

Configurando a autenticação IS-IS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Autenticação de interface](#)

[Autenticação de área](#)

[Autenticação de domínio](#)

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

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

É desejável configurar a autenticação para protocolos de roteamento a fim impedir a introdução de informação maliciosa na tabela de roteamento. Este documento demonstra a autenticação do texto claro entre os roteadores que executam o Intermediate System-to-Intermediate System (IS-IS) para o IP.

Este documento cobre somente a autenticação do texto claro IS-IS. Refira-se a [aumentação da Segurança em uma rede IS-IS](#) para obter mais informações sobre os outros tipos de autenticação IS-IS.

[Pré-requisitos](#)

[Requisitos](#)

Os leitores deste documento devem ser familiares com a operação e a configuração IS-IS.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas. A configuração neste documento foi testada em Cisco 2500 Series Router, a versão do Cisco IOS running 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 do [®]do Cisco IOS permite que três tipos de autenticação IS-IS sejam configurados.

- **Autenticação IS-IS** - Por muito tempo, esta era a única maneira de configurar a autenticação para o IS-IS.
- **Autenticação IS-IS HMAC-MD5** - Esta característica adiciona um resumo HMAC-MD5 a cada unidade de dados do protocolo IS-IS (PDU). Foi introduzida na versão 12.2(13)T do Cisco IOS Software e é apoiada somente em Plataformas de um número limitado.
- **Autenticação aumentada do texto claro** - Com estes novos recursos, a autenticação do texto claro pode ser configurada usando os comandos `new` que permitem que as senhas sejam cifradas quando a configuração de software é indicada. Igualmente facilita senhas controlar e mudar.

Note: Refira a [aumentação da Segurança em uma rede IS-IS](#) para obter informações sobre de ISIS MD-5 e autenticação aumentada do texto claro.

O protocolo IS-IS, como especificado no [RFC 1142](#), prevê a autenticação dos hellos e dos pacotes do estado do link (LSP) através da inclusão da informação da autenticação como parte do LSP. Esta informação da autenticação está codificada enquanto se triplicar do Type Length Value (TLV). O tipo da autenticação TLV é 10; o comprimento do TLV é variável; e o valor do TLV depende do tipo da autenticação que está sendo usado. Por padrão, a autenticação é desabilitada.

[Configurar](#)

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

Note: Para encontrar a informação adicional nos comandos usados neste documento, use os [melhores prática procurando comandos \(clientes registrados somente\)](#).

[Autenticação de interface](#)

Quando você configura a autenticação IS-IS em uma relação, você pode permitir a senha para 2 do nível 1, do nível 2, ou ambos roteamento do nível 1/Level. Se você não especifica um nível, o padrão é o nível 1 e o nível 2. segundo o nível para que a autenticação é configurada, a senha é levado dentro os mensagens Hello Messages correspondentes. O nível de autenticação de interface IS-IS deve rastrear o tipo de adjacência na interface. Use o **comando `show clns neighbor`** encontrar o tipo de adjacência. Não é possível especificar o nível para autenticação de área e domínio.

O diagrama da rede e as configurações para a autenticação de interface no roteador A, no ethernet0 e no roteador B, ethernet0 são mostrados abaixo. O roteador A e o roteador B são configurados com senha `SECr3t isis` para o nível 1 e o nível 2. Essas senhas fazem distinção entre maiúsculas e minúsculas.

Nos roteadores Cisco configurados com serviço de rede sem conexão (CLNS) IS-IS, a adjacência CLNS entre eles é o nível 1/Level 2 à revelia. Portanto, o roteador A e o roteador B terão tipos de adjacência, a menos que seja configurado especificamente para Nível 1 ou Nível 2.

Roteador 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
```

roteador 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 está levada dentro o L1 LSP, CSNP e PSNPS. Todos os roteadores estão na mesma área IS-IS, 49.1234, e estão todos configurados com a senha de área "tiGHter".

Roteador 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
```

roteador 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 C do roteador está na área IS-IS 49.5678; e o roteador D está na área 49.9999. Todos os roteadores estão no mesmo Domínio IS-IS (49) e são configurados com a senha de domínio "seCurity".

Roteador 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
```

roteador 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 domínio, uma área, e uma autenticação de interface. O Roteador A e o Roteador B estão na mesma área e estão configurados com a senha de área "tiGHter". O C do roteador e o roteador D pertencem a duas áreas diferentes do que o roteador A e o roteador B. Todo o Roteadores está no mesmo domínio e compartilha da senha "Segurança do domínio-nível." O roteador B e o C do roteador têm uma configuração da interface para as ligações de Ethernet entre ele. O C do roteador e o roteador D formam somente as adjacências L2 com seus vizinhos e configurar a senha de área não é exigido.

Roteador 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
```

roteador 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
```

Roteador D

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

```
interface ethernet0
```

```
interface ethernet0
ip address 192.168.50.1 255.255.255.0
ip router isis
```

```
ip address 192.168.50.2 255.255.255.0
ip router isis
```

```
router isis
net 49.5678.3333.3333.3333.00
domain-password seCurity
```

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

Verificar

Os determinados comandos de exibição são apoiados pelo [analisador do CLI Cisco \(clientes registrados somente\)](#), que permite que você ver uma análise do emissor de comando de execução.

Para verificar se a autenticação de interface está trabalhando corretamente, use o **comando show clns neighbors** no usuário EXEC ou no modo de exec privilegiado. A saída do comando indica o tipo adjacente e o estado da conexão. Este exemplo de saída do **comando show clns neighbors** mostra um roteador configurado corretamente para a autenticação de interface e indica o estado como ACIMA:

```
RouterA# show clns neighbors
```

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

Para a área e a autenticação do domínio, a verificação de autenticação pode ser feita usando comandos debug como explicado na próxima seção.

Troubleshooting

Se diretamente os roteadores conectados têm a autenticação configurada em um lado de um link, e não no outro, o Roteadores não forma 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 diretamente os roteadores conectados têm a área de autenticação configurada em um lado de um link, a adjacência CLNS IS-IS está formada entre as duas rotas. Contudo, o roteador em que a área de autenticação é configurada, não aceita L1 LSP do vizinho de CLNS sem a área de autenticação configurada. Contudo, o vizinho sem a área de autenticação continua a aceitar L1 e L2 LSP.

Esta é a mensagem debugar no roteador A onde a autenticação de área é configurada e de recepção L1 LSP 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 configura a autenticação do domínio em um roteador, rejeita o L2 LSP do Roteadores que não tem a autenticação do domínio configurada. Roteadores que não tem a autenticação configurada para aceitar os LSP do roteador que tem a autenticação configurada.

A saída de depuração, abaixo, mostra as falhas de autenticação de LSP. O roteador CA é configurado para a área ou a autenticação do domínio e é o nível de recebimento 2 LSP de um roteador (roteador DB) que não seja configurado para o domínio ou a autenticação de 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](#)