/0           1       0/0     1236       0/10          0          0
```

- **show ip eigrp topology *[numero de AS* | *[[direccion ip] mascara]]* *[active* | *all-links* | *pending* | *summary* | *zero-successors]:*** Muestra todos los sucesores factibles en la tabla de topología EIGRP. Todos los argumentos son opcionales y se describen en la siguiente tabla:

numero de AS	Numero de Sistema Autónomo.
direccion ip	Dirección IP, cuando esta se especifica con una mascara, una detallada descripción de la entrada es proporcionada.
Mascara	Mascara de subred.
Active	Muestra solo entradas activas en la tabla de topología EIGRP.
all-links	Muestra todas las entradas en la tabla de topología EIGRP.

Pending	Muestra todas las entradas en la tabla de topología EIGRP que están esperando por una actualización de un vecino o están esperando responder a un vecino.
Summary	Muestra un resumen de la tabla de topología.
zero-successors	Muestra rutas disponibles en la tabla de topología.

Tabla 3.2 Parámetros del comando *show ip eigrp topology*

```
RouterC#show ip eigrp topology
IP-EIGRP Topology Table for AS 65000

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - Reply status

P 2.1.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 2.3.3.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 10.1.1.0/30, 1 successors, FD is 20512000
         via Connected, Serial0/0/0
P 2.2.2.0/24, 1 successors, FD is 20514560
         via 10.1.1.2 (20514560/28160), Serial0/0/0
P 10.1.1.4/30, 1 successors, FD is 20514560
         via 2.3.3.1 (20514560/20512000), FastEthernet0/1
         via 10.1.1.2 (21024000/20512000), Serial0/0/0
```

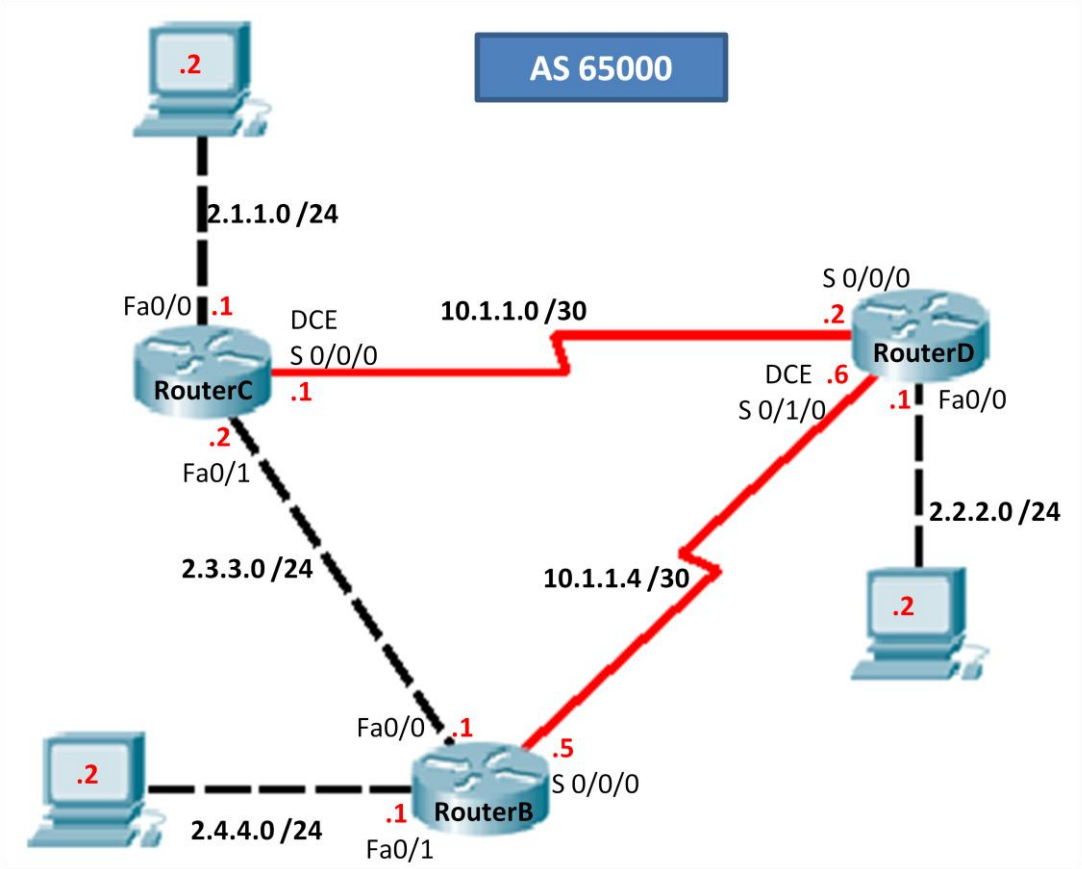
- **show ip eigrp traffic *[numero de AS]***: Muestra el número de paquetes EIGRP que son enviados y recibidos. El argumento es opcional y sirve para mostrar el tráfico de un sistema autónomo en específico.

```
RouterC#show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 65000
  Hellos sent/received: 425/280
  Updates sent/received: 10/10
  Queries sent/received: 0/0
  Replies sent/received:  0/0
  Acks sent/received:  9/8
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
```

- **`debug eigrp fsm:`** Muestra la actividad del sucesor factible EIGRP para ayudar a determinar si el proceso de enrutamiento esta instalando y borrando las actualizaciones de ruta.

- **`debug eigrp packet:`** Muestra la transmisión y recepción de paquetes EIGRP. Este tipo de paquetes pueden ser de actualización, petición, consulta, respuesta o paquetes hello. En el resultado se muestran los números de secuencia y acuse de recibo que utiliza el algoritmo de transporte confiable EIGRP.

EJEMPLO PRÁCTICO 3.3



- **Paso 1.**Se deben realizar las configuraciones básicas en los routers, es decir, la asignación de nombre, contraseñas y direcciones IP de las interfaces.

Para el router C:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterC
RouterC(config)#enable secret fes
RouterC(config)#line vty 0 4
RouterC(config-line)#password unam
RouterC(config-line)#login
RouterC(config-line)#line con 0
RouterC(config-line)#password unam
RouterC(config-line)#login
RouterC(config-line)#exit
RouterC(config)#interface fastethernet 0/0
```

```
RouterC(config-if)#ip address 2.1.1.1 255.255.255.0
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
RouterC(config-if)#interface fastethernet 0/1
RouterC(config-if)#ip address 2.3.3.2 255.255.255.0
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/1, changed state to up
RouterC(config-if)#interface serial 0/0/0
RouterC(config-if)#ip address 10.1.1.1 255.255.255.252
RouterC(config-if)#bandwidth 250
RouterC(config-if)#clock rate 250000
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
RouterC(config-if)#exit
RouterC(config)#
```

Para el router B:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterB
RouterB(config)#enable secret fes
RouterB(config)#line vty 0 4
RouterB(config-line)#password unam
RouterB(config-line)#login
RouterB(config-line)#line con 0
RouterB(config-line)#password unam
RouterB(config-line)#login
RouterB(config-line)#exit
RouterB(config)#interface fastethernet 0/0
RouterB(config-if)#ip address 2.3.3.1 255.255.255.0
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
RouterB(config-if)#interface fastethernet 0/1
RouterB(config-if)#ip address 2.4.4.1 255.255.255.0
```

```
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/1, changed state to up
RouterB(config-if)#interface serial 0/0/0
RouterB(config-if)#ip address 10.1.1.5 255.255.255.252
RouterB(config-if)#bandwidth 250
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
RouterB(config-if)#exit
RouterB(config)#
```

Para el router D:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterD
RouterD(config)#enable secret fes
RouterD(config)#line vty 0 4
RouterD(config-line)#password unam
RouterD(config-line)#login
RouterD(config-line)#line con 0
RouterD(config-line)#password unam
RouterD(config-line)#login
RouterD(config-line)#exit
RouterD(config)#interface fastethernet 0/0
RouterD(config-if)#ip address 2.2.2.1 255.255.255.0
RouterD(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
RouterD(config-if)#interface serial 0/0/0
RouterD(config-if)#ip address 10.1.1.2 255.255.255.252
RouterD(config-if)#bandwidth 250
RouterD(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
RouterD(config-if)#interface serial 0/1/0
RouterD(config-if)#ip address 10.1.1.6 255.255.255.252
RouterD(config-if)#bandwidth 250
RouterD(config-if)#clock rate 250000
RouterD(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
RouterD(config-if)#exit
RouterD(config)#
```

- **Paso 2.** Se configura el protocolo EIGRP y se anuncian las redes que se encuentran conectadas a cada router. También se desactiva el autoresumen ya que se tienen redes discontinuas y el enrutamiento no funcionaria adecuadamente.

Para el router C:

```
RouterC(config)#router eigrp 65000
RouterC(config-router)# network 2.1.1.0 0.0.0.255
RouterC(config-router)# network 10.1.1.0 0.0.0.3
RouterC(config-router)# network 2.3.3.0 0.0.0.255
RouterC(config-router)# no auto-summary
RouterC(config-router)#exit
RouterC(config)#
```

Para el router B:

```
RouterB(config)#router eigrp 65000
RouterB(config-router)# network 2.3.3.0 0.0.0.255
RouterB(config-router)# network 2.4.4.0 0.0.0.255
RouterB(config-router)# network 10.1.1.4 0.0.0.3
RouterB(config-router)# no auto-summary
RouterB(config-router)#exit
RouterB(config)#
```

Para el router D:

```
RouterD(config)#router eigrp 65000
RouterD(config-router)# network 2.2.2.0 0.0.0.255
RouterD(config-router)# network 10.1.1.0 0.0.0.3
RouterD(config-router)# network 10.1.1.4 0.0.0.3
RouterD(config-router)# no auto-summary
RouterD(config-router)#exit
RouterD(config)#
```

- **Paso 3.** Se debe verificar que las interfaces utilizadas de cada router estén activas dentro del proceso EIGRP.

Para el router C:

```
RouterC#show ip eigrp interfaces
IP-EIGRP interfaces for process 65000

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0              0        0/0      1236       0/10          0           0
Fa0/1              1        0/0      1236       0/10          0           0
Se0/0/0            1        0/0      1236       0/10          0           0
```

Para el router B:

```
RouterB#show ip eigrp interfaces
IP-EIGRP interfaces for process 65000

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0              1        0/0      1236       0/10          0           0
Fa0/1              0        0/0      1236       0/10          0           0
Se0/0/0            1        0/0      1236       0/10          0           0
```

Para el router D:

```
RouterD#show ip eigrp interfaces
IP-EIGRP interfaces for process 65000

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0              0        0/0      1236       0/10          0           0
Se0/1/0            1        0/0      1236       0/10          0           0
Se0/0/0            1        0/0      1236       0/10          0           0
```

- **Paso 4.** Se verifica que en la tabla de topología y de enrutamiento EIGRP se encuentren instaladas las rutas hacia todas las redes.

Para el router C:

```
RouterC#show ip eigrp topology
IP-EIGRP Topology Table for AS 65000

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 2.1.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 2.3.3.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 10.1.1.0/30, 1 successors, FD is 10752000
         via Connected, Serial0/0/0
P 2.4.4.0/24, 1 successors, FD is 30720
         via 2.3.3.1 (30720/28160), FastEthernet0/1
P 2.2.2.0/24, 1 successors, FD is 10754560
         via 10.1.1.2 (10754560/28160), Serial0/0/0
P 10.1.1.4/30, 1 successors, FD is 10754560
         via 2.3.3.1 (10754560/10752000), FastEthernet0/1
         via 10.1.1.2 (11264000/10752000), Serial0/0/0

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 4 subnets
C       2.1.1.0 is directly connected, FastEthernet0/0
D       2.2.2.0 [90/10754560] via 10.1.1.2, 00:38:04, Serial0/0/0
C       2.3.3.0 is directly connected, FastEthernet0/1
D       2.4.4.0 [90/30720] via 2.3.3.1, 00:38:10, FastEthernet0/1
     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
D       10.1.1.4 [90/10754560] via 2.3.3.1, 00:38:03, FastEthernet0/1
```

Aquí se observa que para la red 10.1.1.4/30 en la tabla de topología se encuentra una ruta alterna, la cual es llamada sucesor factible y esta no se instala en la tabla de enrutamiento.

Para el router B:

```
RouterB#show ip eigrp topology
IP-EIGRP Topology Table for AS 65000

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 2.3.3.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 2.4.4.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 2.1.1.0/24, 1 successors, FD is 30720
         via 2.3.3.2 (30720/28160), FastEthernet0/0
P 10.1.1.0/30, 1 successors, FD is 10754560
         via 2.3.3.2 (10754560/10752000), FastEthernet0/0
         via 10.1.1.6 (11264000/10752000), Serial0/0/0
P 2.2.2.0/24, 1 successors, FD is 10754560
         via 10.1.1.6 (10754560/28160), Serial0/0/0
P 10.1.1.4/30, 1 successors, FD is 10752000
         via Connected, Serial0/0/0

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 4 subnets
D       2.1.1.0 [90/30720] via 2.3.3.2, 00:50:19, FastEthernet0/0
D       2.2.2.0 [90/10754560] via 10.1.1.6, 00:50:11, Serial0/0/0
C       2.3.3.0 is directly connected, FastEthernet0/0
C       2.4.4.0 is directly connected, FastEthernet0/1
     10.0.0.0/30 is subnetted, 2 subnets
D       10.1.1.0 [90/10754560] via 2.3.3.2, 00:50:19, FastEthernet0/0
C       10.1.1.4 is directly connected, Serial0/0/0
```

Aquí se observa que para la red 10.1.1.0/30 en la tabla de topología se encuentra el sucesor factible.

Para el router D:

```
RouterD#show ip eigrp topology
IP-EIGRP Topology Table for AS 65000

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 2.2.2.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 10.1.1.4/30, 1 successors, FD is 10752000
         via Connected, Serial0/1/0
P 10.1.1.0/30, 1 successors, FD is 10752000
         via Connected, Serial0/0/0
P 2.1.1.0/24, 1 successors, FD is 10754560
         via 10.1.1.1 (10754560/28160), Serial0/0/0
         via 10.1.1.5 (10757120/30720), Serial0/1/0
P 2.3.3.0/24, 2 successors, FD is 10754560
         via 10.1.1.1 (10754560/28160), Serial0/0/0
         via 10.1.1.5 (10754560/28160), Serial0/1/0
P 2.4.4.0/24, 1 successors, FD is 10754560
         via 10.1.1.5 (10754560/28160), Serial0/1/0
         via 10.1.1.1 (10757120/30720), Serial0/0/0

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 4 subnets
D       2.1.1.0 [90/10754560] via 10.1.1.1, 01:07:24, Serial0/0/0
C       2.2.2.0 is directly connected, FastEthernet0/0
D       2.3.3.0 [90/10754560] via 10.1.1.1, 01:07:24, Serial0/0/0
                [90/10754560] via 10.1.1.5, 01:07:23, Serial0/1/0
D       2.4.4.0 [90/10754560] via 10.1.1.5, 01:07:23, Serial0/1/0
     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.1.1.4 is directly connected, Serial0/1/0
```

Aquí se observa que para las redes 2.1.1.0/24 y 2.4.4.0/24 en la tabla de topología se encuentran los sucesores factibles respectivos, pero para la red

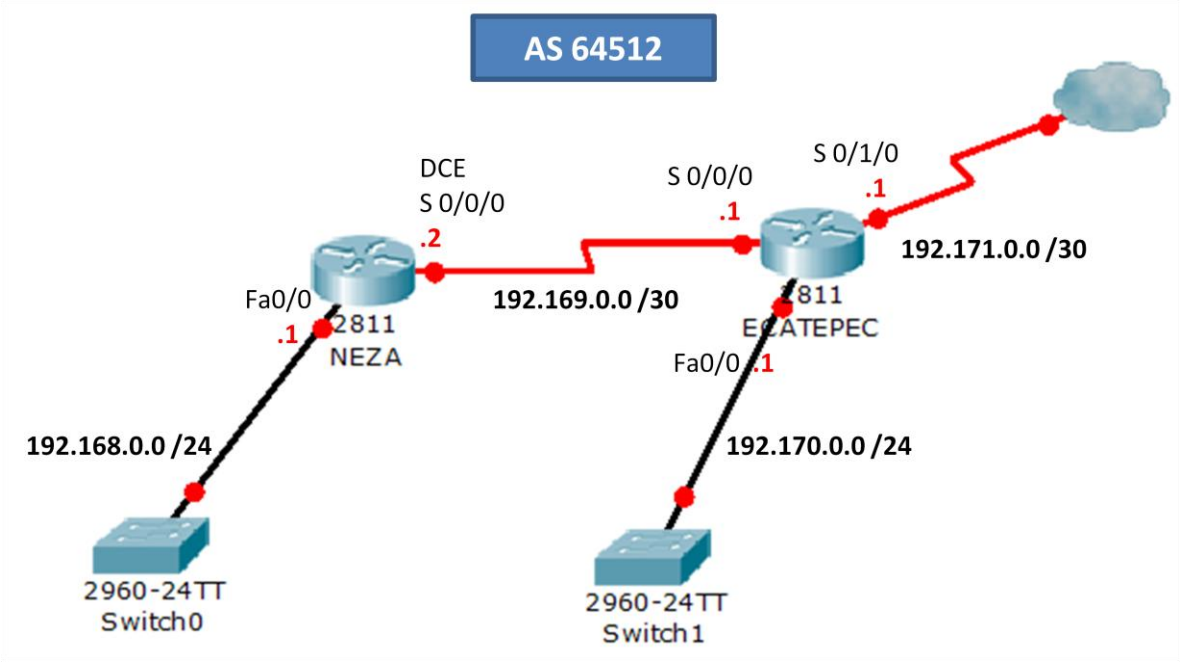
2.3.3.0/24 se tienen 2 sucesores (rutas principales) ya que tienen la misma métrica y por lo tanto las dos rutas se instalan en la tabla de enrutamiento.

- **Paso 5.** Se modifica el multiplicador de varianza en el proceso EIGRP en el router C y se verifica los cambios en la tabla de topología.

```
RouterC(config)#router eigrp 65000
RouterC(config-router)#variance 2
RouterC(config-router)#
%DUAL-5-NBRCHANGE:    IP-EIGRP    65000:    Neighbor    2.3.3.1
(FastEthernet0/1) is up: new adjacency
%DUAL-5-NBRCHANGE:    IP-EIGRP    65000:    Neighbor    10.1.1.2
(Serial0/0/0) is up: new adjacency
RouterC(config-router)#exit
RouterC(config)#exit

RouterC#sh ip eigrp topology
IP-EIGRP Topology Table for AS 65000

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - Reply status

P 2.1.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 2.3.3.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 10.1.1.0/30, 1 successors, FD is 10752000
         via Connected, Serial0/0/0
P 2.4.4.0/24, 1 successors, FD is 30720
         via 2.3.3.1 (30720/28160), FastEthernet0/1
P 10.1.1.4/30, 2 successors, FD is 10754560
         via 2.3.3.1 (10754560/10752000), FastEthernet0/1
         via 10.1.1.2 (11264000/10752000), Serial0/0/0
P 2.2.2.0/24, 1 successors, FD is 10754560
         via 10.1.1.2 (10754560/28160), Serial0/0/0
RouterC#
```

Se observa que ahora existen dos y no un sucesor para la red 10.1.1.4/30, con esto se tiene un equilibrado de carga de manera proporcional a los valores de las métricas.

EJEMPLO PRÁCTICO 3.4



- **Paso 1.**Se deben realizar las configuraciones básicas en los routers, es decir, la asignación de nombre, contraseñas y direcciones IP de las interfaces. Estas configuraciones son las mismas que en el ejemplo práctico 3.2 por lo cual aquí no se repetirán.

- **Paso 2.** Se configura el protocolo EIGRP y se anuncian las redes que se encuentran conectadas a cada router. En el router Ecatepec no será anunciada la subred 192.171.0.0/30. También se desactiva el autoresumen ya que se tiene la subred 192.169.0.0/30.

Para el router Neza:

```
neza(config)#router eigrp 64512
neza(config-router)#network 192.168.0.0 0.0.0.255
neza(config-router)#network 192.169.0.0 0.0.0.255
neza(config-router)#no auto-summary
neza(config-router)#exit
neza(config)#
```

Para el router Ecatepec:

```
ecatepec(config)#router eigrp 64512
ecatepec(config-router)#network 192.169.0.0 0.0.0.3
ecatepec(config-router)#network 192.170.0.0 0.0.0.255
ecatepec(config-router)#no auto-summary
ecatepec(config-router)#exit
ecatepec(config)#
```

- **Paso 3.** Se configura una ruta estática por defecto que salga por la interfaz s0/1/0 del router Ecatepec y se redistribuye dentro de EIGRP. También se configura esta interfaz como pasiva para no intercambiar actualizaciones con el exterior.

```
ecatepec(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0
ecatepec(config)#router eigrp 64512
ecatepec(config-router)#redistribute static
ecatepec(config-router)#passive-interface serial 0/1/0
ecatepec(config-router)#exit
ecatepec(config)#
```

- **Paso 4.** Se checan las tablas de enrutamiento y topología.

Para el router Ecatepec:

```
ecatepec#show ip eigrp topology
IP-EIGRP Topology Table for AS 64512

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.169.0.0/30, 1 successors, FD is 20512000
         via Connected, Serial0/0/0
P 192.170.0.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.0.0/24, 1 successors, FD is 20514560
         via 192.169.0.2 (20514560/28160), Serial0/0/0
P 0.0.0.0/0, 1 successors, FD is 25120000
         via Rstatic (25120000/0)

ecatepec#show ip route
```

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

D      192.168.0.0/24 [90/20514560] via 192.169.0.2, 00:17:18,
Serial0/0/0
     192.169.0.0/30 is subnetted, 1 subnets
C       192.169.0.0 is directly connected, Serial0/0/0
C    192.170.0.0/24 is directly connected, FastEthernet0/0
     192.171.0.0/30 is subnetted, 1 subnets
C       192.171.0.0 is directly connected, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

Se observa que las rutas junto con la ruta estática por defecto se encuentran correctamente instaladas.

Para el router Neza:

```
neza#show ip eigrp topology
IP-EIGRP Topology Table for AS 64512

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.0.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.169.0.0/30, 1 successors, FD is 20512000
         via Connected, Serial0/0/0
P 192.170.0.0/24, 1 successors, FD is 20514560
         via 192.169.0.1 (20514560/28160), Serial0/0/0
P 0.0.0.0/0, 1 successors, FD is 25632000
         via 192.169.0.1 (25632000/25120000), Serial0/0/0

neza#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.169.0.1 to network 0.0.0.0

C    192.168.0.0/24 is directly connected, FastEthernet0/0
     192.169.0.0/30 is subnetted, 1 subnets
C       192.169.0.0 is directly connected, Serial0/0/0
D    192.170.0.0/24 [90/20514560] via 192.169.0.1, 00:33:44, Serial0/0/0
D*EX 0.0.0.0/0 [170/25632000] via 192.169.0.1, 00:22:48, Serial0/0/0
neza#
```

En estas tablas se observa que la ruta estática por defecto fue aprendida por EIGRP y es marcada como externa en la tabla de enrutamiento.

- **Paso 5.** Se configura la autenticación.

```
neza(config)#key chain privado
neza(config-keychain)#key 2
neza(config-keychain-key)#key string aragon
neza(config-keychain-key)#exit
neza(config-keychain)#exit
neza(config)#interface s 0/0/0
neza(config-if)# ip authentication mode eigrp 64512 md5
neza(config-if)# ip authentication key-chain privado eigrp 64512
```

```
ecatepec(config)#key chain privado
ecatepec(config-keychain)#key 2
ecatepec(config-keychain-key)#key string aragon
ecatepec(config-keychain-key)#exit
ecatepec(config-keychain)#exit
ecatepec(config)#interface s 0/0/0
ecatepec(config-if)# ip authentication mode eigrp 64512 md5
ecatepec(config-if)# ip authentication key-chain privado eigrp 64512
```

Se utiliza autenticación md5 que proporciona un nivel más alto de seguridad que el texto plano. El key number y el key string deben ser iguales en ambos lados, en caso contrario la autenticación fallara.

3.3. OSPF (OPEN SHORTEST PATH FIRST)

Los algoritmos de enrutamiento del estado de enlace, también conocidos como algoritmos Primero la Ruta libre más Corta (SPF), mantienen una compleja base de datos de información de topología. El algoritmo de enrutamiento del estado de enlace mantiene información completa sobre routers lejanos y su interconexión. Por otra parte, los algoritmos de vector-distancia proporcionan información no específica sobre las redes lejanas y no obtiene información directamente de los routers distantes.

El protocolo OSPF, Primero la ruta libre más corta (Open Shortest Path First), fue creado a finales de los 80. Se diseñó para cubrir las necesidades de las grandes redes IP que otros protocolos como RIP no podían soportar, incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión. El protocolo OSPF versión 2 es la implementación más actualizada.

OSPF es un protocolo de enrutamiento de estado de enlace basado en estándares abiertos. El término "Open" en "Open Shortest Path First" significa que está abierto al público y no es propiedad de ninguna empresa, lo que significa que muchos fabricantes lo pueden desarrollar y mejorar. La configuración de OSPF en un router Cisco es parecido a la configuración de otros protocolos de enrutamiento. De igual manera, es necesario habilitar OSPF en un router e identificar las redes que serán publicadas por OSPF. OSPF cuenta con varias funciones y procedimientos de configuración únicos. Estas funciones aumentan las capacidades de OSPF como protocolo de enrutamiento, pero también complican su configuración[42].

Los protocolos de enrutamiento del estado de enlace reúnen la información de ruta de todos los demás routers de la red o dentro de un área definida de la red. Una vez que se haya reunido toda la información, cada router calcula las mejores

[42] Lammle Todd, Odom Sean y Wallace Kevin, *CCNP Routing Study Guide,* p.114.

rutas hacia todos los destinos de la red. Dado que cada router mantiene su propia visión de la red, es menos probable que se propague información incorrecta de parte de cualquiera de los routers vecinos.

A continuación, se presentan algunas funciones de los protocolos de enrutamiento del estado de enlace:

- Responden rápidamente a los cambios de red
- Envían actualizaciones desencadenadas sólo cuando se haya producido un cambio de red
- Envían actualizaciones periódicas conocidas como actualizaciones del estado de enlace
- Usan un mecanismo *hello* para determinar la posibilidad de comunicarse con los vecinos

Cada router envía los paquetes *hello* en multicast para realizar un seguimiento del estado de los routers vecinos. Cada router usa varias LSA (Link-State Advertisment) para realizar el seguimiento de todos los routers en el área donde se encuentra la red. Los paquetes *hello* contienen información acerca de las redes conectadas al router. Las LSA proporcionan actualizaciones sobre el estado de los enlaces que son interfaces en otros routers de la red.

Los routers que usan protocolos de enrutamiento de estado de enlace tienen las siguientes características:

- Usan la información *hello* y las LSA que han recibido de otros routers para crear una base de datos de la red
- Usan el algoritmo SPF para calcular la ruta más corta hacia cada red.
- Almacenan la información de ruta en la tabla de enrutamiento

OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área

backbone mediante un router fronterizo. Todos los paquetes enviados desde una dirección de una estación de trabajo de un área a otra de un área diferente atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas. Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone, OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas.

OSPF es un protocolo de enrutamiento por estado de enlace que, a diferencia de RIP e IGRP que publican sus rutas sólo a routers vecinos, envía publicaciones del estado de enlace LSA (Link-State Advertisment) a todos los routers pertenecientes a la misma área jerárquica mediante una multidifusión de IP. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red. Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo SPF (que también se conoce con el nombre de su creador, Dijkstra) para calcular la ruta más corta a cada nodo.

Para determinar qué interfaces reciben las publicaciones de estado de enlace, los routers ejecutan el protocolo OSPF *Hello*. Los routers vecinos intercambian mensajes *hello* para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers.

Cuando se detecta un router vecino, se intercambia información de topología OSPF. Cuando los routers están sincronizados, se dice que han formado una adyacencia.

Las LSA se envían y reciben sólo en adyacencias. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF que define un

proceso fiable de publicación, acuse de recibo y petición para garantizar que la información de la LSA, se distribuye adecuadamente a todos los routers de un área[43].

Los routers OSPF confían en 5 tipos de paquetes para identificar a sus vecinos y para actualizar la información de enrutamiento de estado de enlace. Estos 5 tipos de paquetes hacen de OSPF capaz de llevar a cabo comunicaciones sofisticadas y complejas.

Tipos de paquetes OSPF	Descripción
Tipo 1 → Hello	Establece y mantiene información de adyacencia con los vecinos
Tipo 2 → Database description packet (DBD)	Describe el contenido de la base de datos de estado de enlace en un router OSPF
Tipo 3 → Link - state request (LSR)	Solicita partes específicas de la base de datos de estado de enlace.
Tipo 4 → Link - state update (LSU)	Transporta publicaciones de estado de enlace (LSAs) a routers vecinos
Tipo 5 → (LSAack) Link - state acknowledgement	Acuse de recibo de una LSA de un vecino

Tabla 3.3 Paquetes OSPF

Las interfaces OSPF pueden encontrarse e uno de siete estados. Los vecinos OSPF progresan a través de estos estados, uno a la vez en el siguiente orden:

1. **Estado Desactivado (Down State)**. En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización).

[43] Ariganello Ernesto, *Tecnicas de configuracion de routers Cisco*, p.38.

2. **Estado de Inicialización (Init State)**. Los routers OSPF envían paquetes tipo 1, o paquetes *hello*, a intervalos regulares con el fin de establecer una relación con los routers vecinos. Cuando una interfaz recibe su primer paquete *hello*, el router entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa.

Los dos tipos de relaciones son Dos-Vías y Adyacencia. Un router debe recibir un Hello desde un vecino antes de establecer algún tipo de relación.

3. **Estado de Dos-Vías (Two-Way).** Empleando paquetes *hello*, cada router OSPF intenta establecer el estado de dos-vías, o comunicación bidireccional, con cada router vecino en la misma red IP. Entre otras cosas, el paquete *hello* incluye una lista de los vecinos OSPF conocidos por el origen. Un router ingresa al estado de Dos-vías cuando se ve a sí mismo en un paquete *hello* proveniente de un vecino. El estado de Dos-Vías es la relación más básica que vecinos OSPF pueden tener, pero la información de enrutamiento no es compartida entre estos. Para aprender los estados de enlace de otros routers y eventualmente construir una tabla de enrutamiento, cada router OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre routers OSPF que involucra una serie de estados progresivos que se basa no tan solo en paquetes *hello*, si no que en otros 4 paquetes OSPF. Aquellos routers intentando volverse adyacentes entre ellos intercambian información de enrutamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

4. **Estado ExStart.** Técnicamente, cuando un router y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD). Los dos routers vecinos emplean paquetes *hello* para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos. Aquel router con el mayor

router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de enrutamiento.

5. **Estado de Intercambio (Exchange).** En el Estado de intercambio, los routers vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los routers se describen sus bases de datos de estado de enlace entre ellos. Los routers comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los routers recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de enrutamiento es intercambiada en el estado Cargando.

6. **Estado Cargando (Loading).** Después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un router recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

7. **Estado de Adyacencia (Full Adjacency).** Cuando el estado de carga ha sido completado, los routers se vuelven completamente adyacentes. Cada router mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

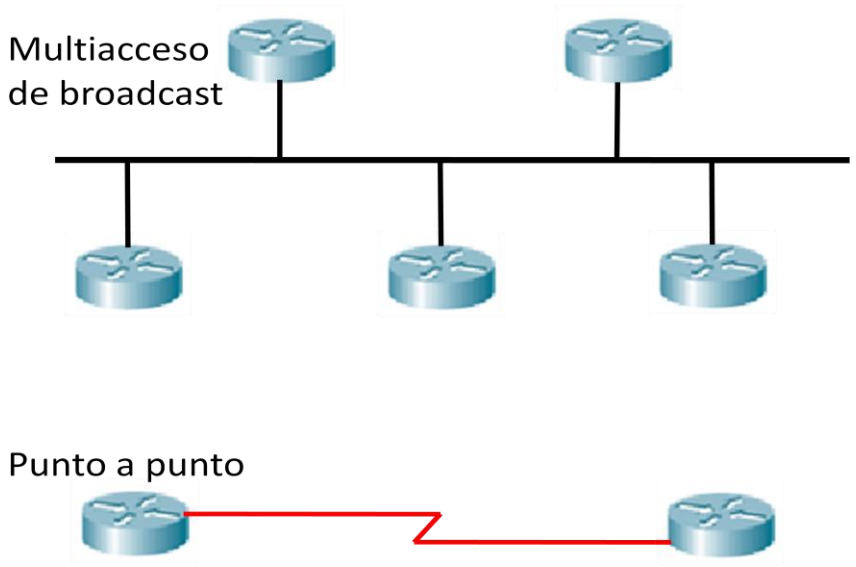
3.3.1. TIPOS DE RED OSPF

Se requiere una relación de vecino para que los routers OSPF puedan compartir la información de enrutamiento. Un router tiende a ser adyacente (o vecino) con por lo menos un router en cada red IP a la cual está conectado. Los routers OSPF determinan con qué routers pueden intentar formar adyacencias tomando como base el tipo e red a la cual están conectados. Algunos routers tratarán de tender a la adyacencia con respecto a todos los routers vecinos. Otros routers tratarán de hacerse adyacentes con respecto a sólo uno o dos de los routers vecinos. Una vez que se forma una adyacencia entre vecinos, se intercambia la información del estado de enlace.

Las interfaces OSPF reconocen tres tipos de redes (véase fig. 3.14):

- Multiacceso de broadcast como por ejemplo Ethernet
- Redes punto a punto.
- Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay

Además de los tres tipos de redes anteriores, un administrador puede configurar un cuarto tipo, punto a multipunto, en una interface.



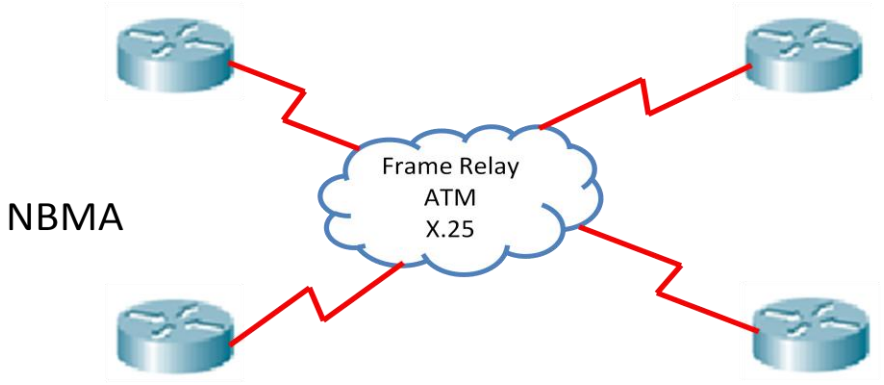


Figura 3.14. Tipos de red en OSPF

En una red multiacceso, no se sabe de antemano cuántos routers estarán conectados. En las redes punto a punto sólo se pueden conectar dos routers.

En un segmento de red multiacceso de broadcast, se pueden conectar muchos routers. Si cada router tuviera que establecer adyacencia completa con cada uno de los otros routers e intercambiar información del estado de enlace con cada vecino, el procesamiento tendría un gasto demasiado grande. Si existieran 5 routers, se necesitarían 10 relaciones de adyacencia y se enviarían 10 estados de enlace. Si existieran 10 routers, entonces se necesitarían 45 adyacencias. Por lo general, para *n* routers, se necesitan *n*(n-1)/2* adyacencias. La solución para este gasto es elegir un router designado (DR). Este router se hace adyacente a todos los demás routers del segmento de broadcast. Todos los demás routers del segmento envían su información del estado de enlace al DR. El DR a su vez actúa como portavoz del segmento. El DR envía información del estado de enlace a todos los demás routers del segmento a través de la dirección de multicast 224.0.0.5 para todos los routers OSPF.

A pesar de la ganancia en eficiencia que permite la elección de DR, existe una desventaja. El DR representa un punto único de falla. Se elige un segundo router como router designado de respaldo (BDR) para que se haga cargo de las responsabilidades del DR en caso de que éste fallara. Para asegurar de que tanto el DR como el BDR vean todos los estados de enlace que los routers envían a través

del segmento, se utiliza la dirección multicast 224.0.0.6 para todos los routers designados.

En las redes punto a punto el router detecta dinámicamente a sus vecinos enviando paquetes *Hello* con la dirección de multidifusión 224.0.0.5. No se lleva acabo elección y no existe concepto de DR ni BDR.

3.3.2. CONFIGURACIÓN DE OSPF EN UNA SOLA ÁREA

Para la configuración de OSPF las interfaces que participan del proceso deben estar configuradas y activas previamente.

El enrutamiento OSPF utiliza el concepto de áreas. Cada router contiene una base de datos completa de los estados de enlace de un área específica. A un área de la red OSPF se le puede asignar cualquier número de 0 a 65535. Sin embargo a una sola área se le asigna el número 0 y se la conoce como área 0. En las redes OSPF con varias áreas, se requiere que todas las áreas se conecten al área 0. El área 0 también se denomina el área backbone.

En el proceso de configuración de OSPF se debe especificar el número de proceso *(process-id)* que identificará el conjunto de routers que participan de ese mismo proceso; el numero puede tener cualquier valor entre 1 y 65535, la mayoría de los administradores de red mantienen el mismo ID de proceso en todo un sistema autónomo, pero esto no es un requisito, aunque rara vez es necesario ejecutar más de un proceso OSPF en un router.

La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de redes o subredes directamente conectadas y la información de área especificadas. Las direcciones de red se configuran con una máscara wildcard y no con una máscara de subred. La máscara wildcard representa las direcciones de enlaces o de host que pueden estar presentes en este segmento.

```
router(config)#router ospf [numero de proceso]
router(config-router)#network[dirección IP – wildcard] area[numero]
```

Cuando se inicia el proceso OSPF, Cisco lOS utiliza la dirección IP activa local más alta como su ID de router OSPF. Si no existe ninguna interface activa, el proceso OSPF no se iniciará. Si la interface activa se desactiva el proceso OSPF se queda sin ID de router y por lo tanto deja de funcionar hasta que la interface vuelve a activarse.

Para asegurar la estabilidad de OSPF, deberá haber una interface activa para el proceso OSPF en todo momento. Es posible configurar una interface de loopback, que es una interface lógica, para este propósito. Al asegurarse una interface loopback, OSPF usa esta dirección como ID del router sin importar el valor. En un router que tiene más de una interface loopback, OSPF toma la direcóón IP de loopback más alta como su ID de router.

Una interfaz loopback se crea con los siguientes comandos:

```
router(config)#interface [numero]
router(config-if)#ip address [dirección IP – mascara de subred]
```

Se considera buena práctica usar interfaces loopback para todos los routers que ejecutan OSPF, este tipo de interfaz se debe configurar con una dirección que use una máscara de subred de 32 bits de 255.255.255.255. Una máscara de subred de 32 bits se denomina una máscara de host porque la máscara de subred especifica la red de un host. Cuando se solicita que OSPF publique una red loopback, siempre se publica como una ruta de host con una máscara de 32 bits.

Como ya se menciono con anterioridad, en las redes multiacceso de broadcast se necesita elegir un DR y un BDR. Un router Designado (DR) lleva a cabo tareas de envío y sincronización. El Router Designado de Reserva (BDR) sólo

actuará si el DR falla. Cada router debe establecer una adyacencia con el DR y el BDR.

- El router con el valor de prioridad más alto es el Router Designado DR. Las prioridades se pueden establecer en cualquier valor de 0 a 255.
- El router con el segundo valor es el router designado de reserva BDR.
- El valor predeterminado de de la prioridad OSPF de la interfaz es 1. Un router con prioridad 0 no es elegible. En caso de empate se usa el ID de router.
- ID del router. Este número de 32 bits identifica únicamente al router dentro de un sistema autónomo. La dirección IP más alta de una interfaz activa se elige por defecto.
- En principio el router intentara utilizar un ID buscando interfaces virtuales o loopback, si no encuentra configuración de las mismas lo hará con la interfaz física con la dirección IP más alta[44].

Se modifica la prioridad OSPF introduciendo el comando de configuración de interfaz **`ip ospf priority`** en una interfaz que participa en OSPF.

```
Router(config-if)#ip ospf priority [0-255]
```

El comando **`show ip ospf interface`** mostrará el valor de prioridad de interfaz así como otra información clave.

```
Router#show ip ospf interface [tipo] [número]
```

```
RouterB#show ip ospf interface fa 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 2.3.3.1/24, Area 0
  Process ID 100, Router ID 10.1.1.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 5
  Designated Router (ID) 10.1.1.5, Interface address 2.3.3.1
  Backup Designated Router (ID) 10.1.1.1, Interface address 2.3.3.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
```

[44] Clare Gough, *CCNP BSCI Exam Certification Guide*, p189.

```
  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 10.1.1.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

3.3.3. MÉTRICA OSPF

La métrica de enrutamiento de OSPF es el costo que se calcula en base al ancho de banda de la interfaz y es configurable por parte del usuario. La fórmula para calcular el costo es:

$$Costo = \frac{10^8}{Ancho\_de\_banda}$$

Cuanto más bajo sea el costo, más probabilidad hay de que la interface sea utilizada para enviar tráfico de datos. Cisco IOS determina automáticamente el costo, en base al ancho de banda de la interface. Resulta esencial para la operación correcta de OSPF que se establezca el ancho de banda de interface correcto.

El ancho de banda por defecto para las interfaces seriales Cisco es 1.544 Mbps o 1544 kbps. La siguiente tabla muestra el ancho de banda nominal de un enlace y su correspondiente costo:

Medio	Ancho de banda nominal	Coste por defecto
9.6 kbps línea	9.6 kbps	10416
56 kbps línea	56 kbps	1785
64 kbps línea	64 kbps	1562
TI circuito	1.544 Mbps	64
E1 circuito	2.048 Mbps	48

Medio	Ancho de banda nominal	Coste por defecto
T3circuito	45 Mbps	2
4 Mbps Token Ring	4 Mbps	25
16 Mbps Token	16 Mbps	6
Ethernet	10 Mbps	10
FastEthernet	100 Mbps	1
GigabitEthernet	1 Gbps	1
10 GigabitEthernet	10 Gbps	1

Tabla 3.4 Costos por defecto en OSPF

Es posible cambiar el costo para afectar el resultado de los cálculos de costo OSPF. Una situación común que requiere un cambio de costo es un entorno de enrutamiento de diversos fabricantes. Un cambio de costo puede asegurar que el valor de costo de un fabricante coincida con el valor de costo de otro fabricante.

Otra situación se produce al utilizar Gigabit Ethernet. Con la configuración por defecto, se asigna el valor de costo más bajo (1) a un enlace de 100 Mbps. En una situación con enlaces Gigabit Ethernet y 100 Mbps, los valores de costo por defecto podrían hacer que el enrutamiento tome una ruta menos deseable a menos que estos se ajusten. El número de costo se puede establecer entre 1 y 65,535.

Utilice el siguiente comando de configuración de interface para establecer el costo del enlace:

```
router(config-if)#ip ospf cost [1-65535]
```

El costo total de una ruta es la suma de costos de las interfaces salientes a lo largo de la ruta[45].

[45] Lammle Todd, Odom Sean y Wallace Kevin, *CCNP Routing Study Guide,* p.128.

3.3.4. TEMPORIZADORES

Los intervalos de *hello* y *dead* por defecto mantienen valores que dependen del tipo de red a la que pertenece la interfaz, a continuación se describen estos valores para diferentes tipos de red:

Point-to-Point Nonbroadcast	Point-to-Point	Broadcast	NBMA	Point-to Multipoint
Hello 30 seg.	Hello 10 seg.	Hello 10 seg.	Hello 30 seg.	Hello 30 seg.
Dead 120 seg.	Dead 40 seg.	Dead 40 seg.	Dead 120 seg.	Dead 120 seg.

Tabla 3.5 Valores de los intervalos *hello* y *dead* de OSPF

Para que este cuadro quede más claro la siguiente lista ejemplifica diferentes topologías de red:

- Para interfaces seriales con encapsulación HDLC, el tipo de red por default es punto a punto y los temporizadores son *hello* 10 y *dead* 40.
- Para interfaces seriales con encapsulación Frame Relay, el tipo de red por default es nonbroadcast y los temporizadores son *hello* 30 y *dead* 120.
- Para interfaces seriales con encapsulación Frame Relay y usando subinterfaces punto a punto, el tipo de red por default es punto a punto y los temporizadores son *hello* 10 y *dead* 40.
- Para interfaces seriales con encapsulación Frame Relay y usando subinterfaces punto a multipunto, el tipo de red por default es nonbroadcast y los temporizadores son *hello* 30 y *dead* 120[46].

De lo anterior se observa que, por default, el intervalo *dead* (muerto) es de cuatro veces el valor del intervalo *hello* (hola), esto significa que un router tiene cuatro oportunidades de enviar un paquete *hello* antes de ser declarado muerto.

[46] Clare Gough, *CCNP BSCI Exam Certification Guide*, p207.

Estos valores pueden modificarse dentro de las interfaces respectivas tomando en cuenta que deben ser iguales para todos los routers del proceso.

```
Router(config-if)#ip ospf hello-interval [segundos]
Router(config-if)#ip ospf dead-interval [segundos]
```

3.3.5. REDISTRIBUCIÓN ESTÁTICA EN OSPF

OSPF redistribuye rutas aprendidas estáticamente dirigidas hacia un destino particular.

```
Router(config)#ip route [red mascara] [dirección IP/interfaz] [distancia]
Router(config)#router ospf [numero de proceso]
Router(config-router)#redistribute static subnet
```

En el comando **ip route**, se puede utilizar la interfaz de salida o la IP del próximo salto. En el comando **redistribute static** se utiliza el parámetro **subnet** si la ruta estática es a una subred.

En OSPF para redistribuir una ruta estática por defecto se utiliza el comando **default-information originate**.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [dirección IP próximo salto/interfaz]
Router(config)#router ospf [numero de proceso]
Router(config-router)#default-information originate
```

3.3.6. INTERFACES PASIVAS

Las interfaces pasivas en OSPF funcionan de la siguiente manera:

- La información de enrutamiento no es enviada ni recibida por una interfaz pasiva.
- La dirección de red de la interfaz pasiva aparece como una red stub en el dominio OSPF.

- Se debe tener cuidado de usar la mascara wildcard apropiada.

```
RouterY(config)#router ospf 100
RouterY(config-router)#network 192.168.1.0 0.0.0.3 area 0
RouterY(config-router)#network 192.168.1.8 0.0.0.3 area 0
RouterY(config-router)#network 192.168.1.12 0.0.0.3 area 0
RouterY(config-router)#passive-interface S 0/0/0
RouterY(config-router)#
```

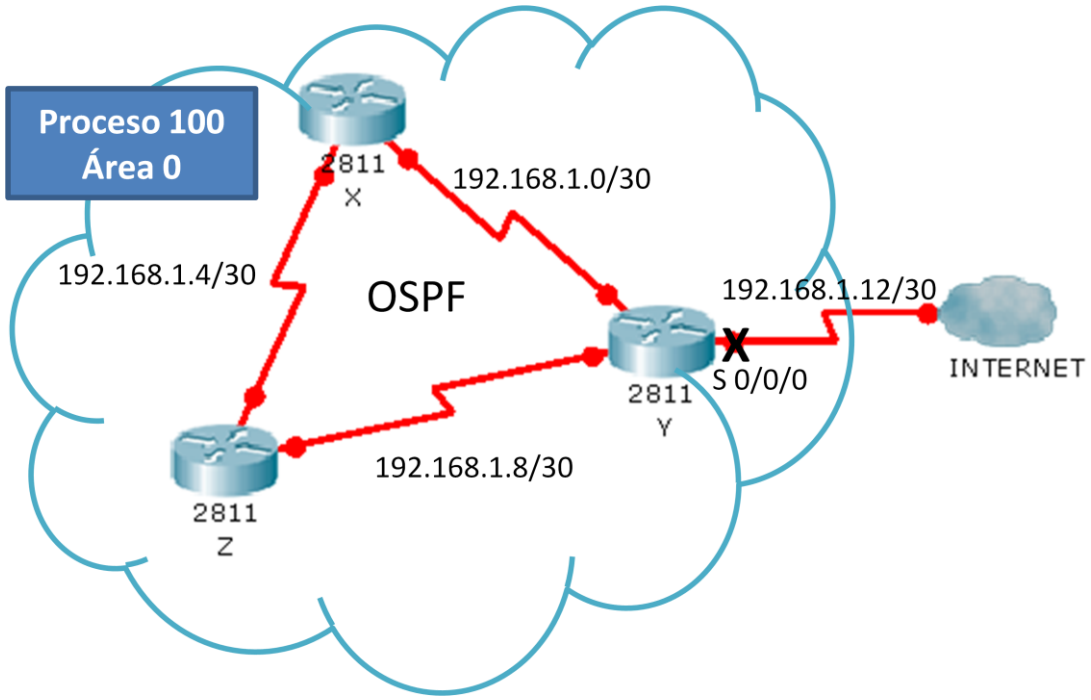


Figura 3.15. Interfaz pasiva en OSPF

3.3.7. FILTRADO DE RUTAS

Los routers OSPF determinan sus rutas basados en la base de datos de estado de enlace y no por las rutas que anuncian sus vecinos, como lo hacen los routers RIP o EIGRP.

Un requisito básico de los protocolos de estado de enlace, es que los routers de un área deben tener idénticas bases de datos de estado de enlace, es por esto

que los filtros de rutas en OSPF no pueden establecerse, a menos que, se coloquen en routers que redistribuyen rutas externas al interior del dominio OSPF, es decir, los filtros solo funcionan para rutas externas.

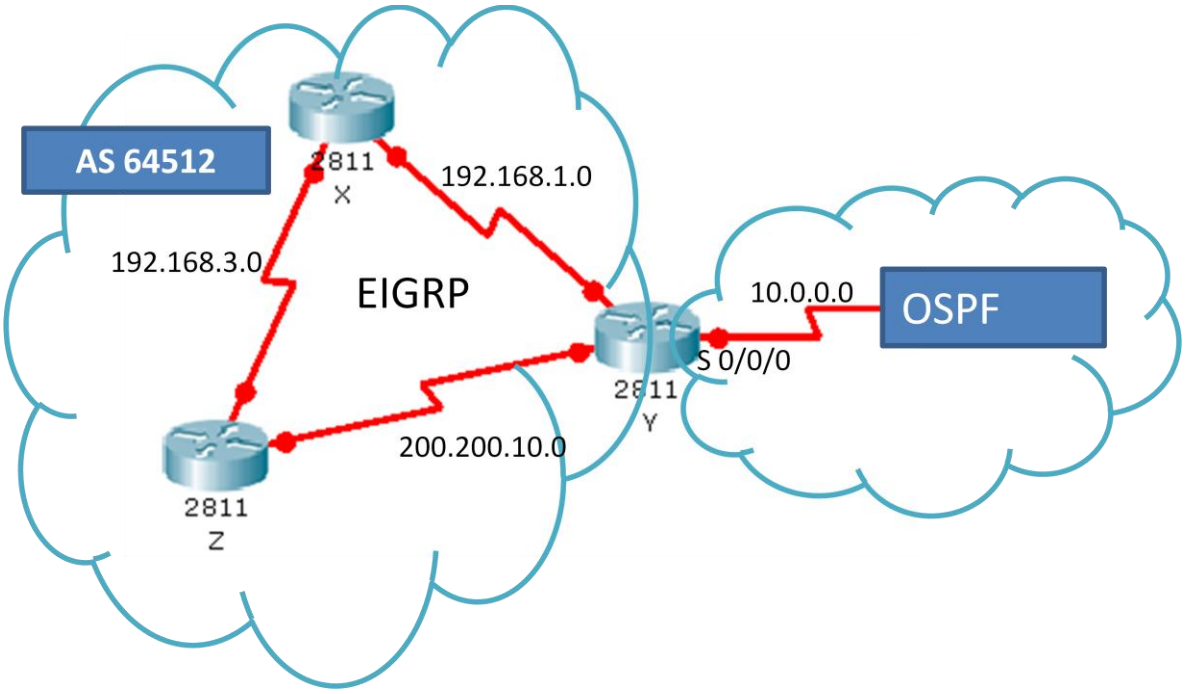


Figura 3.16. Filtros en un punto de redistribución.

A continuación se muestra la configuración de un filtro en el Router Y para que no redistribuya la ruta a 192.168.1.0 dentro del dominio OSPF:

```
RTY(config)#router eigrp 64512
RTY(config-router)#network 192.168.1.0
RTY(config-router)#network 200.200.10.0
RTZ(config-router)#exit
RTY(config)#router ospf 100
RTY(config-router)#network 10.0.0.0 0.0.0.255 area 0
RTY(config-router)#redistribute eigrp 64512 metric 30 subnets
RTY(config-router)#distribute-list 24 out
RTY(config-router)#exit
RTY(config)#access-list 24 deny 192.168.1.0 0.0.0.255
RTY(config)#access-list 24 permit any
```

3.3.8. AUTENTICACIÓN OSPF

Por defecto, un router confía en que la información de enrutamiento proviene de un router que debería estar enviando información. Un router también confía en que la información no haya sido alterada a lo largo de la ruta. Para lograr esto los routers pueden autenticarse entre sí.

Cada interfaz OSPF puede presentar una clave de autenticación para que la usen los routers que envían información de OSPF hacia otros routers del segmento. Esta clave es secreto compartido entre los routers y se utiliza para generar los datos de autenticación en el encabezado del paquete de OSPF. La contraseña puede contener hasta ocho caracteres.

Para crear una contraseña de autenticación en texto simple utilice el siguiente comando dentro de la interfaz:

```
Router(config-if)#ip ospf authentication-key [contraseña]
```

Para establecer un nivel de encriptación en la contraseña de autenticación puede utilizarse el siguiente comando dentro de la interfaz:

```
Router(config-if)#ip  ospf  message-digest-key  [identificador]
                  md5  [tipo de encriptación] [contraseña]
```

La palabra clave MD5 especifica el tipo de algoritmo de hash de message-digest a utilizar y el campo de tipo de cifrado se refiere al tipo de cifrado, donde 0 significa ninguno y 7 significa propietario.

El identificador o key-id puede tomar un valor de 1 a 255 y debe coincidir en cada router a autenticar. La contraseña o Key es alfanumérica y puede ser de hasta 16 caracteres, esta contraseña puede no ser la misma en toda el área pero si debe ser igual entre routers vecinos.

Después de configurar una contraseña se debe habilitar la autenticación para el área en todos los routers que participan en dicha área.

```
router(config)#router ospf [numero de proceso]
router(config-router)#area[numero] authentication
```

```
router(config-router)#area[numero] authentication message-digest
```

La opción `message-digest` se utiliza cuando dentro de la interfaz es usado el `message-digest-key`.

La autenticación MD5 crea un message-digest. Un message-digest son datos cifrados en base a la contraseña y contenido del paquete. El router receptor utiliza la contraseña compartida y el paquete para re calcular el digest. Si los digests coinciden, el router considera que el origen y el contenido del paquete no han sido alterados. El tipo de autenticación identifica qué clase de autenticación, de haber alguna, se está utilizando. En caso de la autenticación del message-digest, el campo de datos de autenticación contiene el key-id y la longitud del message-digest que se ha adjuntado al paquete.

3.3.9. VERIFICACIÓN OSPF

- **`show ip protocols:`** Muestra los protocolos que se están ejecutando en el router. En el caso de OSPF se observa el numero de proceso, los filtros aplicados a las interfaces, el ID del router, redistribuciones, áreas, redes asociadas, las puertas de enlace y la distancia administrativa.

```
RouterD#show ip protocols

Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.1.1
Redistributing External Routes from,
    static
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
  Maximum path: 4
  Routing for Networks:
    2.2.2.0 0.0.0.255 area 0
    10.1.1.0 0.0.0.3 area 0
    10.1.1.4 0.0.0.3 area 0
    172.16.1.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.1             110      00:00:00
    10.1.1.5             110      00:00:00
  Distance: (default is 110)
```

- **`show ip ospf`:** Entre otras cosas muestra la cantidad de veces en que se ha usado el algoritmo SPF. También muestra el intervalo de actualización de estado de enlace si no se han producido cambios topológicos.

```
RouterC#show ip ospf
 Routing Process "ospf 100" with ID 10.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x025b3e
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

- **show ip ospf interface:** Muestra entre otras cosas el tipo de red en que participa la interfaz, el costo, la prioridad, las adyacencias, el estado del router y los intervalos hello dentro del proceso en que participa la interfaz.

```
RouterC#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 2.1.1.1/24, Area 0
  Process ID 100, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.1, Interface address 2.1.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet address is 2.3.3.2/24, Area 0
  Process ID 100, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.1.1.5, Interface address 2.3.3.1
  Backup Designated Router (ID) 10.1.1.1, Interface address 2.3.3.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, 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 10.1.1.5  (Designated Router)
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30, Area 0
  Process ID 100, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 3/3, 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 172.16.1.1
  Suppress hello for 0 neighbor(s)
```

- **show ip ospf neighbor:** Muestra el ID de los routers vecinos, su prioridad, el estado, dirección IP e interfaz de conexión. Se le puede agregar la palabra **detail** para información más detallada.

```
RouterC#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.5          5   FULL/DR         00:00:39    2.3.3.1         FastEthernet0/1
172.16.1.1        0   FULL/  -        00:00:34    10.1.1.2        Serial0/0/0
```

- **show ip ospf database:** Muestra el contenido de la base de datos topológica OSPF. También muestra el ID del router, el ID del proceso OSPF y el numero de enlaces que configuro el router.

```
RouterC#sh ip ospf database
            OSPF Router with ID (10.1.1.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        344         0x80000006 0x00feff 4
172.16.1.1      172.16.1.1      983         0x80000007 0x003eea 6
10.1.1.5        10.1.1.5        345         0x80000006 0x00feff 4

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
2.3.3.1         10.1.1.5        345         0x80000002 0x007ca2

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
172.16.2.1      172.16.1.1      983         0x80000001 0x0084bd 0
```

- **show ip route ospf:** A diferencia del comando **show ip route** que muestra toda la tabla de enrutamiento, este solo muestra las rutas aprendidas por OSPF.

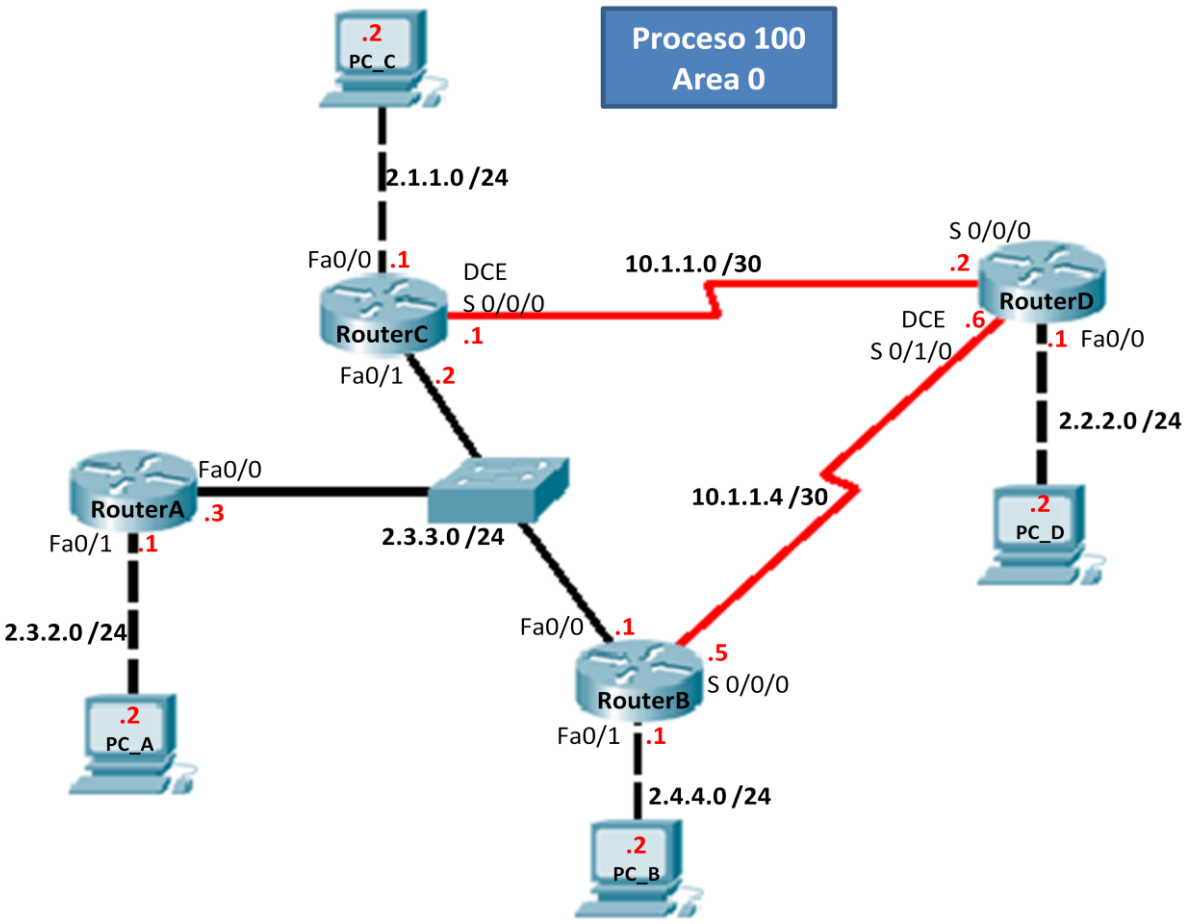
```
RouterD#show ip route ospf
     2.0.0.0/24 is subnetted, 4 subnets
O       2.1.1.0 [110/782] via 10.1.1.1, 00:28:07, Serial0/0/0
O       2.3.3.0 [110/782] via 10.1.1.1, 00:28:07, Serial0/0/0
                [110/782] via 10.1.1.5, 00:28:07, Serial0/1/0
O       2.4.4.0 [110/782] via 10.1.1.5, 00:28:07, Serial0/1/0
```

- **debug ip ospf events:** Informa de todos los eventos OSPF.

```
RouterD#debug ip ospf events
OSPF events debugging is on
RouterD#
02:30:35: OSPF: Rcv hello from 10.1.1.1 area 0 from Serial0/0/0
10.1.1.1
02:30:35: OSPF: End of hello processing
02:30:35: OSPF: Rcv hello from 10.1.1.5 area 0 from Serial0/1/0
10.1.1.5
02:30:35: OSPF: End of hello processing
02:30:45: OSPF: Rcv hello from 10.1.1.1 area 0 from Serial0/0/0
10.1.1.1
02:30:45: OSPF: End of hello processing
02:30:45: OSPF: Rcv hello from 10.1.1.5 area 0 from Serial0/1/0
10.1.1.5
02:30:45: OSPF: End of hello processing
02:30:55: OSPF: Rcv hello from 10.1.1.1 area 0 from Serial0/0/0
10.1.1.1
02:30:55: OSPF: End of hello processing
02:30:55: OSPF: Rcv hello from 10.1.1.5 area 0 from Serial0/1/0
10.1.1.5
02:30:55: OSPF: End of hello processing
```

- **debug ip ospf adj:** Informa los eventos de adyacencia OSPF.

EJEMPLO PRÁCTICO 3.5



- **Paso 1.**Se deben realizar las configuraciones básicas en los routers, es decir, la asignación de nombre, contraseñas y direcciones IP de las interfaces. Estas configuraciones para el router C, B y D son las mismas que en el ejemplo práctico 3.3 por lo cual aquí no se repetirán.

  Para el router A:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterA
RouterA(config)#enable secret fes
RouterA(config)#line vty 0 4
RouterA(config-line)#password unam
RouterA(config-line)#login
RouterA(config-line)#line con 0
RouterA(config-line)#password unam
```

```
RouterA(config-line)#login
RouterA(config-line)#exit
RouterA(config)#interface fastethernet 0/0
RouterA(config-if)#ip address 2.3.3.3 255.255.255.0
RouterA(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
RouterA(config-if)#interface fastethernet 0/1
RouterA(config-if)#ip address 2.3.2.1 255.255.255.0
RouterA(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
RouterA(config-if)#exit
RouterA(config)#
```

- **Paso 2.** Se configura el protocolo OSPF y se anuncian las redes que se encuentran conectadas a cada router.

Para el router A:

```
RouterA(config)#router ospf 100
RouterA(config-router)# network 2.3.3.0 0.0.0.255 area 0
RouterA(config-router)# network 2.3.2.0 0.0.0.255 area 0
RouterA(config-router)# exit
RouterA(config)#
```

Para el router B:

```
RouterB(config)#router ospf 100
RouterB(config-router)# network 2.3.3.0 0.0.0.255 area 0
RouterB(config-router)# network 2.4.4.0 0.0.0.255 area 0
RouterB(config-router)# network 10.1.1.4 0.0.0.3 area 0
RouterB(config-router)# exit
RouterB(config)#
```

Para el router C:

```
RouterC(config)#router ospf 100
```

```
RouterC(config-router)# network 2.1.1.0 0.0.0.255 area 0
RouterC(config-router)# network 10.1.1.0 0.0.0.3 area 0
RouterC(config-router)# network 2.3.3.0 0.0.0.255 area 0
RouterC(config-router)# exit
RouterC(config)#
```

Para el router D:

```
RouterD(config)#router ospf 100
RouterD(config-router)# network 2.2.2.0 0.0.0.255 area 0
RouterD(config-router)# network 10.1.1.0 0.0.0.3 area 0
RouterD(config-router)# network 10.1.1.4 0.0.0.3 area 0
RouterD(config-router)# exit
RouterD(config)#
```

- **Paso 3.** Se despliegan las tablas de enrutamiento de cada router para corroborar que aparezcan todas las redes del escenario.

Para el router A:

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 5 subnets
O       2.1.1.0 [110/2] via 2.3.3.2, 00:54:10, FastEthernet0/0
O       2.2.2.0 [110/402] via 2.3.3.1, 00:54:20, FastEthernet0/0
                [110/402] via 2.3.3.2, 00:54:10, FastEthernet0/0
C       2.3.2.0 is directly connected, FastEthernet0/1
C       2.3.3.0 is directly connected, FastEthernet0/0
O       2.4.4.0 [110/2] via 2.3.3.1, 00:54:20, FastEthernet0/0
     10.0.0.0/30 is subnetted, 2 subnets
O       10.1.1.0 [110/401] via 2.3.3.2, 00:54:10, FastEthernet0/0
O       10.1.1.4 [110/401] via 2.3.3.1, 00:54:20, FastEthernet0/0
```

Se observa que la tabla de enrutamiento del router A tiene instaladas las 7 redes del escenario, 5 fueron aprendidas por OSPF y tiene dos rutas a la red 2.2.2.0

Para el router B:

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 5 subnets
O       2.1.1.0 [110/2] via 2.3.3.2, 01:05:35, FastEthernet0/0
O       2.2.2.0 [110/401] via 10.1.1.6, 01:06:10, Serial0/0/0
O       2.3.2.0 [110/2] via 2.3.3.3, 01:05:35, FastEthernet0/0
C       2.3.3.0 is directly connected, FastEthernet0/0
C       2.4.4.0 is directly connected, FastEthernet0/1
     10.0.0.0/30 is subnetted, 2 subnets
O       10.1.1.0 [110/401] via 2.3.3.2, 01:05:35, FastEthernet0/0
C       10.1.1.4 is directly connected, Serial0/0/0
```

Para el router C:

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 5 subnets
C       2.1.1.0 is directly connected, FastEthernet0/0
O       2.2.2.0 [110/401] via 10.1.1.2, 01:09:09, Serial0/0/0
O       2.3.2.0 [110/2] via 2.3.3.3, 01:08:30, FastEthernet0/1
C       2.3.3.0 is directly connected, FastEthernet0/1
O       2.4.4.0 [110/2] via 2.3.3.1, 01:08:30, FastEthernet0/1
```

```
     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.1.1.4 [110/401] via 2.3.3.1, 01:08:30, FastEthernet0/1
```

Para el router D:

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

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 5 subnets
O       2.1.1.0 [110/401] via 10.1.1.1, 01:12:16, Serial0/0/0
C       2.2.2.0 is directly connected, FastEthernet0/0
O       2.3.2.0 [110/402] via 10.1.1.5, 01:11:41, Serial0/1/0
                [110/402] via 10.1.1.1, 01:11:31, Serial0/0/0
O       2.3.3.0 [110/401] via 10.1.1.5, 01:12:16, Serial0/1/0
                [110/401] via 10.1.1.1, 01:11:31, Serial0/0/0
O       2.4.4.0 [110/401] via 10.1.1.5, 01:12:16, Serial0/1/0
     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.1.1.4 is directly connected, Serial0/1/0
```

- **Paso 4.** Se despliega la tabla topológica de cada router.

Para el router A:

```
RouterA#show ip ospf database
            OSPF Router with ID (2.3.3.3) (Process ID 100)

              Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
2.3.3.3         2.3.3.3         518         0x80000011 0x00fdff 2
10.1.1.5        10.1.1.5        514         0x80000015 0x00fdff 4
10.1.1.1        10.1.1.1        513         0x80000017 0x00fdff 4
10.1.1.6        10.1.1.6        513         0x80000017 0x00fdff 5
```

```
                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
2.3.3.1         10.1.1.5        519         0x8000000d 0x00741b
```

Para el router B:

```
RouterB#show ip ospf database
            OSPF Router with ID (10.1.1.5) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.5        10.1.1.5        260         0x80000015 0x00fdff 4
2.3.3.3         2.3.3.3         265         0x80000011 0x00fdff 2
10.1.1.1        10.1.1.1        260         0x80000017 0x00fdff 4
10.1.1.6        10.1.1.6        259         0x80000017 0x00fdff 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
2.3.3.1         10.1.1.5        265         0x8000000d 0x00741b
```

Para el router C:

```
RouterC#show ip ospf database
            OSPF Router with ID (10.1.1.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        935         0x80000017 0x00fdff 4
2.3.3.3         2.3.3.3         941         0x80000011 0x00fdff 2
10.1.1.5        10.1.1.5        936         0x80000015 0x00fdff 4
10.1.1.6        10.1.1.6        935         0x80000017 0x00fdff 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
2.3.3.1         10.1.1.5        941         0x8000000d 0x00741b
```

Para el router D:

```
RouterD#show ip ospf database
            OSPF Router with ID (10.1.1.6) (Process ID 100)
```

```
                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.6        10.1.1.6        1205        0x80000017 0x00fdff 5
2.3.3.3         2.3.3.3         1211        0x80000011 0x00fdff 2
10.1.1.5        10.1.1.5        1207        0x80000015 0x00fdff 4
10.1.1.1        10.1.1.1        1206        0x80000017 0x00fdff 4

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
2.3.3.1         10.1.1.5        1212        0x8000000d 0x00741b
```

En estas tablas se observa que el ID de cada router es la dirección IP más alta de las interfaces activas y que la tabla topológica es la misma en todos los routers.

- **Paso 5.** Se ejecuta el comando **`show ip ospf interface`** en el router A, B y C.

  Para el router A:

```
RouterA#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 2.3.3.3/24, Area 0
  Process ID 100, Router ID 2.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 10.1.1.5, Interface address 2.3.3.1
  Backup Designated Router (ID) 10.1.1.1, Interface address 2.3.3.2
  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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.1.5  (Designated Router)
    Adjacent with neighbor 10.1.1.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet address is 2.3.2.1/24, Area 0
  Process ID 100, Router ID 2.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.3.3.3, Interface address 2.3.2.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
    Hello due in 00:00:03
  Index 2/2, 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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Para el router B:

```
RouterB#show ip ospf interface
FastEthernet0/1 is up, line protocol is up
  Internet address is 2.4.4.1/24, Area 0
  Process ID 100, Router ID 10.1.1.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.5, Interface address 2.4.4.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Internet address is 2.3.3.1/24, Area 0
  Process ID 100, Router ID 10.1.1.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.5, Interface address 2.3.3.1
  Backup Designated Router (ID) 10.1.1.1, Interface address 2.3.3.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 2/2, 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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.1.1  (Backup Designated Router)
    Adjacent with neighbor 2.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.5/30, Area 0
  Process ID 100, Router ID 10.1.1.5, Network Type POINT-TO-POINT, Cost:
400
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

```
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 3/3, 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 10.1.1.6
  Suppress hello for 0 neighbor(s)
```

Para el router C:

```
RouterC#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 2.1.1.1/24, Area 0
  Process ID 100, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.1, Interface address 2.1.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet address is 2.3.3.2/24, Area 0
  Process ID 100, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.1.1.5, Interface address 2.3.3.1
  Backup Designated Router (ID) 10.1.1.1, Interface address 2.3.3.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, 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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.1.5  (Designated Router)
    Adjacent with neighbor 2.3.3.3
  Suppress hello for 0 neighbor(s)
```

```
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30, Area 0
  Process ID 100, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost:
400
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 3/3, 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 10.1.1.6
  Suppress hello for 0 neighbor(s)
```

Se observa que para la red 2.3.3.0/24 el router designado es el router B (10.1.1.5) que es el que tiene la IP más alta y el router designado de respaldo es el router C (10.1.1.1).

- **Paso 6.** Se modifica la prioridad de la interfaz Fa0/0 del router A para que este sea ahora el router designado.

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#interface fa 0/0
RouterA(config-if)#ip ospf priority 5
RouterA(config-if)#exit
RouterA(config)#
```

Una vez modificada la prioridad se deben reiniciar los routers A y B para que exista otra elección de DR y el cambio de la prioridad sea tomada en cuenta.

```
RouterA#write
RouterA#reload
Proceed with reload? [confirm]y
```

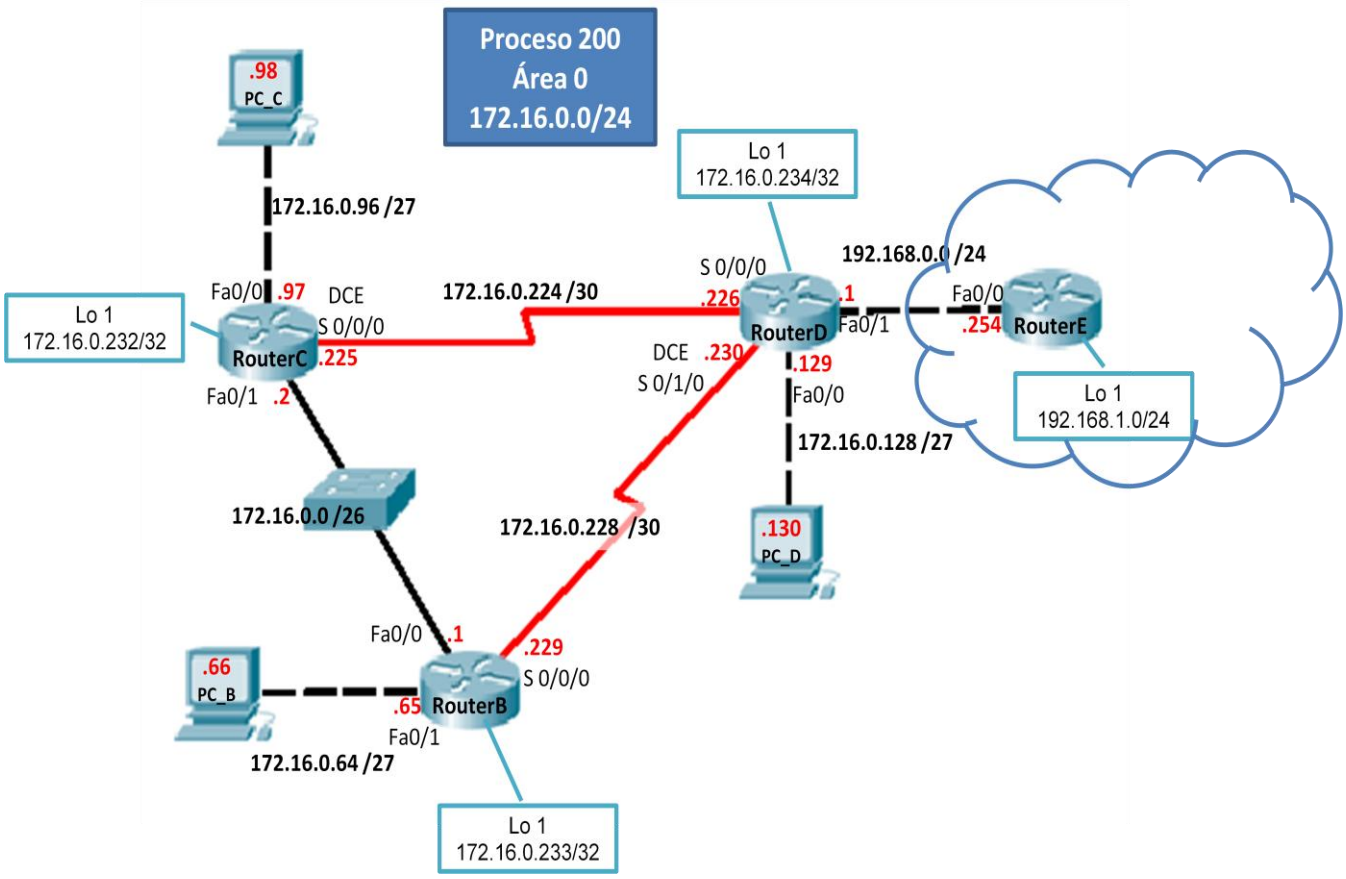
```
RouterB#write
RouterB#reload
Proceed with reload? [confirm]y
```

El comando **`write`** guarda la configuración actual en la configuración de inicio. Se ejecuta el comando **`show ip ospf interface`** en el router A.

```
RouterA#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 2.3.3.3/24, Area 0
  Process ID 100, Router ID 2.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 5
  Designated Router (ID) 2.3.3.3, Interface address 2.3.3.3
  Backup Designated Router (ID) 10.1.1.5, Interface address 2.3.3.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.1.5  (Backup Designated Router)
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet address is 2.3.2.1/24, Area 0
  Process ID 100, Router ID 2.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.3.3.3, Interface address 2.3.2.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 2/2, 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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
RouterA#
```

Ahora el router A (2.3.3.3) es el DR y el router B (10.1.1.5) el BDR.

EJEMPLO PRÁCTICO 3.6



- **Paso 1.**Se deben realizar las configuraciones básicas en los routers, es decir, la asignación de nombre, contraseñas y direcciones IP de las interfaces.

Para el router B:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterB
RouterB(config)#enable secret fes
RouterB(config)#line vty 0 4
RouterB(config-line)#password unam
RouterB(config-line)#login
RouterB(config-line)#line con 0
RouterB(config-line)#password unam
RouterB(config-line)#login
RouterB(config-line)#exit
RouterB(config)#interface fastethernet 0/0
RouterB(config-if)#ip address 172.16.0.1 255.255.255.192
```

```
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:     Line     protocol     on     Interface
FastEthernet0/0, changed state to up
RouterB(config-if)#interface fastethernet 0/1
RouterB(config-if)#ip address 172.16.0.65 255.255.255.224
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
RouterB(config-if)#interface serial 0/0/0
RouterB(config-if)#ip address 172.16.0.229 255.255.255.252
RouterB(config-if)#bandwidth 250
RouterB(config-if)#clock rate 250000
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
RouterB(config-if)#interface loopback 1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
RouterB(config-if)#ip address 172.16.0.233 255.255.255.255
RouterB(config-if)#exit
RouterB(config)#
```

Para el router C:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterC
RouterC(config)#enable secret fes
RouterC(config)#line vty 0 4
RouterC(config-line)#password unam
RouterC(config-line)#login
RouterC(config-line)#line con 0
RouterC(config-line)#password unam
RouterC(config-line)#login
RouterC(config-line)#exit
RouterC(config)#interface fastethernet 0/0
RouterC(config-if)#ip address 172.16.0.97 255.255.255.224
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
RouterC(config-if)#interface fastethernet 0/1
RouterC(config-if)#ip address 172.16.0.2 255.255.255.192
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
RouterC(config-if)#interface serial 0/0/0
RouterC(config-if)#ip address 172.16.0.225 255.255.255.252
RouterC(config-if)#bandwidth 250
RouterC(config-if)#clock rate 250000
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
RouterC(config-if)#interface loopback 1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
RouterC(config-if)#ip address 172.16.0.232 255.255.255.255
RouterC(config-if)#exit
RouterC(config)#
```

Para el router D:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterD
RouterD(config)#enable secret fes
RouterD(config)#line vty 0 4
RouterD(config-line)#password unam
RouterD(config-line)#login
RouterD(config-line)#line con 0
RouterD(config-line)#password unam
RouterD(config-line)#login
RouterD(config-line)#exit
RouterD(config)#interface fastethernet 0/0
RouterD(config-if)#ip address 172.16.0.129 255.255.255.224
RouterD(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
RouterD(config-if)#interface fastethernet 0/1
```

```
RouterD(config-if)# ip address 192.168.0.1 255.255.255.0
RouterD(config-if)# no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
RouterD(config-if)#interface serial 0/0/0
RouterD(config-if)#ip address 172.16.0.226 255.255.255.252
RouterD(config-if)#bandwidth 250
RouterD(config-if)#clock rate 250000
RouterD(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
RouterD(config-if)#interface serial 0/1/0
RouterD(config-if)#ip address 172.16.0.230 255.255.255.252
RouterD(config-if)#bandwidth 250
RouterD(config-if)#clock rate 250000
RouterD(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
RouterD(config-if)#interface loopback 1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
RouterD(config-if)#ip address 172.16.0.234 255.255.255.255
RouterD(config-if)#exit
RouterD(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up
```

Para el router E:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterE
RouterE(config)#enable secret fes
RouterE(config)#line vty 0 4
RouterE(config-line)#password unam
RouterE(config-line)#login
RouterE(config-line)#line con 0
RouterE(config-line)#password unam
RouterE(config-line)#login
RouterE(config-line)#exit
RouterE(config)#interface fastethernet 0/0
RouterE(config-if)#ip address 192.168.0.254 255.255.255.0
```

```
RouterE(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
RouterE(config-if)#interface Loopback 1
RouterE(config-if)#ip address 192.168.1.1 255.255.255.0

%LINK-5-CHANGED: Interface Loopback1, changed state to up
RouterE(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

- **Paso 2.** Se configura el protocolo OSPF y como se tiene una dirección subneteada para todo el dominio OSPF basta con anunciar la red 172.16.0.0/24 en los routers B, C y D. En el router D también se anuncia la red 192.168.0.0/24 y se configura como pasiva la interfaz respectiva.

Para el router B:

```
RouterB(config)#router ospf 200
RouterB(config-router)#network 172.16.0.0 0.0.0.255 area 0
RouterB(config-router)#exit
RouterB(config)#
```

Para el router C:

```
RouterC(config)#router ospf 200
RouterC(config-router)#network 172.16.0.0 0.0.0.255 area 0
RouterC(config-router)#exit
RouterC(config)#
```

Para el router D:

```
RouterD(config)#router ospf 200
RouterD(config-router)# network 172.16.0.0 0.0.0.255 area 0
RouterD(config-router)# network 192.168.0.0 0.0.0.255 area 0
RouterD(config-router)# passive-interface fastethernet 0/1
RouterD(config-router)# exit
RouterD(config)#
```

- **Paso 3.** Se ejecuta el comando **`show ip protocols`** en el router D.

```
RouterD#show ip protocols

Routing Protocol is "ospf 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.0.234
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.0.0 0.0.0.255 area 0
    192.168.0.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.0.225         110      00:17:17
    172.16.0.229         110      00:17:19
  Distance: (default is 110)
```

Entre otras cosas se observan las redes que anuncia para OSPF la interfaz pasiva que se configuro y la dirección de las interfaces de los routers que le envían información de enrutamiento.

- **Paso 4.** Se despliega la base de datos topológica en cada router del dominio OSPF.

```
RouterB#show ip ospf database
            OSPF Router with ID (172.16.0.233) (Process ID 200)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.0.234    172.16.0.234    155         0x80000007 0x0084dd 7
172.16.0.233    172.16.0.233    121         0x80000006 0x00f6bf 5
172.16.0.232    172.16.0.232    121         0x80000006 0x00346c 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.1      172.16.0.233    121         0x80000001 0x00f04f
```

```
RouterC#show ip ospf database
            OSPF Router with ID (172.16.0.232) (Process ID 200)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
Link count
172.16.0.234    172.16.0.234    327         0x80000007 0x0084dd
7
172.16.0.232    172.16.0.232    293         0x80000006 0x00346c
5
172.16.0.233    172.16.0.233    293         0x80000006 0x00f6bf
5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.1      172.16.0.233    293         0x80000001 0x00f04f
```

```
RouterD#show ip ospf database
            OSPF Router with ID (172.16.0.234) (Process ID 200)

                Router Link States (Area 0)

Link ID         ADV Router     Age         Seq#      Checksum Link count
172.16.0.234    172.16.0.234    379         0x80000007 0x0084dd 7
172.16.0.232    172.16.0.232    345         0x80000006 0x00346c 5
172.16.0.233    172.16.0.233    345         0x80000006 0x00f6bf 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.1      172.16.0.233    345         0x80000001 0x00f04f
```

Se observa que los ID de los routers son las interfaces loopback que se configuraron y que las bases de datos topológicas son iguales.

- **Paso 5.** Se configura en el router D una ruta estática a la red 192.168.1.0/24, se redistribuye en OSPF y se checan las tablas de enrutamiento de los routers OSPF.

```
RouterD(config)#ip route 192.168.1.0  255.255.255.0  192.168.0.254
RouterD(config)#router ospf 200
RouterD(config-router)#redistribute static subnets
RouterD(config-router)#exit
RouterD(config)#
```

En el router B:

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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 9 subnets, 4 masks
C       172.16.0.0/26 is directly connected, FastEthernet0/0
C       172.16.0.64/27 is directly connected, FastEthernet0/1
O       172.16.0.96/27 [110/2] via 172.16.0.2, 01:49:12, FastEthernet0/0
O       172.16.0.128/27 [110/401] via 172.16.0.230, 01:49:47, Serial0/0/0
O       172.16.0.224/30 [110/401] via 172.16.0.2, 01:49:12, FastEthernet0/0
C       172.16.0.228/30 is directly connected, Serial0/0/0
O       172.16.0.232/32 [110/2] via 172.16.0.2, 01:49:12, FastEthernet0/0
C       172.16.0.233/32 is directly connected, Loopback1
O       172.16.0.234/32 [110/401] via 172.16.0.230, 01:49:47, Serial0/0/0
O    192.168.0.0/24 [110/401] via 172.16.0.230, 01:49:47, Serial0/0/0
O E2 192.168.1.0/24 [110/20] via 172.16.0.230, 00:11:45, Serial0/0/0
```

En el router C:

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

Gateway of last resort is not set
```

```
     172.16.0.0/16 is variably subnetted, 9 subnets, 4 masks
C       172.16.0.0/26 is directly connected, FastEthernet0/1
O       172.16.0.64/27 [110/2] via 172.16.0.1, 02:09:34, FastEthernet0/1
C       172.16.0.96/27 is directly connected, FastEthernet0/0
O       172.16.0.128/27 [110/401] via 172.16.0.226, 02:10:09, Serial0/0/0
C       172.16.0.224/30 is directly connected, Serial0/0/0
O       172.16.0.228/30 [110/401] via 172.16.0.1, 02:09:34, FastEthernet0/1
C       172.16.0.232/32 is directly connected, Loopback1
O       172.16.0.233/32 [110/2] via 172.16.0.1, 02:09:34, FastEthernet0/1
O       172.16.0.234/32 [110/401] via 172.16.0.226, 02:10:09, Serial0/0/0
O    192.168.0.0/24 [110/401] via 172.16.0.226, 02:10:09, Serial0/0/0
O E2 192.168.1.0/24 [110/20] via 172.16.0.226, 00:32:07, Serial0/0/0
```

Se observa que aparecen todas las redes y subredes del escenario y que la ruta a la red 192.168.1.0/24 que fue redistribuida en OSPF por el router D es aprendida por el protocolo y marcada como externa de tipo dos. Esto significa que no se toma en cuenta el costo interno de la ruta, es por eso que tiene un costo de 20.

En el router D:

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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 9 subnets, 4 masks
O       172.16.0.0/26 [110/401] via 172.16.0.229, 01:44:44, Serial0/1/0
                      [110/401] via 172.16.0.225, 01:44:44, Serial0/0/0
O       172.16.0.64/27 [110/401] via 172.16.0.229, 01:44:44, Serial0/1/0
O       172.16.0.96/27 [110/401] via 172.16.0.225, 01:44:44, Serial0/0/0
C       172.16.0.128/27 is directly connected, FastEthernet0/0
C       172.16.0.224/30 is directly connected, Serial0/0/0
C       172.16.0.228/30 is directly connected, Serial0/1/0
O       172.16.0.232/32 [110/401] via 172.16.0.225, 01:44:44, Serial0/0/0
O       172.16.0.233/32 [110/401] via 172.16.0.229, 01:44:44, Serial0/1/0
C       172.16.0.234/32 is directly connected, Loopback1
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 192.168.0.254
```

En la tabla de enrutamiento del router C se ve que la ruta a la red 192.168.1.0/24 es marcada como estática.

- **Paso 6.** Se elimina la ruta estática a 192.168.1.0/24, se configura en el router D una ruta estática por defecto por la interfaz Fa 0/1, se redistribuye en OSPF y se checan las tablas de enrutamiento y las bases de datos topológicas de los routers OSPF.

```
RouterD(config)#no ip route 192.168.1.0  255.255.255.0  192.168.0.254
RouterD(config)#ip route 0.0.0.0 0.0.0.0 fastEthernet 0/1
RouterD(config)#router ospf 200
RouterD(config-router)#default-information originate
RouterD(config-router)#exit
RouterD(config)#
```

En el router B:

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

Gateway of last resort is 172.16.0.230 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 9 subnets, 4 masks
C       172.16.0.0/26 is directly connected, FastEthernet0/0
C       172.16.0.64/27 is directly connected, FastEthernet0/1
O       172.16.0.96/27 [110/2] via 172.16.0.2, 01:24:19, FastEthernet0/0
O       172.16.0.128/27 [110/401] via 172.16.0.230, 01:24:54, Serial0/0/0
O       172.16.0.224/30 [110/401] via 172.16.0.2, 01:24:19, FastEthernet0/0
C       172.16.0.228/30 is directly connected, Serial0/0/0
O       172.16.0.232/32 [110/2] via 172.16.0.2, 01:24:19, FastEthernet0/0
C       172.16.0.233/32 is directly connected, Loopback1
O       172.16.0.234/32 [110/401] via 172.16.0.230, 01:24:54, Serial0/0/0
O    192.168.0.0/24 [110/401] via 172.16.0.230, 01:24:54, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.0.230, 00:52:54, Serial0/0/0
```

```
RouterB#show ip ospf database
            OSPF Router with ID (172.16.0.233) (Process ID 200)

                Router Link States (Area 0)

Link  ID         ADV Router      Age         Seq#       Checksum Link count
172.16.0.233    172.16.0.233    1566        0x80000008 0x00f3c1 5
172.16.0.234    172.16.0.234    1601        0x8000000a 0x0085d8 7
172.16.0.232    172.16.0.232    1566        0x80000008 0x00316e 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.1      172.16.0.233    1566        0x80000003 0x00ed51

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.16.0.234    1505        0x80000005 0x00fc01 1
```

En el router C:

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

Gateway of last resort is 172.16.0.226 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 9 subnets, 4 masks
C       172.16.0.0/26 is directly connected, FastEthernet0/1
O       172.16.0.64/27 [110/2] via 172.16.0.1, 01:31:56, FastEthernet0/1
C       172.16.0.96/27 is directly connected, FastEthernet0/0
O       172.16.0.128/27 [110/401] via 172.16.0.226, 01:32:26, Serial0/0/0
C       172.16.0.224/30 is directly connected, Serial0/0/0
O       172.16.0.228/30 [110/401] via 172.16.0.1, 01:31:56, FastEthernet0/1
C       172.16.0.232/32 is directly connected, Loopback1
O       172.16.0.233/32 [110/2] via 172.16.0.1, 01:31:56, FastEthernet0/1
O       172.16.0.234/32 [110/401] via 172.16.0.226, 01:32:26, Serial0/0/0
O    192.168.0.0/24 [110/401] via 172.16.0.226, 01:32:26, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.0.226, 01:00:31, Serial0/0/0
```

```
RouterC#show ip ospf database
            OSPF Router with ID (172.16.0.232) (Process ID 200)

                Router Link States (Area 0)

Link  ID         ADV Router      Age         Seq#       Checksum Link count
172.16.0.232    172.16.0.232    271         0x80000009 0x00fdff 5
172.16.0.234    172.16.0.234    306         0x8000000b 0x00fdff 7
172.16.0.233    172.16.0.233    272         0x80000009 0x00fdff 5

               Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.1      172.16.0.233    272         0x80000004 0x00fdff

               Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.16.0.234    210         0x80000007 0x00ff27 1
```

En el router D:

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 9 subnets, 4 masks
O       172.16.0.0/26 [110/401] via 172.16.0.229, 00:01:07, Serial0/1/0
                      [110/401] via 172.16.0.225, 00:01:07, Serial0/0/0
O       172.16.0.64/27 [110/401] via 172.16.0.229, 00:01:07, Serial0/1/0
O       172.16.0.96/27 [110/401] via 172.16.0.225, 00:01:07, Serial0/0/0
C       172.16.0.128/27 is directly connected, FastEthernet0/0
C       172.16.0.224/30 is directly connected, Serial0/0/0
C       172.16.0.228/30 is directly connected, Serial0/1/0
O       172.16.0.232/32 [110/401] via 172.16.0.225, 00:01:07, Serial0/0/0
O       172.16.0.233/32 [110/401] via 172.16.0.229, 00:01:07, Serial0/1/0
C       172.16.0.234/32 is directly connected, Loopback1
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 is directly connected, FastEthernet0/1
```

```
RouterD#show ip ospf database
            OSPF Router with ID (172.16.0.234) (Process ID 200)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.0.234    172.16.0.234    188         0x80000008 0x0088d6 7
172.16.0.232    172.16.0.232    154         0x80000006 0x00346c 5
172.16.0.233    172.16.0.233    154         0x80000006 0x00f6bf 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.1      172.16.0.233    154         0x80000001 0x00f04f

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.16.0.234    198         0x80000001 0x000922 1
```

Se observa que la ruta estática se ha eliminado y se ha instalado la ruta estática por defecto la cual también es marcada como externa.

- **Paso 7.** En el router E es necesario configurar una ruta estática a la red 172.16.0.0/24 para que al ejecutar un ping o un traceroute desde cualquier parte del dominio OSPF al router E sea exitoso.

```
RouterE(config)#ip route 172.16.0.0 255.255.255.0 192.168.0.1
```

```
RouterB#traceroute 192.168.1.1
Type escape sequence to abort.
Tracing the route to 192.168.1.1

  1   172.16.0.230    31 msec   31 msec   16 msec
  2   192.168.0.254   63 msec   47 msec   63 msec
```

```
RouterC#ping 192.168.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.254, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
62/62/63 ms
```

CONCLUSIONES

Todos los temas que se trataron en este trabajo, y en particular el tema central de este trabajo que es el enrutamiento, son de suma importancia para toda la gente dedicada al área de las telecomunicaciones, ya que en la actualidad las redes son una parte muy importante para las personas en su vida personal y laboral.

Toda la información que se transmite o se recibe mediante internet pasa por un router, de ahí la importancia de la tarea que realiza este dispositivo para que la información llegue a su destino. El proceso de configuración del router debe ser muy cauteloso porque un minimo error basta para que el enrutamiento no funcione.

Cuando se estudia una carrera relacionada a las telecomunicaciones es necesario que además de manejar información teórica exista una manera de llevar a la práctica esa información para que realmente sea comprendida y aprovechada para el estudiante, aunque esto suele ser muy difícil por lo complejo que es contar con laboratorios equipados para realizar prácticas.

En este trabajo se desarrollaron los temas de una manera secuencial para que se obtenga un conocimiento teórico pero primordialmente práctico; por lo cual se realizan ejemplos prácticos para comprender cada tema en particular, logrando así una síntesis practica y concreta de estos temas. En su mayoría estos ejemplos pueden desarrollarse en el simulador *Cisco Packet Tracer*. Por lo anterior se puede tomar la información comprendida en este trabajo para elaborar un curso teórico - práctico de enrutamiento.

El único inconveniente de utilizar un simulador para realizar las prácticas, es que no se pueden analizar fallas que usualmente se presentan físicamente como lo son:

- Un cable dañado
- Un cable mal conectado
- Una interfaz dañada
- Una memoria dañada
- El sistema operativo dañado, etc.

El contenido de este trabajo puede considerarse el cimiento, para las personas que deseen profundizar o volverse expertos en la configuración de routers CISCO, pues es muy extensa la cantidad de temas que puede englobar la configuración de un router.

El hecho de estar familiarizado con el sistema operativo CISCO IOS toma gran importancia ya que los dispositivos utilizados en la mayor parte del backbone de Internet y en grandes empresas en todo el mundo son configurados mediante este sistema operativo.

BIBLIOGRAFÍA

- Ariganello Ernesto (2008). *Técnicas de configuración de routers Cisco*. México: Alfaomega

- Beijnum Iljitsch van (2006). *Running IPv6.* Berkeley, CA: Apress

- Benchimol Daniel (2010). *Redes Cisco.* Banfield, Lomas de Zamora: Gradi

- Clare Gough (2004). *CCNP BSCI Exam Certification Guide* (3ª ed.). Indianapolis, IN: Cisco Press

- Couch II Leon W. (1997). *Digital and analog communications systems* (5ª ed.). U.S.A.: Prentice-Hall International Inc.

- *Guía rápida para routers de la serie Cisco 2800 de servicios integrados* (2004). San José, CA: Cisco

- Habraken Joseph (2000). *Routers Cisco.* México: Prentice-Hall.

- Lammle T., Odom S. y Wallace K. (2001). *CCNP Routing Study Guide.* Alameda, CA: SYBEX Inc.

- Stallings William (2004). *Comunicaciones y Redes de computadores* (7ª ed.). Madrid: Pearson Educación S.A

- Stallings William (1997). *Data and computer communications* (5ª ed.). New Jersey: Prentice-Hall Inc.

REFERENCIAS ELECTRÓNICAS

- *Cisco Certified Network Associate Curriculum, Semestre 1*, Version 2.1.2.
- *Cisco Certified Network Associate Curriculum, Semestre 1*, Version 2.1.
- *Cisco Certified Network Associate Curriculum, Semestre 2*, Versón 2.1.
- Graziani Rick*, CCNA 1* versión 3.0,
- http://www.redescisco.net/node/28