Configuración de la autenticación IS-IS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Configurar
Autenticación de la interfaz
Autenticación de área
Autenticación de dominio
Combinación de autenticación de dominio, área e interfaz
Verificación
Troubleshooting
Información Relacionada

Introducción

Es recomendable configurar la autenticación para los protocolos de ruteo con el fin de evitar la incorporación de información maliciosa en la tabla de ruteo. En este documento se explica la autenticación del texto claro entre routers que ejecutan un sistema intermedio a sistema intermedio (IS-IS) para el IP.

Este documento cubre solamente la autenticación del texto claro IS-IS. Refiera a aumentar la Seguridad en una red IS-IS para más información sobre los otros tipos de autenticación IS-IS.

prerrequisitos

Requisitos

Los Quien lea este documento deben ser familiares con la operación y la configuración IS-IS.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. La configuración en este documento fue probada en los Cisco 2500 Series Router, la versión deL Cisco IOS corriente 12.2(24a)

Antecedentes

El IS-IS permite la configuración de una contraseña para un link especificado, un área, o un dominio. Los routers que deseen convertirse en vecinos deben intercambiar la misma contraseña para su nivel de autenticación configurado. Un router que no posee la contraseña adecuada no puede participar en la función correspondiente (es decir, no puede iniciar un link, ser miembro de un área o ser miembro de un dominio de Capa 2 respectivamente).

El software del ® del Cisco IOS permite que configuren a tres tipos de autenticación IS-IS.

- **Autenticación IS-IS** - Durante mucho tiempo, ésta era la única forma de configurar la autenticación para el IS-IS.
- **Autenticación IS-IS HMAC-MD5** - Esta característica agrega una publicación HMAC-MD5 a cada uno protocolo IS-IS la unidad de datos (PDU). Fue introducida en la versión del Cisco IOS Software 12.2(13)T y se soporta solamente en las Plataformas de un número limitado.
- **Autenticación aumentada del texto claro** - Con esta nueva función, la autenticación del texto claro se puede configurar usando los comandos new que permiten que las contraseñas sean cifradas cuando se visualiza la configuración del software. También hace las contraseñas más fáciles manejar y cambiar.

Note: Refiera a aumentar la Seguridad en una red IS-IS para la información sobre ISIS MD-5 y autenticación aumentada del texto claro.

Protocolo IS-IS, como se especifica en el RFC 1142, prevé la autenticación del hellos y de los paquetes del estado del link (LSP) a través de la inclusión de la información de autenticación como parte del LSP. Se codifica esta información de autenticación mientras que un triple del Type Length Value (TLV). El tipo de la autenticación TLV es 10; la longitud del TLV es variable; y el valor del TLV depende del tipo de autenticación que es utilizado. Por defecto, la autenticación está desactivada.

Configurar

Esta sección discute cómo configurar la autenticación del texto claro IS-IS en un link, para un área y para un dominio.

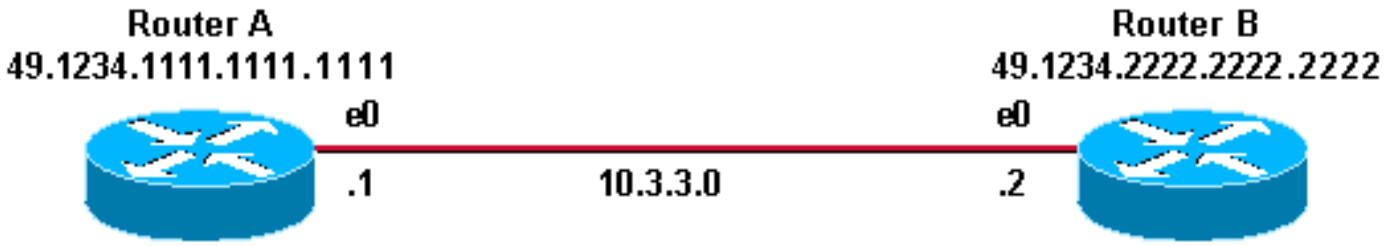
Note: Para encontrar la información adicional en los comandos usados en este documento, utilice las mejores prácticas para buscar los comandos (clientes registrados solamente).

Autenticación de la interfaz

Cuando usted configura la autenticación IS-IS en una interfaz, usted puede habilitar la contraseña para 2 del nivel 1, del nivel 2, o ambos encaminamiento del nivel 1/Level. Si usted no especifica un nivel, el valor por defecto es el nivel 1 y el nivel 2. dependiendo del nivel para el cual se configura la autenticación, la contraseña se lleva adentro los mensajes Hello Messages correspondientes. El nivel de autenticación de la interfaz IS-IS debe realizar un seguimiento del tipo de adyacencia en la interfaz. Utilice el **comando show clns neighbor** de descubrir el tipo de adyacencia. Para la autenticación de área y de dominio, no es posible especificar el nivel.

El diagrama de la red y las configuraciones para la autenticación de canal en el router A, el ethernet0 y el router B, ethernet0 se muestran abajo. Configuran al router A y al router B con la contraseña isis SECr3t para el nivel 1 y el nivel 2. Estas contraseñas distinguen entre mayúsculas y minúsculas.

En los routeres Cisco configurados con el servicio de red sin conexión (CLNS) IS-IS, la adyacencia CLNS entre ellos es el nivel 1/Level 2 por abandono. Entonces, el Router A y el Router B tendrán tipos de adyacencia, a menos que se los configure específicamente para el Nivel 1 o el Nivel 2.



router A

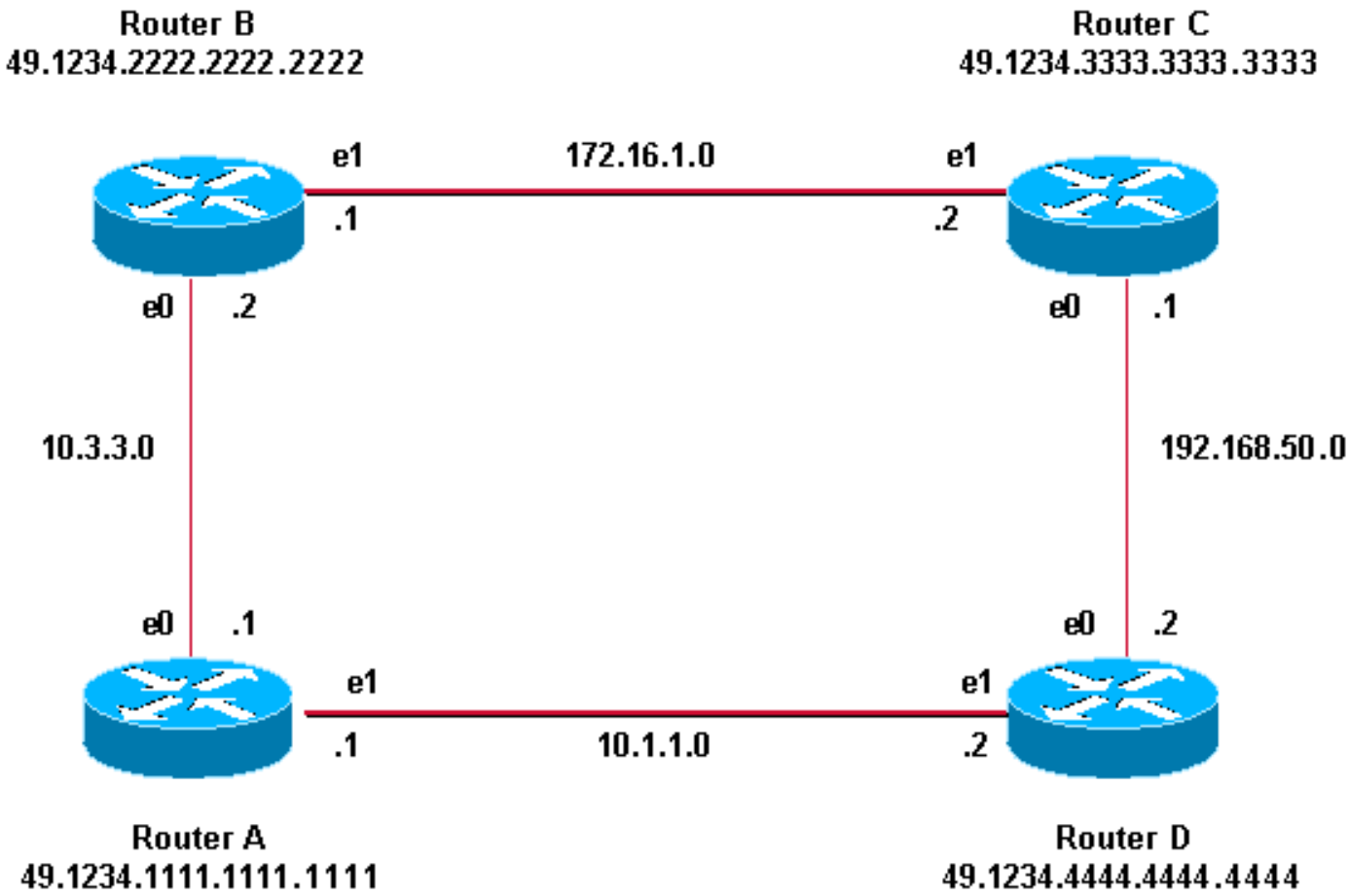
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
```

router B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

Autenticación de área

A continuación, se muestran el diagrama y las configuraciones de la red para la autenticación de área. Cuando se configura la Autenticación de área, la contraseña se lleva adentro el L1 LSP, CSNP y PSNPS. Todos los routers se encuentran en la misma zona IS-IS, 49.1234, y están todos configurados con las contraseñas de zona "tiGHter".



router A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
area-password tiGHter
```

router B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
area-password tiGHter
```

Router C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.1 255.255.255.0
ip router isis

router isis
net 49.1234.3333.3333.3333.00
area-password tiGHter
```

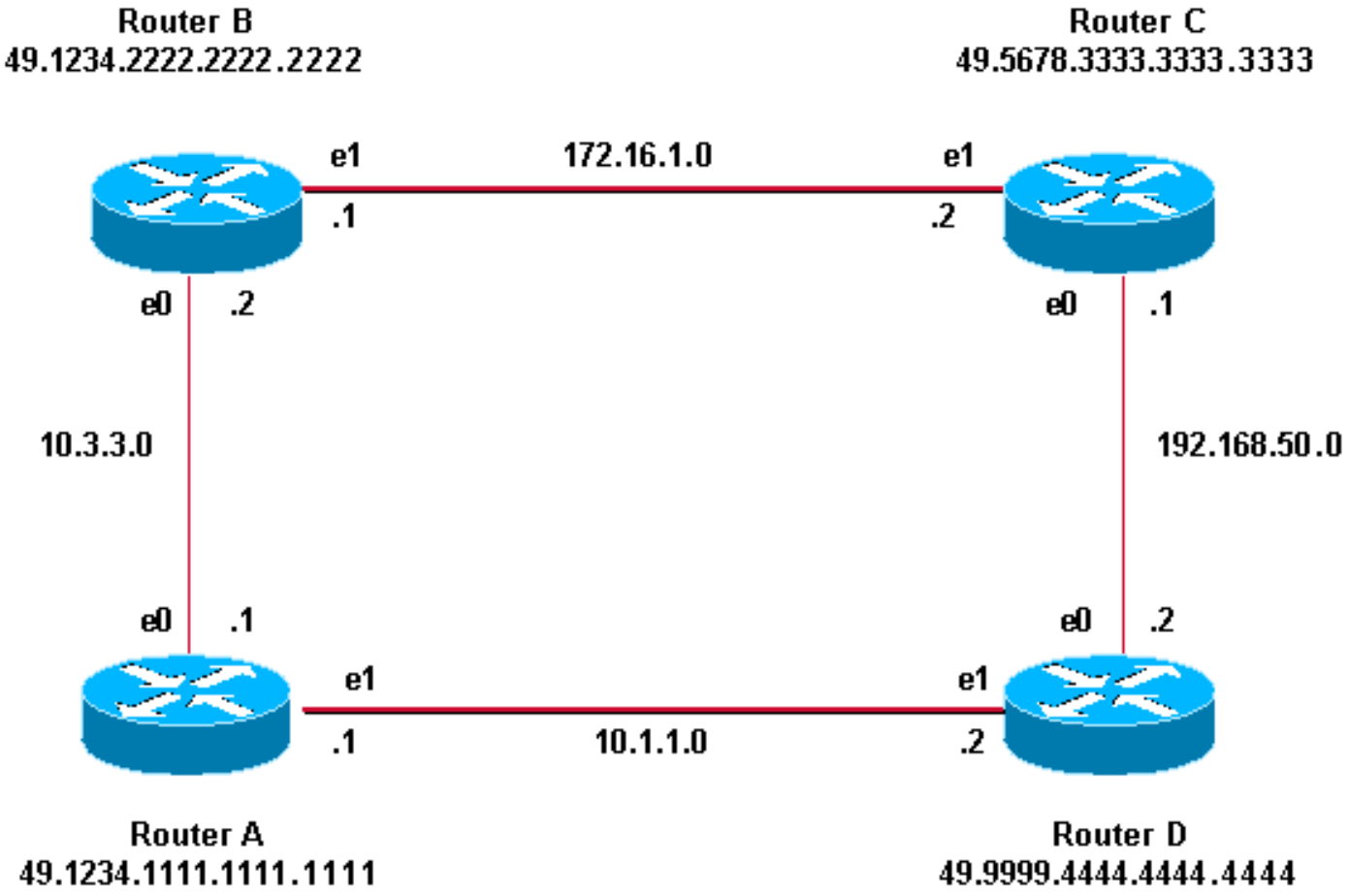
Router D

```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis

router isis
net 49.1234.4444.4444.4444.00
area-password tiGHter
```

Autenticación de dominio

A continuación, se muestran el diagrama y las configuraciones de la red para la autenticación del dominio. El router A y el router B están en área IS-IS 49.1234; El C del router está en área IS-IS 49.5678; y el router D está en el área 49.9999. Todos los routers están en el mismo dominio IS-IS

(49) y están configurados con la contraseña de dominio “seCurity”.



router A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
domain-password seCurity
```

router B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
domain-password seCurity
```

Router C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.1 255.255.255.0
ip router isis

router isis
net 49.5678.3333.3333.3333.00
domain-password seCurity
```

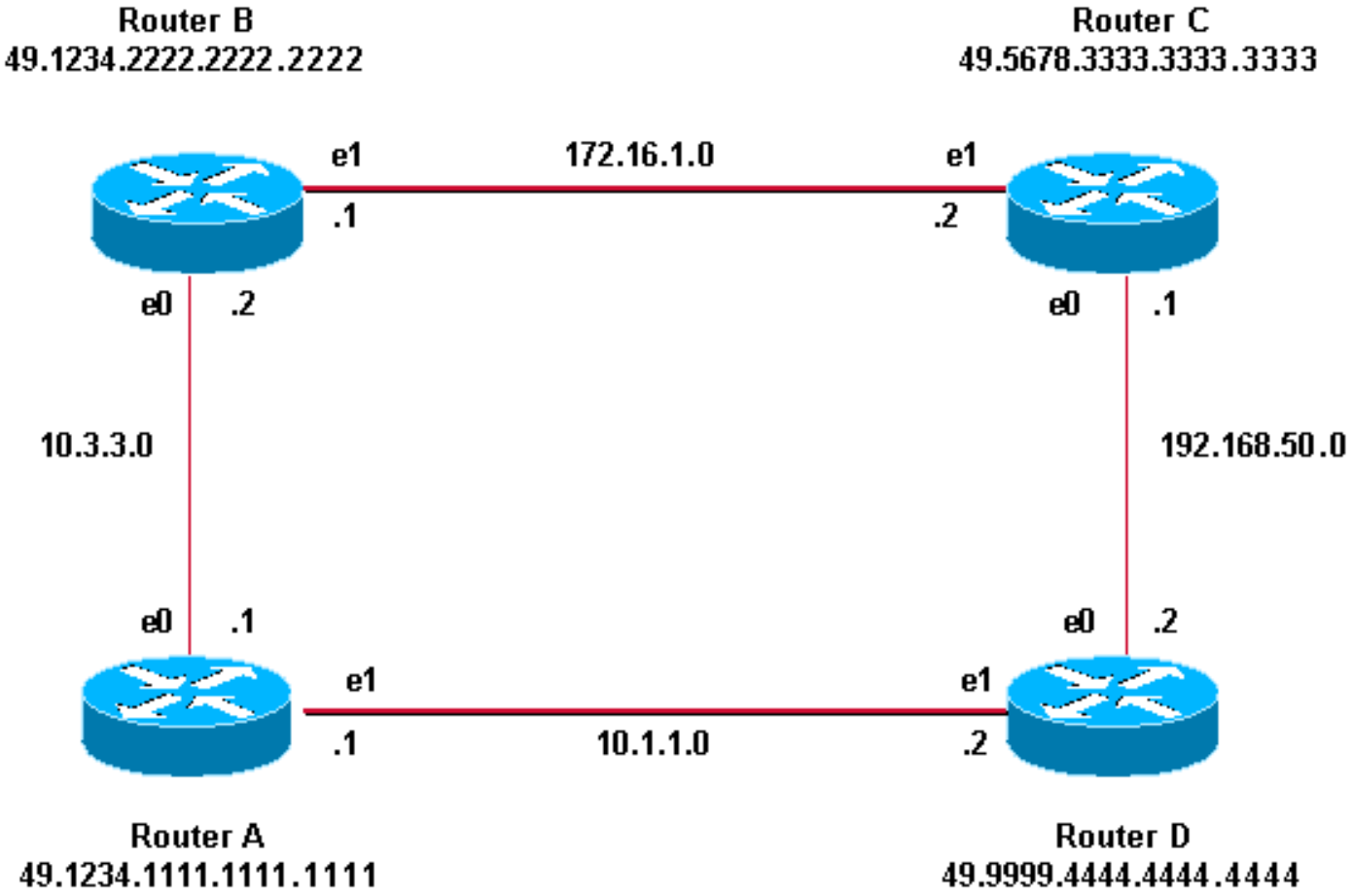
Router D

```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis

router isis
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

Combinación de autenticación de dominio, área e interfaz

La topología y las configuraciones parciales en esta sección ilustran una combinación de dominio,

un área, y una autenticación de canal. El router A y el router B están en la misma área y se configuran con la contraseña de área “más apretada.” El C y el router D del router pertenecen a dos diversas áreas que el router A y el router B. Todo el Routers está en el mismo dominio y comparte la contraseña “Seguridad del dominio-nivel.” El router B y el C del router tienen una configuración de la interfaz para el link Ethernet entre él. El C y el router D del router forman solamente las adyacencias L2 con sus vecinos y configurar la contraseña de área no se requiere.



router A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
domain-password seCurity
area-password tiGHter
```

router B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis
clns router isis
isis password Fri3nd level-2

router isis
net 49.1234.2222.2222.2222.00
domain-passwordseCurity
area-password tiGHter
```

Router C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis
isis password Fri3nd level-2

interfaceethernet0
```

Router D

```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.2 255.255.255.0
```

```
ip address 192.168.50.1 255.255.255.0
ip router isis

router isis
net 49.5678.3333.3333.3333.00
domain-password seCurity
```

```
ip router isis

router isis
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

Verificación

El analizador del CLI de Cisco soportan a los ciertos comandos show (clientes registrados solamente), que permite que usted vea una análisis de la salida del comando show.

Para verificar si la autenticación de canal está trabajando correctamente, utilice el **comando show clns neighbors** en el EXEC del usuario o al modo EXEC privilegiado. La salida del comando visualiza el tipo de adyacencia y el estado de la conexión. Esta salida de muestra del **comando show clns neighbors** muestra a un router configurado correctamente para la autenticación de canal y visualiza el estado como PARA ARRIBA:

```
RouterA# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
RouterB        Et0         0000.0c76.2882  Up     27        L1L2 IS-IS
```

Para el área y la autenticación de dominio, la verificación de la autenticación se puede hacer usando los comandos debug como se explica en la siguiente sección.

Troubleshooting

Si los routeres conectados tienen directamente autenticación configurada en un lado de un link, y no en el otro, el Routers no forma una adyacencia CLNS IS-IS. En el resultado a continuación, el Router B se configura para la autenticación de la interfaz respecto de la interfaz Ethernet 0 y el Router A no está configurado con autenticación en la interfaz adyacente.

```
Router_A# show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Router_B       Et0         00e0.b064.46ec  Init   265       IS   ES-IS

Router_B# show clns neighbors
```

Si los routeres conectados tienen directamente autentificación de área configurada en un lado de un link, la adyacencia CLNS IS-IS se forma entre las dos rutas. Sin embargo, el router en quien se configura la autentificación de área, no valida L1 LSP del vecino CLNS sin la autentificación de área configurada. Sin embargo, el vecino sin la autentificación de área continúa validando L1 y L2 LSP.

Éste es el mensaje del debug en el router A donde está configurada y de recepción la Autenticación de área de L1 LSP de un vecino (router B) sin la Autenticación de área:

```
Router_A# deb isis update-packets
 IS-IS Update related packet debugging is on
 Router_A#
 *Mar 1 00:47:14.755: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1128,
```

```
 *Mar 1 00:47:14.759: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
 *Mar 1 00:47:14.763: ISIS-Upd: LSP authentication failed
 Router_A#
 *Mar 1 00:47:24.455: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1118,
 *Mar 1 00:47:24.459: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
 *Mar 1 00:47:24.463: ISIS-Upd: LSP authentication failed
 RouterA#
```

Si usted configura la autenticación de dominio en un router, rechaza el L2 LSP del Routers que no hace la autenticación de dominio configurar. Routers que no hace la autenticación configurar para validar los LSP del router que hace la autenticación configurar.

El resultado de la depuración a continuación muestra las fallas de autenticación de LSP. Configuran para el área o la autenticación de dominio y es el nivel de recepción al router CA 2 LSP de un router (router DB) que no se configure para el dominio o la autenticación de contraseña.

```
Router_A# debug isis update-packets
IS-IS Update related packet debugging is on
Router_A#
*Mar  1 02:32:48.315: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 374,
*Mar  1 02:32:48.319: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
*Mar  1 02:32:48.319: ISIS-Upd: LSP authentication failed
Router_A#
*Mar  1 02:32:57.723: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 365,
*Mar  1 02:32:57.727: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
*Mar  1 02:32:57.727: ISIS-Upd: LSP authentication failed
```

Información Relacionada

- Página de Soporte de IP Routing
- Soporte Técnico y Documentación - Cisco Systems