配置 IS-IS 认证

目录

简介

配置路由协议的验证为了防止有恶意的信息的介绍到路由表是理想的。本文展示在运行IP的路由器之间的明文验证中间系统对中间系统(IS-IS)。

本文只包括IS-IS明文验证。参考增强在IS-IS网络的安全关于IS-IS验证的更多信息其他类型。

先决条件

要求

本文读者应该熟悉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。在本文的配置在思科2500系列路由器测试了，运行Cisco IOS版本12.2(24a)

背景信息

IS-IS允许一个密码的配置一条指定的链路、区域或者域的。要变为邻居的路由器必须交换他们的已配置的级别的同一个密码验证。一个路由器不拥有适当的密码被禁止参与对应的功能(即可能不初始化链路，是区域的成员或者是2级域的成员，分别)。

Cisco IOS软件允许IS-IS验证的三种类型将配置的。

- **IS-IS验证**-长期地，这是配置IS-IS的验证的唯一方法。
- **IS-IS HMAC-MD5验证**-此功能添加一HMAC-MD5摘要到每IS-IS协议数据单元(PDU)。在Cisco IOS软件版本12.2(13)T介绍和有限数量平台只支持它。
- **增强版明文验证**-使用此新特性，明文验证可以配置使用允许将加密的密码的新的命令，当软件配置显示时。它也使密码更加容易管理和更改。

注意： 参考增强在IS-IS网络的安全关于ISIS MD-5和增强版明文验证的信息。

IS-IS协议，在RFC 1142、提供Hello的验证的和链路状态数据包(LSP)上指定通过认证信息包括作为LSP一部分。三倍，此认证信息编码，当类型长度值(TLV)。验证TLV的种类是10;TLV的长度可变;并且TLV的值取决于使用的认证类型。默认情况下，验证禁用。

配置

此部分讨论如何配置IS-IS明文验证在链路，区域的和域的。

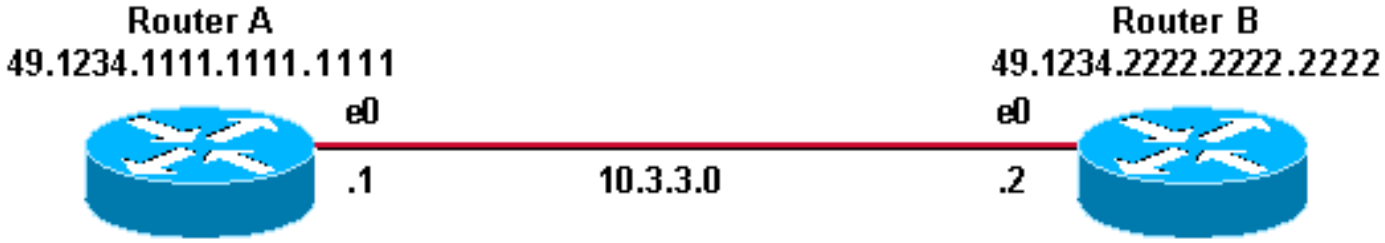
注意： 要寻找关于用于本文的命令的其他信息，请使用最佳实践搜索命令(仅限注册用户)。

接口认证

当您配置在接口时的IS-IS验证，您能启用1级的密码， 2级，或者两L1/L2路由。如果不指定级别，默认是1级，并且级别2.根据验证配置的级别，密码输入对应的Hello消息。级别IS-IS接口验证应该跟踪邻接种类在接口的。请使用**show clns neighbor命令**发现邻接种类。对于区域和域认证，您不能指定级别。

网络图和配置接口认证的在路由器A、Ethernet0和路由器B， Ethernet0如下所示。路由器A和路由器B是两已配置的与isis 1级的密码SECr3t和2级。这些密码区分大小写。

默认情况下在Cisco路由器上配置与无连接网络服务(CLNS) IS-IS，在他们之间的CLNS邻接是L1/L2。因此，路由器A和路由器B将有邻接两个类型，除非特别地配置为1级或2级。



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

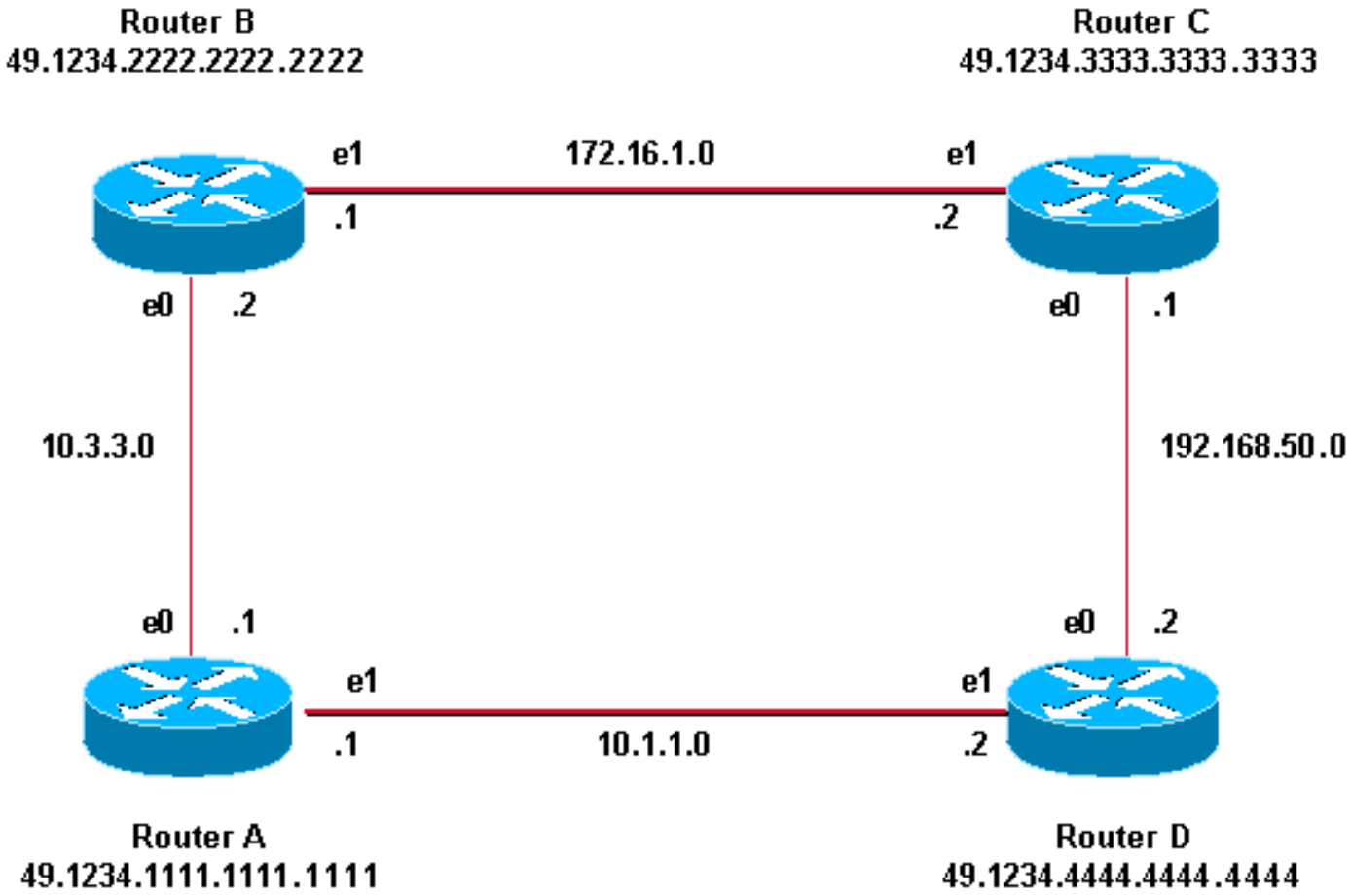
```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

区域验证

网络图和配置区域验证的如下所示。当区域验证配置时，密码输入L1 LSP、CSNPs和PSNPS。所有路由器是在同一个IS-IS区域， 49.1234，并且他们全部用更加严密的区域密码配置“”。



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

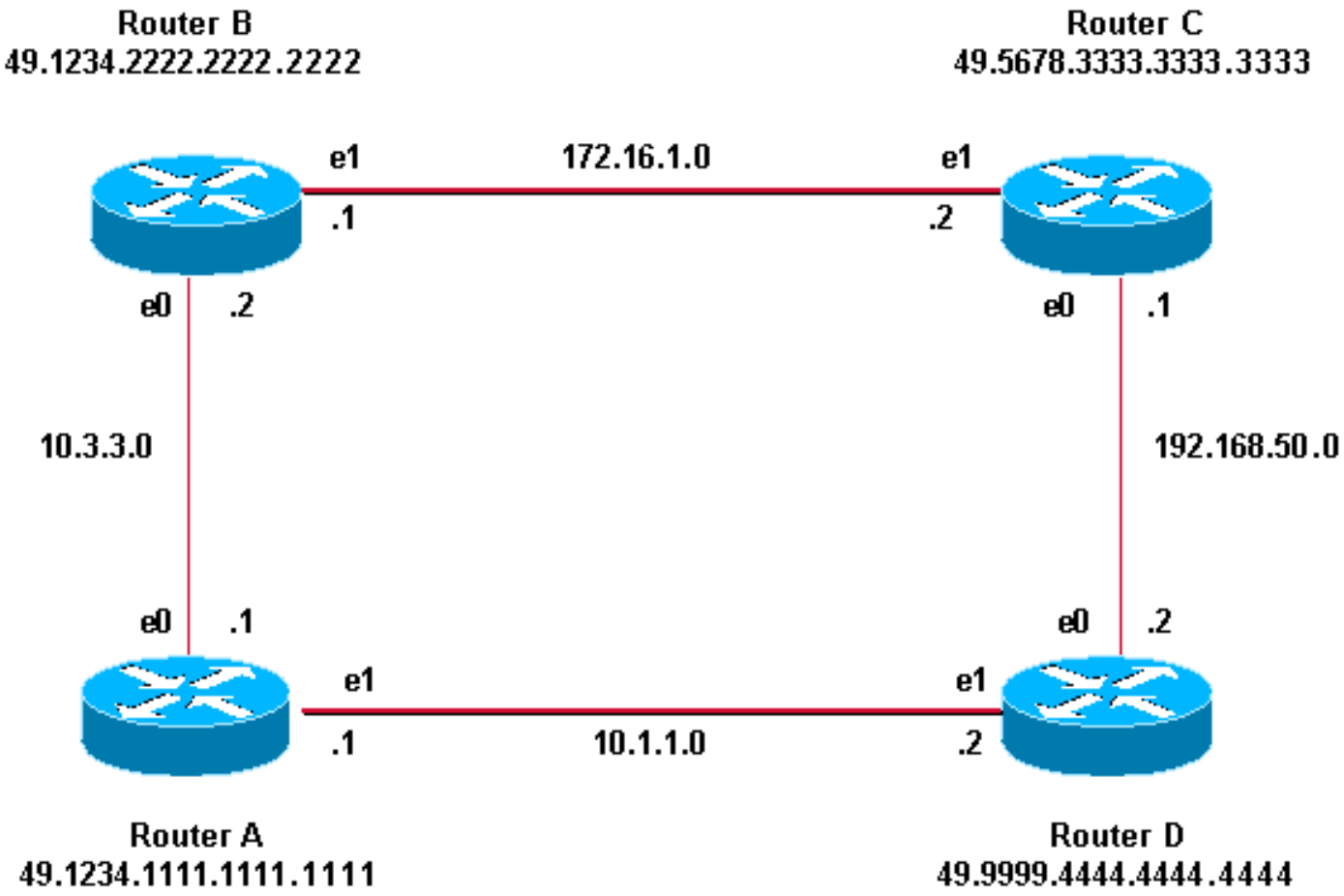
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

域认证

网络图和配置域认证的如下所示。路由器A和路由器B是在IS-IS区域49.1234;路由器C在IS-IS区域49.5678;并且路由器D在区域49.9999。所有路由器是在同一个IS-IS域(49)和用域密码“安全配置”。



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

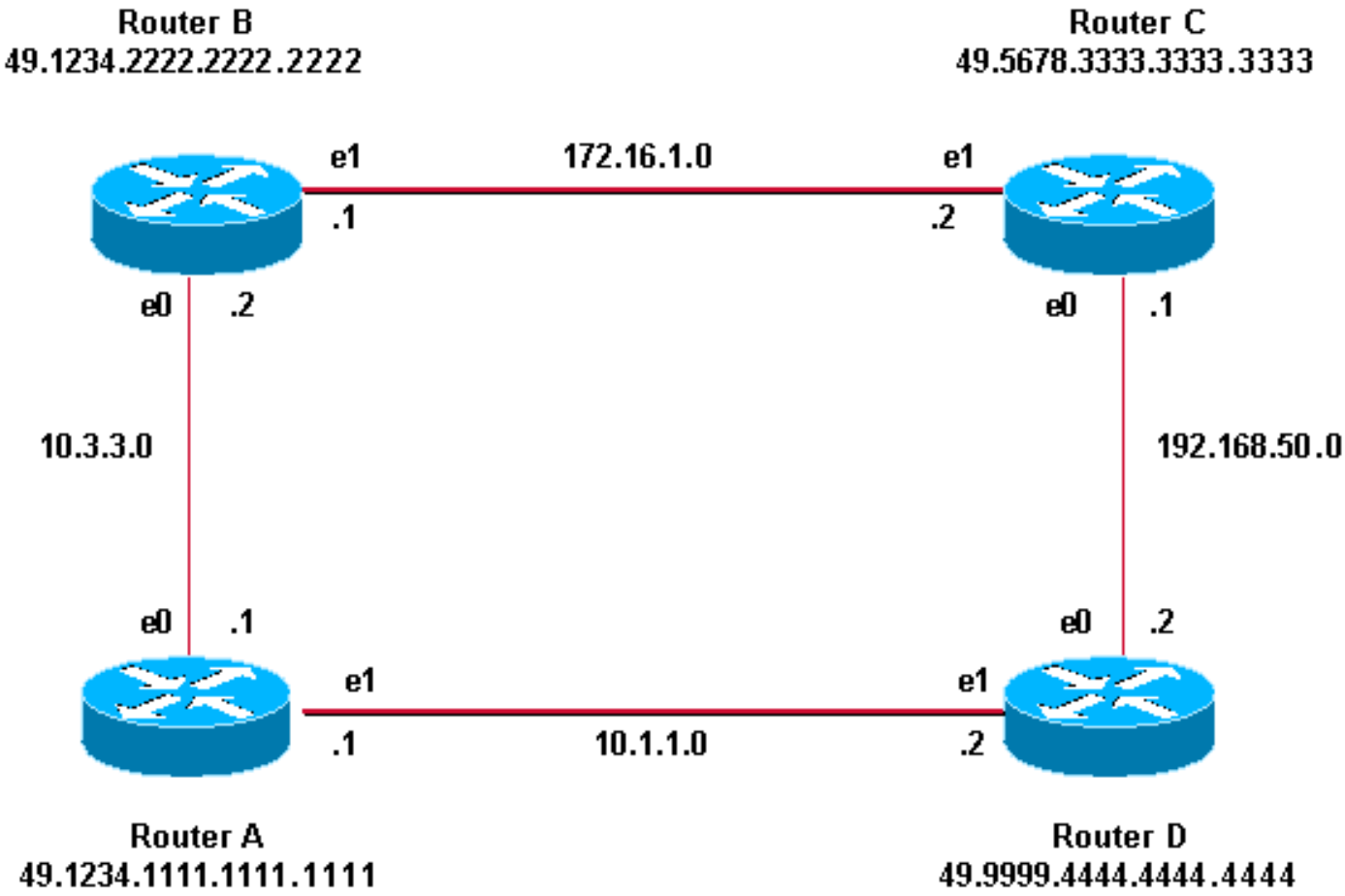
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

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
```

结合域、区域和接口认证

拓扑和部分配置在此部分说明域、区域和接口认证的组合。路由器A和路由器B在同一个区域和用更加严密的区域密码配置“”。路由器C和路由器D比路由器A和路由器B.属于两个不同的区域。所有路由器是在同一个域并且共享域级密码“安全”。路由器B和路由器C有以太网链路的一个接口配置他们之间。路由器C和路由器D形成L2与他们的邻居的仅邻接，并且配置区域密码没有要求。



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
```

验证

确定请**显示**命令支持Cisco CLI分析器(仅限注册用户)，允许您查看show命令输出分析。

要验证，如果接口认证是工作正常，请使用**show clns neighbors命令**在用户EXEC或特权EXEC模式。命令的输出显示连接的邻接类型和状态。从**show clns neighbors命令的**此输出示例:显示为接口认证正确地配置的路由器并且显示状态作为：

```
RouterA# show clns neighbors

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

对于区域和域认证，验证的验证可以完成使用调试指令按照下一部分说明。

故障排除

另一方面如果连接的路由器直接地有在链路的一端配置的验证，和没有，路由器不形成CLNS IS-IS邻接。在下面的输出中，路由器B为在其Ethernet0接口的接口认证配置，并且路由器A没有配置与在其毗邻接口的验证。

```
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
```

如果连接的路由器直接地有在链路的一端配置的区域验证， CLNS IS-IS邻接形成在两个路由之间。然而，区域验证配置的路由器，不接受L1从CLNS邻居的LSP没有配置的区域验证。然而，没有区域验证的邻居继续接受L1和L2 LSP。

这是在区域验证是配置和接收L1从邻居的路由器A的调试消息(没有区域验证的路由器B)的LSP ：

```
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#
```

如果配置在一个路由器的域认证，拒绝从不安排域认证配置的路由器的L2 LSP。不安排验证配置接受从路由器的LSP有配置的验证的路由器。

下面的debug输出显示LSP认证失败。路由器CA为区域或域认证配置并且是从没有为域或密码验证配置的路由器(路由器DB)的接受级别2 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