IS-IS 인증 구성

목차

소개

라우팅 테이블에 악성 정보가 유입되는 것을 방지하기 위해 라우팅 프로토콜에 대한 인증을 구성할 수 없습니다. 이 문서에서는 IP용 IS-IS(Intermediate System-to-Intermediate System)를 실행하는 라우터 간에 일반 텍스트 인증을 보여 줍니다.

이 문서에서는 IS-IS 일반 텍스트 인증만 다룹니다. 다른 유형의 IS-IS 인증에 대한 자세한 내용은 IS-IS 네트워크에서 보안 향상을 참조하십시오.

사전 요구 사항

요구 사항

이 문서의 독자는 IS-IS 작업 및 구성에 익숙해야 합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. 이 문서의 컨피그레이션은 Cisco IOS 버전 12.2(24a)를 실행하는 Cisco 2500 Series 라우터에서 테스트되었습니다.

배경 정보

IS-IS는 지정된 링크, 영역 또는 도메인에 대한 비밀번호를 구성할 수 있습니다. 인접 디바이스가 되려는 라우터는 구성된 인증 레벨에 대해 동일한 비밀번호를 교환해야 합니다. 적절한 비밀번호를

보유하지 않은 라우터는 해당 기능에 참여할 수 없습니다. 즉, 링크를 초기화할 수 없거나, 영역의 구성원이 될 수 없으며, 각각 레벨 2 도메인의 구성원이 될 수 없습니다.

Cisco IOS® 소프트웨어는 세 가지 유형의 IS-IS 인증을 구성할 수 있습니다.

- **IS-IS 인증** - 오랫동안 IS-IS에 대한 인증을 구성하는 유일한 방법입니다.
- **IS-IS HMAC-MD5 인증** - 이 기능은 각 IS-IS PDU(Protocol Data Unit)에 HMAC-MD5 다이제스트를 추가합니다. Cisco IOS 소프트웨어 버전 12.2(13)T에서 소개되었으며 제한된 수의 플랫폼에서만 지원됩니다.
- **향상된 일반 텍스트 인증** - 이 새로운 기능을 사용하면 소프트웨어 컨피그레이션이 표시될 때 비밀번호를 암호화할 수 있는 새 명령을 사용하여 일반 텍스트 인증을 구성할 수 있습니다. 또한 비밀번호를 쉽게 관리하고 변경할 수 있습니다.

참고: ISIS MD-5 및 향상된 일반 텍스트 인증에 대한 자세한 내용은 IS-IS 네트워크의 보안 향상을 참조하십시오.

RFC 1142에 지정된 대로 IS-IS 프로토콜은 LSP의 일부로 인증 정보를 포함시켜 Hello 및 LSP(Link State Packets)의 인증을 제공합니다. 이 인증 정보는 TLV(Type Length Value) 3으로 인코딩됩니다. 인증 TLV의 유형은 10입니다. TLV의 길이는 변수입니다. TLV의 값은 사용 중인 인증 유형에 따라 달라집니다. 기본적으로 인증은 비활성화되어 있습니다.

구성

이 섹션에서는 링크, 영역 및 도메인에 대해 IS-IS 일반 텍스트 인증을 구성하는 방법에 대해 설명합니다.

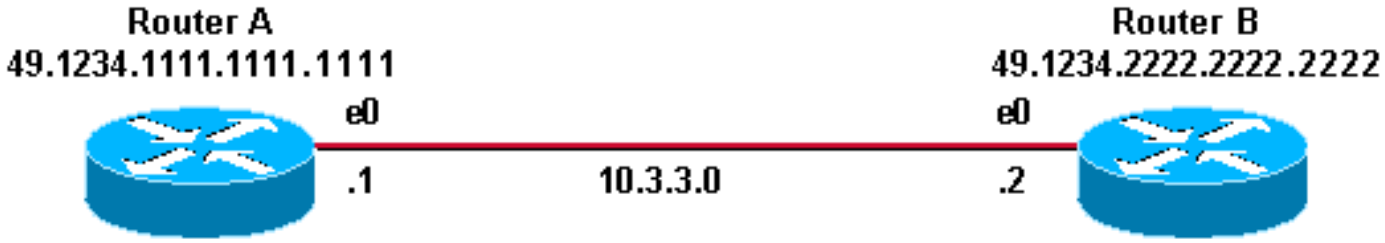
참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 검색 모범 사례(등록된 고객만 해당)를 사용합니다.

인터페이스 인증

인터페이스에서 IS-IS 인증을 구성할 때 레벨 1, 레벨 2 또는 레벨 1/레벨 2 라우팅에 대한 비밀번호를 활성화할 수 있습니다. 레벨을 지정하지 않을 경우 기본값은 레벨 1 및 레벨 2입니다. 인증이 구성된 레벨에 따라 해당 Hello 메시지에 비밀번호가 전달됩니다. IS-IS 인터페이스 인증 레벨은 인터페이스에서 인접성의 유형을 추적해야 합니다. show clns neighbor 명령을 사용하여 인접성의 유형을 확인합니다. 영역 및 도메인 인증의 경우 레벨을 지정할 수 없습니다.

라우터 A, 이더넷 0 및 라우터 B, 이더넷 0에서 인터페이스 인증을 위한 네트워크 다이어그램 및 컨피그레이션이 아래에 나와 있습니다. 라우터 A와 라우터 B는 모두 레벨 1 및 레벨 2에 대해 isis 비밀번호 SECr3t로 구성됩니다. 이러한 비밀번호는 대/소문자를 구분합니다.

CLNS(연결 없는 네트워크 서비스) IS-IS로 구성된 Cisco 라우터에서 CLNS 인접성은 기본적으로 레벨 1/레벨 2입니다. 따라서 Level 1 또는 Level 2에 대해 특별히 구성하지 않는 한 라우터 A와 라우터 B는 두 가지 인접성 유형을 모두 가집니다.



라우터 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
```

라우터 B

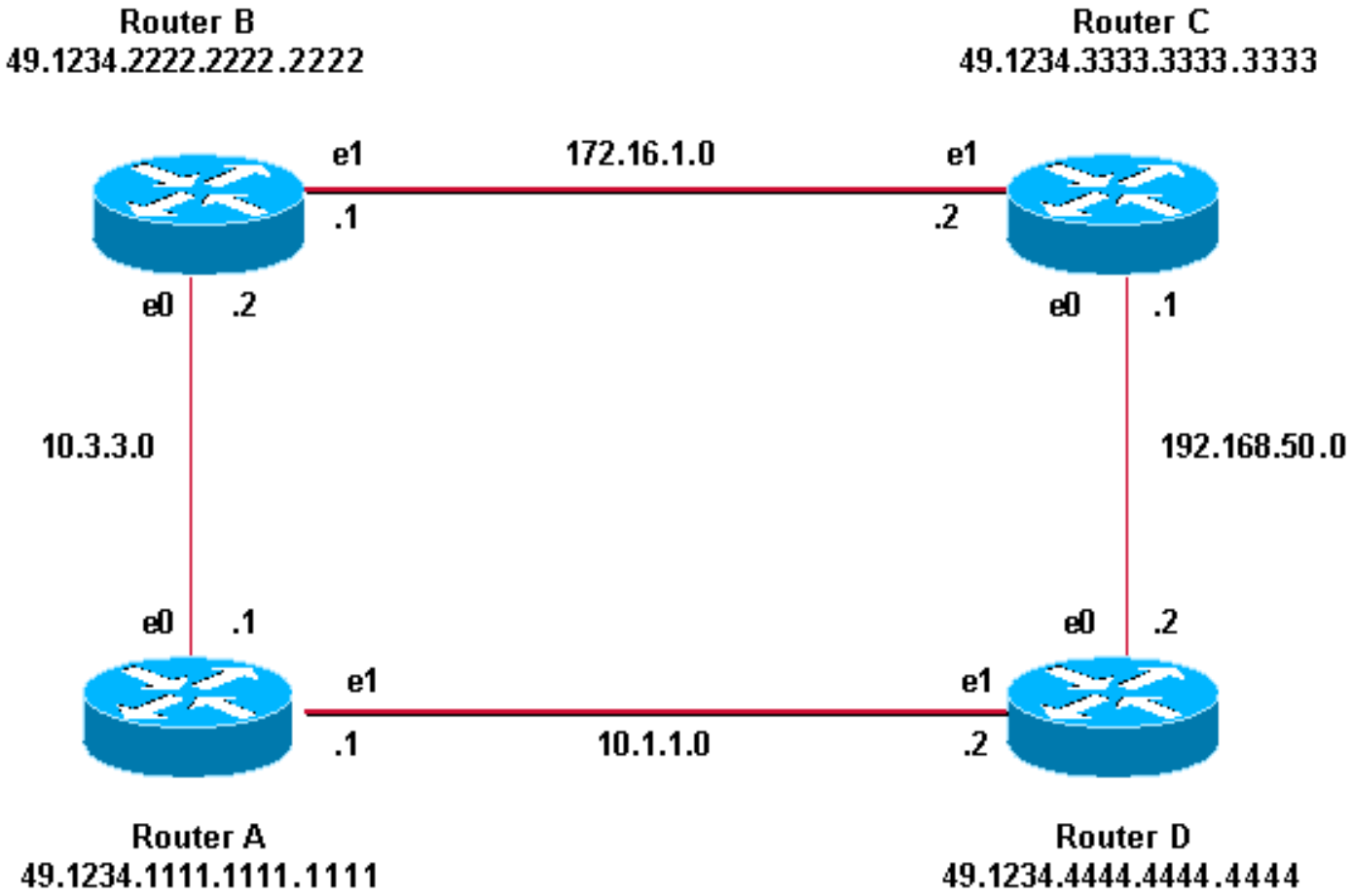
```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

영역 인증

다음은 영역 인증을 위한 네트워크 다이어그램 및 컨피그레이션입니다. 영역 인증이 구성되면 L1 LSP, CSNP 및 PSNPS에서 비밀번호가 전달됩니다. 모든 라우터는 동일한 IS-IS 영역인 49.1234에 있으며 모두 영역 비밀번호 "tiGHter"로 구성됩니다.



라우터 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
```

라우터 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
```

라우터 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
```

```
area-password tiGHter
```

라우터 D

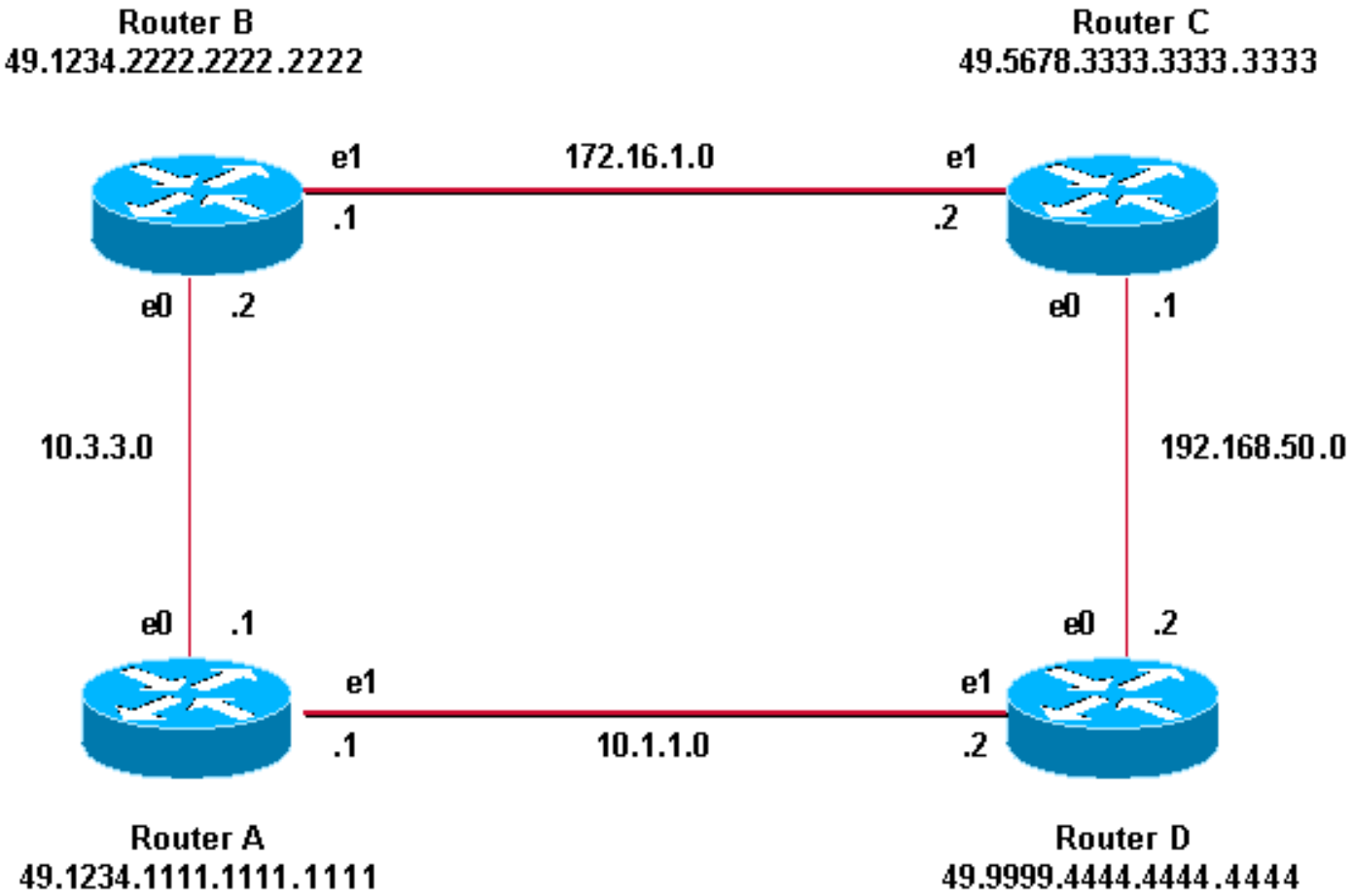
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

도메인 인증

도메인 인증에 대한 네트워크 다이어그램 및 컨피그레이션이 아래에 나와 있습니다. 라우터 A와 라우터 B는 IS-IS 영역 49.1234에 있습니다. 라우터 C는 IS-IS 영역 49.5678에 있습니다. 라우터 D는 49.9999 영역입니다. 모든 라우터는 동일한 IS-IS 도메인(49)에 있으며 도메인 비밀번호 "seCurity"로 구성됩니다.



라우터 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
```

라우터 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 49.1234.1111.1111.1111.00
domain-password seCurity
```

라우터 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 isis
net 49.1234.2222.2222.2222.00
domain-password seCurity
```

라우터 D

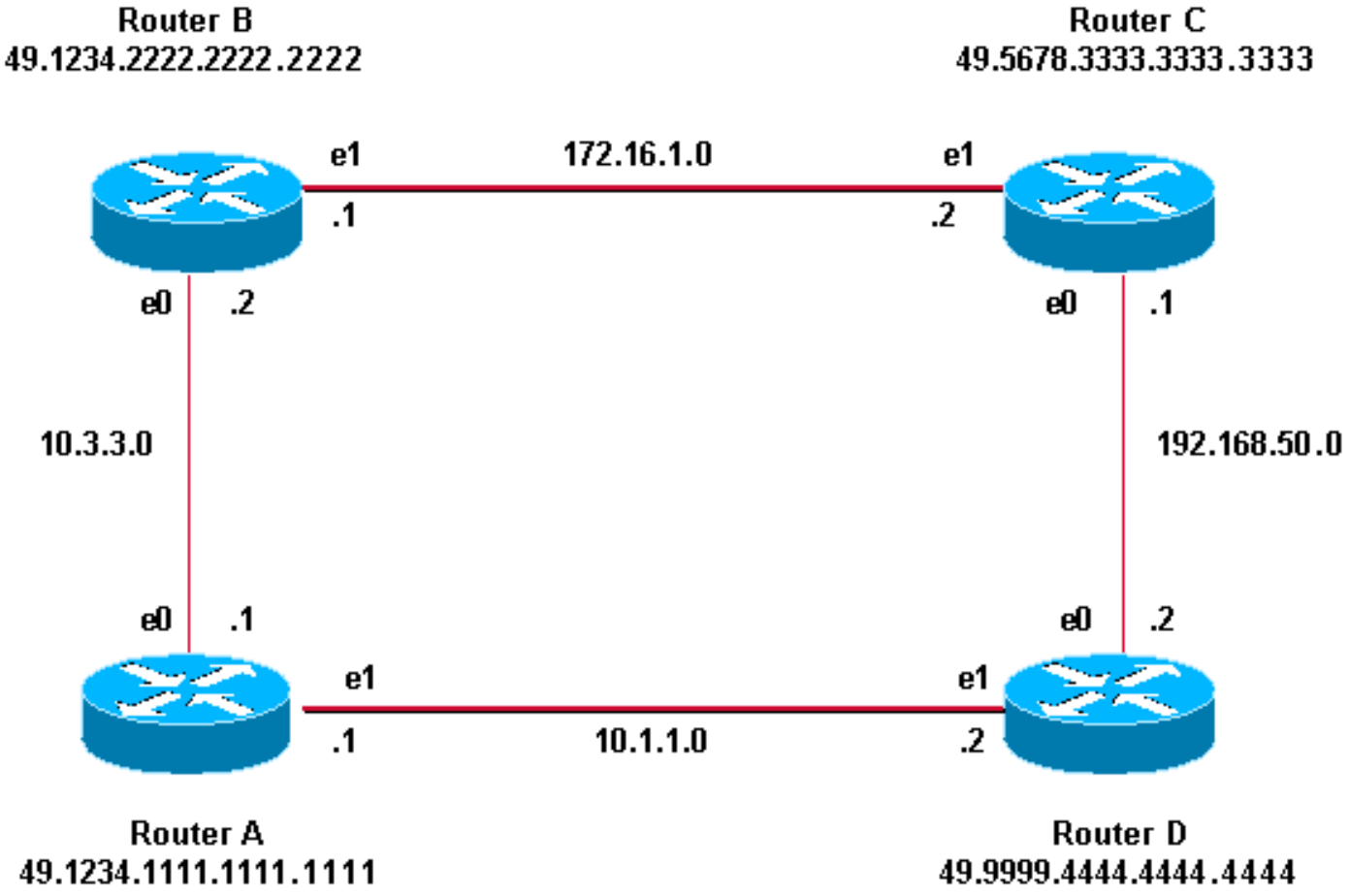
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

도메인, 영역 및 인터페이스 인증 결합

이 섹션의 토폴로지 및 부분 구성은 도메인, 영역 및 인터페이스 인증의 조합을 보여줍니다. 라우터 A와 라우터 B는 같은 영역에 있으며 영역 비밀번호 "tiGHter"로 구성됩니다. 라우터 C와 라우터 D는 라우터 A와 라우터 B가 아닌 두 가지 영역에 속합니다. 모든 라우터는 동일한 도메인에 있으며 도메인 레벨 비밀번호 "seCurity"를 공유합니다. 라우터 B와 라우터 C는 그 사이의 이더넷 링크에 대한 인터페이스 컨피그레이션을 가집니다. 라우터 C 및 라우터 D는 인접 디바이스가 있는 L2 인접성만 형성하며 영역 비밀번호를 구성할 필요가 없습니다.



라우터 A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
```

라우터 B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
```

```
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
```

라우터 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 isis
net 49.5678.3333.3333.3333.00
domain-password seCurity
```

```
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
```

라우터 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
```

다음을 확인합니다.

특정 **show** 명령은 Cisco CLI Analyzer(등록된 고객만 해당)에서 지원되므로 **show** 명령 출력의 분석을 볼 수 있습니다.

인터페이스 인증이 제대로 작동하는지 확인하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show clns neighbors** 명령을 사용합니다. 명령의 출력에는 연결의 인접성 유형 및 상태가 표시됩니다. show clns neighbors 명령의 이 샘플 출력은 인터페이스 인증을 위해 올바르게 구성된 라우터를 표시하고 상태를 UP로 표시합니다.

```
RouterA# show clns neighbors

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

영역 및 도메인 인증의 경우 다음 섹션에 설명된 대로 debug 명령을 사용하여 인증 확인을 수행할 수 있습니다.

문제 해결

직접 연결된 라우터가 링크의 한 쪽에 인증이 구성되어 있고 다른 쪽에 구성되어 있지 않은 경우 라우터는 CLNS IS-IS 인접성을 형성하지 않습니다. 아래 출력에서 라우터 B는 이더넷 0 인터페이스에서 인터페이스 인증을 위해 구성되고 라우터 A는 인접 인터페이스에서 인증으로 구성되지 않습니다.

```
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
```

직접 연결된 라우터에 링크 한 쪽에 영역 인증이 구성된 경우 두 경로 간에 CLNS IS-IS 인접성이 형성됩니다. 그러나 영역 인증이 구성된 라우터는 영역 인증이 구성되지 않은 CLNS 인접 디바이스의 L1 LSP를 허용하지 않습니다. 그러나 area-authentication이 없는 인접 디바이스는 L1 및 L2 LSP를 모두 계속 수락합니다.

영역 인증이 구성되고 영역 인증 없이 네이버(라우터 B)에서 L1 LSP를 수신하는 라우터 A의 디버그 메시지입니다.

```
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#
```

한 라우터에서 도메인 인증을 구성할 경우 도메인 인증이 구성되지 않은 라우터에서 L2 LSP를 거부합니다. 인증이 구성되지 않은 라우터는 인증이 구성된 라우터의 LSP를 수락합니다.

아래 디버그 출력에는 LSP 인증 실패가 표시됩니다. 라우터 CA는 영역 또는 도메인 인증을 위해 구성되었으며 도메인 또는 비밀번호 인증을 위해 구성되지 않은 라우터(라우터 DB)에서 레벨 2 LSP를 수신합니다.

```
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
```

관련 정보

- IP 라우팅 지원 페이지
- 기술 지원 및 문서 – Cisco Systems