RIPv2 中驗證的範例組態

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[背景資訊](#)
[設定](#)
[網路圖表](#)
[組態](#)
[配置純文字檔案身份驗證](#)
[配置MD5身份驗證](#)
[驗證](#)
[驗證明文身份驗證](#)
[檢驗MD5身份驗證](#)
[疑難排解](#)
[疑難排解指令](#)
[相關資訊](#)

簡介

本文件提供針對路由資訊通訊協定第 2 版 (RIPv2)，驗證路由資訊交換程序的範例組態。

RIPv2的思科實施支援兩種身份驗證模式：純文字檔案身份驗證和消息摘要5(MD5)身份驗證。如果啟用了身份驗證，明文身份驗證模式是每個RIPv2資料包中的預設設定。當存在安全問題時，不應使用純文字檔案身份驗證，因為每個RIPv2資料包都會傳送未加密的身份驗證密碼。

注意：RIP第1版(RIPv1)不支援身份驗證。如果要傳送和接收RIPv2資料包，可以在介面上啟用RIP身份驗證。

必要條件

需求

本文檔的讀者應具備以下基本瞭解：

- RIPv1和RIPv2

採用元件

本文件所述內容不限於特定軟體和硬體版本。從Cisco IOS®軟體版本11.1開始，支援RIPv2，因此Cisco IOS®軟體版本11.1及更高版本支援配置中給出的所有命令。

本檔案中的組態會使用以下軟體和硬體版本進行測試和更新：

- Cisco 2500系列路由器
- Cisco IOS軟體版本12.3(3)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

安全性是當今網路設計人員的主要關注點之一。保護網路安全包括保護路由器之間路由資訊的交換，例如確保輸入到路由表中的資訊有效並且不是由試圖破壞網路的人發起或篡改。攻擊者可能會嘗試引入無效更新，誘使路由器將資料傳送到錯誤的目的地，或嚴重降低網路效能。此外，無效路由更新可能由於配置不當(例如未在網路邊界上使用**passive interface**命令)或路由器故障而出現在路由表中。因此，對路由器上運行的路由更新進程進行身份驗證是審慎的做法。

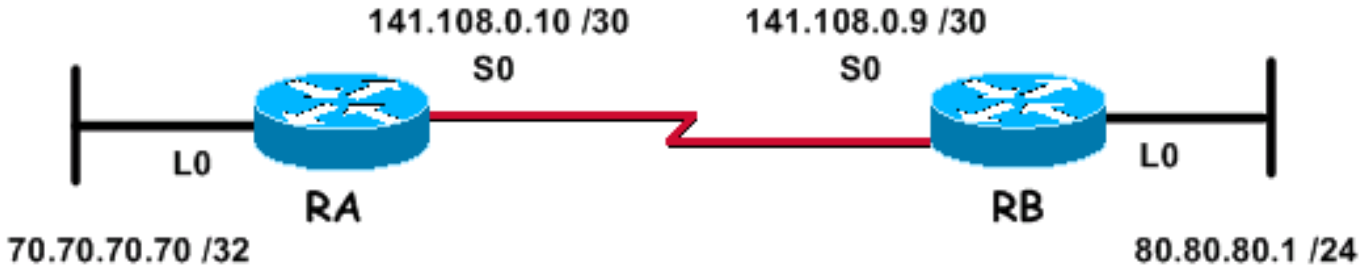
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本文檔使用下圖所示的網路設定。



用於以下配置示例的上述網路包含兩台路由器；路由器RA和路由器RB，它們都運行RIP並定期交換路由更新。必須通過串列鏈路驗證路由資訊的交換。

組態

執行以下步驟在RIPv2中配置身份驗證：

1. 定義具有名稱的金鑰鏈。**註：**金鑰鏈確定可在介面上使用的金鑰集。如果未配置金鑰鏈，則不對該介面執行身份驗證。
2. 定義金鑰鏈上的一個或多個金鑰。
3. 指定要在金鑰中使用的密碼或金鑰字串。這是必須使用要驗證的路由協定在資料包中傳送和接收的身份驗證字串。（在下面給出的示例中，字串的值是234。）
4. 在介面上啟用身份驗證並指定要使用的金鑰鏈。由於身份驗證是針對每個介面啟用的，因此運行RIPv2的路由器可以配置為在某些介面上進行身份驗證，並且可以在其它介面上不進行任何身份驗證的情況下運行。
5. 指定介面是使用純文字檔案還是MD5身份驗證。在上一步中啟用身份驗證時，RIPv2中使用的預設身份驗證是明文身份驗證。因此，如果使用純文字檔案身份驗證，則不需要此步驟。
6. 配置金鑰管理（此步驟是可選的）。金鑰管理是一種控制身份驗證金鑰的方法。這用於從一個身份驗證金鑰遷移到另一個身份驗證金鑰。如需詳細資訊，請參閱設定IP路由通訊協定無關功能的「管理驗證金鑰」一節。

配置純文字檔案身份驗證

RIP更新的兩種認證方式之一是使用純文字檔案認證。如下表所示，可對此進行配置。

RA
key chain kal *!--- Name a key chain. A key chain may contain more than one key for added security. !--- It need not be identical on the remote router.* **key 1** *!--- This is the Identification number of an authentication key on a key chain. !--- It need not be identical on the remote router.* **key-string 234** *!--- The actual password or key-string. !--- It needs to be identical to the key-string on the remote router.* ! interface Loopback0 ip address 70.70.70.70 255.255.255.255 ! interface Serial0 ip address 141.108.0.10 255.255.255.252 **ip rip authentication key-chain kal** *!--- Enables authentication on the interface and configures !--- the key chain that will be used.* ! router rip version 2 network 141.108.0.0 network 70.0.0.0

RB
key chain kal **key 1** **key-string 234** **!** interface Loopback0 ip address 80.80.80.1 255.255.255.0 ! interface Serial0

```
 ip address 141.108.0.9 255.255.255.252
 ip rip authentication key-chain kal
 clockrate 64000
!
router rip
 version 2
 network 141.108.0.0
 network 80.0.0.0
```

有關命令的詳細資訊，請參閱Cisco IOS IP命令參考。

配置MD5身份驗證

MD5身份驗證是思科新增到原始RFC 1723-defined plain text authentication中的可選身份驗證模式。除了使用其它命令ip rip authentication mode md5 外，該配置與純文字檔案身份驗證的配置相同。使用者必須在鏈路的兩端配置路由器介面以使用MD5身份驗證方法，並確保兩端的金鑰號和金鑰字串匹配。

RA

```
key chain kal
!--- Need not be identical on the remote router. key 1
!--- Needs to be identical on remote router. key-string
234
!--- Needs to be identical to the key-string on the
remote router. ! interface Loopback0 ip address
70.70.70.70 255.255.255.255 ! interface Serial0 ip
address 141.108.0.10 255.255.255.252 ip rip
authentication mode md5
!--- Specifies the type of authentication used !--- in
RIPv2 packets. !--- Needs to be identical on remote
router. !-- To restore clear text authentication, use
the no form of this command. ip rip authentication key-
chain kal
 !
 router rip
  version 2
  network 141.108.0.0
  network 70.0.0.0
```

RB

```
key chain kal
key 1
key-string 234
!
interface Loopback0
 ip address 80.80.80.1 255.255.255.0
!
interface Serial0
 ip address 141.108.0.9 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain kal
 clockrate 64000
!
router rip
 version 2
 network 141.108.0.0
 network 80.0.0.0
```

有關命令的詳細資訊，請參閱Cisco IOS命令參考。

驗證

驗證明文身份驗證

本節提供的資訊用於確認您的組態是否正常運作。

通過如上所示配置路由器，所有路由更新交換在接受之前都要經過身份驗證。這可以通過觀察 debug ip rip 和show ip route 命令的輸出來驗證。

注意：發出debug命令之前，請參閱有關Debug命令的重要資訊**。**

```
RB#debug ip rip
 RIP protocol debugging is on
*Mar  3 02:11:39.207: RIP: received packet with text authentication 234
*Mar  3 02:11:39.211: RIP: received v2 update from 141.108.0.10 on Serial0
```

```
*Mar  3 02:11:39.211: RIP: 70.0.0.0/8 via 0.0.0.0 in 1 hops
```

```
RB#show ip route
```

```
R    70.0.0.0/8 [120/1] via 141.108.0.10, 00:00:25, Serial0
     80.0.0.0/24 is subnetted, 1 subnets
C       80.80.80.0 is directly connected, Loopback0
     141.108.0.0/30 is subnetted, 1 subnets
C       141.108.0.8 is directly connected, Serial0
```

使用明文身份驗證可防止新增由無意參與本地路由交換過程的路由器發起的路由更新，從而改善網路設計。但是，這種型別的身份驗證不安全。密碼（在本例中為234）以純文字檔案格式交換。它可以被輕易地捕獲並利用。如前所述，當存在安全問題時，MD5身份驗證必須優先於純文字檔案身份驗證。

檢驗MD5身份驗證

通過如上所示配置RA和RB路由器，所有路由更新交換在接受之前都要經過身份驗證。這可以通過觀察debug ip rip 和show ip route 命令的輸出來驗證。

```
RB#debug ip rip
```

```
 RIP protocol debugging is on
```

```
*Mar  3 20:48:37.046: RIP: received packet with MD5 authentication
```

```
*Mar  3 20:48:37.046: RIP: received v2 update from 141.108.0.10 on Serial0
```

```
*Mar  3 20:48:37.050:  70.0.0.0/8 via 0.0.0.0 in 1 hops
```

```
RB#show ip route
```

```
R    70.0.0.0/8 [120/1] via 141.108.0.10, 00:00:03, Serial0
     80.0.0.0/24 is subnetted, 1 subnets
C       80.80.80.0 is directly connected, Loopback0
     141.108.0.0/30 is subnetted, 1 subnets
C       141.108.0.8 is directly connected, Serial0
```

MD5身份驗證使用單向的MD5雜湊演算法，公認是一個強大的雜湊演算法。在此驗證模式下，路由更新不會攜帶用於驗證目的的密碼。相反，通過在密碼上運行MD5演算法生成的128位消息，該消息將隨傳送以進行身份驗證。因此，建議使用MD5身份驗證而不是純文字檔案身份驗證，因為它更加安全。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

debug ip rip 命令可用於排除RIPv2身份驗證相關問題。

注意：發出**debug指令之前，請先參閱**有關Debug指令的重要資訊。

注意：以下是**debug ip rip 命令輸出的示例，其中相鄰路由器之間需要相同的任何身份驗證相關引數都不匹配。**這可能會導致一台或兩台路由器在其路由表中不安裝接收的路由。

```
RA#debug ip rip

   RIP protocol debugging is on



   *Mar 1 06:47:42.422: RIP: received packet with text authentication 234

   *Mar 1 06:47:42.426: RIP: ignored v2 packet from 141.108.0.9 (invalid authentication)


   RB#debug ip rip

   RIP protocol debugging is on



   *Mar 1 06:48:58.478: RIP: received packet with text authentication 235

   *Mar 1 06:48:58.482: RIP: ignored v2 packet from 141.108.0.10 (invalid authentication)
```

show ip route 命令的以下輸出顯示路由器沒有通過RIP獲取任何路由：

```
RB#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

80.0.0.0/24 is subnetted, 1 subnets

   C 80.80.80.0 is directly connected, Loopback0

   141.108.0.0/30 is subnetted, 1 subnets

   C 141.108.0.8 is directly connected, Serial0

   RB#
```

附註1:使用純文字檔案身份驗證模式時，請確保相鄰路由器上的以下引數匹配以便成功進行身份驗證。

- Key-string
- 身份驗證模式

附註2:使用MD5身份驗證模式時，為成功進行身份驗證，請確保相鄰路由器上的以下引數匹配。

- Key-string
- 金鑰編號
- 身份驗證模式

相關資訊

- 路由資訊協定(RIP)簡介
- 配置RIP
- 配置IP路由協定 — 獨立功能
- RIP命令
- Cisco IOS IP命令參考，第2卷，共4卷：路由協定版本12.3
- RIP技術支援頁
- IP路由通訊協定技術支援頁面
- 技術支援 - Cisco Systems