

Routing Dinámico

Evolución del protocolo de routing dinámico

Los protocolos de routing dinámico se utilizan en el ámbito de las redes desde finales de la década de los ochenta. Uno de los primeros protocolos de routing fue el RIPv1.

Las redes han evolucionado y se han vuelto mas complejas motivado a esta situación surgieron nuevos protocolos de enrutamiento. RIPv1 se actualizo a RIPv2, sin embargo, este protocolo no escala en redes de tamaños de considerables en la actualidad. Para satisfacer las necesidades de entornos más complejos y grandes, se desarrollaron protocolos de enrutamiento como por ejemplo OSPF, IS-IS. Cisco definió y desarrolló un protocolo de enrutamiento como es IGRP el cual fue mejorado por EIGRP.

La necesidad de interconectar diferentes redes a nivel mundial mediante la Internet y proporcionar un enrutamiento adecuado promovió el desarrollo de protocolos tales como BGP el cual es comúnmente utilizado entre los ISP (Proveedores de Servicios de Internet).

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

Uso del routing estático

El routing estático todavía es una modalidad utilizada en redes hoy en día. De hecho, las redes generalmente poseen una combinación entre routing dinámico y estático. A continuación, se mostrará los usos principales del routing estático:

Facilita el mantenimiento en redes las cuales no tienen previsto que crezcan significativamente

Permite acceder a una única ruta predeterminada (la cual es utilizada para representar una ruta hacia cualquier red que no tiene una coincidencia mas especifica con otra ruta en la tabla de routing)

Ventajas y desventajas del routing estático

Ventajas	Desventajas
Fácil de implementar en una red pequeña.	Adecuado solamente para topologías simples o para fines específicos, como una ruta estática predeterminada.
Muy seguro. No se envían anuncios, a diferencia del caso de los protocolos de routing dinámico.	La complejidad de la configuración aumenta notablemente a medida que crece la red.
La ruta hacia el destino siempre es la misma.	Se requiere intervención manual para volver a enrutar el tráfico.
Dado que no se requieren algoritmos de routing ni mecanismos de actualización, no se necesitan recursos adicionales (CPU o RAM).	

Ventajas y desventajas del routing dinámico

Ventajas	Desventajas
Adecuado en todas las topologías donde se requieren varios routers.	La implementación puede ser más compleja.
Por lo general, es independiente del tamaño de la red.	Menos seguro. Se requieren opciones de configuración adicionales para proporcionarle protección.
Si es posible, adapta automáticamente la topología para volver a enrutar el tráfico.	La ruta depende de la topología actual.
	Requiere CPU, RAM y ancho de banda de enlace adicionales.

Modo de configuración de RIP en el router

Como bien se sabe el protocolo RIP es utilizado con muy poca frecuencia en las redes modernas, sin embargo, es útil para comprender el routing de red básico.

Para habilitar rip, utilice el comando `router rip`, este comando no inicia en forma directa el proceso del RIP.

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```

En cambio, proporciona acceso al modo de configuración del router, donde se configuran los parámetros de routing RIP. Al habilitar RIP, la versión predeterminada es RIPv1.

Para deshabilitar y eliminar RIP, utilice el comando de configuración global `no router rip`. Este comando elimina y detiene todas las configuraciones RIP existentes

Verificar el routing del RIP

El comando `show ip protocols` muestra los parámetros del protocolo de routing IPv4 configurados actualmente en el router.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip

  Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  GigabitEthernet0/0  1     1  2
  Serial0/0/0        1     1  2

  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0

  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2      120          00:00:15
  Distance: (default is 120)
```

Habilitación y verificación de RIPv2

De manera predeterminada, cuando hay un proceso de RIP configurado en un router Cisco, este ejecuta RIPv1. Sin embargo, a pesar de que el router sólo envía mensajes de RIPv1, puede interpretar los mensajes de RIPv1 y RIPv2. Los routers RIPv1 simplemente ignoran los campos de RIPv2 en la entrada de ruta.

Utilice el comando del modo de configuración del router `version 2` para habilitar RIPv2

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# ^Z
R1#
R1# show ip protocols | section Default
  Default version control: send version 2, receive version 2
  Interface          Send Recv Triggered RIP Key-chain
  GigabitEthernet0/0  2     2
  Serial0/0/0        2     2
R1#
```

Deshabilite el resumen automático

RIPv2 resume automáticamente las redes en los límites de red principales de manera predeterminada, al igual que RIPv1.

```
R1(config)# router rip
R1(config-router)# no auto-summary
R1(config-router)# end
R1#
*Mar 10 14:11:49.659: %SYS-5-CONFIG_I: Configured from
console by console
R1# show ip protocols | section Automatic
Automatic network summarization is not in effect
R1#
```

Configuración de interfaces pasivas

De manera predeterminada, las actualizaciones de RIP se reenvían por todas las interfaces con RIP habilitado. Sin embargo, las actualizaciones de RIP solo se deben enviar por interfaces conectadas a otros routers con RIP habilitado

El envío de actualizaciones innecesarias a una LAN impacta en la red de tres maneras:

- **Desperdicio de ancho de banda:** se utiliza ancho de banda para transportar actualizaciones innecesarias. Dado que las actualizaciones de RIP se transmiten por difusión o multidifusión, los switches también reenvían las actualizaciones por todos los puertos.
- **Desperdicio de recursos:** todos los dispositivos en la LAN deben procesar la actualización hasta las capas de transporte, punto en el cual los dispositivos descartan la actualización.
- **Riesgo de seguridad:** el anuncio de actualizaciones en una red de difusión constituye un riesgo de seguridad. Las actualizaciones RIP pueden interceptarse con software analizador de protocolos. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico.

Utilice el comando de configuración del router **passive-interface** para evitar que las actualizaciones de routing se transmitan a través de una interfaz del router y permitir que esa red se siga anunciando a otros routers. El comando detiene las actualizaciones de routing a través de la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas a otras interfaces.

Propagar una ruta predeterminada

Para propagar una ruta predeterminada en RIP, el router perimetral debe estar configurado con lo siguiente:

- Una ruta estática predeterminada, mediante el comando `ip route 0.0.0.0 0.0.0.0`.
- El comando de configuración del router **default-information originate**. Esto le ordena al R1 que produzca información predeterminada mediante la propagación de la ruta estática predeterminada en actualizaciones RIP.

Entradas de la tabla de routing

Entradas conectadas directamente

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. **C** identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa. **L** identifica que la ruta es local. Las rutas locales se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa.
- **Red de destino:** la dirección de la red remota y la forma en que se conecta esa red.
- **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

Entradas conectadas directamente

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. **C** identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa. **L** identifica que la ruta es local. Las rutas locales se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa.
- **Red de destino:** la dirección de la red remota y la forma en que se conecta esa red.
- **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C    172.16.1.0/24 is directly connected, GigabitEthernet0/0
L    172.16.1.1/32 is directly connected, GigabitEthernet0/0
R    172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:21, Serial0/0/0
R    172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:21, Serial0/0/0
R    172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:21, Serial0/0/0
R    192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:16, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
R    209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:21, Serial0/0/0
C    209.165.200.232/30 is directly connected, Serial0/0/1
L    209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Entradas remotas

La entrada indica la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta.
- **Red de destino:** identifica la dirección de la red remota.
- **Distancia administrativa (AD):** identifica la confiabilidad del origen de la ruta. La AD para las rutas estáticas es 1 y la AD para las rutas conectadas es 0. Los protocolos de routing dinámico tienen una AD mayor que 1 según el protocolo.
- **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas. La métrica para rutas estáticas y conectadas es 0.
- **Siguiente salto:** identifica la dirección IPv4 del router siguiente al que se debe reenviar el paquete.
- **Marca de hora de la ruta:** identifica cuándo fue la última comunicación con la ruta.
- **Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Términos de la tabla de routing

La tabla de enrutamiento IP de Cisco no es una base de datos plana. La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes. Dentro de esta estructura, la jerarquía incluye varios niveles.

Las rutas se analizan en términos de lo siguiente:

- Ruta final
- Ruta de nivel 1
- Ruta principal de nivel 1
- Rutas secundarias de nivel 2

Ruta final

Una ruta final es una entrada de la tabla de routing que contiene una dirección IPv4 del siguiente salto o una interfaz de salida. Las rutas conectadas directamente, las rutas descubiertas dinámicamente y las rutas locales son rutas finales.

Ruta de nivel 1

Una ruta de nivel 1 es una ruta con una máscara de subred igual o inferior a la máscara con clase de la dirección de red. Por lo tanto, una ruta de nivel 1 puede ser cualquiera de las siguientes:

- **Ruta de red:** una ruta de red que tiene una máscara de subred igual a la de la máscara con clase.
- **Ruta de superred:** una dirección de red con una máscara menor que la máscara con clase, por ejemplo, una dirección de resumen.
- **Ruta predeterminada:** una ruta estática con la dirección 0.0.0.0/0.

El origen de la ruta de nivel 1 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico.

Ruta primaria de nivel 1

Las rutas principales son rutas de red de nivel 1 que se dividen en subredes. Una ruta principal nunca puede ser una ruta final. Una ruta principal nunca puede ser una ruta final.

Ruta secundaria de nivel 2

Una ruta secundaria de nivel 2 es una ruta que constituye una subred de una dirección de red con clase. Al igual que en las rutas de nivel 1, el origen de una ruta de nivel 2 puede ser una red conectada directamente, una ruta estática o una ruta descubierta en forma dinámica. Las rutas secundarias de nivel 2 también son rutas finales.

Proceso de búsqueda de rutas

Cuando un paquete llega a una interfaz del router, el router analiza el encabezado de IPv4, identifica la dirección IPv4 de destino y continúa a través del proceso de búsqueda del router

El router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv4:

1. Si la mejor coincidencia es una ruta final de nivel 1, se utiliza esa ruta para reenviar el paquete.
2. Si la mejor coincidencia es una ruta principal de nivel 1, se continúa con el siguiente paso.
3. Si hay una coincidencia con una ruta secundaria de nivel 2, se utiliza esa subred para reenviar el paquete.
4. Si no hay una coincidencia con ninguna de las rutas secundarias de nivel 2, se continúa con el paso siguiente.
5. Si ahora hay una coincidencia menor con las rutas predeterminadas o de superred de nivel 1, el router usa esa ruta para reenviar el paquete.
6. Si no hay coincidencia con ninguna ruta de la tabla de enrutamiento, el router descarta el paquete.

Nota: Una ruta que solo hace referencia a una dirección IP de siguiente salto y no a una interfaz de salida se debe resolver a una ruta con una interfaz de salida, si no se está utilizando Cisco Express Forwarding (CEF). Sin CEF, se realiza una búsqueda recurrente en la dirección IP de siguiente salto hasta que la ruta se resuelva con una interfaz de salida. CEF está habilitado de forma predeterminada.

Mejor ruta = coincidencia más larga

Para que haya una coincidencia entre la dirección IPv4 de destino de un paquete y una ruta en la tabla de routing, una cantidad mínima de los bits del extremo izquierdo deben coincidir entre la dirección IPv4 del paquete y la ruta en la tabla de routing. La máscara de subred de la ruta en la tabla de routing se utiliza para determinar la cantidad mínima de bits del extremo izquierdo que deben coincidir. Recuerde que un paquete IPv4 solo contiene la dirección IPv4 y no la máscara de subred.

La mejor coincidencia es la ruta de la tabla de routing que contiene la mayor cantidad de bits del extremo izquierdo coincidentes con la dirección IPv4 de destino del paquete. La ruta con la mayor

cantidad de bits del extremo izquierdo equivalentes, o la coincidencia más larga, es siempre la ruta preferida.

Entradas de la tabla de routing IPv6

Los componentes de la tabla de routing IPv6 son muy similares a los de la tabla de routing IPv4. Por ejemplo, se completa con las interfaces conectadas directamente, con las rutas estáticas y con las rutas descubiertas de forma dinámica.

Dado que IPv6 fue diseñado como un protocolo sin clase, todas las rutas son en realidad rutas finales de nivel 1. No hay rutas principales de nivel 1 para rutas secundarias de nivel 2.

Entradas conectadas directamente

En las entradas de las rutas conectadas directamente se muestra la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta (“C” identifica una red conectada directamente, mientras que “L” identifica que esta es una ruta local).
- **Red conectada directamente:** la dirección IPv6 de la red conectada directamente.
- **Distancia administrativa:** identifica la confiabilidad del origen de la ruta. IPv6 utiliza las mismas distancias que IPv4. El valor 0 indica el mejor origen y el más confiable.
- **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

Entradas de redes IPv6 remotas

La entrada indica la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Los códigos comunes incluyen O (OSPF), D (EIGRP), R (RIP) y S (ruta estática).
- **Red de destino:** identifica la dirección de la red IPv6 remota.
- **Distancia administrativa:** identifica cuán confiable es el origen de la ruta. IPv6 utiliza las mismas distancias que IPv4.
- **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Siguiente salto:** identifica la dirección IPv6 del router siguiente al que se debe reenviar el paquete.
- **Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Cuando un paquete IPv6 llega a una interfaz del router, el router analiza el encabezado de IPv6 e identifica la dirección IPv6 de destino. A continuación, el router continúa con el proceso de búsqueda del siguiente router.

El router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv6. Al igual que en IPv4, la coincidencia más larga es la mejor coincidencia. Por ejemplo, si hay varias coincidencias en la tabla de routing, el router elige la ruta con la coincidencia

más larga. La coincidencia se encuentra entre los bits del extremo izquierdo de la dirección IPv6 de destino del paquete y el prefijo IPv6 y la duración de prefijo en la tabla de routing IPv6.

Resumen

Los routers utilizan protocolos de routing dinámico para facilitar el intercambio de información de routing entre ellos. El propósito de los protocolos de routing dinámico incluye lo siguiente: detección de redes remotas, mantenimiento de información de routing actualizada, selección de la mejor ruta hacia las redes de destino y búsqueda de una mejor ruta nueva si la ruta actual deja de estar disponible. Si bien los protocolos de routing dinámico requieren menos sobrecarga administrativa que el routing estático, requieren dedicar parte de los recursos de un router a la operación del protocolo, incluidos tiempo de CPU y ancho de banda del enlace de red.

Las redes generalmente utilizan una combinación de routing estático y dinámico. El routing dinámico es la mejor opción para las redes grandes, y el routing estático es más adecuado para las redes de rutas internas.