Konfigurieren der IS-IS-Authentifizierung

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Schnittstellenauthentifizierung
Bereichsauthentifizierung
Domänenauthentifizierung
Kombinieren der Domänen-, Bereichs- und Schnittstellenauthentifizierung
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

Es empfiehlt sich, die Authentifizierung für Routing-Protokolle zu konfigurieren, um die Einfügung schädlicher Informationen in die Routing-Tabelle zu verhindern. Dieses Dokument veranschaulicht die Klartext-Authentifizierung zwischen Routern, auf denen IS-IS (Intermediate System-to-Intermediate System) für IP ausgeführt wird.

Dieses Dokument behandelt nur die IS-IS Clear Text Authentication. Weitere Informationen zu den anderen Arten der IS-IS-Authentifizierung finden Sie unter Erhöhte Sicherheit in einem IS-IS-Netzwerk.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten mit dem IS-IS-Betrieb und der IS-Konfiguration vertraut sein.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt. Die Konfiguration in diesem Dokument wurde auf Cisco Routern der Serie 2500 mit Cisco IOS Version 12.2(24a) getestet.

Hintergrundinformationen

IS-IS ermöglicht die Konfiguration eines Kennworts für eine angegebene Verbindung, einen Bereich oder eine Domäne. Router, die Nachbarn werden möchten, müssen dasselbe Kennwort für die konfigurierte Authentifizierungsstufe austauschen. Ein Router, der nicht im Besitz des entsprechenden Kennworts ist, darf nicht an der entsprechenden Funktion teilnehmen (d. h. er darf keine Verbindung initialisieren, Mitglied eines Bereichs sein oder Mitglied einer Level-2-Domäne sein).

Die Cisco IOS® Software ermöglicht die Konfiguration von drei Arten der IS-IS-Authentifizierung.

- **IS-IS-Authentifizierung** - Lange Zeit war dies die einzige Möglichkeit, die Authentifizierung für IS-IS zu konfigurieren.
- **IS-IS HMAC-MD5-Authentifizierung** - Mit dieser Funktion wird jeder IS-IS-Protokolldateneinheit (PDU) ein HMAC-MD5-Digest hinzugefügt. Sie wurde in der Cisco IOS-Softwareversion 12.2(13)T eingeführt und wird nur auf Plattformen mit einer begrenzten Anzahl unterstützt.
- **Enhanced Clear Text Authentication** - Mit dieser neuen Funktion kann die Klartext-Authentifizierung mithilfe neuer Befehle konfiguriert werden, mit denen Kennwörter verschlüsselt werden können, wenn die Softwarekonfiguration angezeigt wird. Außerdem wird die Verwaltung und Änderung von Passwörtern vereinfacht.

Hinweis: Informationen zur ISIS MD-5- und zur erweiterten Klartextauthentifizierung finden Sie unter Erhöhte Sicherheit in einem IS-IS-Netzwerk.

Das IS-IS-Protokoll, wie in RFC 1142 festgelegt, ermöglicht die Authentifizierung von Hellos und Link State Packets (LSPs) durch die Aufnahme von Authentifizierungsinformationen als Teil des LSP. Diese Authentifizierungsinformationen werden als TLV-Triple (Type Length Value) codiert. Der Authentifizierungstyp TLV ist 10. die Länge der TLV variabel ist; und der Wert der TLV hängt vom verwendeten Authentifizierungstyp ab. Standardmäßig ist die Authentifizierung deaktiviert.

Konfigurieren

In diesem Abschnitt wird erläutert, wie die IS-IS-Klartext-Authentifizierung für einen Link, für einen Bereich und für eine Domäne konfiguriert wird.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie die Best Practices zum Durchsuchen von Befehlen (nur registrierte Kunden).

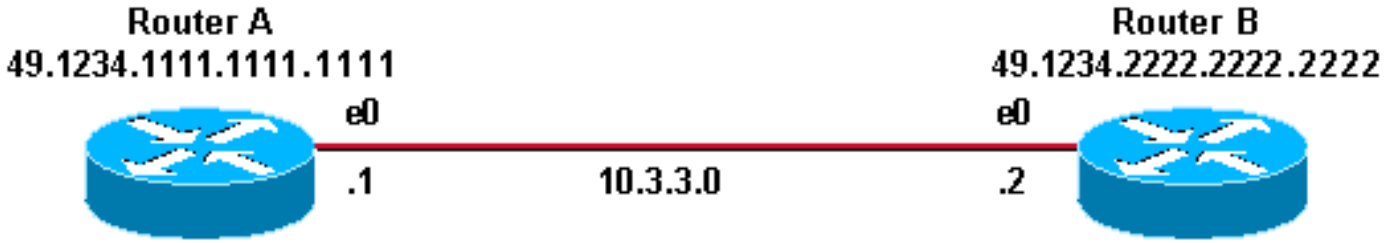
Schnittstellenauthentifizierung

Wenn Sie die IS-IS-Authentifizierung auf einer Schnittstelle konfigurieren, können Sie das Kennwort für Level 1-, Level 2- oder Level 1-/Level 2-Routing aktivieren. Wenn Sie keine Ebene angeben, ist die Standardeinstellung Level 1 und Level 2. Je nach Ebene, für die die Authentifizierung konfiguriert ist, wird das Kennwort in den entsprechenden Hello-Nachrichten übertragen. Die Ebene der IS-IS-Schnittstellenauthentifizierung sollte den Adjacency-Typ auf der Schnittstelle verfolgen. Verwenden Sie den Befehl **show clns neighbor**, um den Adjacency-Typ zu ermitteln. Für die Gebiets- und Domänenauthentifizierung können Sie die Ebene nicht angeben.

Das Netzwerkdiagramm und die Konfigurationen für die Schnittstellenauthentifizierung auf Router A, Ethernet 0 und Router B, Ethernet 0 sind nachfolgend aufgeführt. Router A und Router B sind beide mit dem ISIS-Kennwort SECr3t für Stufe 1 und Stufe 2 konfiguriert. Bei diesen Kennwörtern

wird die Groß- und Kleinschreibung beachtet.

Auf Cisco Routern, die mit dem Connectionless Network Service (CLNS) IS-IS konfiguriert sind, ist die CLNS-Adjacency zwischen ihnen standardmäßig Level 1/Level 2. Router A und Router B verfügen also über beide Adjacency-Typen, sofern sie nicht speziell für die Stufe 1 oder 2 konfiguriert wurden.



Router A

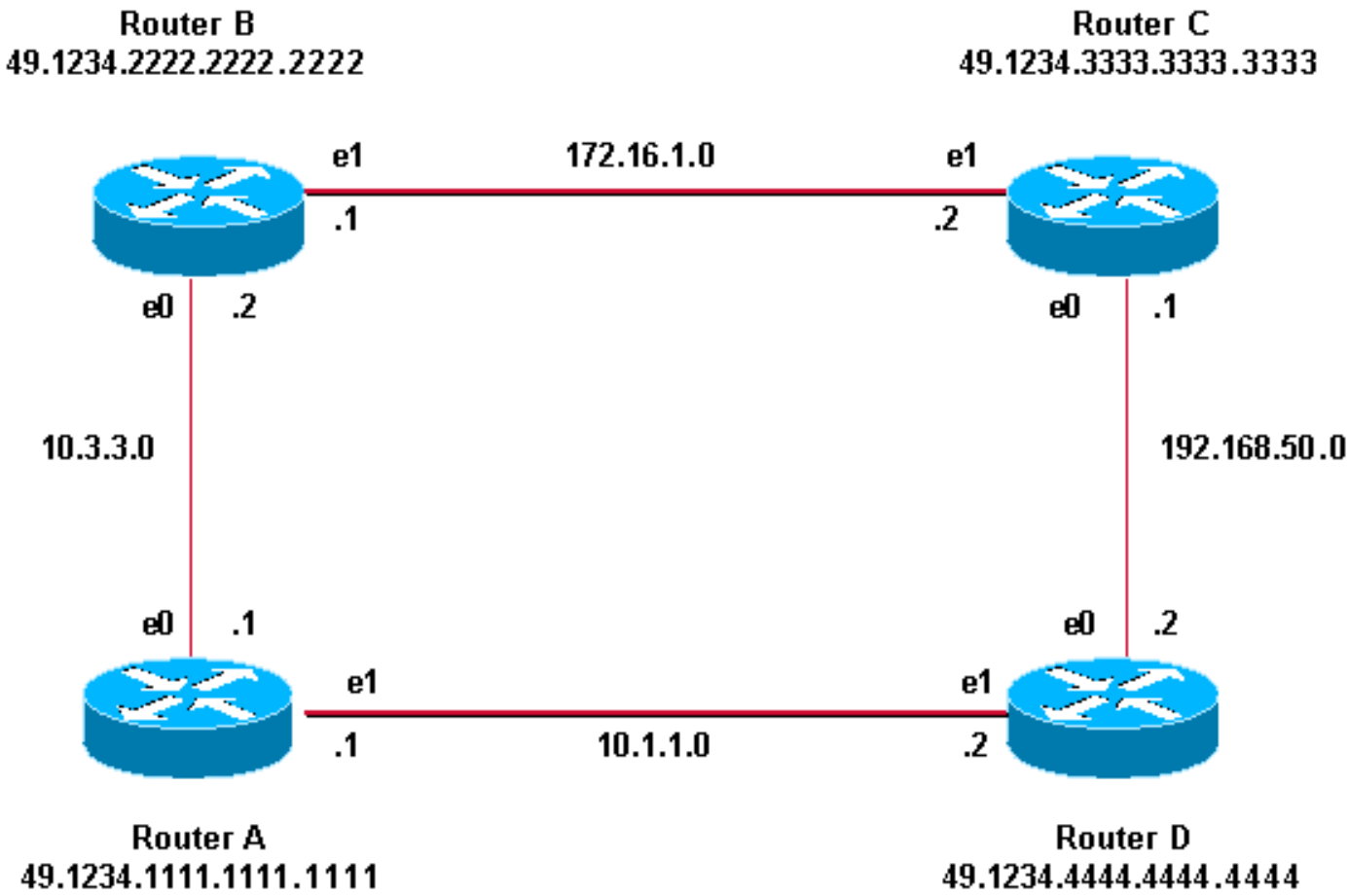
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

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
```

Bereichsauthentifizierung

Das Netzwerkdiagramm und die Konfigurationen für die Bereichsauthentifizierung sind unten aufgeführt. Wenn die Bereichsauthentifizierung konfiguriert ist, wird das Kennwort in den L1-LSPs, CSNPs und PSNPS übertragen. Alle Router befinden sich im gleichen IS-IS-Bereich (49.1234) und sind mit dem Area Password "tiGHter" konfiguriert.



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
```

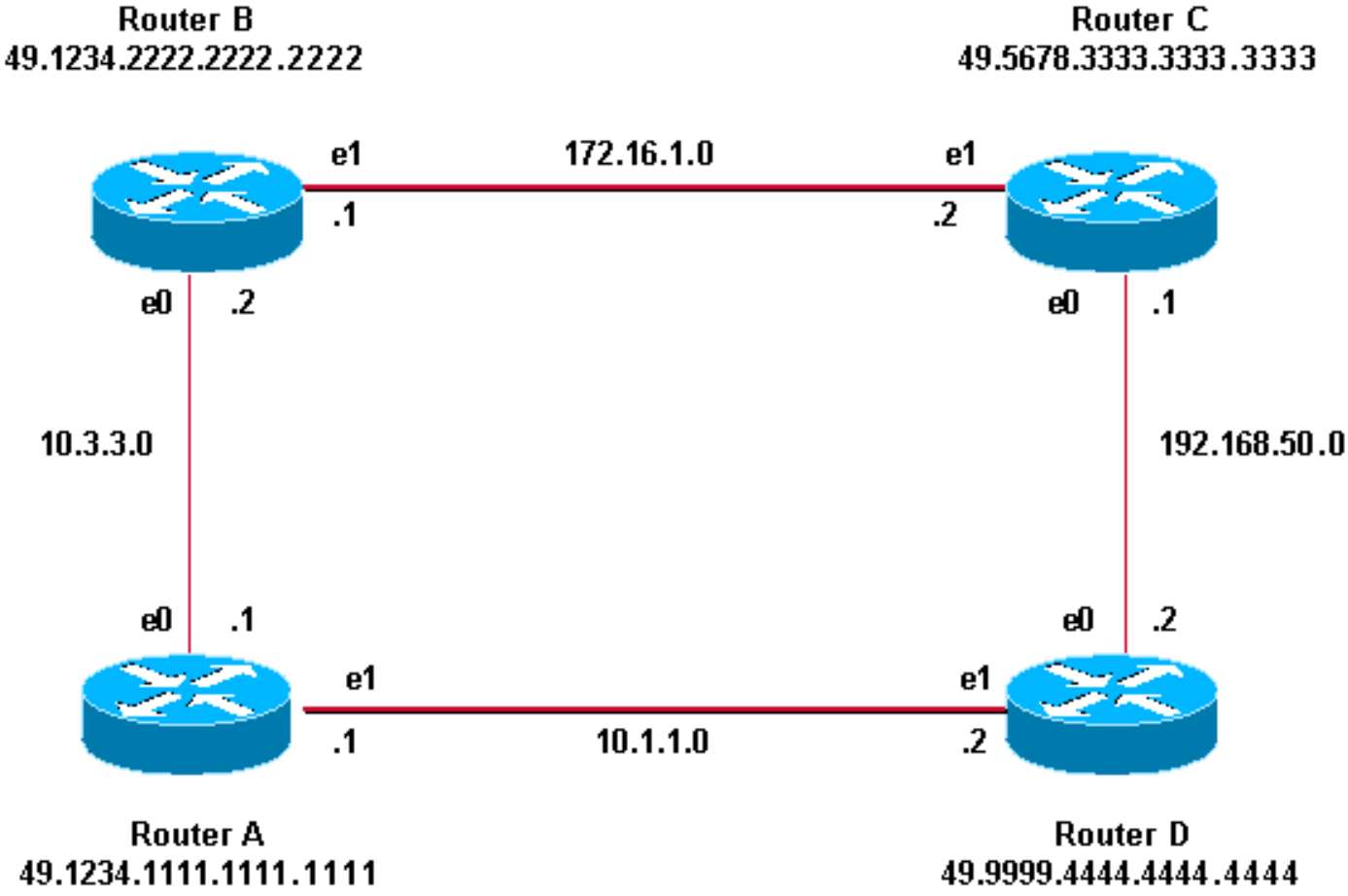
Router D

```
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
```

Domänenauthentifizierung

Das Netzwerkdiagramm und die Konfigurationen für die Domänenauthentifizierung sind unten aufgeführt. Router A und Router B befinden sich im IS-IS-Bereich 49.1234; Router C befindet sich im IS-IS-Bereich 49.5678; und Router D befindet sich im Bereich 49.999. Alle Router befinden sich

in derselben IS-IS-Domäne (49) und sind mit dem Domänenkennwort "seSecurity" konfiguriert.



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
```

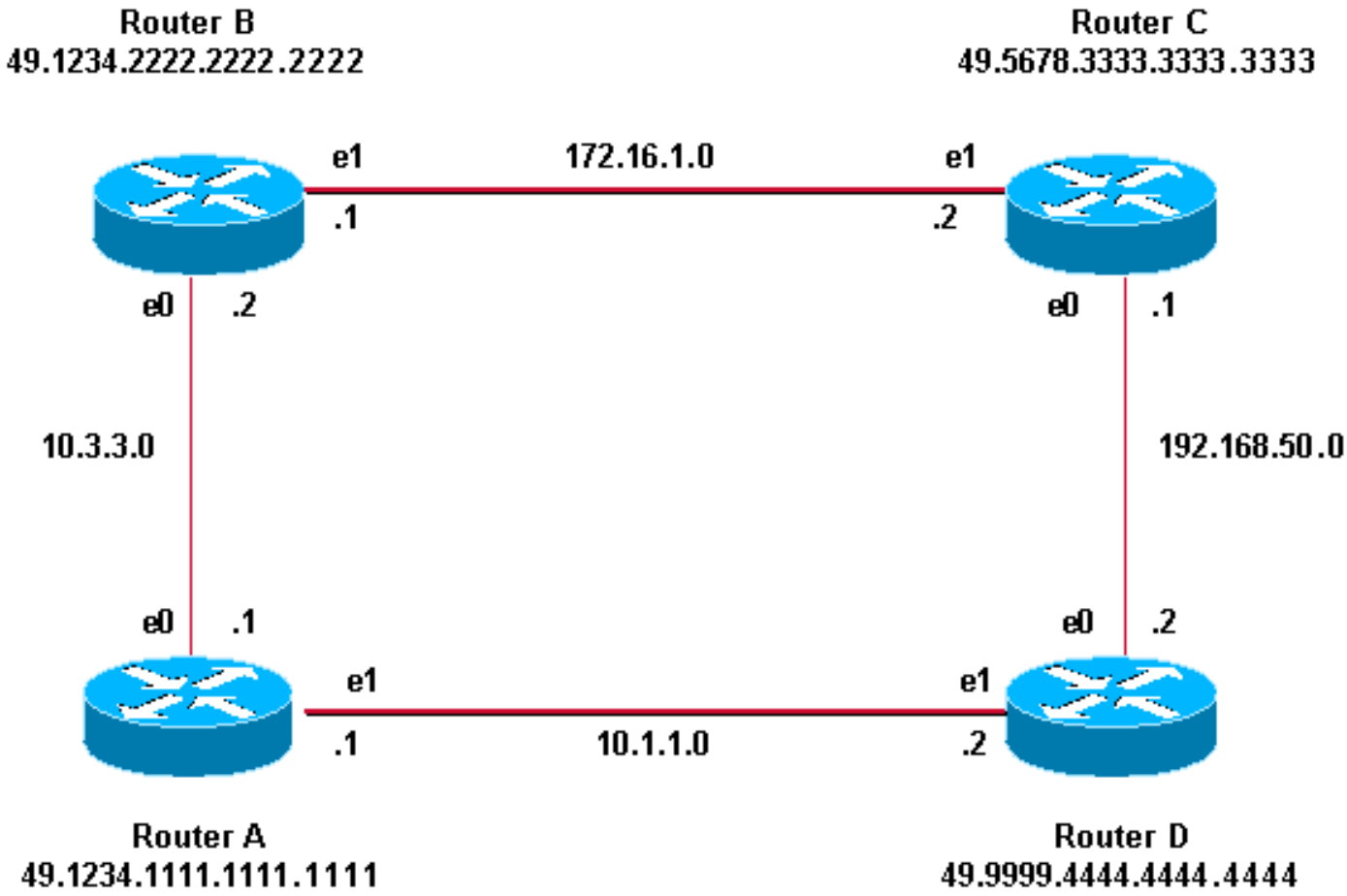
Router D

```
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
```

Kombinieren der Domänen-, Bereichs- und Schnittstellenauthentifizierung

Die Topologie und Teilkonfigurationen in diesem Abschnitt veranschaulichen eine Kombination

aus Domänen-, Bereich- und Schnittstellenauthentifizierung. Router A und Router B befinden sich im gleichen Bereich und werden mit dem Bereichskennwort "tiGHter" konfiguriert. Router C und Router D gehören zu zwei unterschiedlichen Bereichen als Router A und Router B. Alle Router befinden sich in derselben Domäne und verwenden das Kennwort "seSecurity" auf Domänenebene. Router B und Router C verfügen über eine Schnittstellenkonfiguration für die Ethernet-Verbindung zwischen ihnen. Router C und Router D bilden nur L2-Adjacencies mit Nachbarn, und das Konfigurieren des Area-Passworts ist nicht erforderlich.



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
```

Router 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
```

Überprüfen

Bestimmte **show**-Befehle werden vom Cisco CLI Analyzer (nur registrierte Kunden) unterstützt, mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Um zu überprüfen, ob die Schnittstellenauthentifizierung ordnungsgemäß funktioniert, verwenden Sie den Befehl **show clns neighbors** im Benutzer-EXEC- oder privilegierten EXEC-Modus. In der Ausgabe des Befehls werden der Adjacency-Typ und der Status der Verbindung angezeigt. Diese Beispielausgabe des Befehls **show clns neighbors** zeigt einen Router an, der korrekt für die Schnittstellenauthentifizierung konfiguriert wurde, und zeigt den Status als UP an:

```
RouterA# show clns neighbors

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

Für die Area- und Domänen-Authentifizierung kann die Authentifizierung mithilfe von Debugbefehlen überprüft werden, wie im nächsten Abschnitt erläutert.

Fehlerbehebung

Wenn auf einer Seite einer Verbindung und nicht auf der anderen Seite auf direkt verbundenen Routern eine Authentifizierung konfiguriert ist, bilden die Router keine CLNS IS-IS-Adjacency. In der unten stehenden Ausgabe wird Router B für die Schnittstellenauthentifizierung auf seiner Ethernet 0-Schnittstelle konfiguriert, Router A ist auf seiner angrenzenden Schnittstelle nicht mit Authentifizierung konfiguriert.

```
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
```

Wenn auf einer Seite einer Verbindung für direkt verbundene Router eine Bereichsauthentifizierung konfiguriert ist, wird zwischen den beiden Routen eine CLNS IS-IS-Adjacency gebildet. Der Router, auf dem die Bereichsauthentifizierung konfiguriert ist, akzeptiert jedoch keine L1-LSPs des CLNS-Nachbarn, für die keine Bereichsauthentifizierung konfiguriert wurde. Der Nachbar ohne Bereichsauthentifizierung akzeptiert jedoch weiterhin L1- und L2-LSPs.

Dies ist die Debug-Meldung auf Router A, wo die Bereichsauthentifizierung konfiguriert ist und L1 LSP von einem Nachbarn (Router B) ohne Bereichsauthentifizierung empfängt:

```
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#
```

Wenn Sie die Domänenauthentifizierung auf einem Router konfigurieren, werden die L2-LSPs von Routern abgelehnt, für die keine Domänenauthentifizierung konfiguriert wurde. Router, für die keine Authentifizierung konfiguriert ist, akzeptieren die LSPs des Routers, für den die Authentifizierung konfiguriert ist.

Die folgende Debug-Ausgabe zeigt LSP-Authentifizierungsfehler. Die Router-CA ist für die Area- oder Domänen-Authentifizierung konfiguriert und empfängt Level-2-LSPs von einem Router (Router DB), der nicht für die Domänen- oder Kennwortauthentifizierung konfiguriert ist.

```
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
```

Zugehörige Informationen

- Support-Seite für IP-Routing
- Technischer Support und Dokumentation - Cisco Systems