Configuración de la autenticación IS-IS

Contenido

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 sólo cubre la autenticación de texto sin cifrar IS-IS. Refiérase a Mejora de la Seguridad en una Red IS-IS para obtener más información sobre los otros tipos de autenticación IS-IS.

Prerequisites

Requirements

Los lectores de este documento deben estar familiarizados con la operación y 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 se probó en los Cisco 2500 Series Routers, ejecutando Cisco IOS versión 12.2(24a)

Antecedentes

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 Cisco IOS® permite configurar tres tipos de autenticación IS-IS.

- **Autenticación IS-IS**: durante mucho tiempo, esta fue la única manera de configurar la autenticación para IS-IS.
- **Autenticación IS-IS HMAC-MD5**: esta función agrega un resumen HMAC-MD5 a cada unidad de datos del protocolo IS-IS (PDU). Se introdujo en la versión 12.2(13)T del software del IOS de Cisco y sólo se admite en una serie limitada de plataformas.
- **Autenticación de texto claro mejorada**: con esta nueva función, la autenticación de texto sin formato se puede configurar usando nuevos comandos que permiten cifrar las contraseñas cuando se muestra la configuración de software. También facilita la administración y el cambio de las contraseñas.

Nota: Refiérase a Mejora de la Seguridad en una Red IS-IS para obtener información sobre ISIS MD-5 y Autenticación de Texto Limpio Mejorado.

El protocolo IS-IS, como se especifica en RFC 1142, proporciona la autenticación de Hellos y de los Paquetes de Estado de Link (LSP) mediante la inclusión de información de autenticación como parte del LSP. Esta información de autenticación se codifica como triple valor de longitud de tipo (TLV). El tipo de TLV de autenticación es 10; la longitud del TLV es variable; y el valor del TLV depende del tipo de autenticación que se utiliza. Por defecto, la autenticación está desactivada.

Configurar

Esta sección trata sobre cómo configurar la autenticación de texto sin cifrar IS-IS en un link, para un Área y para un Dominio.

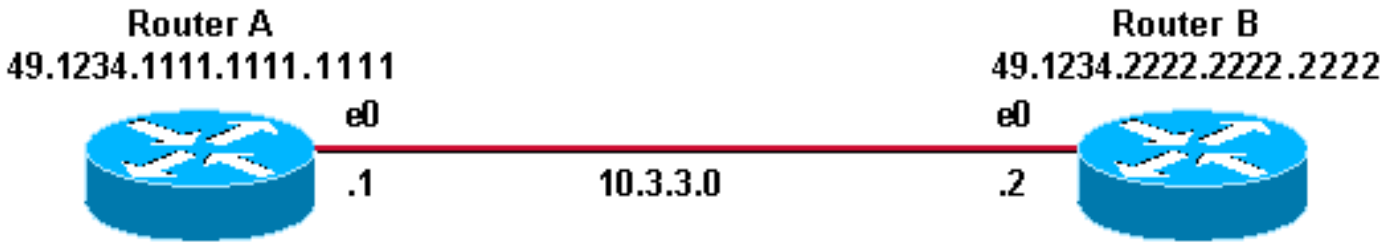
Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice las Prácticas Recomendadas para los Comandos de Búsqueda (sólo clientes registrados).

Autenticación de la interfaz

Cuando configura la autenticación IS-IS en una interfaz, puede habilitar la contraseña para el ruteo de Nivel 1, Nivel 2 o ambos Nivel 1/Nivel 2. Si no especifica un nivel, el valor predeterminado es Nivel 1 y Nivel 2. Según el nivel para el que se configure la autenticación, la contraseña se transporta en los mensajes Hello 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** para averiguar el tipo de adyacencia. Para la autenticación de área y de dominio, no es posible especificar el nivel.

A continuación se muestran el diagrama de red y las configuraciones para la autenticación de la interfaz en el router A, Ethernet 0 y el router B, Ethernet 0. El router A y el router B están configurados con la contraseña de isis SECr3t tanto para el nivel 1 como para el nivel 2. Estas contraseñas distinguen entre mayúsculas y minúsculas.

En los routers Cisco configurados con el servicio de red sin conexión (CLNS) IS-IS, la adyacencia CLNS entre ellos es el nivel 1/nivel 2 de forma predeterminada. 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

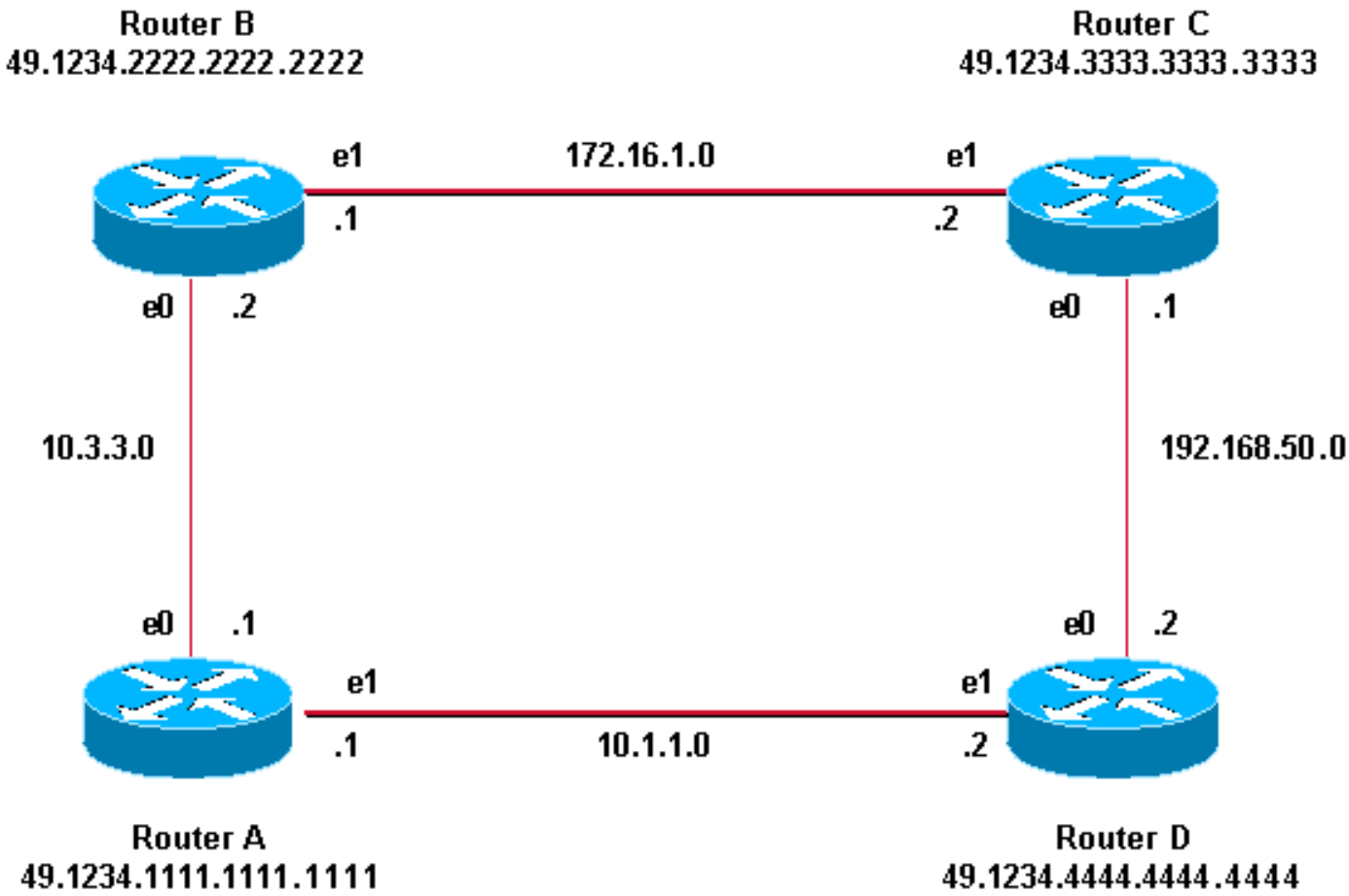
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

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 transporta en los LSPs L1, CSNPs 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
```

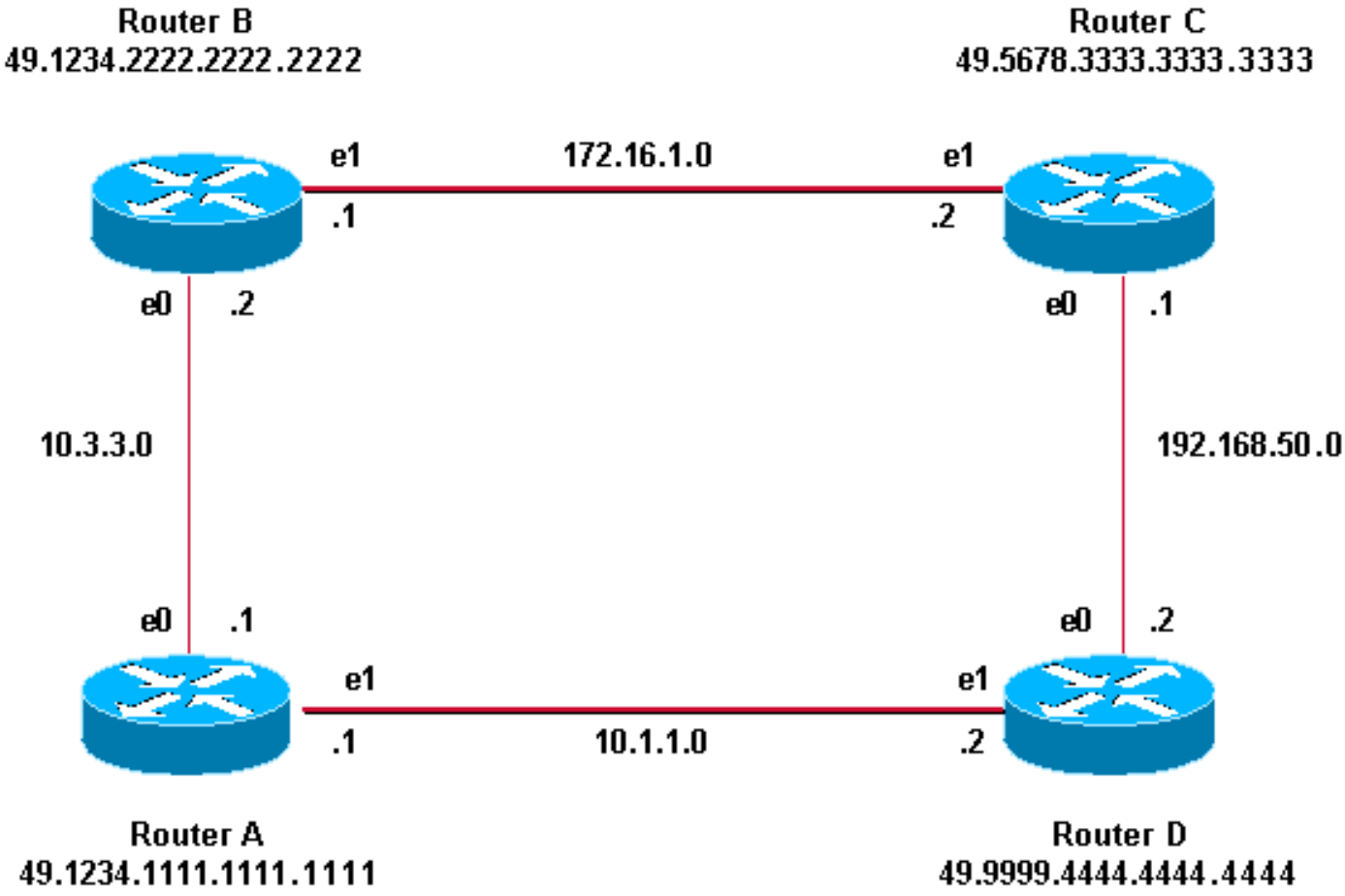
Router D

```
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 el área IS-IS 49.1234; El Router C está en el 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
```

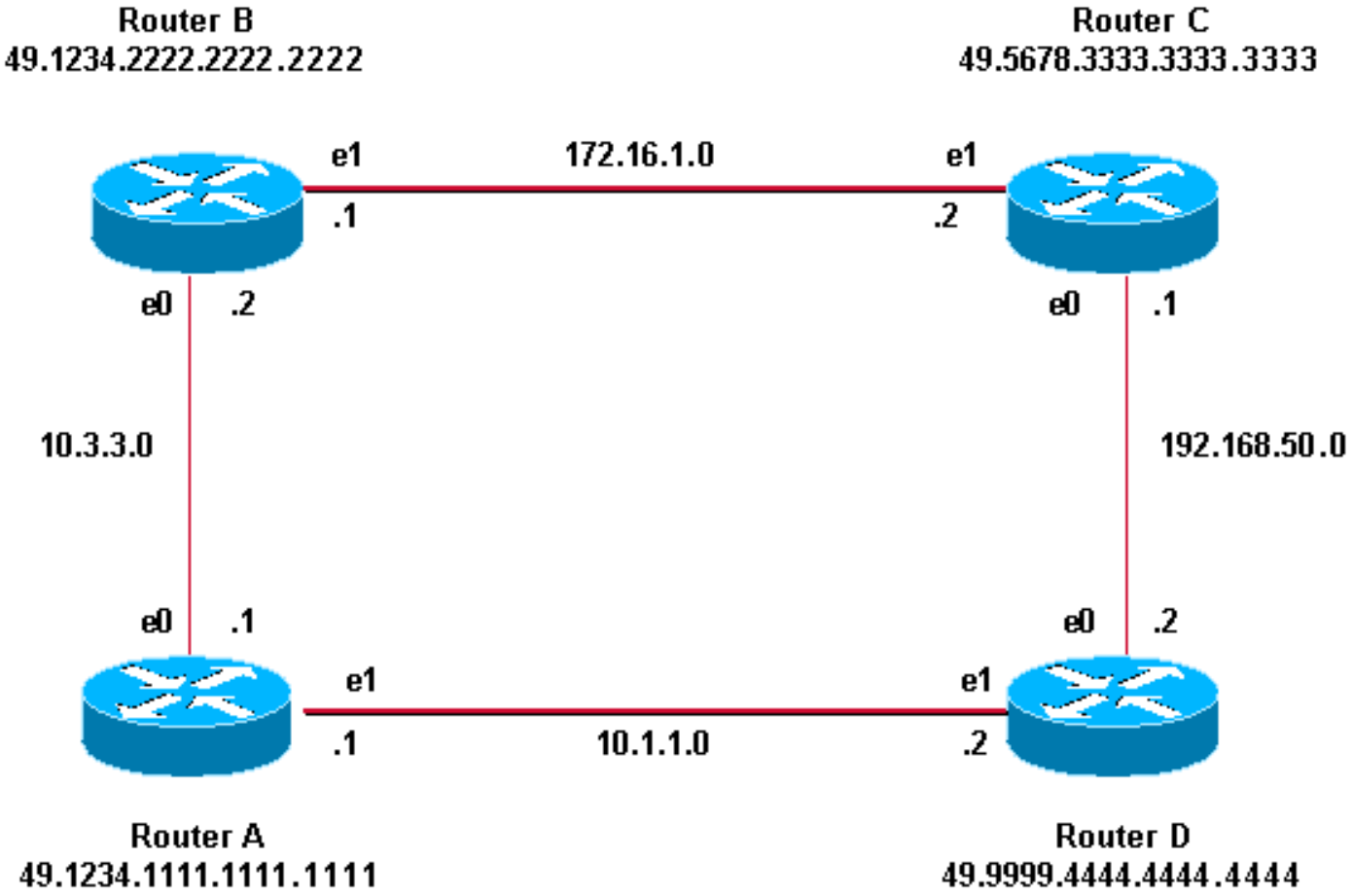
Router D

```
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 de esta sección ilustran una combinación de

autenticación de dominio, área e interfaz. El router A y el router B se encuentran en la misma área y se configuran con la contraseña de área "tiGHter". El Router C y el Router D pertenecen a dos áreas diferentes a las del Router A y el Router B. Todos los routers se encuentran en el mismo dominio y comparten la contraseña de nivel de dominio "seCety". El Router B y el Router C tienen una configuración de interfaz para el link Ethernet entre ellos. El router C y el router D sólo forman adyacencias L2 con sus vecinos y no es necesario configurar la contraseña de área.



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

Ciertos **comandos show** son soportados por el Analizador Cisco CLI (sólo clientes registrados) , lo que le permite ver un análisis del resultado del comando show.

Para verificar si la autenticación de la interfaz funciona correctamente, utilice el comando **show clns neighbors** en el modo EXEC del usuario o EXEC privilegiado. El resultado del comando muestra el tipo de adyacencia y el estado de la conexión. Este ejemplo de salida del comando **show clns neighbors** muestra un router configurado correctamente para la autenticación de la interfaz y muestra el estado como UP:

```
RouterA# show clns neighbors

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

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

Troubleshoot

Si los routers conectados directamente tienen la autenticación configurada en un lado de un link y no en el otro, los routers no forman 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 routers conectados directamente tienen la autenticación 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 el que se configura la autenticación de área no acepta LSP L1 del vecino CLNS sin ninguna autenticación de área configurada. Sin embargo, el vecino sin autenticación de área continúa aceptando LSPs L1 y L2.

Este es el mensaje de depuración en el Router A donde se configura la autenticación de área y se recibe L1 LSP de un vecino (Router B) sin 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 configura la autenticación de dominio en un router, rechaza los LSPs L2 de los routers que no tienen la autenticación de dominio configurada. Los routers que no tienen la autenticación configurada aceptan los LSP del router que tiene la autenticación configurada.

El resultado de la depuración a continuación muestra las fallas de autenticación de LSP. El router CA se configura para la autenticación de área o dominio y recibe LSP de nivel 2 de un router (Router DB) que no está configurado para la autenticación de dominio o 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