Configurazione dell'autenticazione IS-IS

Sommario

Introduzione

Èpreferibile configurare l'autenticazione per i protocolli di routing al fine di impedire l'introduzione di informazioni dannose nella tabella di routing. In questo documento viene mostrata un'autenticazione in chiaro tra i router con protocollo IS-IS (Intermediate System-to-Intermediate System) per IP.

Questo documento copre solo l'autenticazione IS-IS Clear Text. Per ulteriori informazioni sugli altri tipi di autenticazione IS-IS, fare riferimento a Miglioramento della sicurezza in una rete IS-IS.

Prerequisiti

Requisiti

I lettori di questo documento devono conoscere il funzionamento e la configurazione di IS-IS.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. La configurazione descritta in questo documento è stata testata su router Cisco serie 2500 con Cisco IOS versione 12.2(24a)

Premesse

IS-IS consente di configurare una password per un collegamento, un'area o un dominio specificato. I router che vogliono diventare router adiacenti devono scambiarsi la stessa password per il livello di autenticazione configurato. Ai router che non dispongono della password appropriata non è consentito partecipare alla funzione corrispondente, ovvero non può inizializzare un collegamento, essere membro di un'area o essere membro di un dominio di livello 2, rispettivamente.

Il software Cisco IOS® consente di configurare tre tipi di autenticazione IS-IS.

- **Autenticazione IS-IS** - Per molto tempo, questo è stato l'unico modo per configurare l'autenticazione per IS-IS.
- **Autenticazione IS-IS HMAC-MD5** - Questa funzione aggiunge un digest HMAC-MD5 a ciascuna unità dati del protocollo (PDU) IS-IS. È stato introdotto nel software Cisco IOS versione 12.2(13)T ed è supportato solo su un numero limitato di piattaforme.
- **Autenticazione avanzata testo non crittografato**: questa nuova funzionalità consente di configurare l'autenticazione del testo non crittografato utilizzando nuovi comandi che consentono di crittografare le password quando viene visualizzata la configurazione software. Semplifica inoltre la gestione e la modifica delle password.

Nota: per informazioni su ISIS MD-5 e Autenticazione avanzata testo non crittografato, fare riferimento a Miglioramento della sicurezza in una rete IS-IS.

Il protocollo IS-IS, come specificato nella RFC 1142, prevede l'autenticazione degli Hellos e dei pacchetti dello stato del collegamento (LSP) tramite l'inclusione di informazioni di autenticazione come parte dell'LSP. Queste informazioni di autenticazione sono codificate come triplo TLV (Type Length Value). il tipo di TLV di autenticazione è 10; la lunghezza del TLV è variabile; e il valore del TLV dipende dal tipo di autenticazione utilizzato. Per impostazione predefinita, l'autenticazione è disabilitata.

Configurazione

In questa sezione viene descritto come configurare l'autenticazione in testo non crittografato IS-IS su un collegamento, per un'area e per un dominio.

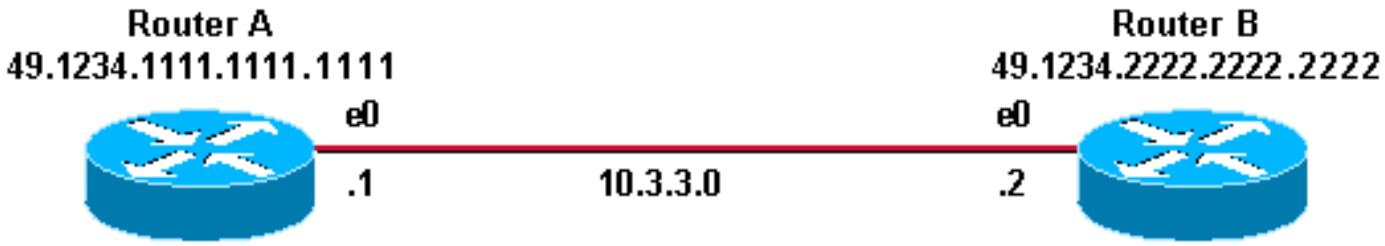
Nota: per ulteriori informazioni sui comandi menzionati in questo documento, consultare le procedure consigliate per la ricerca di comandi (solo utenti registrati).

Autenticazione interfaccia

Quando si configura l'autenticazione IS-IS su un'interfaccia, è possibile abilitare la password per il routing di livello 1, livello 2 o entrambi. Se non si specifica un livello, il valore predefinito è Livello 1 e Livello 2. A seconda del livello per il quale è configurata l'autenticazione, la password viene inserita nei messaggi Hello corrispondenti. Il livello di autenticazione dell'interfaccia IS-IS deve tenere traccia del tipo di adiacenza sull'interfaccia. Per individuare il tipo di adiacenza, utilizzare il comando **show clns neighbors**. Per l'autenticazione di area e dominio, non è possibile specificare il livello.

Di seguito sono riportati il diagramma di rete e le configurazioni per l'autenticazione dell'interfaccia sul router A, Ethernet 0 e il router B, Ethernet 0. Il router A e il router B sono entrambi configurati con la password isis SECr3t per i livelli 1 e 2. Queste password fanno distinzione tra maiuscole e minuscole.

Sui router Cisco configurati con il servizio di rete senza connessione (CLNS) IS-IS, l'adiacenza CLNS tra i due è per impostazione predefinita livello 1/livello 2. Pertanto, il router A e il router B avranno entrambi i tipi di adiacenza, a meno che non siano configurati specificamente per il livello 1 o il livello 2.



Router A

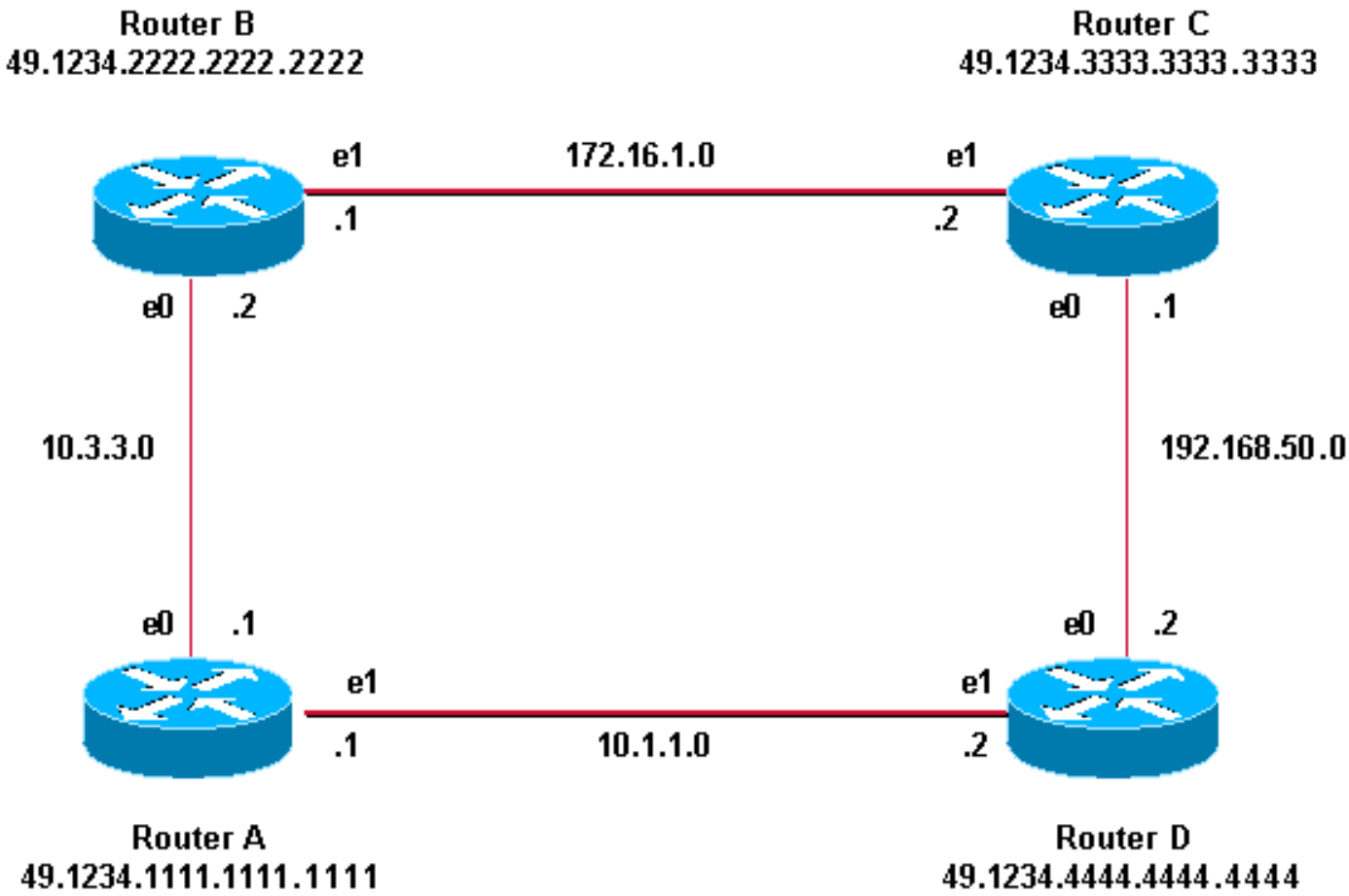
```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

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
```

Autenticazione area

Di seguito sono riportati il diagramma di rete e le configurazioni per l'autenticazione dell'area. Quando è configurata l'autenticazione di area, la password viene trasferita nei provider L1 LSP, CSNP e PSNP. Tutti i router si trovano nella stessa area IS-IS, la versione 49.1234, e sono tutti configurati con la password dell'area "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
```

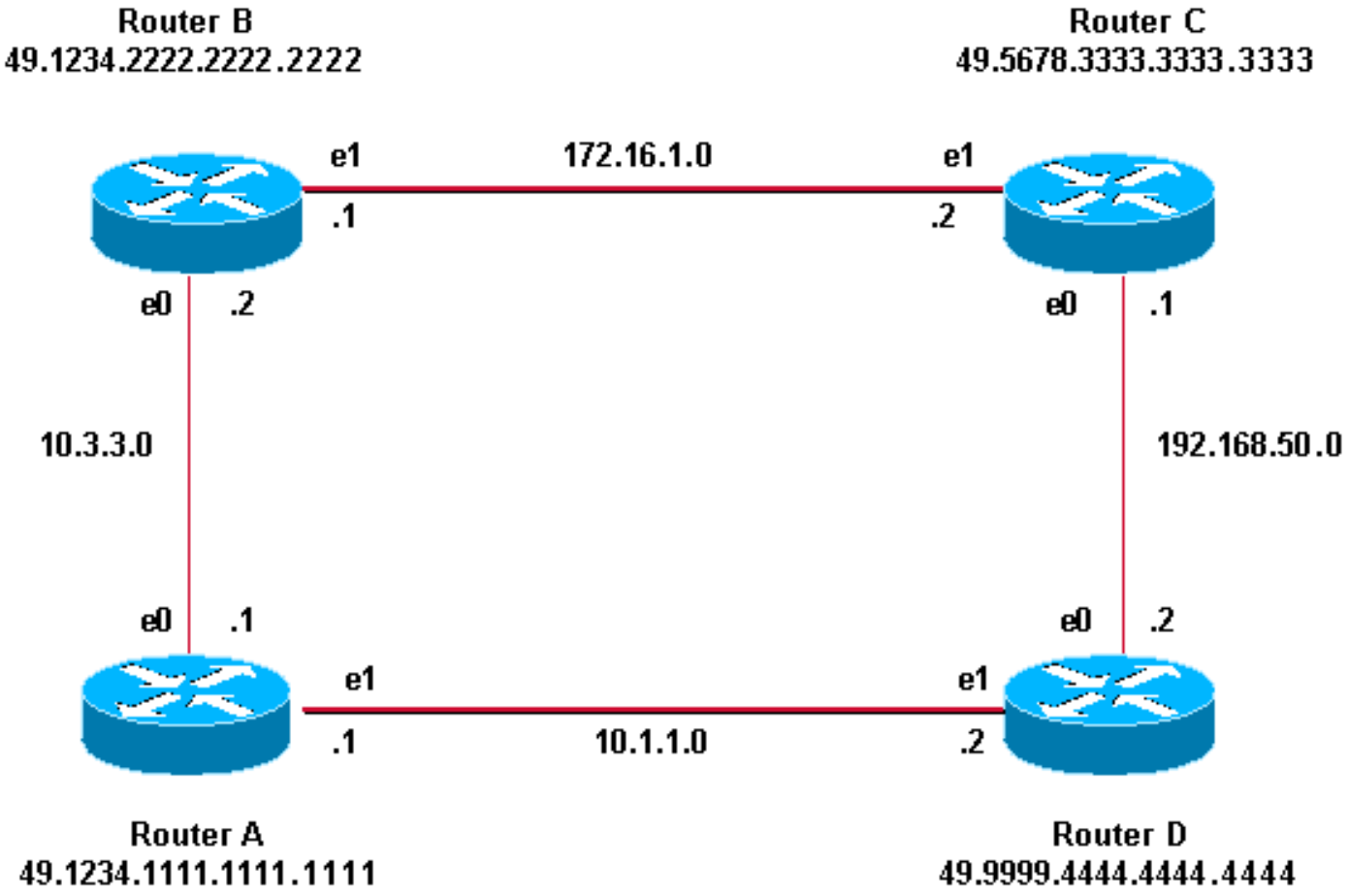
Router D

```
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
```

Autenticazione del dominio

Di seguito sono riportati il diagramma di rete e le configurazioni per l'autenticazione del dominio. Il router A e il router B si trovano nell'area IS-IS 49.1234; Il router C è nell'area IS-IS 49.5678; e il router D si trova nell'area 49.999. Tutti i router si trovano nello stesso dominio IS-IS (49) e sono

configurati con la password di dominio "seSecurity".



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
```

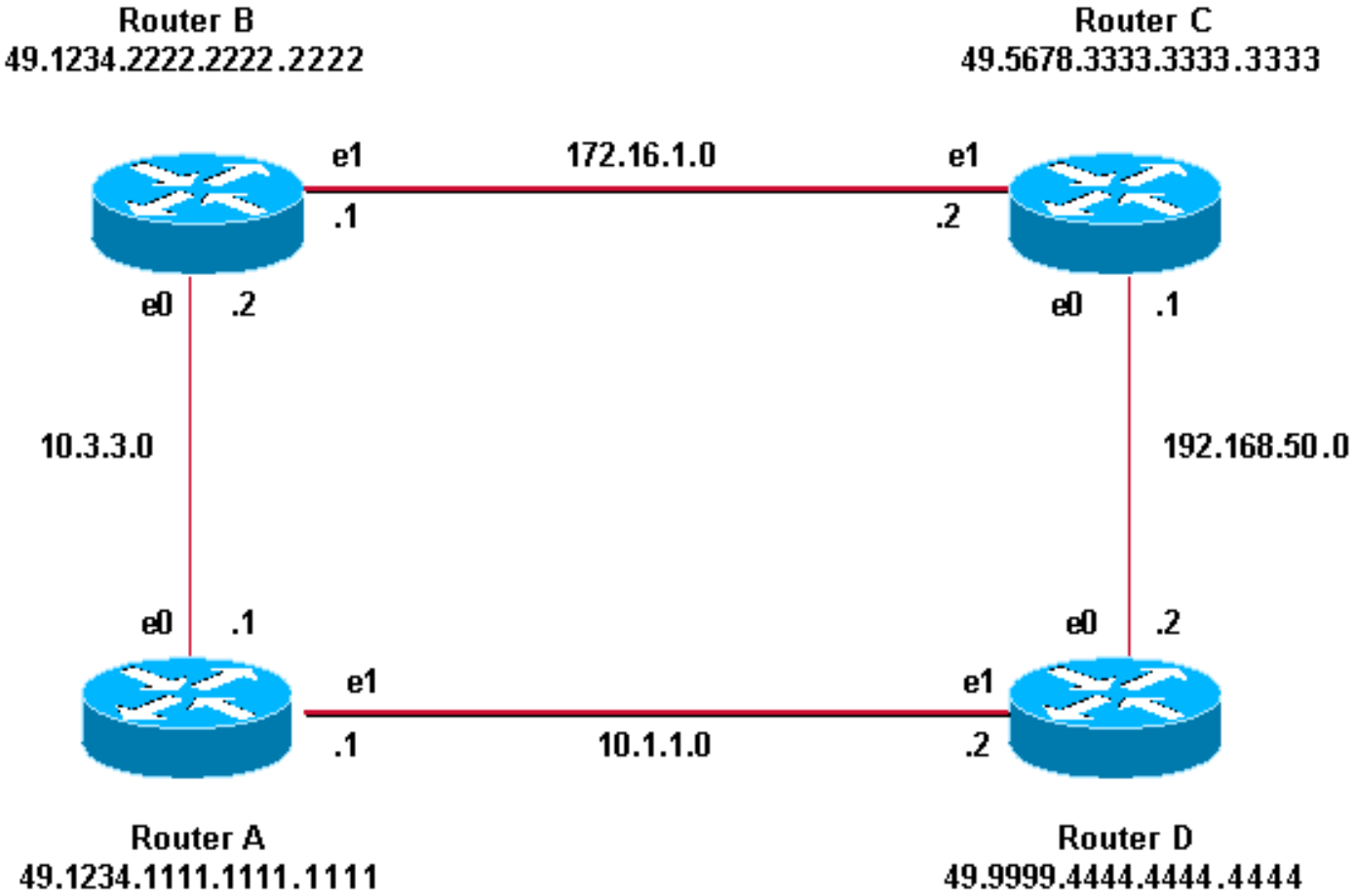
Router D

```
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
```

Combinazione di autenticazione di dominio, area e interfaccia

La topologia e le configurazioni parziali in questa sezione illustrano una combinazione di

autenticazione di dominio, area e interfaccia. Il router A e il router B si trovano nella stessa area e sono configurati con la password dell'area "tiGHter". Il router C e il router D appartengono a due aree diverse dal router A e dal router B. Tutti i router si trovano nello stesso dominio e condividono la password a livello di dominio "seSecurity". Il router B e il router C hanno una configurazione di interfaccia per il collegamento Ethernet che li collega. I router C e D formano solo adiacenze L2 con i router adiacenti e non è richiesta la configurazione della password dell'area.



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
```

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 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

router isis
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

Verifica

Alcuni comandi **show** sono supportati da Cisco CLI Analyzer (solo per i clienti registrati), che permette di visualizzare un'analisi dell'output dei comandi **show**.

Per verificare il corretto funzionamento dell'autenticazione dell'interfaccia, utilizzare il comando **show clns neighbors** in modalità di esecuzione utente o in modalità di esecuzione privilegiata. L'output del comando visualizza il tipo di adiacenza e lo stato della connessione. In questo output di esempio del comando **show clns neighbors** viene mostrato un router configurato correttamente per l'autenticazione dell'interfaccia e viene visualizzato lo stato UP:

```
RouterA# show clns neighbors

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

Per l'autenticazione di area e dominio, è possibile eseguire la verifica dell'autenticazione utilizzando i comandi di debug, come descritto nella sezione successiva.

Risoluzione dei problemi

Se l'autenticazione dei router connessi direttamente è configurata su un lato del collegamento e non sull'altro, i router non formano un'adiacenza IS-IS CLNS. Nell'output seguente, il router B è configurato per l'autenticazione dell'interfaccia sull'interfaccia Ethernet 0 e il router A non è configurato per l'autenticazione sull'interfaccia adiacente.

```
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
```

Se l'autenticazione di area dei router connessi direttamente è configurata su un lato del collegamento, tra le due route viene creata l'adiacenza IS-IS del CLNS. Tuttavia, il router su cui è configurata l'autenticazione di area non accetta gli LSP L1 dal sistema CLNS adiacente senza alcuna autenticazione di area configurata. Tuttavia, il router adiacente senza autenticazione dell'area continua ad accettare entrambi gli LSP L1 e L2.

Questo è il messaggio di debug sul router A, dove è configurata l'autenticazione area e si riceve l'LSP L1 da un router adiacente (router B) senza autenticazione area:

```
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#
```

Se si configura l'autenticazione di dominio su un router, i provider di servizi di traduzione L2 dei router per cui non è configurata l'autenticazione di dominio verranno rifiutati. I router per i quali non è configurata l'autenticazione accettano gli LSP dal router per il quale è configurata l'autenticazione.

L'output del comando debug seguente mostra gli errori di autenticazione LSP. La CA del router è configurata per l'autenticazione di area o dominio e riceve LSP di livello 2 da un router (DB router) non configurato per l'autenticazione di dominio o password.

```
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
```

Informazioni correlate

- Pagina di supporto per il routing IP
- Documentazione e supporto tecnico – Cisco Systems