Configuration de l'authentification IS-IS

Contenu

Introduction

Il est desirable de configurer l'authentification pour des protocoles de routage afin d'empêcher l'introduction des informations malveillantes dans la table de routage. Ce document explique l'authentification en mode texte claire entre les Routeurs exécutant le Protocole IS-IS (Intermediate System-to-Intermediate System) pour l'IP.

Ce document couvre seulement l'authentification en mode texte d'espace libre IS-IS. Référez-vous à améliorer 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 devraient être au courant de l'exécution et de la configuration IS-IS.

Composants utilisés

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

Informations générales

L'IS-IS tient compte de la configuration d'un mot de passe pour un lien spécifié, une zone, ou un domaine. Les Routeurs qui veulent devenir des voisins doivent permuter le même mot de passe pour leur niveau configuré de l'authentification. Un routeur pas en possession du mot de passe approprié est interdit de participer à la fonction correspondante (c'est-à-dire, elle peut ne pas initialiser un lien, soit un membre d'une zone, ou soit un membre d'un domaine du niveau 2, respectivement).

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

- **Authentification IS-IS** - Pendant longtemps, c'était la seule manière de configurer l'authentification pour l'IS-IS.
- **Authentification IS-IS HMAC-MD5** - Cette caractéristique ajoute un condensé HMAC-MD5 à chaque Protocol Data Unit IS-IS (PDU). Il a été introduit dans la version de logiciel 12.2(13)T de Cisco IOS et est seulement pris en charge sur des Plateformes d'un nombre limité.
- **Authentification en mode texte claire améliorée** - Avec cette nouvelle configuration, l'authentification en mode texte claire peut être configurée utilisant les nouvelles commandes qui permettent des mots de passe à chiffrer quand la configuration du logiciel est affichée. Il facilite également des mots de passe pour gérer et changer.

Note: Référez-vous à améliorer la Sécurité dans un réseau IS-IS pour les informations sur l'ISIS MD-5 et l'authentification en mode texte claire améliorée.

Le protocole IS-IS, comme spécifié dans RFC 1142, prévoit l'authentification de Hellos et de paquets d'État de lien (LSP) par l'intégration des informations d'authentification en tant qu'élément du LSP. Ces informations d'authentification sont encodées pendant qu'un triple de la valeur de longueur de type (TLV). Le type de la TLV d'authentification est 10 ; la longueur de la TLV est variable ; et la valeur de la TLV dépend du type d'authentification étant utilisé. Par défaut, l'authentification est désactivée.

Configurez

Cette section discute comment configurer l'authentification en mode texte claire IS-IS sur un lien, pour une zone et pour un domaine.

Note: Pour trouver les informations complémentaires sur les commandes utilisées dans ce document, utilisez les pratiques recommandées pour rechercher des commandes (clients enregistrés seulement).

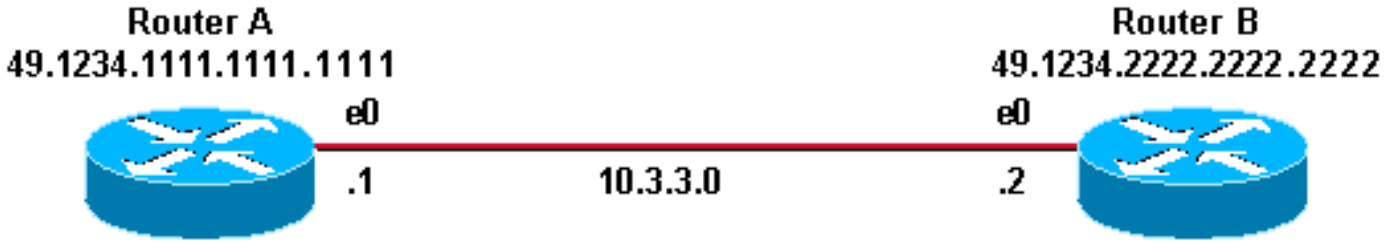
Authentification d'interface

Quand vous configurez l'authentification IS-IS sur une interface, vous pouvez activer le mot de passe pour 2 du niveau 1, du niveau 2, ou les deux routage du niveau 1/Level. Si vous ne spécifiez pas un niveau, le par défaut est le niveau 1 et le niveau 2. selon le niveau pour lequel l'authentification est configurée, le mot de passe est porté dedans les messages Hello correspondants. Le niveau de l'authentification d'interface IS-IS devrait dépister le type de contiguïté sur l'interface. Utilisez la **commande neighbor de show clns** de découvrir le type de contiguïté. Pour la zone et l'authentification de domaine, vous ne pouvez pas spécifier le niveau.

Le schéma de réseau et les configurations pour l'authentification d'interface sur le routeur A, les Ethernet 0 et le routeur B, des Ethernet 0 sont affichés ci-dessous. Le routeur A et le routeur B sont configurés avec l'isis password SECr3t pour le niveau 1 et le niveau 2. Ces mots de passe

distinguent les majuscules et minuscules.

Sur des Routeurs de Cisco configurés avec l'IS-IS sans connexion de service réseau (CLNS), la contiguïté de CLNS entre eux est le niveau 1/Level 2 par défaut. Ainsi, le routeur A et le routeur B auront les deux types de contiguïté, à moins que configuré spécifiquement pour le niveau 1 ou le niveau 2.



routeur A

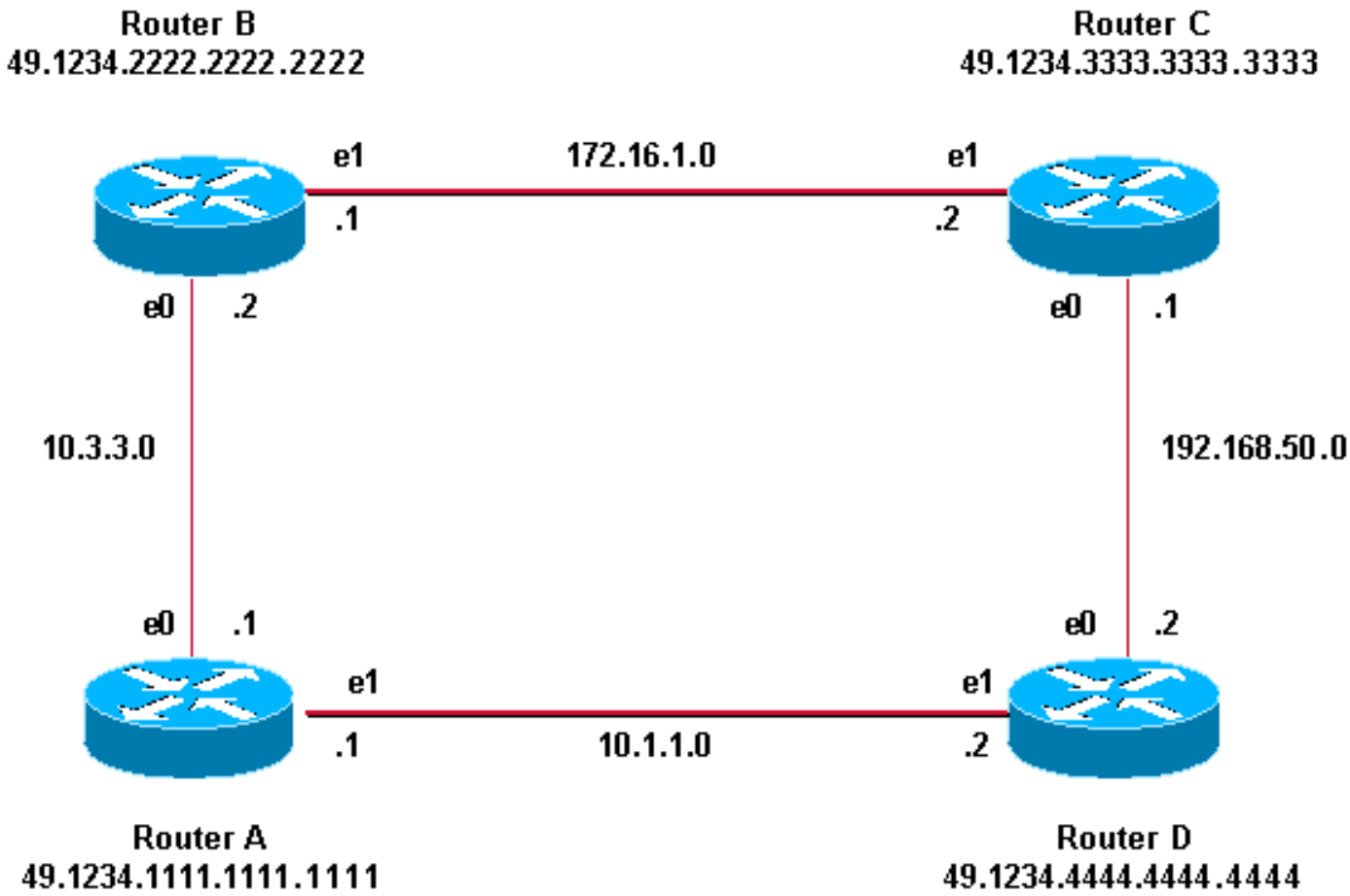
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
```

routeur 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
```

Area authentication

Le schéma de réseau et les configurations pour l'area authentication sont affichés ci-dessous. Quand l'area authentication est configuré, le mot de passe est porté dedans le L1 LSP, CSNPs et PSNPS. Tous les Routeurs sont dans la même zone IS-IS, 49.1234, et ils tous sont configurés avec le mot de passe de zone « plus serré. »



routeur 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
```

routeur 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
```

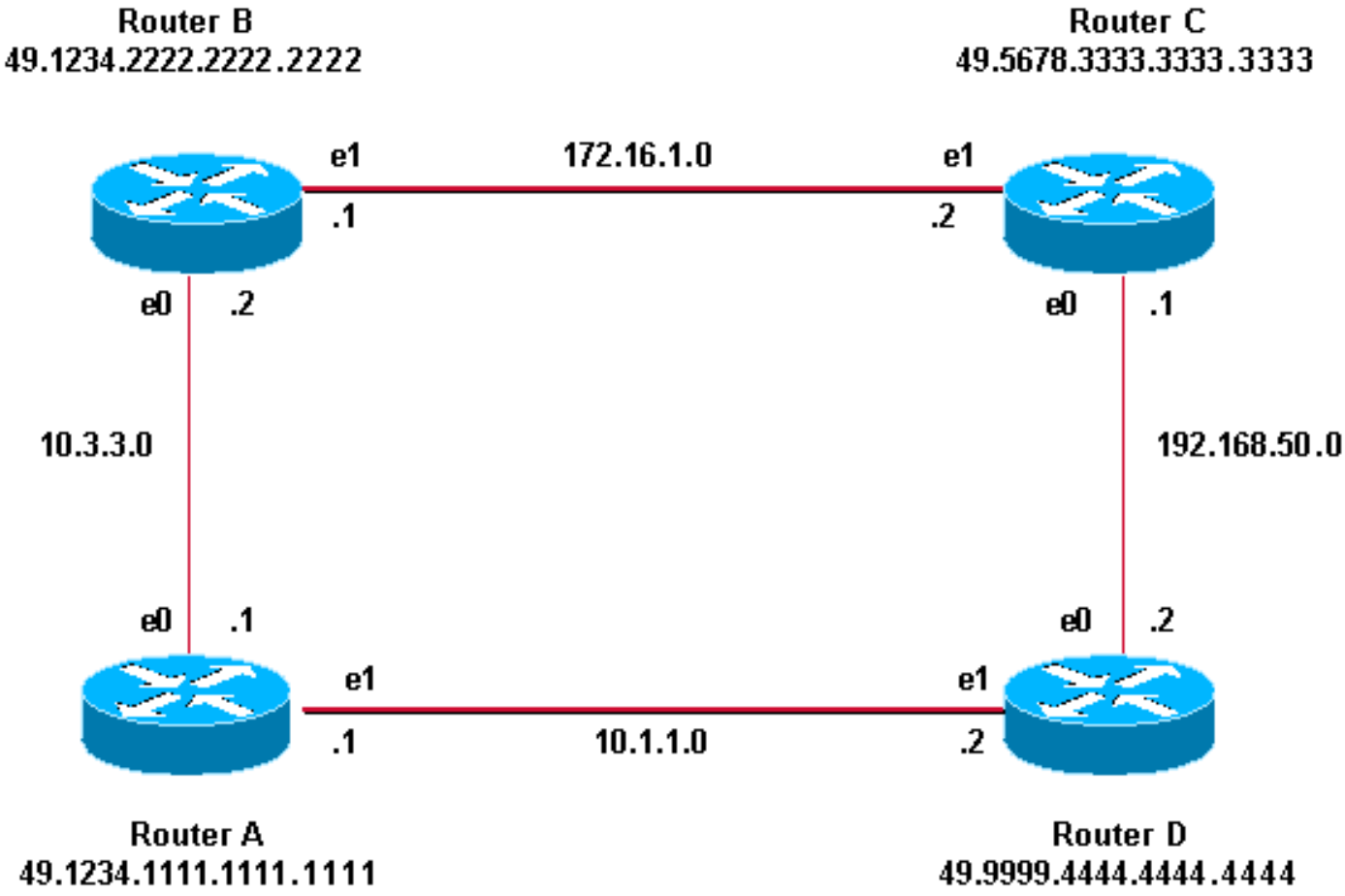
Routeur D

```
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 de domaine

Le schéma de réseau et les configurations pour l'authentification de domaine sont affichés ci-dessous. Le routeur A et le routeur B sont dans la zone 49.1234 IS-IS ; Le routeur C est dans la zone 49.5678 IS-IS ; et le routeur D est dans la zone 49.9999. Tous les Routeurs sont dans le

même domaine IS-IS (49) et sont configurés avec le mot de passe la « Sécurité de domaine. »



routeur 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
```

routeur 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
```

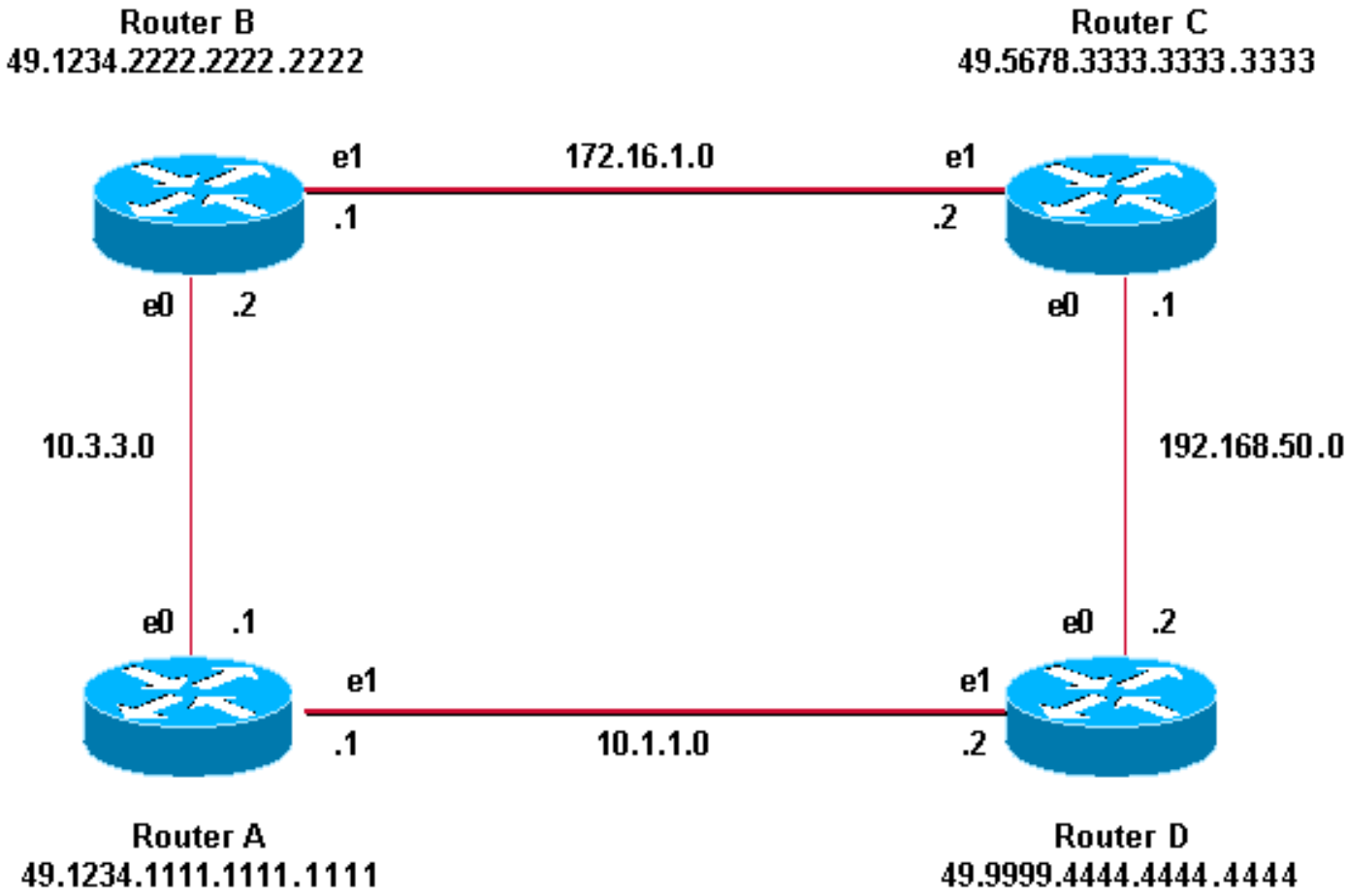
Routeur D

```
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 du domaine, de la zone, et de l'authentification d'interface

La topologie et les configurations partielles dans cette section illustrent une combinaison de

domaine, de zone, et d'authentification d'interface. Le routeur A et le routeur B sont dans la même zone et sont configurés avec le mot de passe de zone « plus serré. » Le routeur C et le routeur D appartiennent à deux zones différentes que le routeur A et le routeur B. Tous les Routeurs sont dans le même domaine et partagent le mot de passe niveau du domaine « Sécurité. » Le routeur B et le routeur C ont une configuration d'interface pour le lien d'Ethernets entre eux. Le routeur C et le routeur D forment seulement les contiguïtés L2 avec leurs voisins et configurer le mot de passe de zone n'est pas exigé.



routeur 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
```

routeur 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

interface ethernet0
```

```
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
```

```
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
```

Vérifiez

Certaines **commandes show** sont prises en charge par l'analyseur de Cisco CLI (clients enregistrés seulement), qui te permet pour visualiser une analyse de sortie de commande show.

Pour vérifier si l'authentification d'interface fonctionne correctement, utilisez le **show clns neighbors** commandent dans l'Exec de l'utilisateur ou le mode d'exécution privilégié. La sortie de la commande affiche le type de contiguïté et l'état de la connexion. Cette sortie témoin du **show clns neighbors** commandent des expositions un routeur correctement configuré pour l'authentification d'interface et affichent l'état en tant que :

```
RouterA# show clns neighbors

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

Pour la zone et l'authentification de domaine, la vérification de l'authentification peut être faite utilisant des commandes de débogage comme expliqué dans la section suivante.

Dépannez

Si directement les routeurs connectés ont l'authentification configurée d'un côté d'un lien, et pas de l'autre, les Routeurs ne forment pas une contiguïté IS-IS de CLNS. Dans la sortie ci-dessous, le routeur B est configuré pour l'authentification d'interface sur son interface d'Ethernet 0, et le routeur A n'est pas configuré avec l'authentification sur son interface contiguë.

```
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 directement les routeurs connectés ont l'area authentication configuré d'un côté d'un lien, la contiguïté IS-IS de CLNS est formée entre les deux artères. Cependant, le routeur sur lequel l'area authentication est configuré, ne reçoit pas L1 LSP du CLNS voisin sans l'area authentication configuré. Cependant, le voisin sans l'area authentication continue à recevoir L1 et L2 LSP.

C'est le message de débogage sur le routeur A où l'area authentication est configuré et recevant L1 LSP d'un voisin (routeur B) sans area authentication :

```
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 le L2 LSP des Routeurs qui ne font pas configurer l'authentification de domaine. Routeurs qui ne font pas configurer l'authentification pour recevoir les LSP du routeur qui fait configurer l'authentification.

La sortie de débogage au-dessous des échecs d'authentification des expositions LSP. Le routeur CA est configuré pour la zone ou l'authentification de domaine et reçoit le niveau 2 LSP d'un routeur (DB de 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