

Configurando a autenticação IS-IS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Autenticação de interface](#)

[Autenticação de área](#)

[Autenticação de domínio](#)

[Combinando domínio, área e autenticação de interface](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

É desejável configurar a autenticação dos protocolos de roteamento para evitar a introdução de informações mal-intencionadas na tabela de roteamento. Este documento demonstra a autenticação de texto claro entre roteadores que executam o IS-IS (Intermediate System-to-Intermediate System) para IP.

Este documento abrange apenas a Autenticação de Texto Limpo IS-IS. Consulte [Aprimoramento da segurança em uma rede IS-IS](#) para obter mais informações sobre os outros tipos de autenticação IS-IS.

[Prerequisites](#)

[Requirements](#)

Os leitores deste documento devem estar familiarizados com a operação e a configuração do IS-IS.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas. A configuração neste documento foi testada nos Cisco 2500 Series Routers, executando o Cisco IOS versão 12.2(24a)

Informações de Apoio

O IS-IS permite a configuração de uma senha para um link especificado, uma área ou um domínio. Os roteadores que desejam se tornar vizinhos devem trocar a mesma senha para seu nível configurado de autenticação. Um roteador que não esteja de posse da senha apropriada é proibido de participar da função correspondente (isto é, ele não pode inicializar um link, ser membro de uma área ou de um domínio de Nível 2, respectivamente).

O software Cisco IOS[®] permite a configuração de três tipos de autenticação IS-IS.

- **Autenticação IS-IS** - Durante muito tempo, esta foi a única maneira de configurar a autenticação para IS-IS.
- **Autenticação IS-IS HMAC-MD5** - Este recurso adiciona um resumo HMAC-MD5 a cada unidade de dados de protocolo (PDU) IS-IS. Ele foi introduzido no software Cisco IOS versão 12.2(13)T e só é suportado em um número limitado de plataformas.
- **Autenticação de texto claro aprimorada** - Com esse novo recurso, a autenticação de texto claro pode ser configurada usando novos comandos que permitem que as senhas sejam criptografadas quando a configuração do software for exibida. Também facilita o gerenciamento e a alteração de senhas.

Observação: consulte [Aprimoramento da segurança em uma rede IS-IS](#) para obter informações sobre ISIS MD-5 e Autenticação de texto claro aprimorada.

O protocolo IS-IS, conforme especificado no [RFC 1142](#), fornece a autenticação de pacotes Hellos e Link State (LSPs) através da inclusão de informações de autenticação como parte do LSP. Essas informações de autenticação são codificadas como um triplo de Valor de comprimento de tipo (TLV). O tipo de TLV de autenticação é 10; O comprimento do TLV é variável; e o valor do TLV depende do tipo de autenticação que está sendo usado. Por padrão, a autenticação é desabilitada.

Configurar

Esta seção discute como configurar a autenticação de texto claro IS-IS em um link, para uma área e para um domínio.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use as [Melhores formas de aprendizado para pesquisar Comandos \(somente clientes registrados\)](#) .

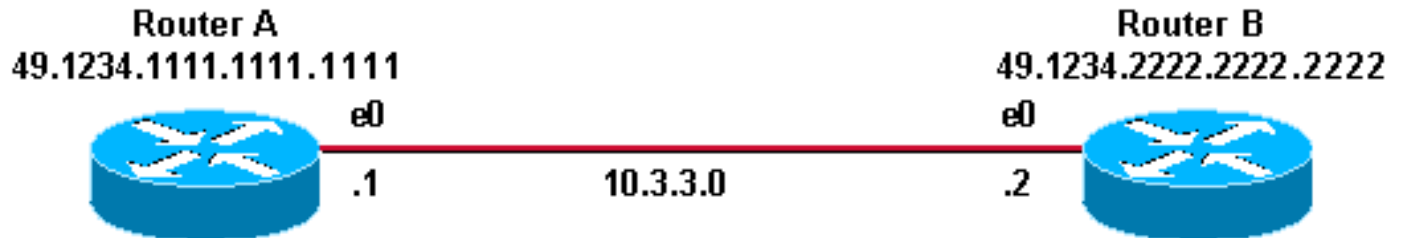
Autenticação de interface

Quando você configura a autenticação IS-IS em uma interface, você pode habilitar a senha para o roteamento de Nível 1, Nível 2 ou de Nível 1/Nível 2. Se você não especificar um nível, o padrão será Nível 1 e Nível 2. Dependendo do nível para o qual a autenticação é configurada, a senha é transportada nas mensagens de saudação correspondentes. O nível de autenticação de interface IS-IS deve rastrear o tipo de adjacência na interface. Use o comando **show clns neighbor** para descobrir o tipo de adjacência. Não é possível especificar o nível para autenticação de área e domínio.

O diagrama de rede e as configurações para autenticação de interface nos roteadores A, Ethernet

0 e B, Ethernet 0 são mostrados abaixo. Os roteadores A e B estão configurados com a senha SECr3t do isis para os Níveis 1 e 2. Essas senhas fazem distinção entre maiúsculas e minúsculas.

Nos roteadores Cisco configurados com o IS-IS (Connectionless Network Service) CLNS, a adjacência CLNS entre eles é Nível 1/Nível 2 por padrão. Portanto, o roteador A e o roteador B terão tipos de adjacência, a menos que seja configurado especificamente para Nível 1 ou Nível 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

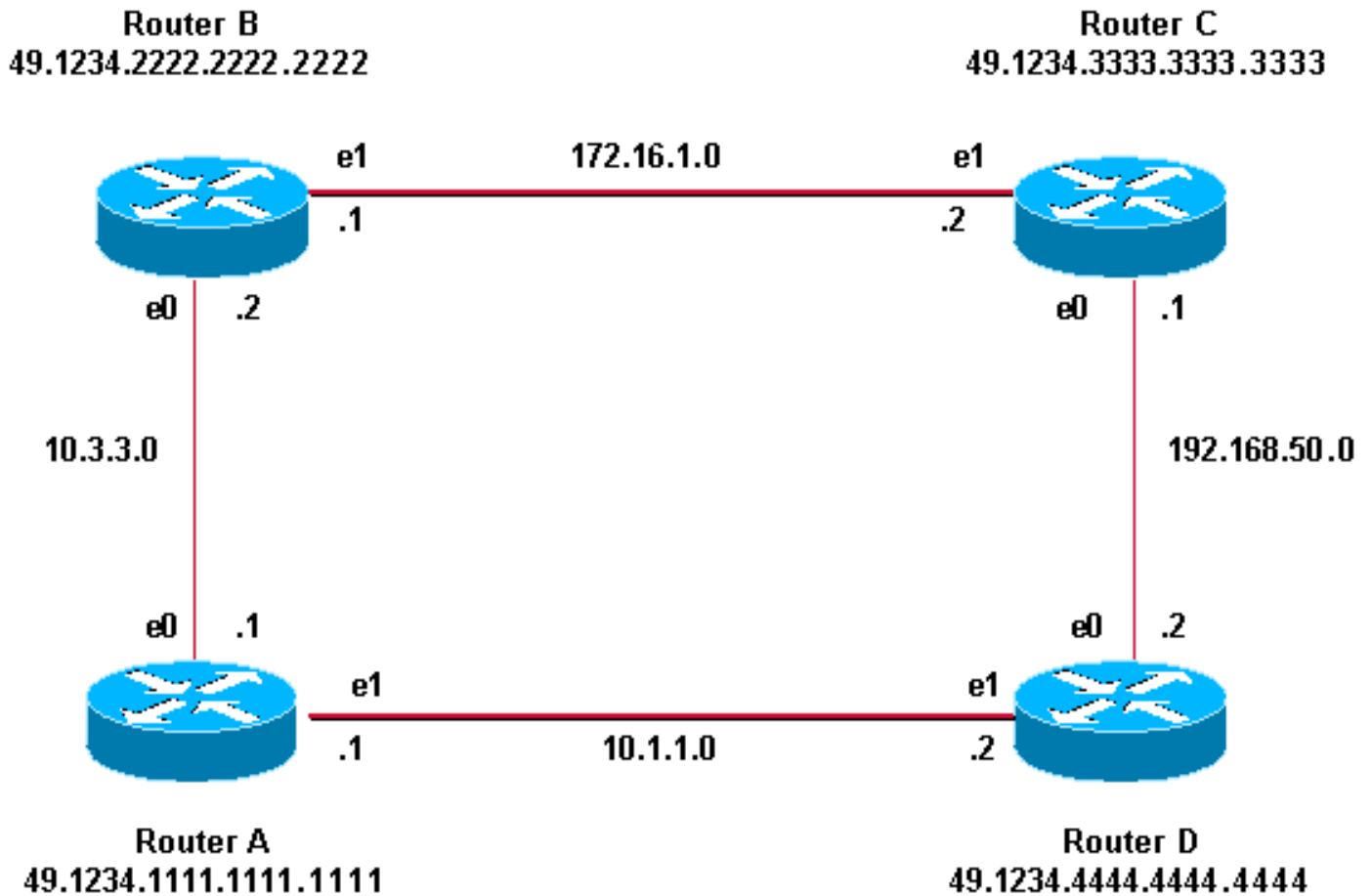
```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

Autenticação de área

O diagrama de rede e as configurações para a autenticação de área são mostrados abaixo. Quando a autenticação de área é configurada, a senha é transportada nos LSPs L1, CSNPs e PSNPs. Todos os roteadores estão na mesma área IS-IS, 49.1234, e estão todos configurados com a senha de área "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
```

Roteador 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 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
```

Roteador D

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

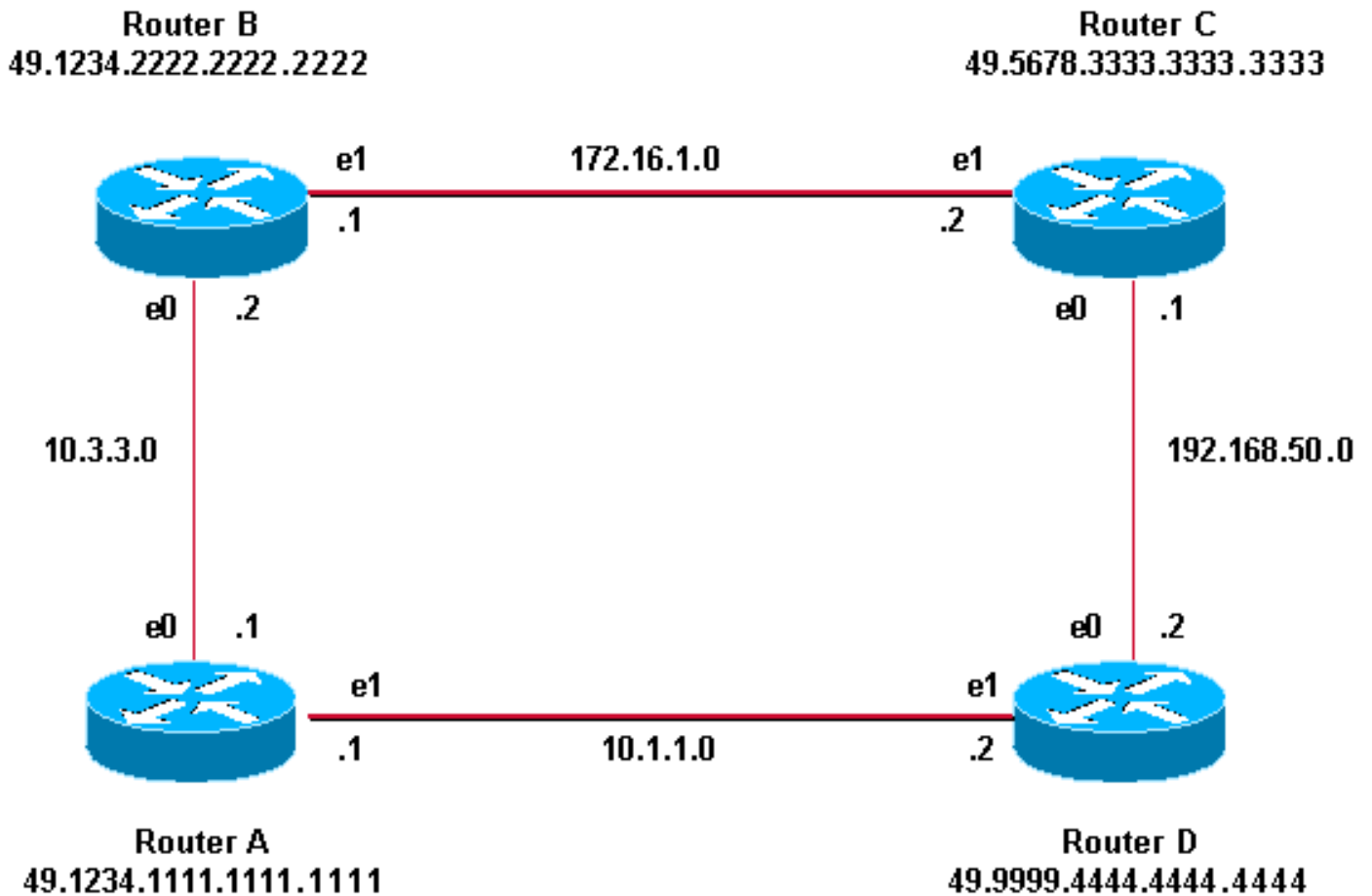
```
interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis
```

```
router isis
net 49.1234.4444.4444.4444.00
area-password tiGhter
```

Autenticação de domínio

O diagrama de rede e configurações para a autenticação de domínio são mostrados abaixo. O Roteador A e o Roteador B estão na área IS-IS 49.1234; O roteador C está na área IS-IS 49.5678; e o Roteador D está na área 49.999. Todos os roteadores estão no mesmo Domínio IS-

IS (49) e são configurados com a senha de domínio "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
```

Roteador 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 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
```

Roteador D

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

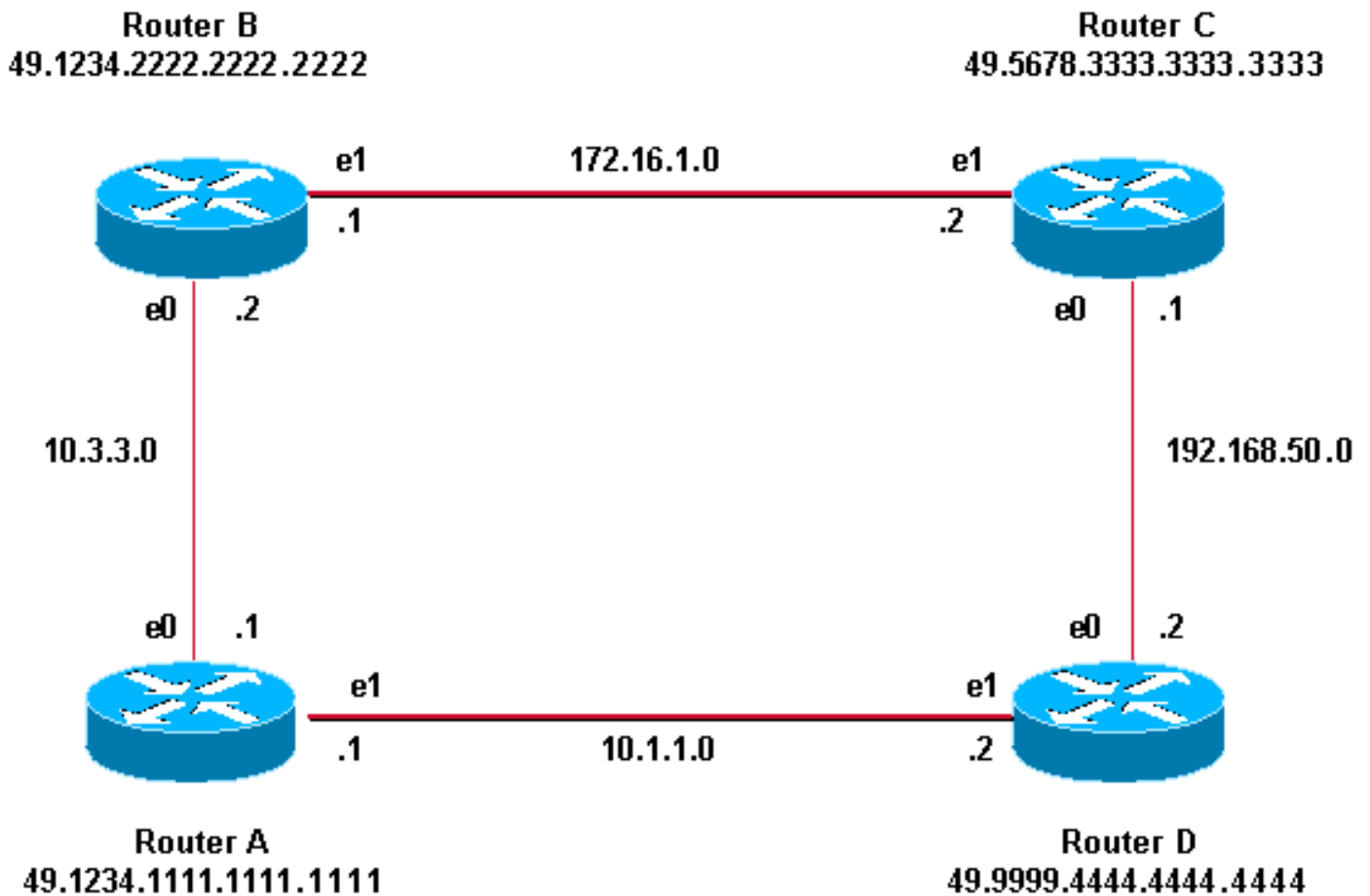
```
interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis
```

```
router isis
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

Combinando domínio, área e autenticação de interface

A topologia e as configurações parciais nesta seção ilustram uma combinação de autenticação de

domínio, área e interface. O Roteador A e o Roteador B estão na mesma área e estão configurados com a senha de área "tiGHter". O Roteador C e o Roteador D pertencem a duas áreas diferentes dos Roteadores A e B. Todos os roteadores estão no mesmo domínio e compartilham a senha de nível de domínio "seSecurity". Os roteadores B e C têm uma configuração de interface para o link Ethernet entre eles. O Roteador C e o Roteador D formam apenas adjacências de L2 com seus vizinhos e não é necessário configurar a senha da 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
```

Roteador C

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

interface ethernet0
```

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-password seCurity
area-password tiGHter
```

Roteador 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
```

Verificar

Determinados comandos **show** são suportados pelo [Cisco CLI Analyzer](#) ([somente](#) clientes [registrados](#)) , que permite que você veja uma análise da saída do comando.

Para verificar se a autenticação de interface está funcionando corretamente, use o comando **show clns neighbors** no modo EXEC usuário ou EXEC privilegiado. A saída do comando exibe o tipo de adjacência e o estado da conexão. Este exemplo de saída do comando **show clns neighbors** mostra um roteador corretamente configurado para autenticação de interface e exibe o 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 a autenticação de área e domínio, a verificação da autenticação pode ser feita usando comandos debug, como explicado na próxima seção.

Troubleshoot

Se os roteadores conectados diretamente tiverem a autenticação configurada em um lado de um link, e não no outro, os roteadores não formam uma adjacência CLNS IS-IS. No resultado abaixo, o roteador B está configurado para autenticação na sua interface Ethernet 0 e o roteador A não está configurado com autenticação na sua interface adjacente.

```
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
```

Se os roteadores conectados diretamente tiverem a autenticação de área configurada em um lado de um link, a adjacência CLNS IS-IS é formada entre as duas rotas. No entanto, o roteador no qual a autenticação de área está configurada não aceita LSPs L1 do vizinho CLNS sem autenticação de área configurada. No entanto, o vizinho sem autenticação de área continua a aceitar LSPs L1 e L2.

Esta é a mensagem de depuração no Roteador A onde a autenticação de área é configurada e recebe LSP L1 de um vizinho (Roteador B) sem autenticação 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#
```

Se você configurar a autenticação de domínio em um roteador, ele rejeitará os LSPs L2 dos roteadores que não têm a autenticação de domínio configurada. Os roteadores que não têm autenticação configurada aceitam os LSPs do roteador que tem autenticação configurada.

A saída de depuração, abaixo, mostra as falhas de autenticação de LSP. A CA do roteador está configurada para autenticação de área ou domínio e está recebendo LSPs de nível 2 de um roteador (DB do roteador) que não está configurado para autenticação de domínio ou senha.

```
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
```

[Informações Relacionadas](#)

- [Página de Suporte do IP Routing](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)