Title:
Cisco CCNP / BSCI Exam Tutorial: RIP Update Packet Authentication

Word Count:
536

Summary:
Configuring RIP update packet authentication is an important skill for the BSCI exam and the real world! Learn how to perform this tricky configuration from Chris Bryant, CCIE #12933.

Keywords:
Ccnp, bsci, exam, rip, packet, authentication, clear, text, md5, interface, command, pass, free, tutorial, certification

Article Body:
When you earned your CCNA, you thought you learned everything there is to know about RIP. Close, but not quite! There are some additional details you need to know to pass the BSCI exam and get one step closer to the CCNP exam, and one of those involves RIP update packet authentication.

You're familiar with some advantages of using RIPv2 over RIPv1, support for VLSM chief among them. But one advantage that you're not introduced to in your CCNA studies is the ability to configure routing update packet authentication.

You have two options, clear text and MD5. Clear text is just that - a clear text password that is visible by anyone who can pick a packet off the wire. If you're going to go to the trouble of configuring update authentication, you should use MD5. The MD stands for "Message Digest", and this is the algorithm that produces the hash value for the password that will be contained in the update packets.

Not only must the routers agree on the password, they must agree on the authentication method. If one router sends an MD5-hashed password to another router that is configured for clear-text authentication, the update will not be accepted. debug ip rip is a great command for troubleshooting authenticated updates.

R1, R2, and R3 are running RIP over a frame relay cloud. Here is how RIP authentication would be configured on these three routers.

R1#conf t

```
R1(config)#key chain RIP

< The key chain can have any name. >

R1(config-keychain)#key 1

< Key chains can have multiple keys. Number them carefully when using multiples.
>

R1(config-keychain-key)#key-string CISCO

< This is the text string the key will use for authentication. >


R1(config)#int s0

R1(config-if)#ip rip authentication mode text

< The interface will use clear-text mode. >

R1(config-if)#ip rip authentication key-chain RIP

< The interface is using key chain RIP, configured earlier. >

R2#conf t

R2(config)#key chain RIP

R2(config-keychain)#key 1

R2(config-keychain-key)#key-string CISCO

R2(config)#int s0.123

R2(config-subif)#ip rip authentication mode text

R2(config-subif)#ip rip authentication key-chain RIP

R3#conf t

R3(config)#key chain RIP

R3(config-keychain)#key 1
```

```
R3(config-keychain-key)#key-string CISCO

R3(config)#int s0.31

R3(config-subif)#ip rip authentication mode text

R3(config-subif)#ip rip authentication key-chain RIP
```

To use MD5 authentication rather than clear-text, simply replace the word "text" in the ip rip authentication mode command with md5.

Here's what a successfully authentication RIPv2 packet looks like, courtesy of debug ip rip. Clear-text authentication is in effect and the password is "cisco".

```
3d04h: RIP: received packet with text authentication cisco

3d04h: RIP: received v2 update from 150.1.1.3 on Ethernet0

3d04h: 100.0.0.0/8 via 0.0.0.0 in 1 hops

3d04h: 150.1.2.0/24 via 0.0.0.0 in 1 hops
```

Here's what it looks like when the remote device is set for MD5 authentication and the local router is set for clear-text. You'll also see this message if the password itself is incorrect.

```
3d04h: RIP: ignored v2 packet from 150.1.1.3 (invalid authentication)
```

"Debug ip rip" may be a simple command as compared to the debugs for other protocols. but it's also a very powerful debug. Start using debugs as early as possible in your Cisco studies to learn how router commands really work!