配置 IS-IS 认证

目录

简介

它希望为路由协议配置身份验证，以防止恶意信息引入路由表。本文档演示运行IP中间系统到中间系统(IS-IS)的路由器之间的明文身份验证。

本文档仅介绍IS-IS明文身份验证。有关其他类型的IS-IS身份验证的详细信息，请参阅“增强IS-IS网络中的安全”。

先决条件

要求

本文档的读者应熟悉IS-IS操作和配置。

使用的组件

本文档不限于特定的软件和硬件版本。本文档中的配置已在运行Cisco IOS版本12.2(24a)的Cisco 2500系列路由器上测试

背景信息

IS-IS允许为指定链路、区域或域配置密码。要成为邻居的路由器必须为其配置的身份验证级别交换相同的密码。禁止未拥有适当密码的路由器参与相应的功能（即，它不能初始化链路、分别成为区域成员或第2级域成员）。

Cisco IOS®软件允许配置三种类型的IS-IS身份验证。

- **IS-IS身份验证** — 长期以来，这是为IS-IS配置身份验证的唯一方法。
- **IS-IS HMAC-MD5身份验证** — 此功能向每个IS-IS协议数据单元(PDU)添加HMAC-MD5摘要。它在Cisco IOS软件版本12.2(13)T中引入，仅在数量有限的平台上受支持。
- **增强的明文身份验证** — 使用此新功能，可以使用新命令配置明文身份验证，这些命令允许在显示软件配置时加密口令。它还使密码更易于管理和更改。

注：有关ISIS MD-5和增强的明文身份验证的信息，请参阅增强IS-IS网络中的安全。

IS-IS协议(如RFC 1142中所述)通过在LSP中包含身份验证信息，为Hello和链路状态数据包(LSP)提供身份验证。此身份验证信息编码为类型长度值(TLV)三重。身份验证TLV的类型为10;TLV的长度是可变的；TLV的值取决于所使用的身份验证类型。默认情况下，身份验证处于禁用状态。

配置

本节讨论如何在链路、区域和域上配置IS-IS明文身份验证。

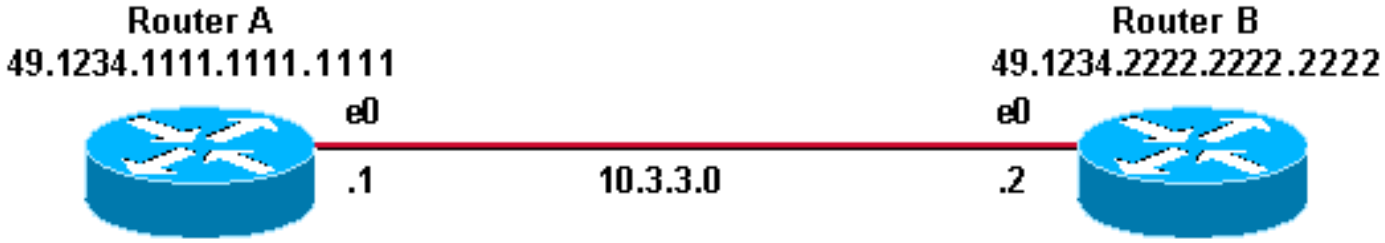
注意：要查找有关本文档中使用的命令的其他信息，请使用"搜索命令的最佳实践"(仅限注册客户)。

接口认证

在接口上配置IS-IS身份验证时，可以为1级、2级或2级1/2级路由启用密码。如果未指定级别，则默认值为1级和2级。根据配置身份验证的级别，密码将在相应的Hello消息中传输。IS-IS接口身份验证级别应跟踪接口上的邻接类型。使用**show clns neighbor**命令查找邻接类型。对于区域和域身份验证，不能指定级别。

路由器A、以太网0和路由器B、以太网0上接口身份验证的网络图和配置如下所示。路由器A和路由器B都配置了isis口令SECr3t，用于1级和2级。这些口令区分大小写。

在配置了无连接网络服务(CLNS)IS-IS的思科路由器上，它们之间的CLNS邻接默认为1级/2级。因此，除非为1级或2级进行专门配置，否则路由器A和路由器B将具有这两种邻接关系。



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

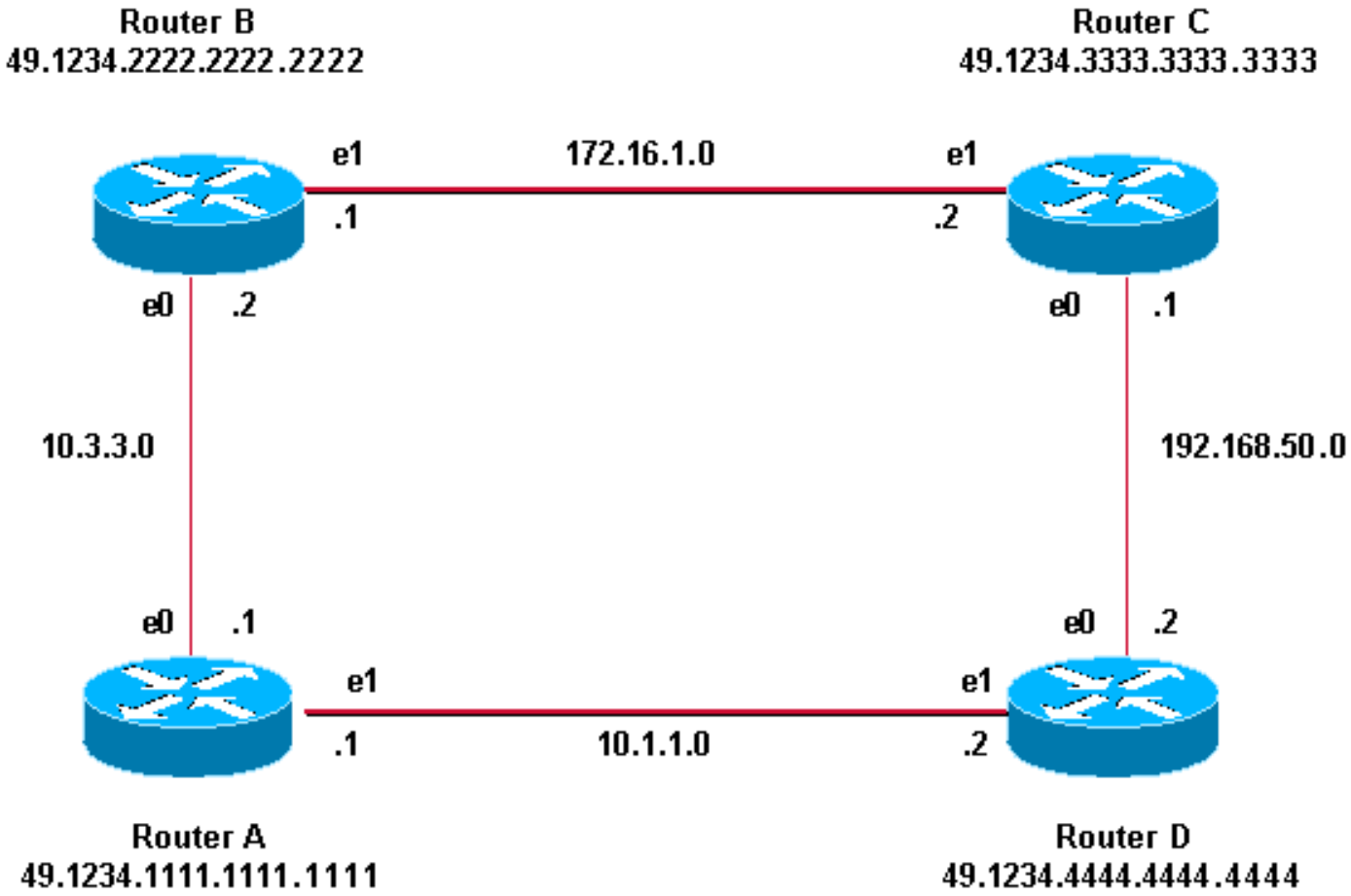
```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

区域验证

区域身份验证的网络图和配置如下所示。当配置区域身份验证时，口令在L1 LSP、CSNP和PSNPS中传输。所有路由器都位于同一IS-IS区域49.1234中，并且都配置了区域密码“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
```

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

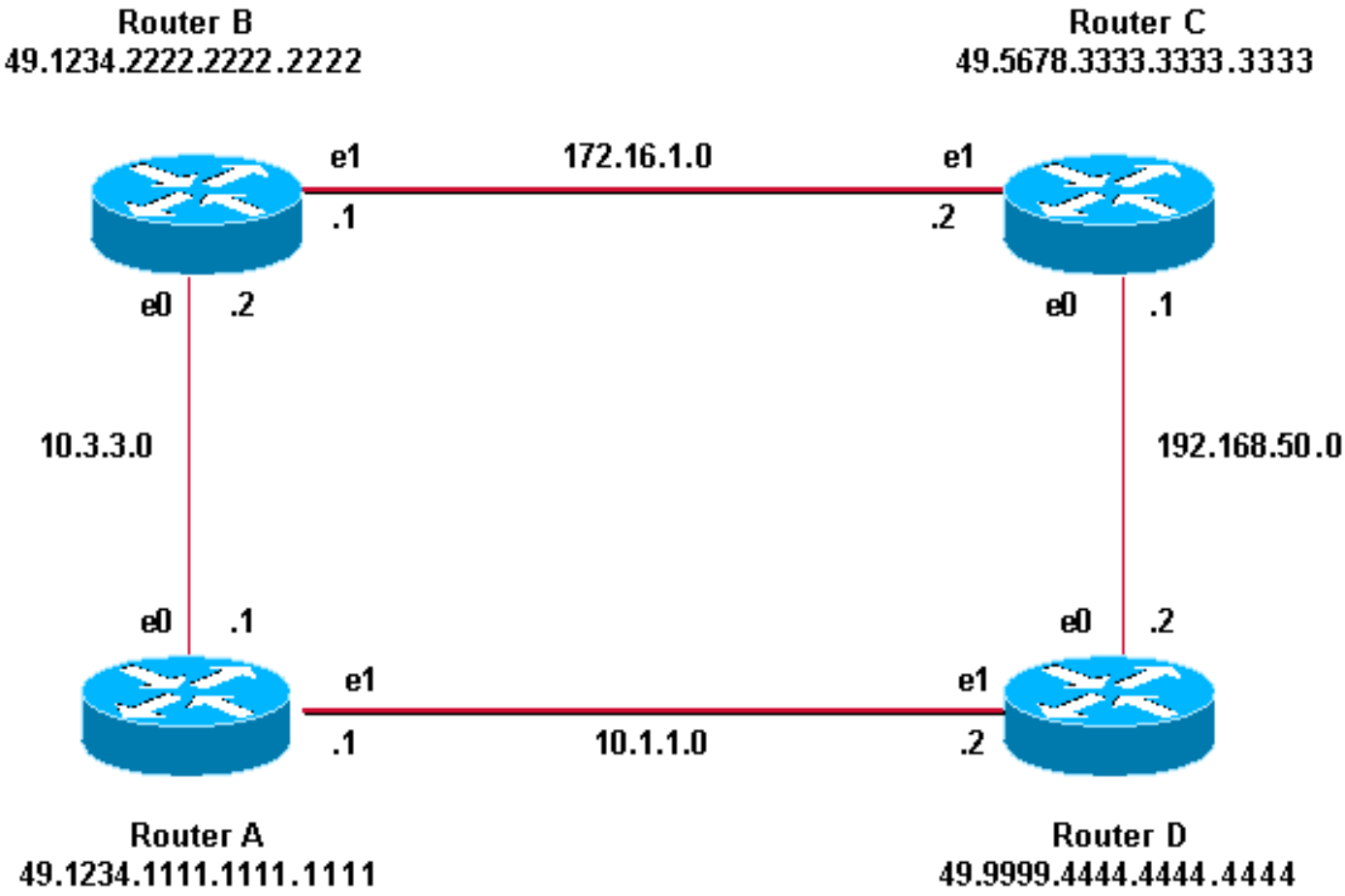
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

域认证

网络图和域身份验证配置如下所示。路由器A和路由器B位于IS-IS区域49.1234中；路由器C位于IS-IS区域49.5678中；路由器D位于区域49.9999中。所有路由器都位于同一IS-IS域(49)中，并且配置了域密码“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
```

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

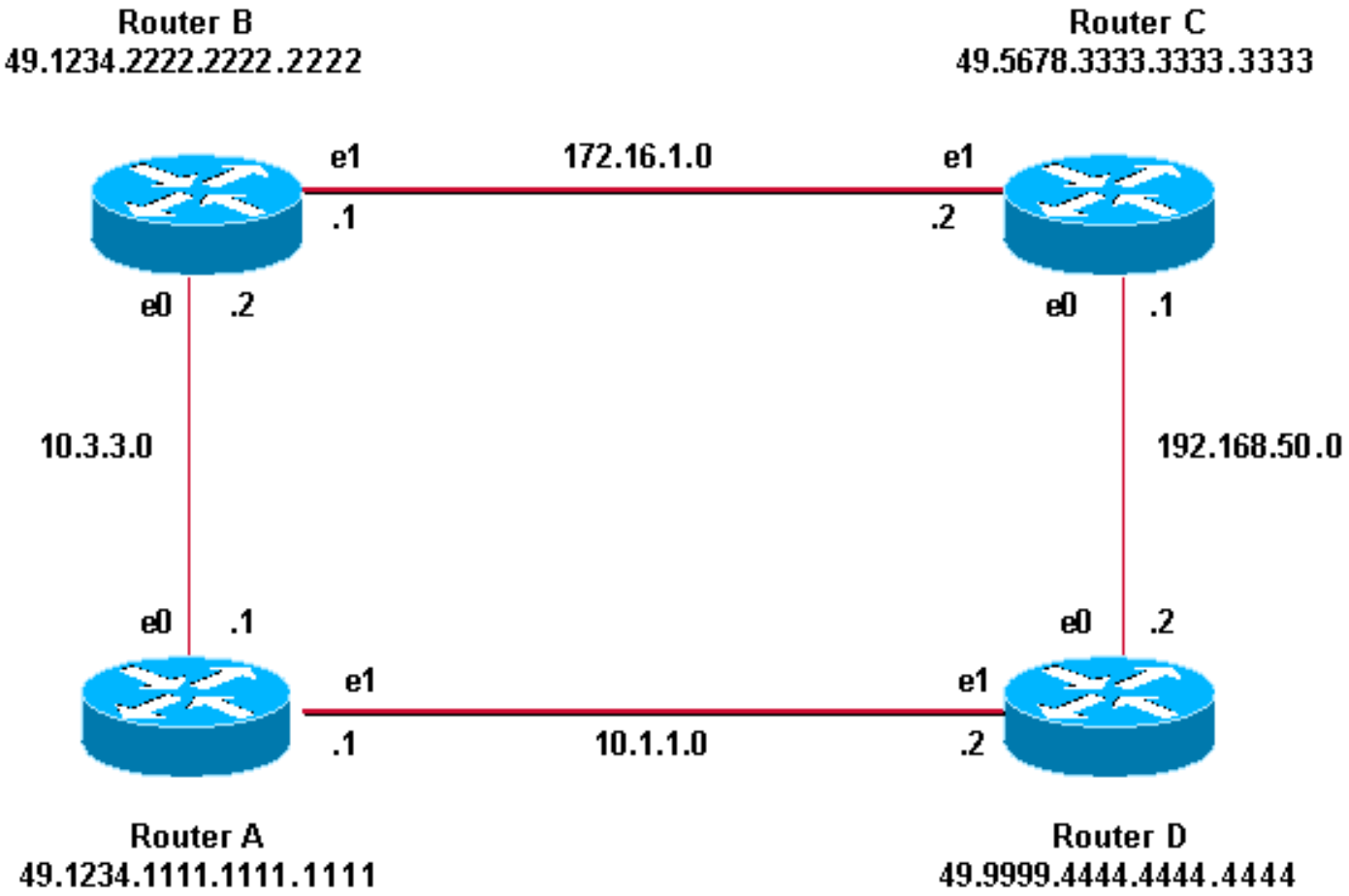
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

组合域、区域和接口身份验证

本部分的拓扑和部分配置说明了域、区域和接口身份验证的组合。路由器A和路由器B位于同一区域，并配置了区域密码“tiGHter”。 路由器C和路由器D与路由器A和路由器B属于两个不同区域。所有路由器都位于同一域中，并共享域级密码“seSecurity”。 路由器B和路由器C之间有以太网链路的接口配置。路由器C和路由器D仅与邻居形成L2邻接关系，无需配置区域密码。



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
```

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
```

验证

Cisco CLI Analyzer (仅限注册客户)支持某些**show**命令，它允许您查看对show命令输出的分析。

要验证接口身份验证是否正常工作，请在用户EXEC模式或特权EXEC模式下使用**show clns neighbors**命令。命令的输出显示连接的邻接类型和状态。show clns neighbors命令的**输出示例**显示路由器已正确配置用于接口身份验证，并将状态显示为UP:

```
RouterA# show clns neighbors

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

对于区域和域身份验证，可以使用debug命令进行身份验证验证，如下一节所述。

故障排除

如果直连路由器在链路的一端配置了身份验证，而在另一端未配置身份验证，则路由器不会形成CLNS IS-IS邻接关系。在以下输出中，路由器B在其Ethernet 0接口上配置了接口身份验证，而路由器A在其相邻接口上未配置身份验证。

```
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
```

如果直连路由器在链路的一端配置了区域身份验证，则两条路由之间会形成CLNS IS-IS邻接关系。但是，配置了区域身份验证的路由器不接受来自未配置区域身份验证的CLNS邻居的L1 LSP。但是，没有区域身份验证的邻居继续接受L1和L2 LSP。

以下是路由器A上的调试消息，其中配置了区域身份验证，并从邻居（路由器B）接收L1 LSP，而不进行区域身份验证：

```
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验证，它将拒绝未配置域身份验证的路由器的L2 LSP。未配置身份

验证的路由器接受来自已配置身份验证的路由器的LSP。

以下调试输出显示LSP身份验证失败。路由器CA配置为进行区域或域身份验证，并且从未配置域或密码身份验证的路由器（路由器DB）接收第2级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
```

相关信息

- IP 路由 支持页
- 技术支持和文档 - Cisco Systems