**Autenticación OSPF**

**Autenticación MD5**

**Resumen**

OSPF admite tres tipos de autenticación: nula, autenticación por contraseña simple y autenticación MD5. La autenticación MD5 de OSPF se puede configurar globalmente o por interfaz. Para verificar que la autenticación MD5 de OSPF esté habilitada, use el comando show ip ospf interface del modo EXEC privilegiado.

# 1. Ataques al Router

La función de los **routers** en una red es tan importante que, con frecuencia, **son el blanco de ataques de red**. Los administradores de red deben tener en cuenta que los routers corren el mismo riesgo de sufrir ataques que los sistemas para usuarios finales.

En general, se puede atacar a los sistemas de routing mediante la **perturbación de los peers de routing** o la **falsificación de los datos** que se transportan en el protocolo de routing.

En general, la información de routing falsificada se puede usar para causar que los sistemas intercambien información errónea (se mientan), provoquen un ataque por denegación de servicio (DoS) u ocasionen que el tráfico tome una ruta que normalmente no seguiría.

Las consecuencias de falsificar información de routing son las siguientes:

- Redireccionamiento del tráfico para crear bucles de routing
- Redireccionamiento del tráfico para que se lo pueda controlar en un enlace no seguro
- Redireccionamiento del tráfico para descartarlo

## Para mitigar los ataques a los protocolos de routing, puede configurar la autenticación de OSPF.

# 2. Tipos de Autenticación OSPF

Cuando en un router está configurada la autenticación de vecinos, el router autentica el origen de cada paquete de actualización de routing que recibe. Esto se logra mediante el

intercambio de una clave de autenticación (a veces llamada «**contraseña**«) que conocen tanto el router que envía el paquete como el que lo recibe.

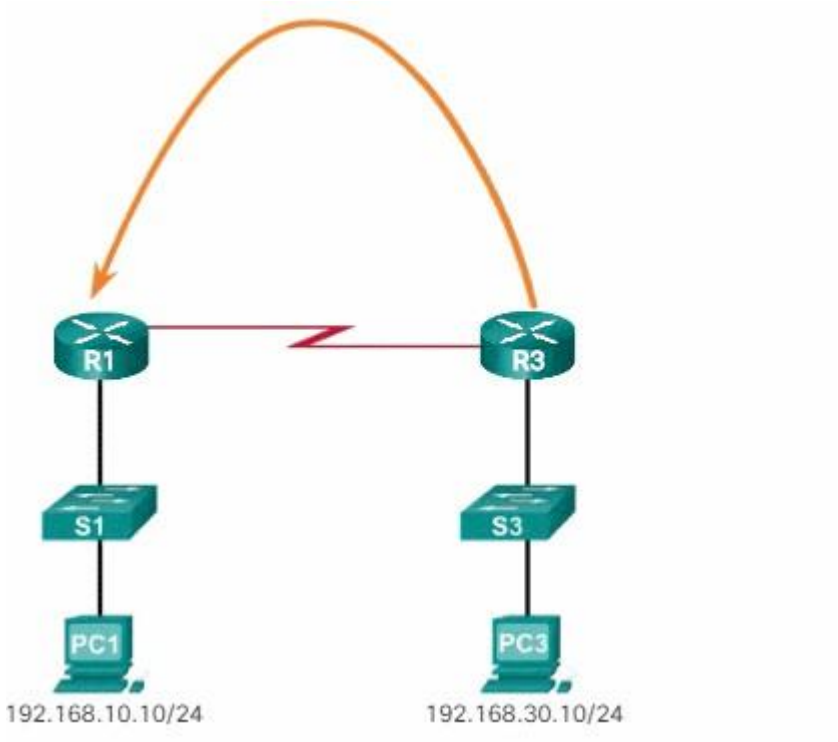
Para intercambiar información de actualización de routing de manera segura, se debe habilitar la autenticación de OSPF. La autenticación de OSPF puede ser ninguna (nula), sencilla o de síntesis del mensaje 5 (MD5).

OSPF admite tres tipos de autenticación:

- **Null (nula)**: este es el método predeterminado y significa que no se usa ninguna autenticación para OSPF.
- **Simple password authentication (autenticación por contraseña simple)**: también se conoce como «autenticación con texto no cifrado», porque la contraseña en la actualización se envía como texto no cifrado a través de la red.

# Este método se considera un método antiguo de autenticación de OSPF.

- **MD5 authentication (autenticación MD5)**: se trata del método de autenticación más seguro y recomendado. La autenticación MD5 proporciona mayor seguridad, dado que la contraseña nunca se intercambia entre peers. En cambio, se calcula mediante el algoritmo MD5. La coincidencia de los resultados autentica al emisor.




Cómo se usa la autenticación MD5

**Nota**: RIPv2, EIGRP, OSPF, IS-IS y BGP admiten varias formas de autenticación MD5.

# 3. Autenticación MD5

En el siguiente ejemplo, se muestra cómo se usa la autenticación MD5 para autenticar dos routers OSPF vecinos.

En la Imagen 1, el R1 combina el mensaje de routing con la clave secreta previamente compartida y calcula la firma con el algoritmo MD5. La firma también se conoce como «**valor de hash**«.

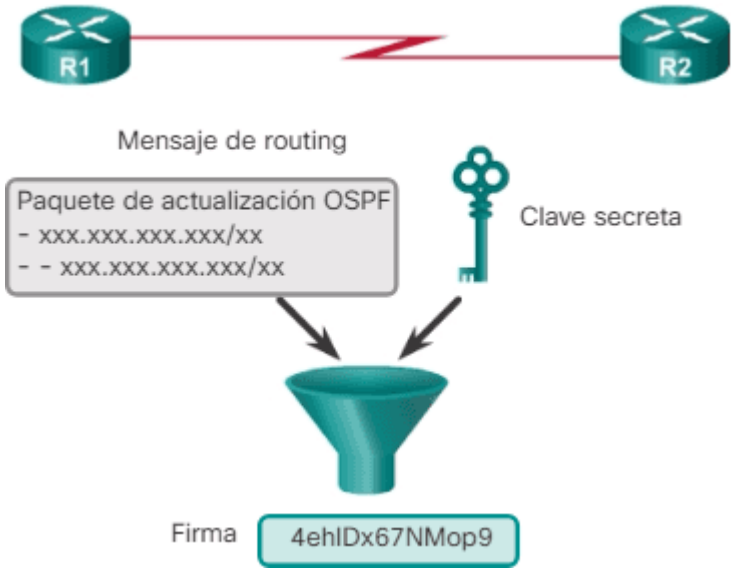



Imagen 1: Funcionamiento del algoritmo MD5
En la Imagen 2, el R1 agrega la firma al mensaje de routing y lo envía al R2.


Imagen 2: El R1 envía un mensaje de routing con autenticación MD5

MD5 no cifra el mensaje; por eso, el contenido se puede leer fácilmente.

En la Imagen 3, el R2 abre el paquete, combina el mensaje de routing con la clave secreta previamente compartida y calcula la firma con el algoritmo MD5.

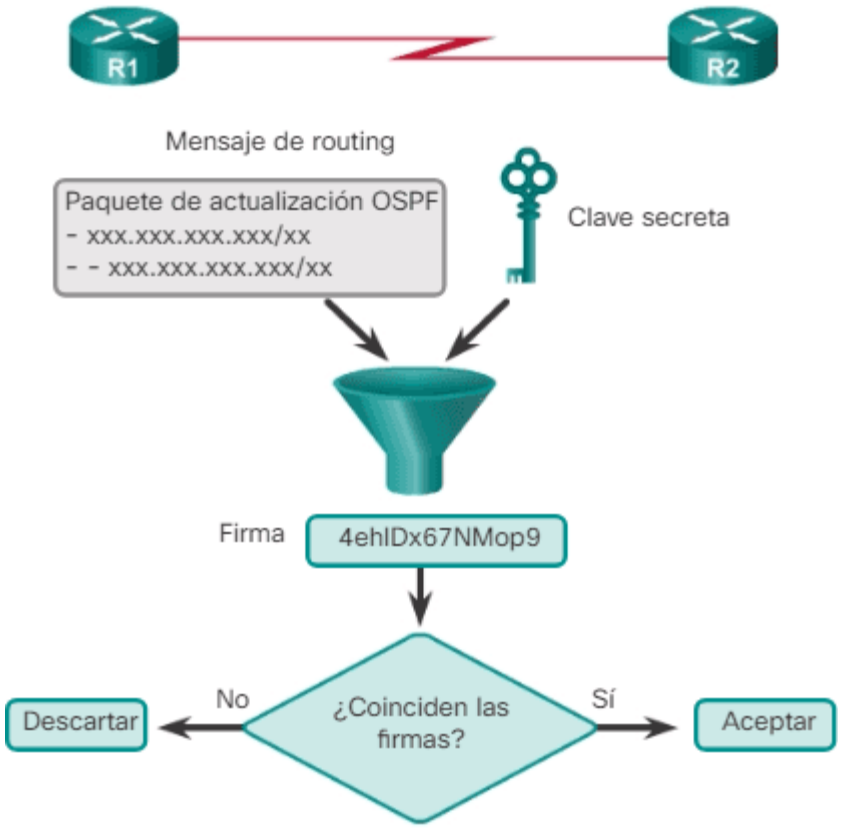


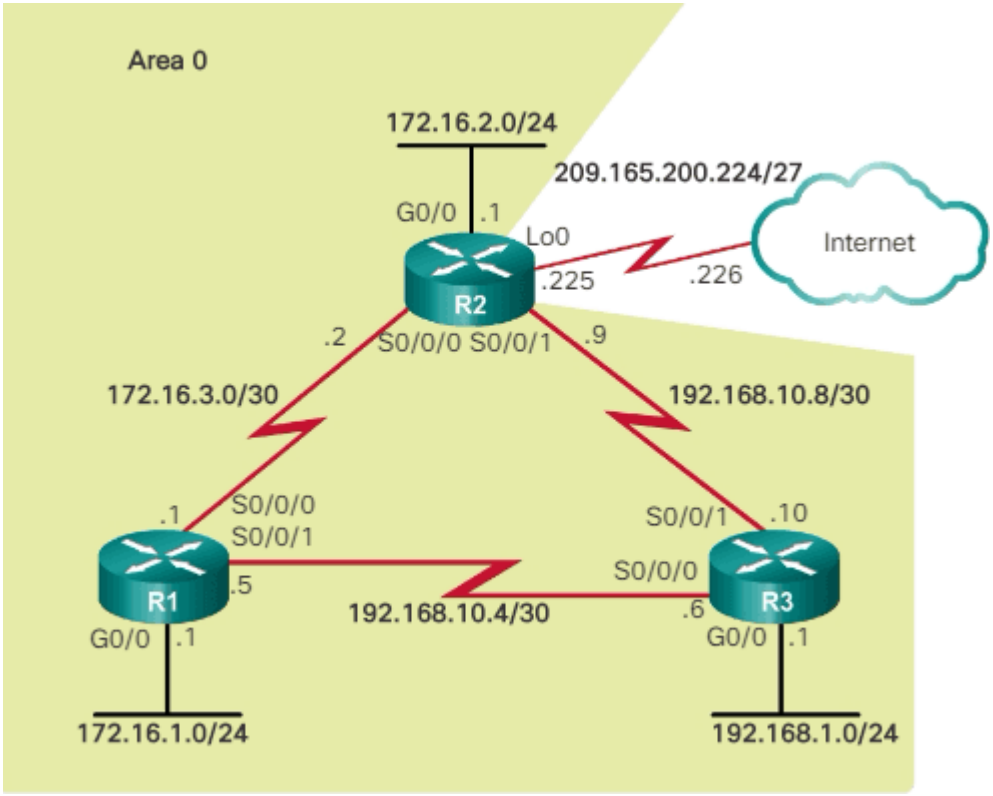

Imagen 3: Funcionamiento de la autenticación MD5

- Si las firmas coinciden, el R2 acepta la actualización de routing.
- Si las firmas no coinciden, el R2 descarta la actualización.

**OSPFv3 (OSPF para IPv6) no incluye ninguna capacidad de autenticación propia**. En cambio, depende por completo de IPSec para proteger las comunicaciones entre vecinos con el comando ipv6 ospf authentication ipsec spi del modo de configuración de interfaz. Esto resulta beneficioso, ya que simplifica el protocolo OSPFv3 y estandariza su mecanismo de autenticación.

# 4. Configuración de la autenticación MD5 de OSPF

OSPF admite la autenticación de protocolos de routing mediante MD5. La autenticación MD5 se puede habilitar globalmente para todas las interfaces o para cada interfaz deseada.




Para habilitar la autenticación MD5 de OSPF globalmente, configure lo siguiente:

Comando del modo de configuración de interfaz:

```
ip ospf message-digest-key key md5 password
```

Comando del modo de configuración del router:

```
area area-id authentication message-digest
```

Este método impone la autenticación en todas las interfaces con OSPF habilitado. Si una interfaz no está configurada con el comando **ip ospf message-digest-key**, no podrá establecer adyacencias con otros vecinos OSPF.

Syslog

Para proporcionar más flexibilidad, ahora se admite la autenticación por interfaz. Para habilitar la autenticación MD5 por interfaz, configure lo siguiente:

Comando del modo de configuración de interfaz:

```
ip ospf message-digest-key key md5 password
```

Comando del modo de configuración de interfaz:

```
ip ospf authentication message-digest
```

Los métodos de autenticación MD5 de OSPF global y por interfaz pueden usarse en el mismo router. Sin embargo, la configuración por interfaz reemplaza la configuración global. Las contraseñas de autenticación MD5 no tienen que ser las mismas en toda un área; sin embargo, **tienen que ser las mismas entre vecinos**.

Por ejemplo, suponga que todos los routers en la ilustración convergieron mediante OSPF y que el routing funciona correctamente. La autenticación de OSPF se implementará en todos los routers.

# 4.1. Ejemplo de autenticación MD5 de OSPF

En el ejemplo de la Imagen 4, se muestra cómo configurar el R1 para habilitar la autenticación MD5 de OSPF en todas las interfaces.

Observe que los mensajes informativos indican que las adyacencias de vecinos OSPF con el R2 y el R3 cambiaron al estado Down (inactivo), porque todavía no se configuraron el R2 ni el R3 para que admitan autenticación MD5.

Habilitación de la autenticación MD5 de OSPF de forma global en R1

```
R1(config)# router ospf 10
R1(config-router)# area 0 authentication message-digest
R1(config-router)# exit
R1(config)#
*Apr  8 09:58:09.899: %OSPF-5-ADJCHG: Process 10,
Nbr 2.2.2.2 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
R1(config)#
*Apr  8 09:58:28.627: %OSPF-5-ADJCHG: Process 10,
Nbr 3.3.3.3 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)#
```

Imagen 4: Ejemplo de autenticación MD5 de OSPF

Como una alternativa a la habilitación global de la autenticación MD5, en el ejemplo de la Imagen 5 se muestra cómo configurar el R1 para habilitar la autenticación MD5 de OSPF por interfaz. Observe que, también en este caso, las adyacencias de vecinos OSPF cambiaron al estado Down.

Habilitación de la autenticación MD5 de OSPF en las interfaces de  R1

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
*Apr  8 10:20:10.647: %OSPF-5-ADJCHG: Process 10,
Nbr 2.2.2.2 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
R1(config)#
*Apr  8 10:20:50.007: %OSPF-5-ADJCHG: Process 10,
Nbr 3.3.3.3 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
R1(config)#
```

Imagen 5: Configuración de autenticación MD5 de OSPF

A continuación, se habilita la autenticación MD5 de OSPF globalmente en el R2 y por interfaz en el R3.

```
R2(config)# router ospf 10
R2(config-router)# area 0 authentication message-digest
R2(config-router)# interface GigabitEthernet 0/0
R2(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R2(config-if)# interface Serial 0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R2(config-if)# interface Serial 0/0/1
R2(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R2(config-if)# end
R2(config)#
*Apr 8 10:26:46.783: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2(config)#
```

*Apr 8 10:27:16.435: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired

R2#

Aquí también aparecen mensajes informativos. El primer mensaje se debe a que se volvió a establecer la adyacencia de vecino con el R1. Sin embargo, la adyacencia con el R3 cambió al estado Down, porque todavía no se configuró el R3.

```
R3(config)# interface GigabitEthernet 0/0
R3(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# interface Serial 0/0/0
R3(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# interface Serial 0/0/1
R3(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# end
R3#
*Apr 8 10:29:21.859: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
*Apr 8 10:29:27.315: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R3#
```

```
R3#
```

Después de configurar el R3, se volvieron a establecer todas las adyacencias de vecinos.

# 5. Verificación de la autenticación MD5 de OSPF

Para verificar que la autenticación MD5 de OSPF esté habilitada, use el comando **show ip ospf interface** del modo EXEC privilegiado. Al verificar que la tabla de routing está completa, se puede confirmar que la autenticación se realizó correctamente.

En la Imagen 6, se muestra la verificación de la autenticación MD5 de OSPF en la interfaz serial 0/0/0 en el R1.

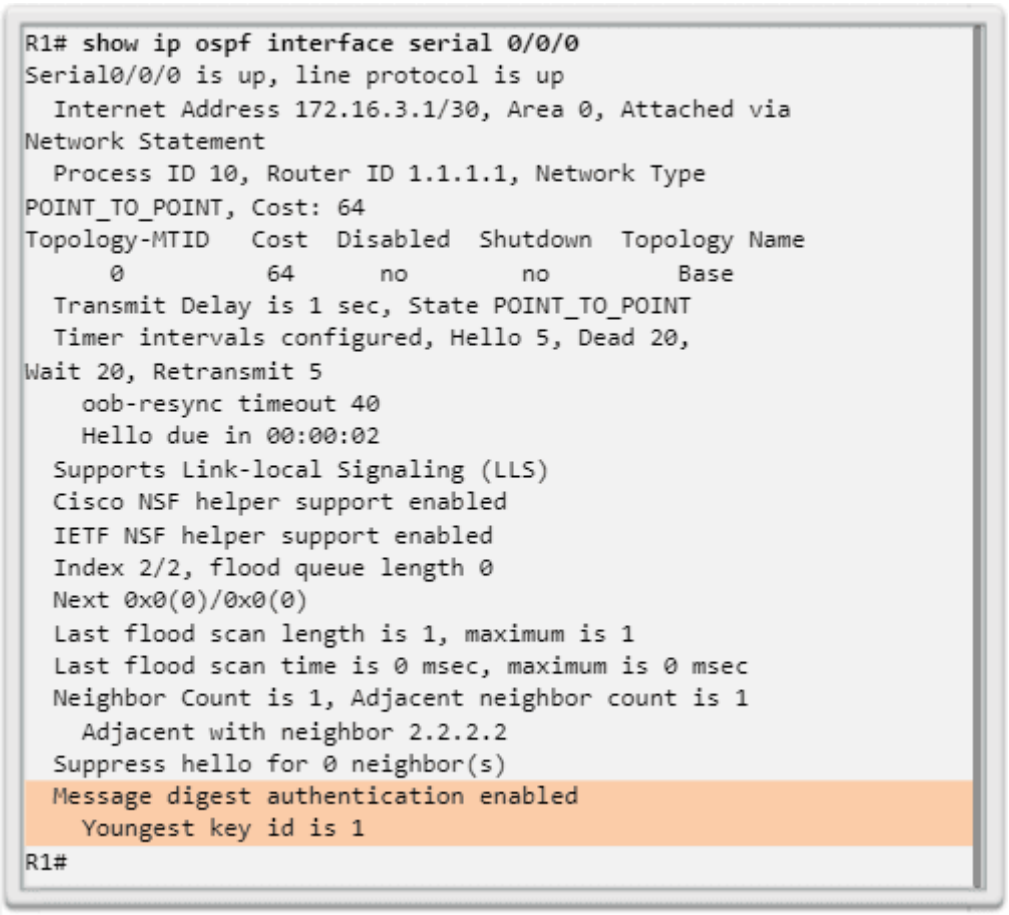


Imagen 6: Verificación de autenticación MD5 de OSPF
En la Imagen 7, se confirma que la autenticación se realizó correctamente.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF, IA - OSPF
        inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1
       E2 - OSPF external type 2
       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
       H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17,
Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets,
3 masks
O        172.16.2.0/24 [110/65] via 172.16.3.2,
00:33:17, Serial0/0/0
O     192.168.1.0/24 [110/65] via 192.168.10.6,
00:30:43, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets,
 2 masks
O        192.168.10.8/30 [110/128] via 192.168.10.6,
00:30:43, Serial0/0/1
                         [110/128] via 172.16.3.2,
00:33:17, Serial0/0/0
R1#
```

# 6.- Autenticación MD5 de EIGRP

EIGRP admite la autenticación de protocolos de routing mediante MD5. La configuración de la autenticación de mensajes EIGRP consta de dos pasos: la creación de un llavero y una clave, y la configuración de la autenticación de EIGRP para usar el llavero y la llave.

**Paso 1. Crear un llavero y una clave**

Para funcionar, la autenticación del routing requiere una clave en un llavero. Para que se pueda habilitar la autenticación, cree un llavero y, al menos, una clave.

a. En el modo de configuración global, cree el llavero. Aunque pueden configurarse varias claves, esta sección se centra en el uso de una sola clave.

```
Router(config)# key chain name-of-chain
```

b. Especifique la ID de la clave. La ID de la clave es el número que se usa para identificar una clave de autenticación dentro de un llavero. El intervalo de claves es de 0 a 2 147 483 647. Se recomienda que el número de clave sea el mismo en todos los routers en la configuración.

```
Router(config-keychain)# key key-id
```

c. Especifique la cadena de clave para la clave. La cadena de clave es parecida a una contraseña. Los routers que intercambian claves de autenticación deben configurarse con la misma cadena de clave.

```
Router(config-keychain-key )# key-string key-string-text
```

**Paso 2. Configurar la autenticación de EIGRP con el llavero y la clave**

Configure EIGRP para realizar la autenticación de mensajes con la clave definida anteriormente. Complete esta configuración en todas las interfaces habilitadas para EIGRP.

a. En el modo de configuración global, especifique la interfaz en la que configurará la autenticación de mensajes EIGRP.

```
Router(config)# interface type number
```

b. Habilite la autenticación de mensajes EIGRP. La palabra clave md5 indica que se usará el hash MD5 para la autenticación.

```
Router(config-if)# ip authentication mode eigrp as-number md5
```

c. Especifique el llavero que debe usarse para la autenticación. El argumento name-of-chain especifica el llavero que se creó en el paso 1.

```
Router(config-if)# ip authentication key-chain eigrp as-number
name-of-chain
```

Cada clave tiene su propia ID de clave, que se almacena localmente. La combinación de la ID de la clave y la interfaz asociada al mensaje identifica de manera exclusiva el algoritmo de autenticación y la clave de autenticación MD5 en uso.

El llavero y la actualización de routing se procesan con el algoritmo MD5 para producir una firma única.

## Ejemplo de autenticación de EIGRP

Para autenticar las actualizaciones de routing, todas las interfaces con EIGRP habilitado deben estar configuradas para admitir la autenticación. En la Imagen 1, se muestra la topología IPv4 y las interfaces que tienen autenticación configurada.

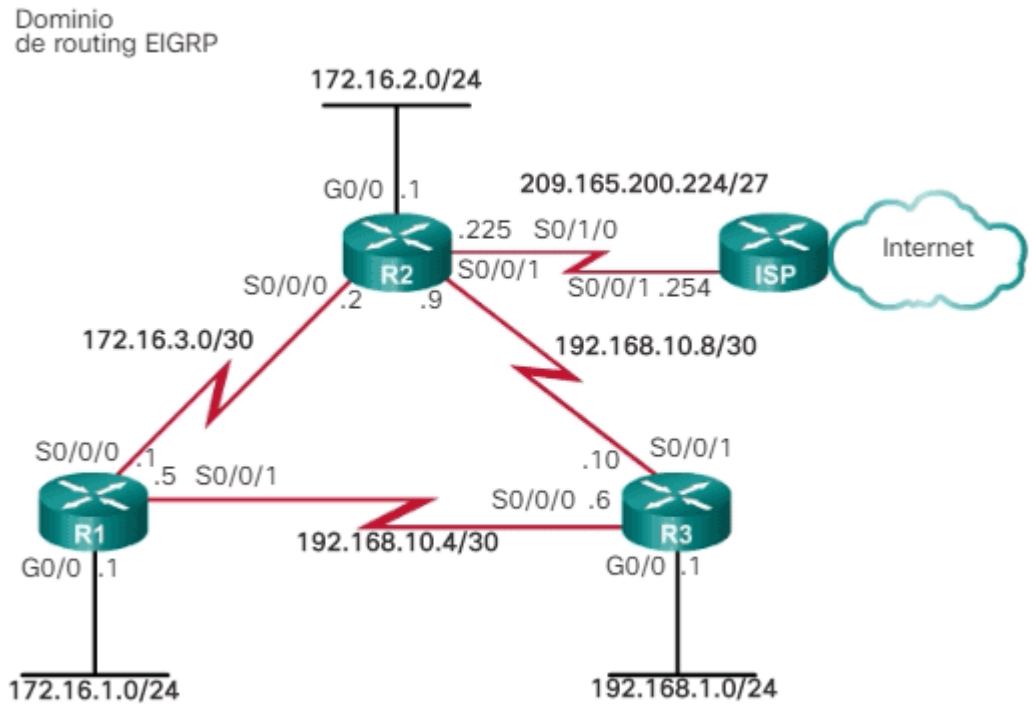



Imagen 1: Topología EIGRP para IPv4

En la Imagen 2, se muestra la configuración para el router R1 con el llavero EIGRP_KEY y la cadena de clave cisco123.

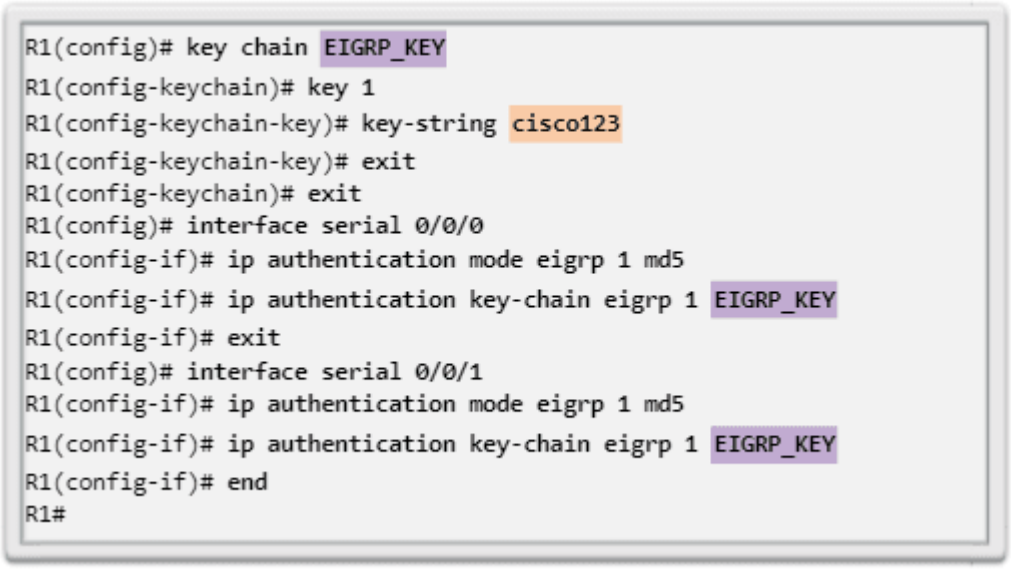



Imagen 2: Configuración de la autenticación MD5 de EIGRP en el R1

Una vez que el R1 está configurado, los otros routers reciben actualizaciones de routing autenticadas. Las adyacencias se pierden hasta que se configura la autenticación del protocolo de routing en los vecinos.