Sample Configuration for Authentication in RIPv2

Document ID: 13719

Introduction

This document shows sample configurations for authenticating the routing information exchange process for Routing Information Protocol version 2 (RIPv2).

Cisco implementation of RIPv2 supports two modes of authentication: plain text authentication and Message Digest 5 (MD5) authentication. Plain text authentication mode is the default setting in every RIPv2 packet, when authentication is enabled. Plain text authentication should not be used when security is an issue, because the unencrypted authentication password is sent in every RIPv2 packet.

Note: RIP version 1 (RIPv1) does not support authentication. If you are sending and receiving RIPv2 packets, you can enable RIP authentication on an interface.

Prerequisites

Requirements

Readers of this document should have the basic understanding of the following:

- RIPv1 and RIPv2

Components Used

This document is not restricted to specific software and hardware versions. Starting from Cisco IOS® Software Version 11.1, RIPv2 is supported and therefore all the commands given in the configuration are supported on Cisco IOS® Software Version 11.1 and later.

The configuration in the document is tested and updated using these software and hardware versions:

- Cisco 2500 Series Router
- Cisco IOS Software Version 12.3(3)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Background Information

Security is one of the primary concerns of network designers today. Securing a network includes securing the exchange of routing information between routers, such as ensuring that the information entered into the routing table is valid and not originated or tampered by someone trying to disrupt the network. An attacker might try to introduce invalid updates to trick the router into sending data to the wrong destination, or to seriously degrade network performance. In addition, invalid route updates might end up in the routing table due to poor configuration (such as not using the **passive interface** command on the network boundary), or due to a malfunctioning router. Because of this it is prudent to authenticate the routing update process running on a router.

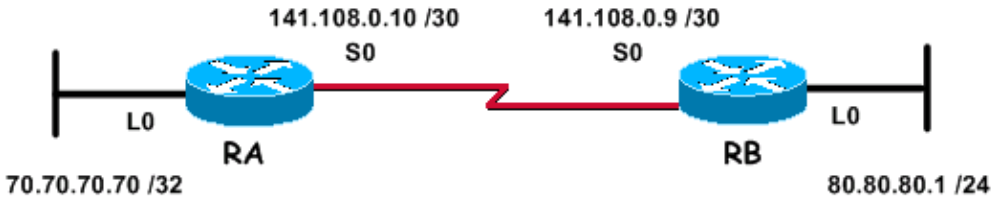
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in the diagram below.



The network above, which is used for the following configuration examples, consists of two routers; router RA and router RB, both of which are running RIP and periodically exchanging routing updates. It is required that this exchange of routing information over the serial link be authenticated.

Configurations

Carry out these steps to configure authentication in RIPv2:

1. Define a key chain with a name.

Note: The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed on that interface.

2. Define the key or keys on the key chain.
3. Specify the password or key−string to be used in the key.

   This is the authentication string that must be sent and received in the packets using the routing protocol being authenticated. (In the example given below, the value of the string is 234.)
4. Enable authentication on an interface and specify the key chain to be used.

   Since authentication is enabled on a per interface basis, a router running RIPv2 can be configured for authentication on certain interfaces and can operate without any authentication on other interfaces.
5. Specify whether the interface will use plain text or MD5 authentication.

   The default authentication used in RIPv2 is plain text authentication, when authentication is enabled in the previous step. So, if using plain text authentication, this step is not required.
6. Configure key management (This step is optional).

   Key management is a method of controlling authentication keys. This is used to migrate form one authentication key to another. For more information, refer to the "Manage Authentication Keys" section of Configuring IP Routing Protocol−Independent Features.

Configuring Plain Text Authentication

One of the two ways in which RIP updates can be authenticated is using plain text authentication. This can be configured as shown in the tables below.

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
```

For detailed information on the commands, refer to the Cisco IOS IP command reference.

Configuring MD5 Authentication

MD5 authentication is an optional authentication mode added by Cisco to the original RFC 1723−defined plain text authentication. The configuration is identical to that for plain text authentication, except for the use of the additional command **ip rip authentication mode md5** . Users must configure router interfaces on both sides of the link for the MD5 authentication method, making sure the key number and key string match on both sides.

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
```

For detailed information on the commands, refer to the Cisco IOS command reference .

Verify

Verifying Plain Text Authentication

This section provides information to confirm your configuration is working properly.

By configuring the routers as shown above, all routing update exchanges will be authenticated before being accepted. This can be verified by observing the output obtained from the **debug ip rip** and **show ip route** commands.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

```
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
```

Using plain text authentication improves the network design by preventing the addition of routing updates originated by routers not meant to take part in the local routing exchange process. However, this type of authentication is not secure. The password (234 in this example) is exchanged in plain text. It can be captured easily and thus exploited. As mentioned before, MD5 authentication must be preferred over plain text authentication when security is an issue.

Verifying MD5 Authentication

By configuring the RA and RB routers as shown above, all routing update exchanges will be authenticated before being accepted. This can be verified by observing the output obtained from the **debug ip rip** and **show ip route** commands.

```
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 authentication uses the one−way, MD5 hash algorithm, acknowledged to be a strong hashing algorithm. In this mode of authentication, the routing update does not carry the password for the purpose of authentication. Rather, a 128−bit message, generated by running the MD5 algorithm on the password, and the message are sent along for authentication. Thus, it is recommended to use MD5 authentication over plain text authentication since it is more secure.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

The **debug ip rip** command can be used for troubleshooting RIPv2 authentication−related problems.

Note: Before issuing **debug** commands, see Important Information on Debug Commands.

Note: Following is an example of the **debug ip rip** command output, when any of the authentication−related parameters that need to be identical between the neighboring routers is not matching. This may result in either

one or both the routers not installing the received routes in their routing table.

```
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)
```

The following output from the **show ip route** command shows that the router is not learning any routes via RIP:

```
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#
```

Note 1: When using plain text authentication mode, make sure that the following parameters are matching on neighboring routers for successful authentication.

- Key-string
- Authentication mode

Note 2: When using MD5 authentication mode, for successful authentication make sure that the following parameters are matching on neighboring routers.

- Key-string
- Key number
- Authentication mode

Related Information

- **Introduction to Routing Information Protocol (RIP)**
- **Configuring RIP**
- **Configuring IP Routing Protocols−Independent Features**
- **RIP Commands**
- **Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3**
- **RIP Technology Support Page**
- **IP Routing Protocols Technology Support Page**
- **Technical Support − Cisco Systems**

Updated: Aug 10, 2005 Document ID: 13719
