Configuration de l'authentification IS-IS

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Configuration](#)
[Authentification d'interface](#)
[Authentification de zone](#)
[Authentification du domaine](#)
[Combinaison de l'authentification du domaine, de la zone et de l'interface](#)
[Vérification](#)
[Dépannage](#)
[Informations connexes](#)

Introduction

Il est souhaitable de configurer l'authentification pour les protocoles de routage afin d'empêcher l'introduction d'informations malveillantes dans la table de routage. Ce document montre l'authentification en texte clair entre les routeurs exécutant le protocole IS-IS (Intermediate System-to-Intermediate System) pour IP.

Ce document couvre uniquement l'authentification en texte clair IS-IS. Référez-vous à Amélioration de la sécurité dans un réseau IS-IS pour plus d'informations sur les autres types d'authentification IS-IS.

Conditions préalables

Conditions requises

Les lecteurs de ce document doivent connaître le fonctionnement et la configuration de l'IS-IS.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. La configuration de ce document a été testée sur les routeurs de la gamme Cisco 2500, exécutant Cisco IOS version 12.2(24a)

Informations générales

IS-IS permet de configurer un mot de passe pour une liaison, une zone ou un domaine spécifiés. Les routeurs qui veulent devenir voisins doivent échanger le même mot de passe pour leur niveau d'authentification configuré. Il est interdit à un routeur qui ne possède pas le mot de passe approprié de participer à la fonction correspondante (c'est-à-dire qu'il ne peut pas initialiser une liaison, être membre d'une zone ou être membre d'un domaine de niveau 2, respectivement).

Le logiciel Cisco IOS® permet de configurer trois types d'authentification IS-IS.

- **Authentification IS-IS** - Pendant longtemps, c'était la seule façon de configurer l'authentification IS-IS.
- **Authentification HMAC-MD5 IS-IS** : cette fonction ajoute un résumé HMAC-MD5 à chaque unité de données de protocole (PDU) IS-IS. Il a été introduit dans la version 12.2(13)T du logiciel Cisco IOS et n'est pris en charge que sur un nombre limité de plates-formes.
- **Enhanced Clear Text Authentication** - Avec cette nouvelle fonctionnalité, l'authentification en texte clair peut être configurée à l'aide de nouvelles commandes qui permettent de chiffrer les mots de passe lors de l'affichage de la configuration logicielle. Elle facilite également la gestion et le changement des mots de passe.

Remarque : reportez-vous à Amélioration de la sécurité dans un réseau IS-IS pour plus d'informations sur ISIS MD-5 et Enhanced Clear Text Authentication.

Le protocole IS-IS, tel que spécifié dans RFC 1142, prévoit l'authentification des paquets HELLO et LSP (Link State Packets) par l'inclusion d'informations d'authentification dans le LSP. Ces informations d'authentification sont codées comme une valeur de longueur de type (TLV) triple. Le type de TLV d'authentification est 10 ; la longueur du TLV est variable ; et la valeur du TLV dépend du type d'authentification utilisé. Par défaut, l'authentification est désactivée.

Configuration

Cette section explique comment configurer l'authentification en texte clair IS-IS sur une liaison, pour une zone et pour un domaine.

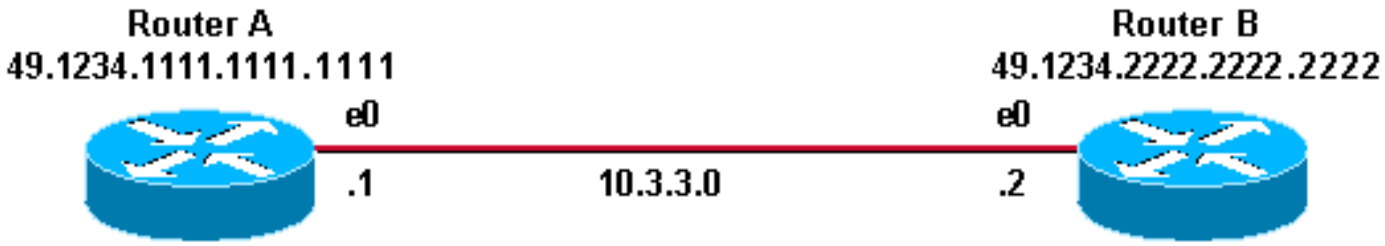
Remarque : Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez les Méthodes Recommandées pour la recherche de commandes (clients enregistrés uniquement).

Authentification d'interface

Lorsque vous configurez l'authentification IS-IS sur une interface, vous pouvez activer le mot de passe pour le routage de niveau 1, niveau 2 ou les deux niveaux 1/2. Si vous ne spécifiez pas de niveau, la valeur par défaut est Niveau 1 et Niveau 2. Selon le niveau pour lequel l'authentification est configurée, le mot de passe est transmis dans les messages Hello correspondants. Le niveau d'authentification de l'interface IS-IS doit suivre le type de contiguïté sur l'interface. Utilisez la commande **show clns neighbor** pour connaître le type de contiguïté. Pour l'authentification de zone et de domaine, vous ne pouvez pas spécifier le niveau.

Le schéma de réseau et les configurations pour l'authentification d'interface sur les routeurs A, Ethernet 0 et B, Ethernet 0 sont présentés ci-dessous. Les routeurs A et B sont tous deux configurés avec le mot de passe isis SECr3t pour les niveaux 1 et 2. Ces mots de passe sont sensibles à la casse.

Sur les routeurs Cisco configurés avec l'IS-IS CLNS (Connectionless Network Service), la contiguïté CLNS entre eux est de niveau 1/niveau 2 par défaut. Ainsi, les routeurs A et B auront les deux types de contiguïté, sauf s'ils sont configurés spécifiquement pour le niveau 1 ou le niveau 2.



Router A

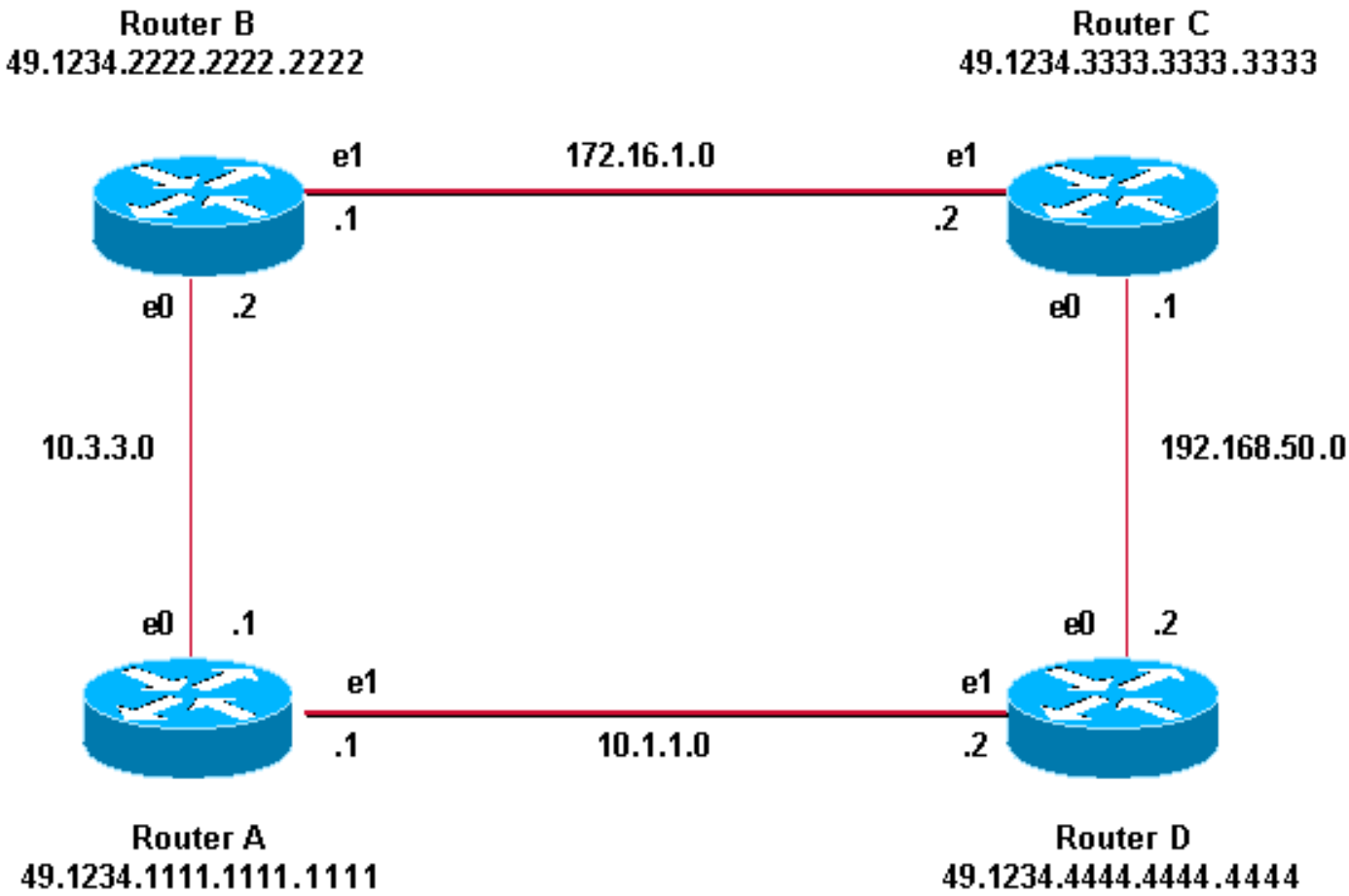
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

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
```

Authentification de zone

Le schéma de réseau et les configurations pour l'authentification de zone sont présentés ci-dessous. Lorsque l'authentification de zone est configurée, le mot de passe est transporté dans les LSP de couche 1, les CSNP et les PSNPS. Tous les routeurs se trouvent dans la même zone IS-IS, 49.1234, et ils sont tous configurés avec le mot de passe de zone « 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
```

Routeur 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
```

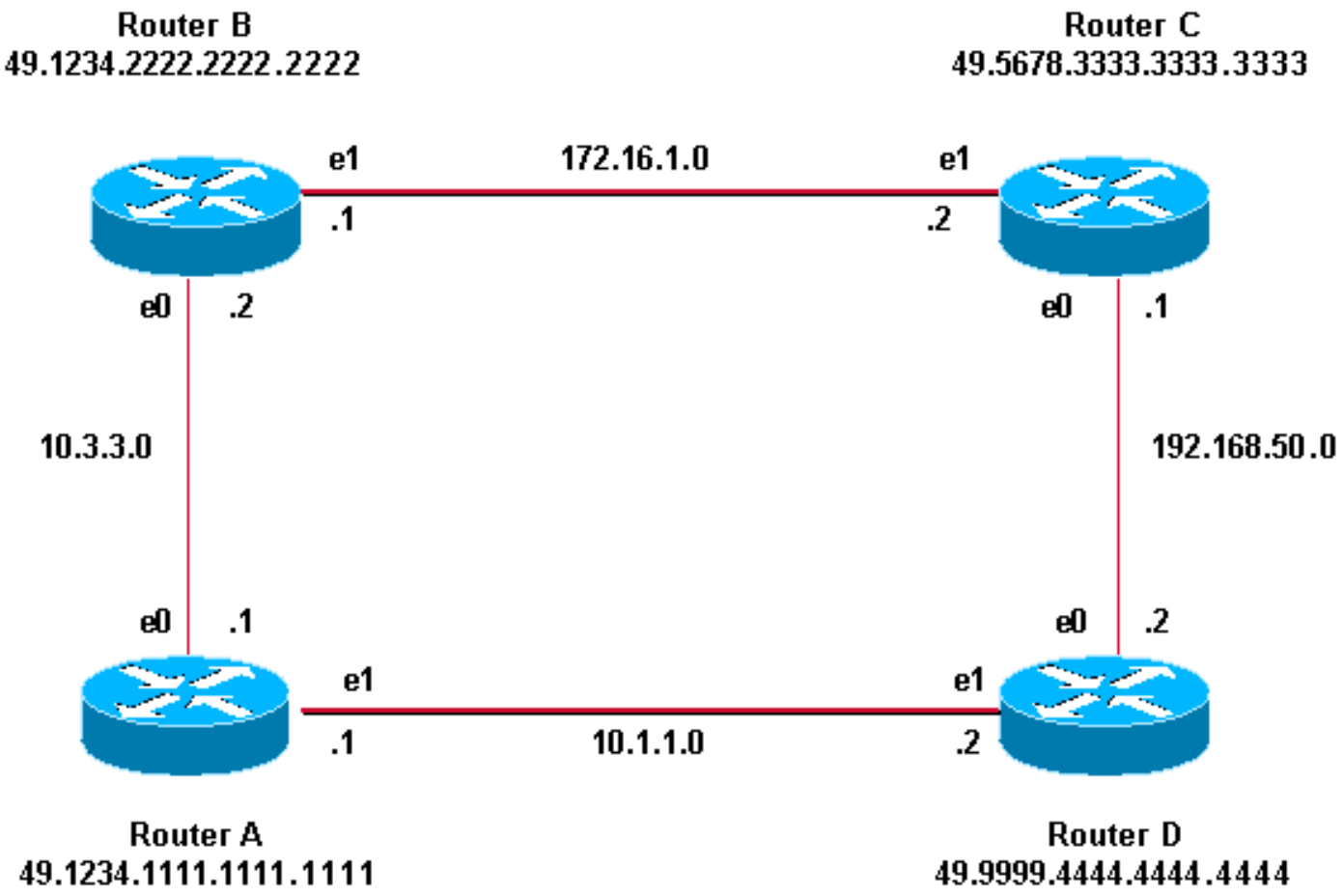
Routeur D

```
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
```

Authentification du domaine

Le schéma de réseau et les configurations pour l'authentification de domaine sont présentés ci-dessous. Les routeurs A et B se trouvent dans la zone IS-IS 49.1234 ; Le routeur C se trouve dans la zone IS-IS 49.5678 ; et le routeur D se trouve dans la zone 49.999. Tous les routeurs se

trouvent dans le même domaine IS-IS (49) et sont configurés avec le mot de passe de domaine « seCtrict ».



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
```

Routeur C

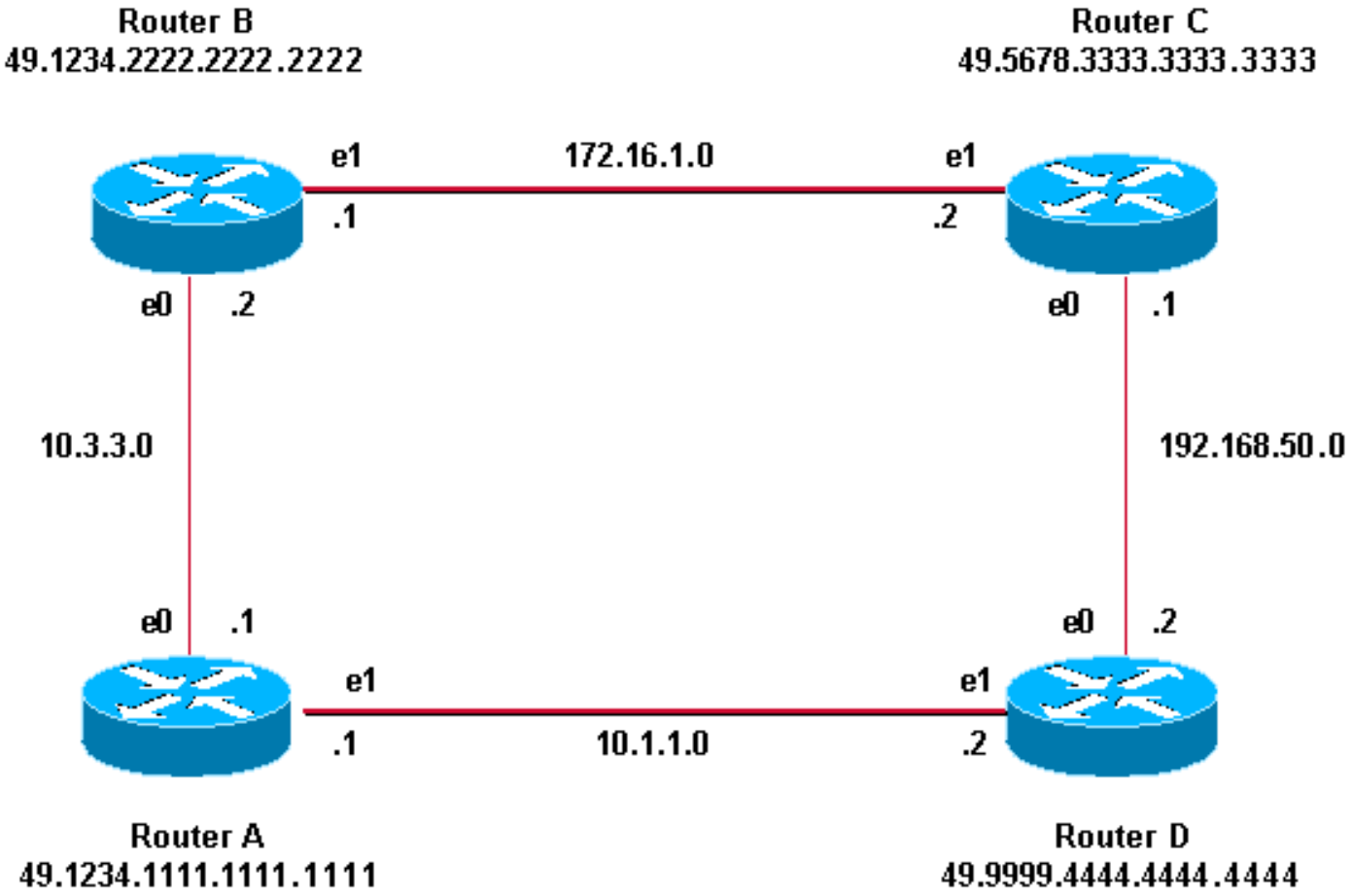
```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis

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
```

Routeur 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
```

Combinaison de l'authentification du domaine, de la zone et de l'interface

La topologie et les configurations partielles de cette section illustrent une combinaison d'authentification de domaine, de zone et d'interface. Les routeurs A et B se trouvent dans la même zone et sont configurés avec le mot de passe de zone « tiGHter ». Les routeurs C et D appartiennent à deux zones différentes des routeurs A et B. Tous les routeurs se trouvent dans le même domaine et partagent le mot de passe de niveau domaine « seCure. » Les routeurs B et C disposent d'une configuration d'interface pour la liaison Ethernet entre eux. Les routeurs C et D forment uniquement des contiguïtés de couche 2 avec leurs voisins et la configuration du mot de passe de zone n'est pas requise.



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
```

Routeur C

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

Routeur D

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

```
interfaceethernet0
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
```

```
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
```

Vérification

Certaines commandes **show** sont prises en charge par Cisco CLI Analyzer (clients enregistrés uniquement) , qui vous permet d'afficher une analyse des **résultats de la** commandeshow.

Pour vérifier si l'authentification de l'interface fonctionne correctement, utilisez la commande **show clns neighbors** en mode d'exécution utilisateur ou privilégié. Le résultat de la commande affiche le type de contiguïté et l'état de la connexion. Cet exemple de sortie de la commande **show clns neighbors** montre un routeur correctement configuré pour l'authentification d'interface et affiche l'état UP :

```
RouterA# show clns neighbors

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

Pour l'authentification de zone et de domaine, la vérification de l'authentification peut être effectuée à l'aide des commandes debug comme expliqué dans la section suivante.

Dépannage

Si l'authentification est configurée sur un côté d'une liaison et non sur l'autre, les routeurs ne forment pas de contiguïté IS-IS CLNS. Dans le résultat ci-dessous, le routeur B est configuré pour l'authentification d'interface sur son interface Ethernet 0 et le routeur A n'est pas configuré avec l'authentification sur son 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
```

Si l'authentification de zone est configurée sur un côté d'une liaison sur les routeurs connectés directement, la contiguïté IS-IS CLNS est formée entre les deux routes. Cependant, le routeur sur lequel l'authentification de zone est configurée n'accepte pas les LSP de couche 1 du voisin CLNS sans authentification de zone configurée. Cependant, le voisin sans authentification de zone continue à accepter les LSP L1 et L2.

Il s'agit du message de débogage sur le routeur A où l'authentification de zone est configurée et reçoit le LSP de couche 1 d'un voisin (routeur B) sans authentification de zone :

```
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 vous configurez l'authentification de domaine sur un routeur, elle rejette les LSP de couche 2 des routeurs qui n'ont pas configuré l'authentification de domaine. Les routeurs dont l'authentification n'est pas configurée acceptent les LSP du routeur dont l'authentification est configurée.

La sortie de débogage ci-dessous montre les échecs d'authentification LSP. L'autorité de certification du routeur est configurée pour l'authentification de zone ou de domaine et reçoit des LSP de niveau 2 d'un routeur (base de données du routeur) qui n'est pas configuré pour l'authentification de domaine ou de mot de passe.

```
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
```

Informations connexes

- Page de support pour le routage IP
- Support et documentation techniques - Cisco Systems