設定 IS-IS 驗證

目錄

簡介

建議設定路由通訊協定驗證，以免將惡意資訊導入路由表。本文件說明在使用中繼系統到中繼系統 (IS-IS) 的路由器之間的 IP 純文字驗證。

本文檔僅介紹IS-IS明文身份驗證。有關其他型別的IS-IS身份驗證的詳細資訊，請參閱增強IS-IS網路中的安全性。

必要條件

需求

本文檔的讀者應熟悉IS-IS操作和配置。

採用元件

本文件所述內容不限於特定軟體和硬體版本。本文檔中的配置已在運行Cisco IOS版本12.2(24a)的Cisco 2500系列路由器上進行了測試

背景資訊

IS-IS允許為指定連結、區域或域配置密碼。想要成為鄰居的路由器必須交換相同的密碼用於其配置的身份驗證級別。沒有適當密碼的路由器被禁止參與相應功能（即它不能初始化鏈路、不能初始化區域的成員，也不能成為第2級域的成員）。

Cisco IOS®軟體允許設定三種型別的IS-IS驗證。

- **IS-IS身份驗證** — 長期以來，這是為IS-IS配置身份驗證的唯一方法。
- **IS-IS HMAC-MD5身份驗證** — 此功能向每個IS-IS協定資料單元(PDU)新增HMAC-MD5摘要。它是在Cisco IOS軟體版本12.2(13)T中匯入，而且僅在有限數量的平台上支援。
- **增強型明文身**份驗證 — 使用此新功能，您可以使用允許在顯示軟體配置時加密口令的新命令配置明文身份驗證。它還使密碼更易於管理和更改。

註：有關ISIS MD-5和增強型明文身份驗證的資訊，請參閱在IS-IS網路中增強安全性。

RFC 1142中指定的IS-IS協定通過包含身份驗證資訊作為LSP的一部分，為Hello和鏈路狀態資料包(LSP)提供身份驗證。此驗證資訊已編碼為型別長度值(TLV)三重。身份驗證TLV的型別為10;TLV長度可變；而TLV的值取決於使用的身份驗證型別。預設情況下，身份驗證處於禁用狀態。

設定

本節討論如何為連結、區域和域配置IS-IS明文身份驗證。

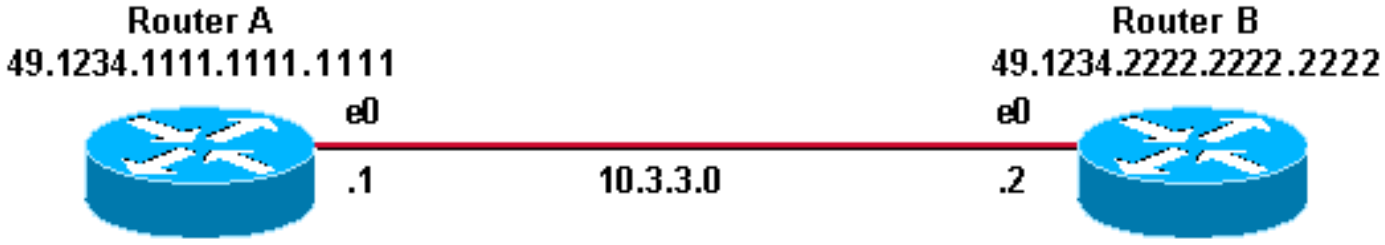
注意：要查詢有關本文檔中使用的命令的其他資訊，請使用搜尋命令的最佳實踐(僅限註冊客戶)。

介面驗證

在介面上配置IS-IS身份驗證時，可以為1級、2級或同時為1級/2級路由啟用密碼。如果不指定級別，則預設為級別1和級別2。根據配置的身份驗證級別，密碼將出現在相應的Hello消息中。IS-IS介面身份驗證的級別應跟蹤介面上的鄰接型別。使用**show clns neighbor**命令查詢鄰接型別。對於區域和域身份驗證，不能指定級別。

路由器A、乙太網0和路由器B、乙太網0上的介面身份驗證的網路圖和配置如下所示。路由器A和路由器B都使用isis密碼SECr3t為級別1和級別2配置。這些密碼區分大小寫。

在配置了無連線網路服務(CLNS)IS-IS的Cisco路由器上，它們之間的CLNS鄰接關係預設為1級/2級。因此，路由器A和路由器B將具有兩種鄰接關係，除非專門為級別1或級別2配置。



路由器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
```

路由器B

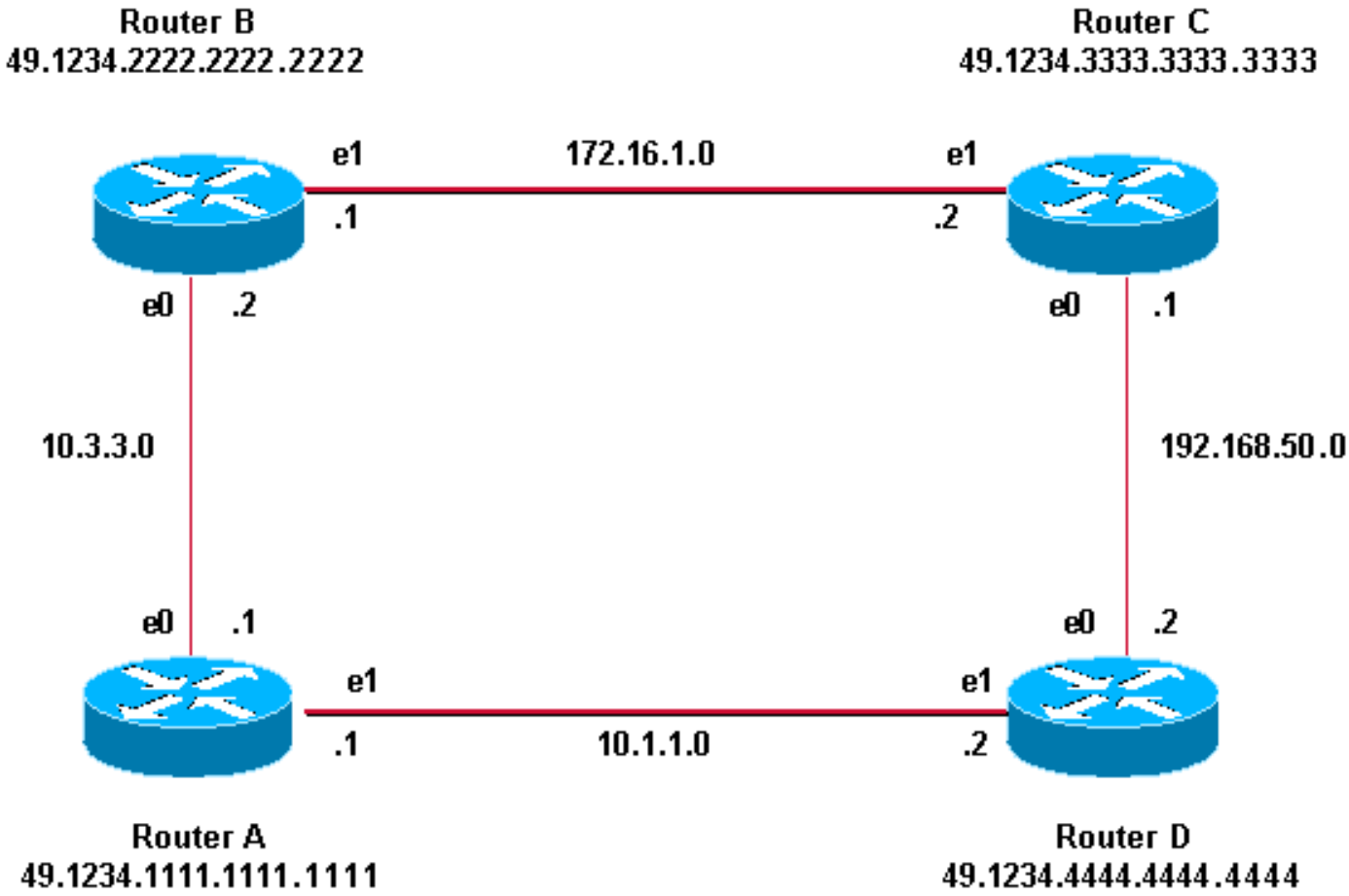
```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

區域驗證

區域身份驗證的網路圖和配置如下所示。配置區域身份驗證後，密碼將傳送在L1 LSP、CSNP和PSNPS中。所有路由器都位於同一個IS-IS區域(49.1234)中，並且都配置了區域密碼「tiGHter」。



路由器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
```

路由器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
```

路由器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
```

路由器D

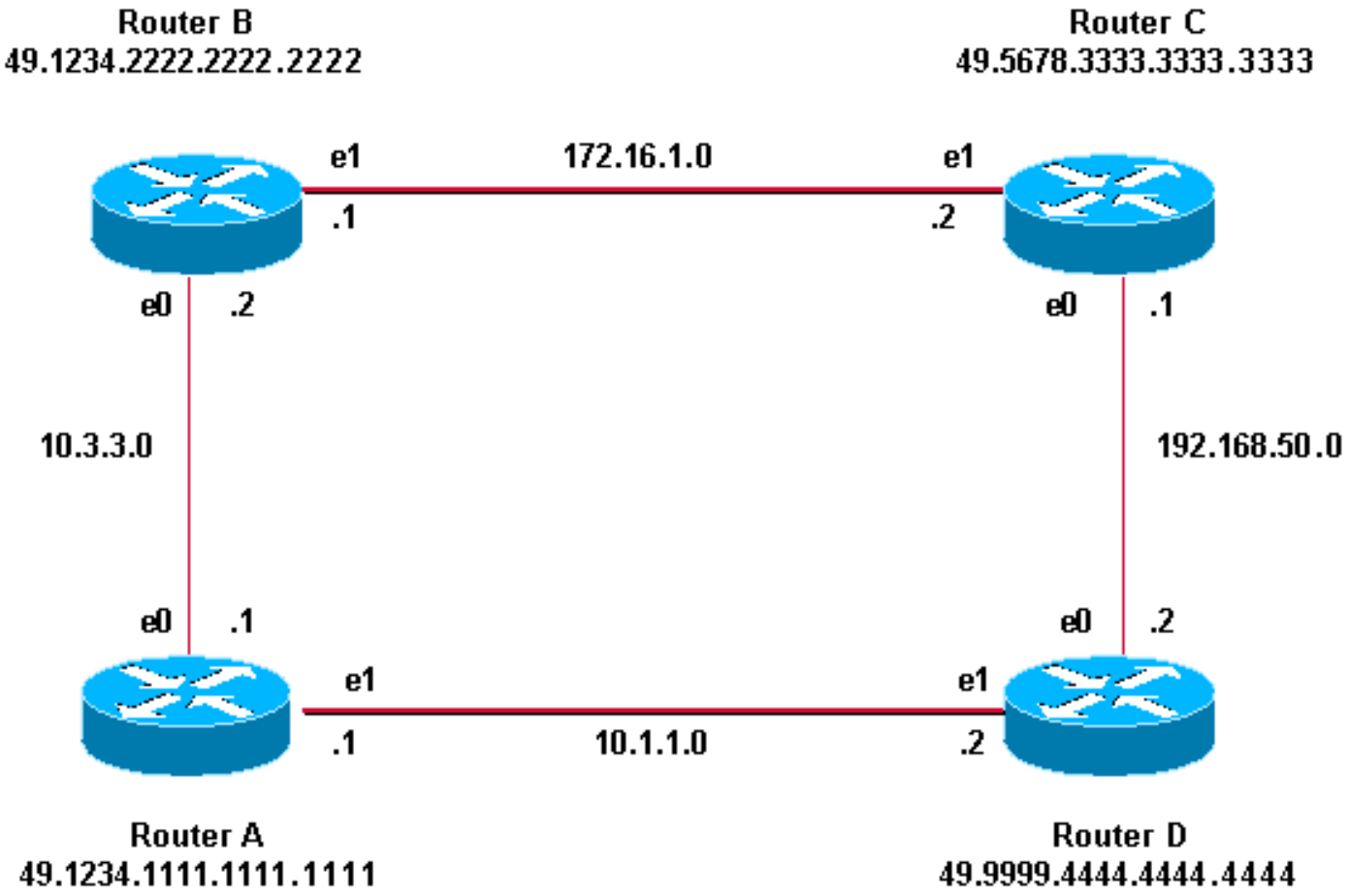
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

網域驗證

下面顯示了域身份驗證的網路圖和配置。路由器A和路由器B位於IS-IS區域49.1234;路由器C位於IS-IS區域49.5678;路由器D位於區域49.9999。所有路由器都位於同一個IS-IS域(49)中，並且都配置了域密碼「seCurity」。



路由器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
```

路由器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
```

路由器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
```

路由器D

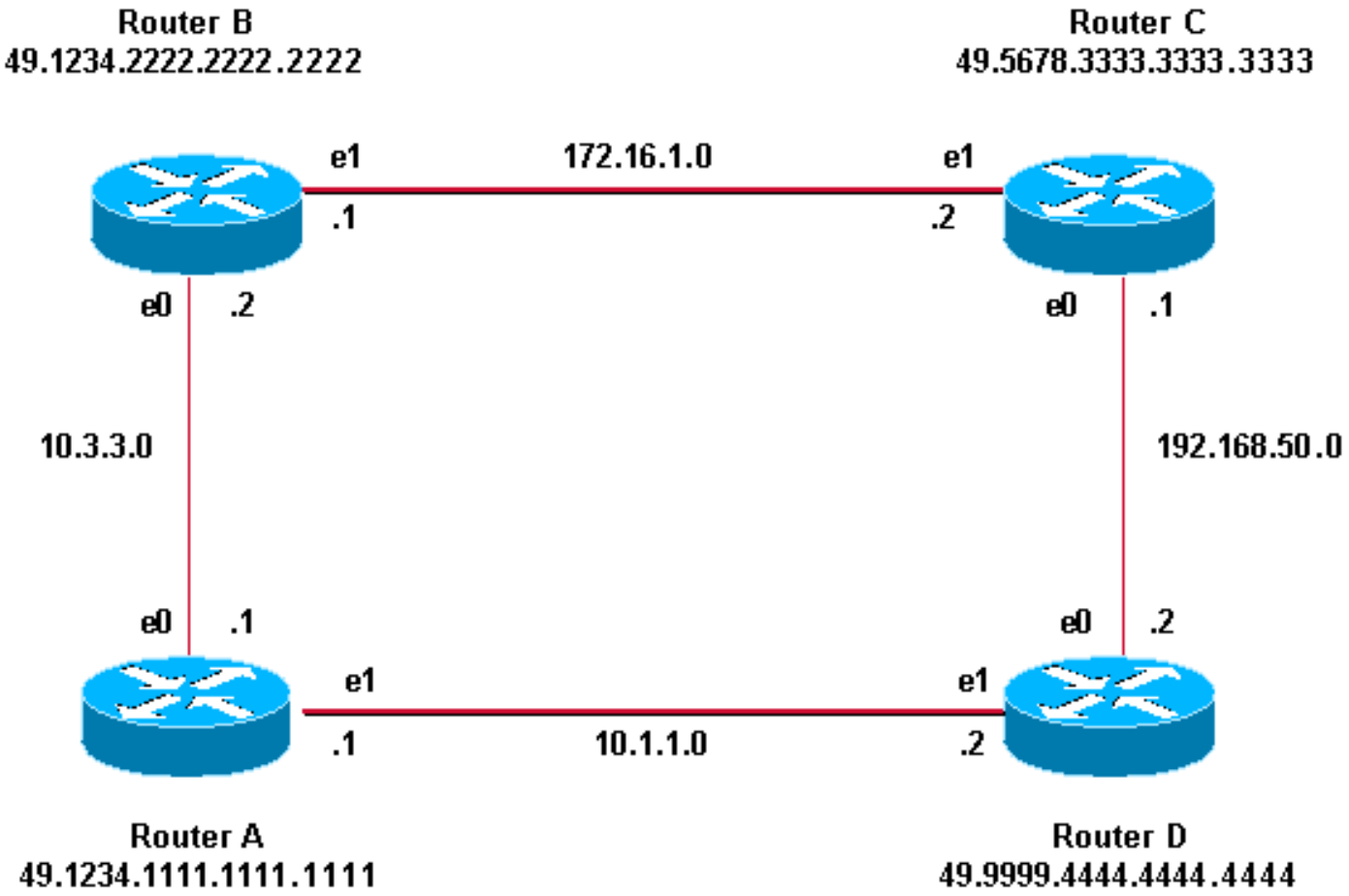
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

合併域、區域和介面身份驗證

本節中的拓撲和部分配置說明了域、區域和介面身份驗證的組合。路由器A和路由器B位於同一區域，並配置了區域密碼「tiGHter」。 路由器C和路由器D與路由器A和路由器B屬於兩個不同的區域。所有路由器都位於同一個域中，並且共用域級別的密碼「seCurity」。 路由器B和路由器C之間乙太網鏈路的介面配置。路由器C和路由器D僅與其鄰居建立L2鄰接關係，不需要配置區域密碼。



路由器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
```

路由器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
```

路由器C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis
isis password Fri3nd level-2

interfaceethernet0
```

路由器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
```

驗證

Cisco CLI Analyzer 支援某些 **show** 指令（僅限註冊客戶），它允許您查看 **show** 指令輸出的分析。

要驗證介面身份驗證是否正常工作，請在使用者EXEC模式或特權EXEC模式下使用**show clns neighbors**命令。命令的輸出顯示了連線的鄰接型別和狀態。**show clns neighbors** 命令的輸出示例顯示已正確配置用於介面身份驗證的路由器，並將狀態顯示為UP:

```
RouterA# show clns neighbors

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

對於區域和域身份驗證，可以使用debug命令完成身份驗證驗證，如下一節所述。

疑難排解

如果直連路由器在鏈路的一端配置了身份驗證，而在另一端沒有配置，則路由器不會形成CLNS IS-IS鄰接關係。在下面的輸出中，路由器B在其乙太網0介面上配置介面身份驗證，而路由器A在其鄰接介面上未配置身份驗證。

```
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
```

如果直連路由器在鏈路的一側配置了區域身份驗證，則兩個路由之間會形成CLNS IS-IS鄰接關係。但是，配置了area-authentication的路由器不接受未配置area-authentication的CLNS鄰居的L1 LSP。但是，沒有區域身份驗證的鄰居會繼續接受L1和L2 LSP。

這是路由器A上的調試消息，其中配置了區域身份驗證，並從鄰居（路由器B）接收第1層LSP，但未進行區域身份驗證：

```
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#
```

如果在一台路由器上配置域身份驗證，它會拒絕未配置域身份驗證的路由器的L2 LSP。未配置身份驗證的路由器接受來自已配置身份驗證的路由器的LSP。

以下調試輸出顯示LSP身份驗證失敗。路由器CA已配置為進行區域或域身份驗證，並且正在從未配置為進行域或口令身份驗證的路由器（路由器DB）接收第2級LSP。

```
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
```

相關資訊

- IP 路由支援頁面
- 技術支援與文件 - Cisco Systems