# IS-IS-verificatie configureren

## Inhoud



## Inleiding

Het is wenselijk om authenticatie voor het routeren van protocollen te configureren om de introductie van kwaadwillige informatie in de routingtabel te voorkomen. Dit document demonstreert duidelijke tekstverificatie tussen routers die Intermediate System-to-Intermediate System (IS-IS) voor IP uitvoeren.

Dit document heeft alleen betrekking op de IS-IS Clear Text Verificatie. Raadpleeg Beveiliging in een IS-IS netwerk verbeteren voor meer informatie over de andere typen IS-IS verificatie.

## Voorwaarden

### Vereisten

Lezers van dit document moeten bekend zijn met de IS-IS bediening en configuratie.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies. De configuratie in dit document is getest op Cisco 2500 Series routers en Cisco IOS-versie 12.2(24a)

## Achtergrondinformatie

IS-IS maakt het mogelijk om een wachtwoord te configureren voor een gespecificeerde link, een

gebied of een domein. Routers die buren willen worden, moeten hetzelfde wachtwoord uitwisselen voor het geconfigureerde niveau van verificatie. Een router die niet in het bezit is van het juiste wachtwoord, mag niet deelnemen aan de corresponderende functie (dat wil zeggen, hij mag geen link initialiseren, geen lid zijn van een gebied, of lid zijn van een niveau 2-domein, respectievelijk).

Met Cisco IOS®-software kunnen drie typen IS-IS verificatie worden geconfigureerd.

- **IS-IS verificatie** - Gedurende lange tijd was dit de enige manier om verificatie voor IS-IS te configureren.
- **IS-IS HMAC-MD5-verificatie** - Deze functie voegt een HMAC-MD5-overzicht toe aan elke IS-IS protocol gegevenseenheid (PDU). Het is geïntroduceerd in Cisco IOS-softwarerelease 12.2(13)T en wordt alleen ondersteund op een beperkt aantal platforms.
- **Uitgebreide Wis Tekstverificatie** - met deze nieuwe functie kan duidelijke tekstverificatie worden ingesteld met behulp van nieuwe opdrachten die wachtwoorden kunnen worden versleuteld wanneer de softwareconfiguratie wordt weergegeven. Het maakt ook wachtwoorden makkelijker te beheren en te wijzigen.

**N.B.:** Raadpleeg Beveiliging in een IS-IS netwerk voor informatie over ISIS MD-5 en uitgebreide tekstverificatie.

Het IS-IS-protocol, zoals gespecificeerd in RFC 1142, voorziet in de authenticatie van Hellos en Link State Packets (LSP's) door het opnemen van authenticatie-informatie als onderdeel van het LSP. Deze echtheidsinformatie wordt gecodeerd als een drievoudige typemarge (TLV). het type van het echtheidssysteem is 10; de lengte van de TLV varieert; en de waarde van de TLV hangt af van het type echtheidscontrole dat wordt gebruikt. Verificatie is standaard uitgeschakeld.

# Configureren

In deze sectie wordt besproken hoe u IS-IS duidelijke tekstverificatie kunt configureren op een link, voor een gebied en voor een domein.

**Opmerking:** Als u aanvullende informatie wilt vinden over de opdrachten die in dit document worden gebruikt, gebruikt u de beste praktijken voor het doorzoeken van opdrachten (alleen geregistreerde klanten).

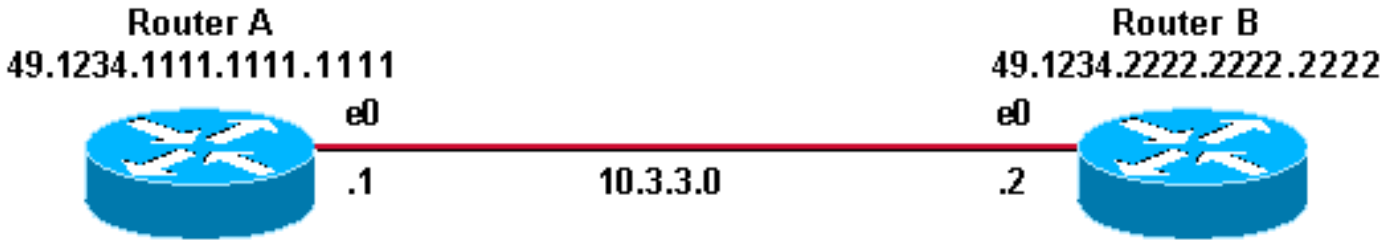
## Interfaceverificatie

Wanneer u IS-IS authenticatie op een interface configureren kunt u het wachtwoord inschakelen voor routing niveau 1, niveau 2 of beide niveau 1/niveau 2. Als u geen niveau specificeert, is de standaardinstelling Niveau 1 en Niveau 2. Afhankelijk van het niveau waarvoor de authenticatie wordt ingesteld, wordt het wachtwoord in de corresponderende Hallo berichten overgebracht. Het niveau van IS-IS interface authenticatie zou het type van nabijheid op de interface moeten volgen. Gebruik de opdracht **Show clns buurman** om het type nabijheid te ontdekken. Voor gebied- en domeinverificatie kunt u het niveau niet specificeren.

Het netwerkdiagram en de configuraties voor interfaceverificatie op router A, Ethernet 0 en router B, Ethernet 0 worden hieronder getoond. Router A en router B worden beide met zijn wachtwoord SECr3t voor zowel niveau 1 als niveau 2 ingesteld. Deze wachtwoorden zijn hoofdlettergevoelig.

Op Cisco routers die zijn geconfigureerd met Connectionless Network Service (CLNS) IS-IS is de CLNS-nabijheid tussen deze routers standaard niveau 1/niveau 2. Dus, zullen router A en router B

beide soorten nabijheid hebben, tenzij specifiek gevormd voor Niveau 1 of Niveau 2.




**router A**

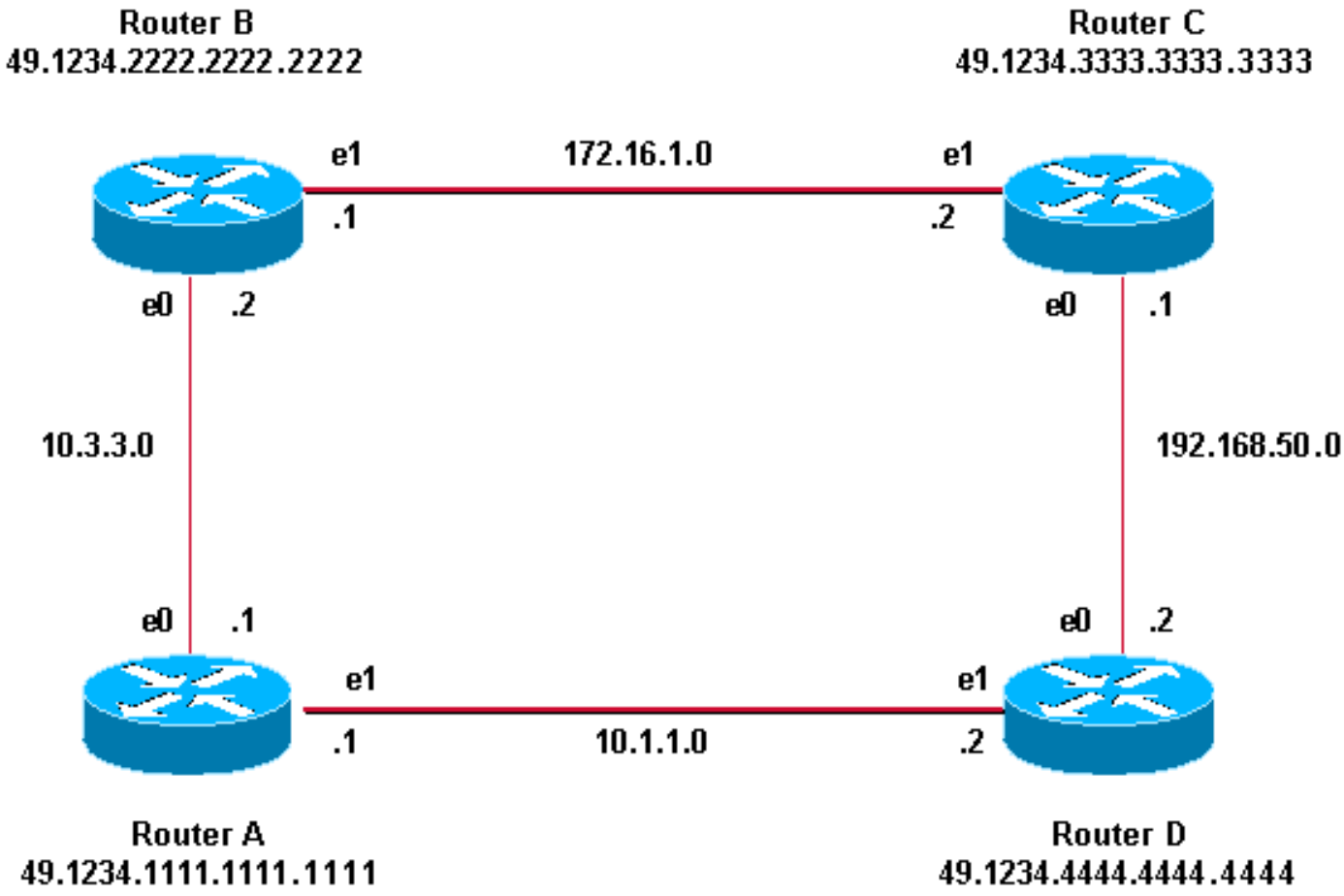
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

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
```

## Gebiedsverificatie

Het netwerkdiagram en de configuraties voor gebiedsverificatie worden hieronder weergegeven. Wanneer de gebiedsverificatie is ingesteld, wordt het wachtwoord in L1 LSP's, CSNP's en PSNPS uitgevoerd. Alle routers bevinden zich in hetzelfde IS-IS gebied, 49.1234, en ze zijn allemaal ingesteld met het gebiedswachtwoord "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

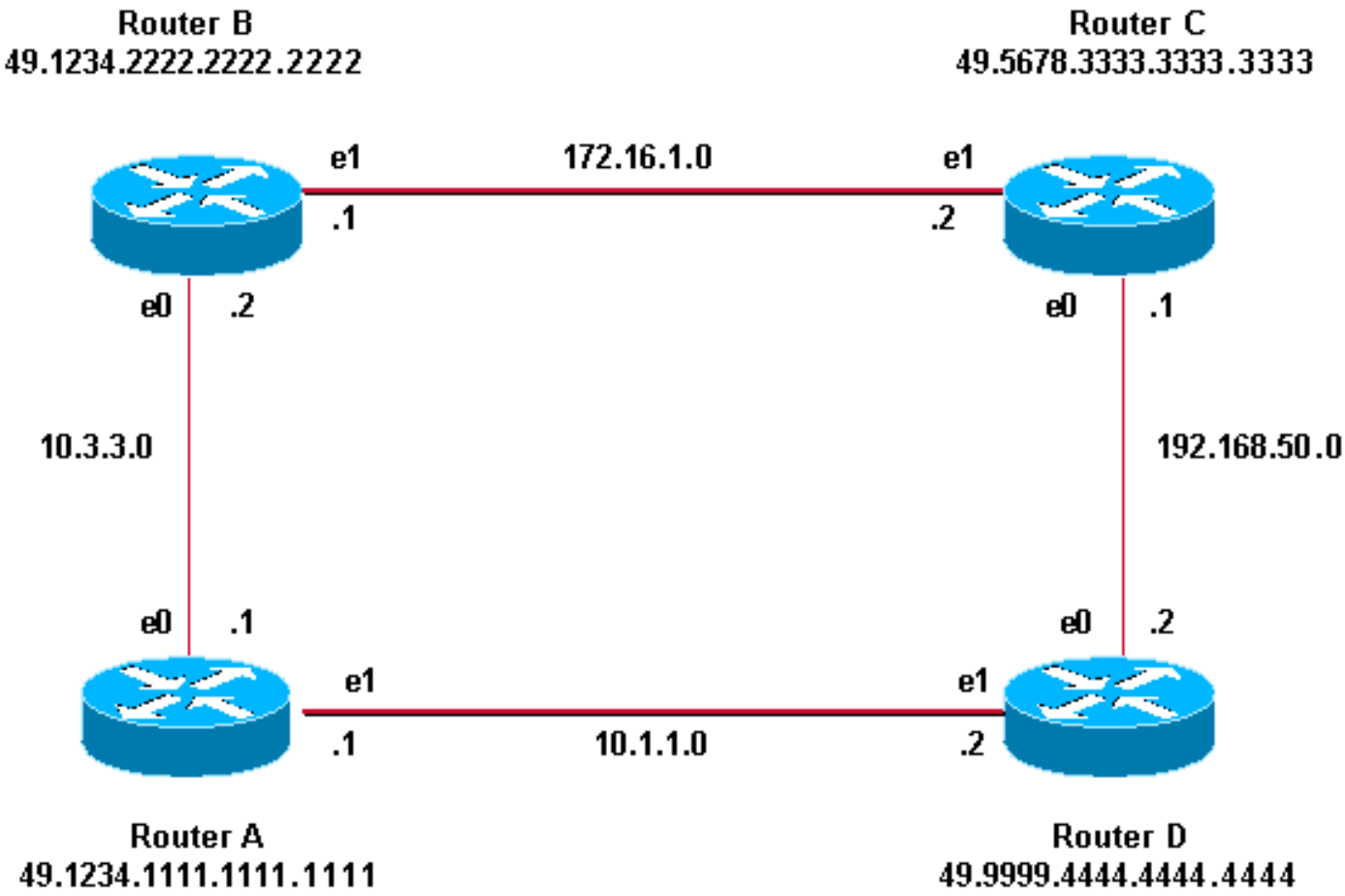
```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis

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
```

## Domain Authentication

Het netwerkdiagram en de configuraties voor domeinverificatie worden hieronder weergegeven. router A en router B bevinden zich in IS-IS gebied 49.1234; router C bevindt zich in IS-IS-gebied 49.5678; en router D bevindt zich in gebied 49.999. Alle routers bevinden zich in hetzelfde IS-IS-domein (49) en zijn geconfigureerd met het domeinwachtwoord "Beveiliging".




### 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
```

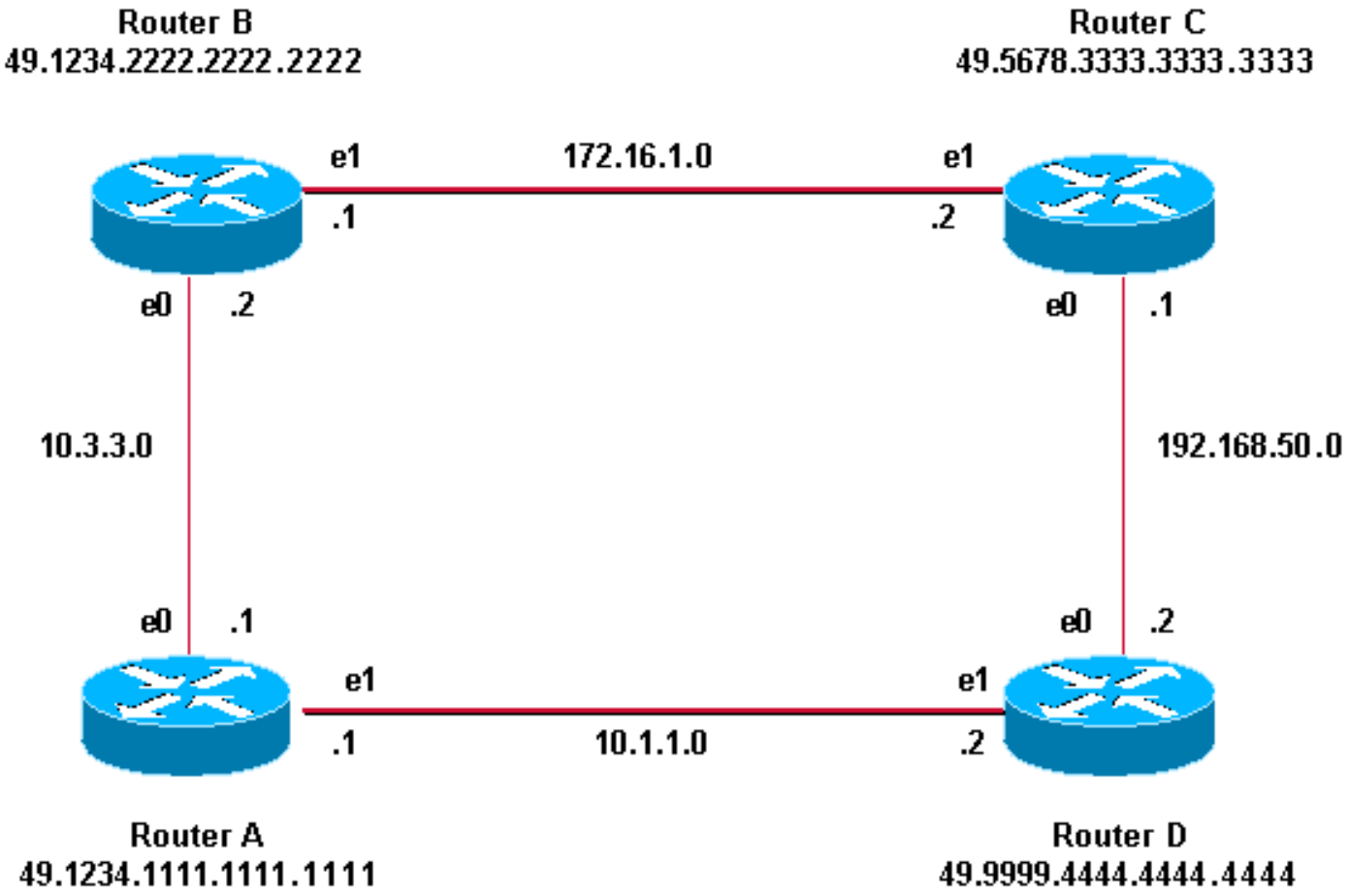
### router D

```
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
```

## Domain, Area and Interface-verificatie combineren

De topologie en gedeeltelijke configuraties in deze sectie illustreren een combinatie van domein, gebied, en interface authenticatie. router A en router B bevinden zich in hetzelfde gebied en zijn ingesteld met het gebiedswachtwoord "tiGHter." De router C en router D behoren tot twee

verschillende gebieden dan router A en router B. Alle routers zijn binnen hetzelfde domein en delen het wachtwoord op domeinniveau "Beveiliging". De router B en de router C hebben een interfaceconfiguratie voor de Ethernet verbinding tussen hen. Router C en router D formulier slechts L2 nabijheid met hun buren en het configureren van gebiedswachtwoord is niet vereist.




### 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
ip address 192.168.50.1 255.255.255.0
ip router isis
```

### 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
```

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

```
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

# Verifiëren

Bepaalde opdrachten worden ondersteund door de Cisco CLI Analyzer (alleen geregistreerde klanten), waardoor u een analyse van de **show**-opdrachtoutput kunt bekijken.

Om te verifiëren of de interfaceverificatie goed werkt, gebruik de opdracht **show clns buren** in de gebruiker EXEC of bevoorrechte EXEC modus. De uitvoer van de opdracht toont het nabijheidstype en de staat van de verbinding. Deze steekproefuitvoer van het bevel van de **show clans buren** toont een router correct gevormd voor interface authenticatie en toont de staat zoals UP:

```
RouterA# show clns neighbors

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

Voor Area and Domain Authenticatie kan de verificatie van authenticatie worden uitgevoerd met debug opdrachten zoals uitgelegd in de volgende sectie.

# Problemen oplossen

Als direct aangesloten routers Verificatie op één kant van een link hebben ingesteld en niet op de andere, vormen de routers geen CLNS IS-IS nabijheid. In de output hieronder, wordt router B gevormd voor interface-authenticatie op zijn Ethernet 0 interface, en router A wordt niet gevormd met authenticatie op zijn aangrenzende interface.

```
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
```

Als direct aangesloten routers gebied-authenticatie ingesteld hebben aan één kant van een link, wordt de CLNS IS-IS nabijheid gevormd tussen de twee routes. Maar de router waarop gebied-authenticatie is ingesteld, accepteert L1 LSPs niet vanuit de CLNS buurman zonder dat er een gebied-verificatie is ingesteld. Echter, de buurman zonder gebied-authenticatie blijft zowel L1 als L2 LSPs accepteren.

Dit is het debug-bericht op router A waar gebiedsverificatie is ingesteld en L1 LSP van een buurman (router B) zonder gebiedsverificatie wordt ontvangen:

```
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#
```

Als u domeinauthenticatie op één router configureren, verwerpt het L2 LSPs van routers die geen domeinverificatie hebben geconfigureerd. Routers die geen authenticatie hebben ingesteld aanvaarden de LSP's van de router die geen verificatie heeft ingesteld.

De debug uitvoer hieronder toont LSP-authenticatiefouten. De router CA is ingesteld voor gebied- of domeinverificatie en ontvangt Level 2 LSP's van een router (routerDB) die niet is ingesteld voor domein- of wachtwoordverificatie.

```
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
```

## Gerelateerde informatie

- Ondersteuningspagina voor IP-routing
- Technische ondersteuning en documentatie – Cisco Systems