Capítulo 5

EIGRP: PROTOCOLO DE ENCAMINAMIENTO IP

EIGRP (Enhanced Interior Gateway Routing Protocol) es un protocolo de enrutamiento propietario de Cisco, concebido para que funcione en aquellas redes implementadas solamente con equipos marca Cisco. No obstante, la fortaleza de este protocolo consiste en que es fácil de configurar, eficiente, confiable y soporta características que se requieren en las grandes redes: máscara de longitud variable y CIDR (Classless Interdomain Routing). La eficiencia de EIGRP se basa en que distribuye únicamente información de las rutas que cambian y que lo hace solamente en el momento en que se presenta el cambio. En una red estable, los encaminadores que utilizan EIGRP solamente requieren intercambiar unos paquetes denominados "Hello", esto con el propósito de verificar la disponibilidad de los encaminadores vecinos. OSPF es una alternativa a EIGRP con características similares, pero con la ventaja adicional de ser un protocolo abierto, por ser estándar. En el presente capítulo se aborda la configuración de redes que utilizan el protocolo de enrutamiento EIGRP y la verificación del funcionamiento de las mismas.

Objetivo

Al finalizar el presente módulo, el estudiante estará en capacidad de:

- Configurar el protocolo de enrutamiento EIGRP.
- Verificar y monitorear el funcionamiento del protocolo EIGRP.

Procedimiento

Configuración de EIGRP

El comando *router eigrp* selecciona a EIGRP como protocolo de enrutamiento IP.

Tareas Globales

R1(config)# *router eigrp* process-ID-number

El comando anterior define a EIGRP como protocolo de enrutamiento IP. Después de ejecutar dicho comando, el indicador del sistema cambia para señalar que el usuario está en modo de configuración específica del protocolo de enrutamiento EIGRP.

R1(config-router)# *network* network-number

La configuración del protocolo de enrutamiento EIGRP es obligatoria para el proceso de enrutamiento IP. El comando *network* es requerido porque permite que el proceso de enrutamiento determine cuáles interfaces participarán en el intercambio (envío y recepción) de las actualizaciones de enrutamiento (routing updates).

El campo *network-number* especifica una o varias redes que se encuentran directamente conectadas al encaminador, este campo está basado en los números de red classful, no en números de subred o en direcciones IP individuales.

Ejemplo de configuración de EIGRP para la red de la Figura 4.1:

R1(config)# *router* eigrp 100
R1(config-router)# *network* 10.0.0.0
R1(config-router)# *network* 8.0.0.0

R2(config)# *router* eigrp 100
R2(config-router)# *network* 30.0.0.0
R2(config-router)# *network* 8.0.0.0

Después de configurar las respectivas direcciones IP en las interfaces de R1, el comando *router eigrp 100* selecciona a EIGRP (con el número de identificación del proceso igual a 100) como protocolo de enrutamiento IP, mientras que los comandos *network 10.0.0.0* y *network 8.0.0.0* especifican

las redes directamente conectadas al encaminador R1; las interfaces de R1 conectadas a estas redes intercambiarán información de enrutamiento (por medio de EIGRP) con otros encaminadores vecinos que se conecten directamente a dichas redes.

Monitoreo de IP

El comando *show ip protocols* muestra los valores de los filtros, temporizadores de enrutamiento e información de la red asociada con el encaminador. El comando *show ip route* muestra el contenido de la tabla de enrutamiento; ésta contiene las redes y subredes que el encaminador conoce y un código que indica cómo se obtuvo la información.

R1# *show ip protocols*

```
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
  10.0.0.0/8 for Serial0/0
  Summarizing with metric 281600
  8.0.0.0/8 for FastEthernet0/0, FastEthernet0/1
  Summarizing with metric 2169856
  Maximum path: 4
  Routing for Networks:
  8.0.0.0
  10.0.0.0
  Routing Information Sources:
  Gateway Distance Last Update
  (this router) 90 00:01:11
  Gateway Distance Last Update
  8.3.1.6 90 00:00:52
  Distance: internal 90 external 170
```

R1# *show ip route*

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, 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

 8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D 8.0.0.0/8 is a summary, 00:05:59, Null0
C 8.3.1.4/30 is directly connected, Serial0/0
 10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.3.1.0/24 is directly connected, FastEthernet0/0
D 10.0.0.0/8 is a summary, 00:05:59, Null0
C 10.3.2.0/24 is directly connected, FastEthernet0/1
D 30.0.0.0/8 [90/2195456] via 8.3.1.6, 00:05:33, Serial0/0
```

El comando *terminal monitor* redirige la salida de los mensajes que normalmente van a consola, haciendo que estos vayan hacia la sesión vty que se haya establecido con el encaminador. El comando *debug* permite que el encaminador presente lo que realmente está sucediendo con un protocolo específico.

R1# *terminal monitor*
R1# *debug ip eigrp transmit*

```
R1# EIGRP protocol debugging is on
Sep 11 08:37:39.599: First peer: startup anchor at serno 1, target serno 6
Sep 11 08:37:39.599: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 8.3.1.6
(Serial0/0) is up: new adjacency
Sep 11 08:37:39.603: New peer 8.3.1.6 on Serial0/0
Sep 11 08:37:39.603: Enqueuing NULL update to 8.3.1.6, flags 0x1
Sep 11 08:37:39.611: Building unicast STARTUP packet for 8.3.1.6, serno 0-0
Sep 11 08:37:39.611: No items in range
Sep 11 08:37:39.615: Packetizing timer expired on Serial0/0
Sep 11 08:37:39.615: Packets pending on Serial0/0
Sep 11 08:37:39.615: Intf Serial0/0 startup packetized UPDATE 1-5
Sep 11 08:37:39.615: Interface is now quiescent
Sep 11 08:37:39.691: Packet acked from 8.3.1.6 (Serial0/0), serno 0-0
Sep 11 08:37:39.695: Startup update acked from 8.3.1.6, serno 0-0
```

El comando *show ip interface* muestra las características de funcionamiento de las interfaces del encaminador.

R1# *show ip interface*

```
FastEthernet0/0 is up, line protocol is up
Internet address is 10.3.1.1/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

Serial0/0 is up, line protocol is up
Internet address is 8.3.1.5/30
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
–Salida truncada por brevedad–
```

Informe

Por medio del software Configmaker de Cisco, interconecte dos redes de área local sobre las cuales corren aplicaciones TCP/IP. Utilizar dos encaminadores Cisco de la serie 1600, un enlace HDLC a 64.000 bps (bits por segundo) y el protocolo EIGRP. Interpretar los archivos de configuración generados y hacer los respectivos comentarios sobre las líneas más importantes que usted desconozca.

Explique las ventajas y desventajas de utilizar EIGRP en lugar de RIP v2.0. Compare el protocolo EIGRP con el protocolo OSPF.

Ejercicios de laboratorio

Este ejercicio de laboratorio tiene como finalidad configurar los encaminadores R1, R2 y R3 de la red en la Figura 4.2, utilizando el protocolo de enrutamiento EIGRP. Configurar los encaminadores R1, R2 y R3 para que intercambien tablas de enrutamiento utilizando el protocolo EIGRP.

Información complementaria

EIGRP usa el algoritmo de actualización difusa –Diffusing Update Algorithm (DUAL)– el cual permite: que cada encaminador de la red se asegure de que su tabla de enrutamiento esté libre de bucles; que un encaminador use simultáneamente varios caminos posibles hacia un mismo destino, siempre y cuando estos caminos tengan igual métrica o costo; que cuando un camino hacia el mismo destino tenga una métrica mayor, éste quede como candidato para remplazar al mejor camino, en caso que este último falle.

En contraste con EIGRP, el problema principal con los protocolos vector distancia –RIP V1.0 e IGRP (predecesor de EIGRP)– es que estos convergen muy lentamente y tienen dificultades con los bucles de enrutamiento, dichas limitaciones se tratan a continuación.

Convergencia

Es definida como el tiempo que se requiere para que todos los encaminadores conozcan la topología de la red.

Debido a que los protocolos tipo vector distancia usan periodos temporizados para anunciar sus tablas, la convergencia es lenta, esto se agudiza cuando la red está conformada por muchos encaminadores.

A modo de ejemplo, suponiendo que se tienen las redes Net1, Net2, Net3 y Net4 interconectadas por medio de los encaminadores R1, R2 y R3, y

que se presenta un evento en el cual falla la interfaz Ethernet de R1 que se conecta a Net1 (R1 elimina a Net1 en su tabla de enrutamiento), y suponiendo también que el periodo del temporizador de R1 es de 30 segundos, entonces: R1 deberá esperar un tiempo que puede llegar a ser hasta de 30 segundos para anunciar dicho evento a R2; a su vez, cuando R2 reciba la actualización (y elimine de su tabla de enrutamiento a Net1), deberá esperar un tiempo que puede llegar a ser hasta de 30 segundos para anunciar el evento a R3 (y para que este último elimine la entrada de Net1). Como se puede apreciar, el tiempo de convergencia de esta internet puede llegar a ser de 60 segundos; tiempo que puede ser superior, si la internet es más grande, es decir, si la conforman un mayor número de encaminadores y de redes.

Actualizaciones provocadas (Triggered updates)

Un problema al usar periodos temporizados es que la convergencia es muy lenta. Para aumentar la rapidez de convergencia, algunos protocolos vector distancia usan actualizaciones provocadas. Tan pronto como se presenta un cambio en la topología, el encaminador inmediatamente difunde su tabla de enrutamiento. IGRP es un ejemplo de un protocolo de enrutamiento que usa actualizaciones provocadas. La desventaja de usar este tipo de actualizaciones se observa cuando se tiene una ruta que oscila; cada cambio en el estado de una red conectada a un encaminador causará que éste difunda su tabla de enrutamiento, creando posiblemente una tormenta de "broadcast".

Bucles de Enrutamiento

Otro problema con los protocolos vector distancia radica en que estos son propensos a bucles de enrutamiento, lo cual básicamente consiste en un desacuerdo acerca de cómo alcanzar una red destino. La Figura 4.1 se puede utilizar para describir un caso muy simple de bucle de enrutamiento, si se supone que la Tabla 5.1 representa las entradas en la respectiva tabla de enrutamiento de R1 y R2.

Tabla 5.1 Entradas en la tabla de enrutamiento de R1 y R2

Tabla de enrutamiento de R1			Tabla de enrutamiento de R2		
Network	**Next Hop**	**Interface**	**Network**	**Next Hop**	**Interface**
10.3.1.0/24	Directa	E0	8.3.1.4/30	Directa	S0
10.3.2.0/24	Directa	E1	30.0.0.0/8	Directa	E0
8.3.1.4/30	Directa	S0	10.3.1.0/24	8.3.1.5	S0
30.0.0.0/8	8.3.1.6	S0	10.3.2.0/24	8.3.1.5	S0
20.0.0.0/8	**8.3.1.6**	**S0**	**20.0.0.0/8**	**8.3.1.5**	**S0**

En este caso el encaminador R1 cree que para alcanzar la red 20.0.0.0/8 deberá reenviar el tráfico (paquetes IP) al encaminador R2; no obstante, el encaminador R2 cree que para alcanzar la misma red (20.0.0.0/8) le debe reenviar el tráfico a R1, por lo cual se ha formado un bucle de enrutamiento.

Los protocolos vector distancia tienen ciertos mecanismos que pueden usar para resolver los bucles de enrutamiento. No obstante, dichas soluciones crean un problema adicional: los protocolos vector distancia convergen muy lentamente, en comparación con los protocolos de estado de enlace (link state), como OSPF, y con los protocolos híbridos, como EIGRP.

Conteo a infinito

Un síntoma de un bucle de enrutamiento es llamado "conteo a infinito". En esta condición, existe un bucle de enrutamiento y cada datagrama IP con destino a la red 20.0.0.0/8 (continuando con el ejemplo anterior) quedará circulando continuamente alrededor del anillo, gastando ancho de banda y ciclos de CPU en los encaminadores que forman parte del bucle.

Para prevenir este problema, los protocolos vector distancia definen el máximo número de encaminadores (hops) que se le permite visitar a un datagrama IP. Esto asegura que, si se presentase un bucle, los datagramas IP no circularán indefinidamente. En IP, esta función la hace el campo TTL (Time-To-Live) del encabezado del datagrama IP. No obstante, este mecanismo no resuelve el problema de los bucles de enrutamiento; lo que hace es evitar que los datagramas IP circulen indefinidamente, descartándolos después de que exceden su TTL. El RIP de IP y el RIP de IPX, por defecto, permiten un máximo número de saltos (hop count) de 15, mientras que IGRP permite, por defecto, un máximo número de saltos de 100.

Para resolver los problemas de los bucles de enrutamiento, los protocolos vector distancia implementan diversas soluciones, algunas se describen a continuación.

División horizontal (Split horizon)

La primera solución, Split horizon, ayuda a resolver problemas de bucles de enrutamiento pequeñas; establece que, si un encaminador vecino (R2) envía información sobre una ruta que conoce hacia otro encaminador (R1), el encaminador que recibe la información de la ruta (R1) no debe propagarla de regreso por la misma interfaz que fue previamente recibida.

Si en la Figura 4.1 se asume que el encaminador R2 le anuncia la red 30.0.0.0/8 (la cual está conectada a su interfaz de Lan Ethernet 0) al encaminador R1 y que posteriormente la interfaz Ethernet 0 de R2 falla, se tiene que, sin split horizon en efecto, el encaminador R1 anunciaría la red

30.0.0.0/8 de regreso al encaminador R2, indicándole que para alcanzar dicha red el encaminador R2 debería enviar los datagramas IP al encaminador R1. Obviamente, de acuerdo a la topología de la Figura 4.1, esto sería imposible, puesto que solamente el encaminador R2 está conectado a la red 30.0.0.0/8. Con split horizon en efecto, el Encaminador R1 solamente anunciará al encaminador R2 las dos redes que tiene directamente conectadas (10.3.1.0/24 y 10.3.2.0/24) y que no han podido ser previamente anunciadas por el encaminador R2.

Envenenamiento de ruta (Route poisoning)

Para resolver los problemas de bucles de enrutamiento grandes, los protocolos vector distancia utilizan dos soluciones complementarias: envenenamiento de ruta y temporizadores de cuenta regresiva. El envenenamiento de ruta se deriva de split horizon, se basa en que, cuando el encaminador detecta un cambio en una entrada de la tabla de enrutamiento (por falla de una de sus interfaces), envenenará dicha entrada asignándole una métrica infinita, haciéndola muy indeseable para ser escogida. Por ejemplo, en RIP, un número de saltos de 16 es considerado como una red inalcanzable (métrica infinita); RIP permite que el tráfico tenga un máximo de 15 saltos. Cuando el encaminador comparte la ruta envenenada con los encaminadores vecinos, estos enviarán de regreso hacia el encaminador origen de la ruta envenenada un envenenamiento inverso (poison reverse). En tal circunstancia, los encaminadores que envían el envenenamiento inverso violan las reglas de split horizon. Esta violación excepcional se permite para asegurase que todos los encaminadores reciban el cambio anunciado por el encaminador que envía la ruta envenenada.

Una ruta envenenada es una ruta que tiene asignada una métrica infinita. Las rutas envenenadas se usan para resolver problemas de bucles de enrutamiento grandes. Cuando un encaminador recibe una ruta envenenada, viola las reglas de split horizon y envía una actualización de envenenamiento inverso de regreso al origen de la ruta envenenada.

Temporizadores de cuenta regresiva (Hold down timers)

Con el propósito de que los encaminadores tengan suficiente tiempo para propagar las rutas envenenadas, y asegurarse de que no ocurran bucles inadvertidamente mientras esto está sucediendo, los encaminadores emplean un mecanismo denominado “temporizadores de cuenta regresiva” (hold-down timers), que congelan las rutas envenenadas en la tabla de enrutamiento por un periodo de tiempo específico. Este intervalo es usualmente igual a tres veces el intervalo del periodo de actualización.

Cada temporizador hará una cuenta regresiva durante la cual mantendrá congelada la ruta envenenada en la tabla de enrutamiento (con su métrica en infinito) hasta que la cuenta llegue a cero. No obstante, si el encaminador recibe una actualización de un encaminador vecino que anuncia una métrica mejor de la que tenía la ruta original antes de ser envenenada, el encaminador eliminará el temporizador y actualizará su tabla de enrutamiento con el nuevo camino hacia la red destino. Si el encaminador recibe una actualización de un encaminador vecino con una métrica peor que la de la ruta original, asumirá que este camino alterno es parte del bucle de enrutamiento, ignorará la información y continuará con el conteo regresivo. Mientras este proceso está ocurriendo, la tabla de enrutamiento en el encaminador mostrará la ruta como posiblemente caída (possibly down).

Los temporizadores de cuenta regresiva trabajan en conjunto con el envenenamiento de ruta. Con el fin de dar suficiente tiempo a una ruta envenenada para que se propague a través de la red, los encaminadores la congelan en la tabla de enrutamiento hasta que el temporizador de cuenta regresiva expire o hasta que estos aprendan un camino alterno para alcanzar el destino, siempre y cuando este camino tenga una mejor métrica que el camino original.

Ejemplo de ruta envenenada y temporizadores de cuenta regresiva

Con la finalidad de proporcionar un ejemplo sobre el funcionamiento de la ruta envenenada y los temporizadores de cuenta regresiva, se asumirá que en los encaminadores de la Figura 4.2 se está ejecutando RIP V1.0. En este caso, se asume que la red conectada al encaminador R1, la red 192.168.1.0/24, falla. Sin actualizaciones provocadas, el encaminador R1 tendrá que esperar la expiración del temporizador de actualización de enrutamiento antes de poder difundir su tabla de enrutamiento hacia los encaminadores R2 y R3. Para RIP V1.0 de IP, por defecto, este temporizador está configurado en 30 segundos. En esta circunstancia, el encaminador R1 envenenará la ruta, asignándole una métrica infinita (de 16). Cuando los encaminadores R2 y R3 reciban la ruta envenenada, enviarán de regreso al encaminador R1 un envenenamiento inverso y congelarán la ruta envenenada (en su tabla de enrutamiento) por un periodo de tiempo igual al indicado en el temporizador de cuenta regresiva (en el caso de RIP V1.0, tiene un valor de 180 segundos). Los encaminadores R2 y R3 también anunciarán a las intefaces restantes la existencia de la ruta envenenada. No obstante, para realizar dicho anuncio, tendrán que esperar a que su temporizador de actualización de enrutamiento expire (30 segundos). Al tiempo que esto ocurre, los encaminadores R2 y R3 estarán haciendo un conteo regresivo de su temporizador de cuenta regresiva.

Si otro encaminador anuncia un camino alterno para llegar a la red 192.168.1.0/24 con una métrica mayor a la que estuvo anunciando el encaminador R1 (en el caso de RIP V1.0, la métrica se basa en el número de saltos), los encaminadores R2 y R3 no utilizarán dicho anuncio hasta que expire el temporizador de cuenta regresiva, la razón: el camino anunciado puede corresponder a un bucle y no ser un camino válido. El problema con este enfoque se presenta cuando existe otro camino alterno real para alcanzar la red 192.168.1.0/24, aunque con una métrica peor, puesto que, debido a las reglas de los temporizadores de cuenta regresiva, los encaminadores R2 y R3 no pueden usar dicho camino hasta que sus temporizadores expiren.

Si en cualquier momento se restaura la conexión de la red 192.168.1.0/24 con la interfaz del encaminador R1, éste empezará a anunciar la disponibilidad de dicha red a los encaminadores R2 y R3. Por lo que la métrica que el encaminador R1 anuncia ahora para la red 192.168.1.0/24 no es peor que la de la ruta original, los encaminadores R2 y R3 inmediatamente remplazarán la ruta envenenada con la ruta anunciada.

Problemas

1. Si un conmutador tiene 10 interfaces VLAN capa 3 (Vlan1 a Vlan10) con sus respectivas direcciones IP configuradas (192.168.1.1/24 para Vlan1, 192.168.2.1/24 para Vlan2, etc.), explique cuál es el resultado de los siguientes comandos:

```
SW1(config)# router eigrp 100
SW1(config-router)# network 192.168.0.0 0.0.255.255
SW1(config-router)# no auto-summary
SW1(config-router)# passive-interface default
SW1(config-router)# no passive-interface Vlan10
```

2. Al configurar los temporizadores “hello intervalo” en 4 segundos y “hold time” en 12 segundos en la interfaz serial 0 ¿cuál es el resultado respecto al funcionamiento del protocolo EIGRP (con número de identificación del proceso igual a 100)?

```
R1(config)# interface Serial 0
R1(config-if)# ip hello-interval eigrp 100 4
R1(config-if)# ip hold-time eigrp 100 12
```

3. Intente configurar a R1 y R2 de la Figura 4.1 para habilitar la autenticación del protocolo EIGRP. Ayuda: el siguiente trozo de código configura la autenticación MD5 de eigrp 100 en el encaminador R1.

```
R1(config)# key chain LAB
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string laboratorio
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0
R1(config-if)# ip authentication mode eigrp 100 md5
R1(config-if)# ip authentication key-chain eigrp 100 LAB
```

4. Después de configurar las direcciones IP de las respectivas interfaces de los dos encaminadores de la Figura 4.1, y de habilitar el protocolo eigrp 100 en R1 y R2, intente configurar a R1 para que distribuya solo la ruta por defecto y suprima el resto de rutas. Ayuda: utilice el siguiente trozo de código.

```
R1(config)# interface serial 0
R1(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0
R1(config-if)# end
```

Glosario

Bucle de enrutamiento: es cuando se presentan inconsistencias en la información que contienen las tablas de enrutamiento, causando que un datagrama IP quede viajando en un círculo vicioso.

Convergencia: se presenta cuando todos los encaminadores de la red logran tener la misma información topológica de ella.

Enrutamiento: proceso que permite decidir la interfaz por la que se debe enviar un datagrama IP y la dirección IP del próximo equipo al que se le debe enviar.

Envenenamiento de ruta: mecanismo por el cual se asocia un costo excesivamente alto a una entrada de la tabla de enrutamiento con el propósito de evitar que dicha entrada sea considerada por el proceso de enrutamiento.

Red tipo classful: hace referencia a una red clase A (máscara 255.0.0.0), clase B (máscara 255.255.0.0) o clase C (máscara 255.255.255.0).

Bibliografía

BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.

DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook ™*. 2nd Ed. Sebastopol, CA: O'Reilly.

DOYLE, J.; CARROLL, J. (2007). *Routing TCP/IP*. 2nd Ed. Indianapolis, IN: Cisco Press. Vol. 1.