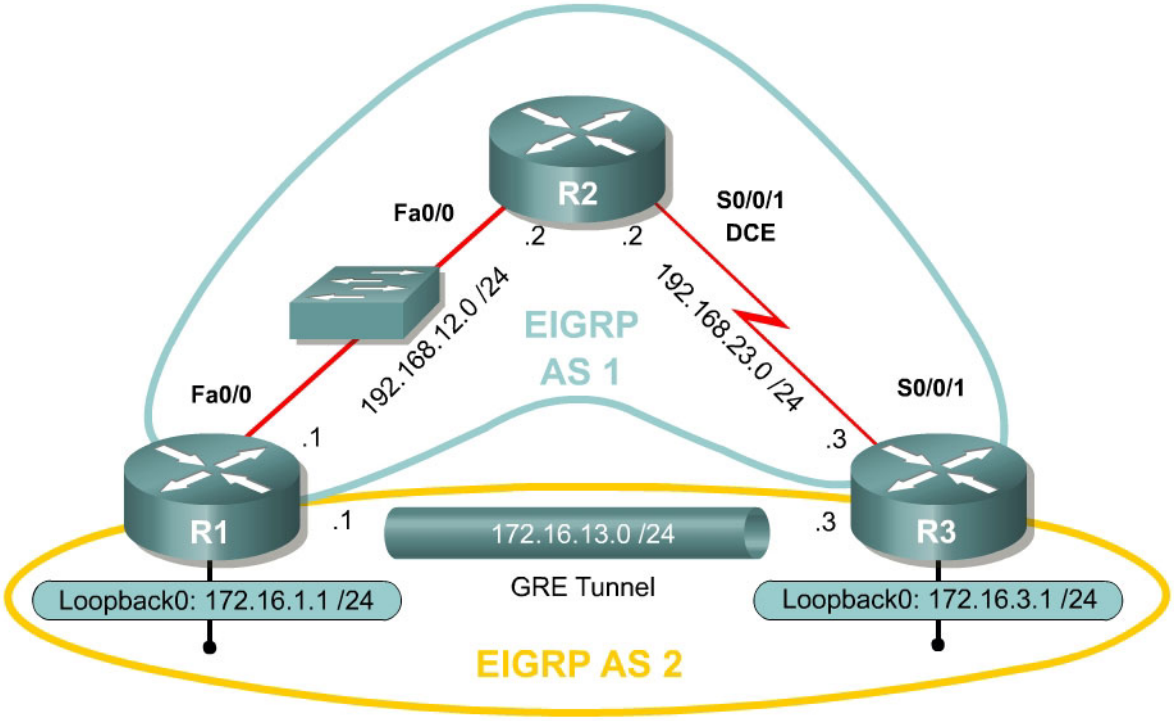
Lab 3.7 Configuring a Secure GRE Tunnel with the IOS CLI

Learning Objectives

- Configure EIGRP on the routers
- Create a GRE tunnel between two routers
- Use IPsec to secure the GRE tunnel

Topology Diagram



Scenario

In this lab, you will use the Cisco Command Line Interface (CLI) to configure a secure generic routing encapsulation (GRE) tunnel using IPsec. You will also use IPsec to secure traffic going through the tunnel. It will help you to have previously completed Labs 3.2 and 3.5 since this lab is a combination of the two. Lab 3.8 also addresses a newer way to configure this type of tunnel, in the configuring IPsec VTIs lab. This newer method combines encryption into the tunnel configuration.

Step 1: Configure Addressing

Configure the interfaces with the addresses as shown in the topology above. Set the clock rate on the appropriate interfaces and issue the **no shutdown**

command as necessary. Verify that you have connectivity across the local subnet with the **ping** command. Do not set up the tunnel interface until the next step.

```
R1# configure terminal
R1(config)# interface loopback0
R1(config-if)# ip address 172.16.1.1 255.255.255.0
R1(config-if)# interface fastethernet0/0
R1(config-if)# ip address 192.168.12.1 255.255.255.0
R1(config-if)# no shutdown

R2# configure terminal
R2(config)# interface fastethernet0/0
R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface serial0/0/1
R2(config-if)# ip address 192.168.23.2 255.255.255.0
R2(config-if)# clockrate 64000
R2(config-if)# no shutdown

R3# configure terminal
R3(config)# interface loopback0
R3(config-if)# ip address 172.16.3.1 255.255.255.0
R3(config-if)# interface serial0/0/1
R3(config-if)# ip address 192.168.23.3 255.255.255.0
R3(config-if)# no shutdown
```

Step 2: Configure EIGRP AS 1

Configure EIGRP AS 1 for the major networks 192.168.12.0/24 and 192.168.23.0/24. Do not include the networks in the diagram falling in the 172.16.0.0/16 range. The Class C networks will serve as the transit networks for the tunnel network. Make sure you disable EIGRP automatic summarization.

```
R1(config)# router eigrp 1
R1(config-router)# no auto-summary
R1(config-router)# network 192.168.12.0

R2(config)# router eigrp 1
R2(config-router)# no auto-summary
R2(config-router)# network 192.168.12.0
R2(config-router)# network 192.168.23.0

R3(config)# router eigrp 1
R3(config-router)# no auto-summary
R3(config-router)# network 192.168.23.0
Verify that R1 and R3 can see the remote transit network with show ip route
```

Step 3: Configure the GRE Tunnel

To configure a GRE tunnel, enter interface configuration mode with the **interface tunnel** *number* command from global configuration mode. For simplicity, use tunnel number 0 on both routers. Next, configure an IP address with **ip address** *address mask* the way you would on any other interface. Finally, assign a source and destination address for the tunnel with **tunnel source** *address* and **tunnel destination** *address*, respectively. The source can also be specified by interface. These addresses specify the endpoints of the

tunnel, so our GRE traffic will be encapsulated with the source address and decapsulated at the destination address. You will not need to configure a tunnel mode because the default tunnel mode is GRE.

```
R1(config)# interface tunnel 0
R1(config-if)# ip address 172.16.13.1 255.255.255.0
R1(config-if)# tunnel source fastethernet0/0
R1(config-if)# tunnel destination 192.168.23.3

R3(config)# interface tunnel0
R3(config-if)# ip address 172.16.13.3 255.255.255.0
R3(config-if)# tunnel source serial0/0/1
R3(config-if)# tunnel destination 192.168.12.1
```

Verify that you can **ping** across the tunnel to the other side. If you can do this, you have successfully set up the tunnel.

```
R1# ping 172.16.13.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/69/72 ms

R3# ping 172.16.13.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.13.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/68/72 ms
```

With what source and destination IP address are these packets sent out of the FastEthernet0/0 interface on R1? Why?

What IP protocol number do these packets have?

Step 4: Configure EIGRP AS 2 over the Tunnel

Now that you set up the GRE tunnel, implement routing through it the way you would any other interface. Configure EIGRP AS 2 to route the entire 172.16.0.0/16 major network. Disable automatic summarization. Remember

that R2 is not participating in this routing process and will not need to be configured with EIGRP AS 2.

```
R1(config)# router eigrp 2
R1(config-router)# no auto-summary
R1(config-router)# network 172.16.0.0

R3(config)# router eigrp 2
R3(config-router)# no auto-summary
R3(config-router)# network 172.16.0.0
```

You should observe EIGRP neighbor adjacencies become active with messages logged to the console. If not, troubleshoot by ensuring that you can ping from 192.168.12.1 to 192.168.23.3 and vice versa. Also check that you have configured the tunnel interfaces above correctly.

If you have configured this step correctly, you should be able to ping from R1's loopback interface to R3's loopback successfully.

Step 5: Create IKE Policies and Peers

Configure an Internet Key Exchange (IKE) policy and peer key. Create an IKE policy using the information that follows. If your IOS image doesn't support all of the settings, configure what you can. Just make sure your VPN settings match on both ends of the connection.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 3600

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 3600
```

Of the three authentication methods available, which is considered the weakest?

What is currently the most secure encryption algorithm?

What is currently the most secure hash algorithm?

Which of the Diffie-Hellman groups is considered weakest?

Next, configure each peer using the key “cisco” for Internet Security Association and Key Management Protocol (ISAKMP).

```
R1(config)# crypto isakmp key cisco address 192.168.23.3

R3(config)# crypto isakmp key cisco address 192.168.12.1
```

Step 7: Create IPsec Transform Sets

On both endpoint routers, create an IPsec transform set with the following settings. If your routers do not support these settings, use whichever settings you can. Just keep it consistent on both routers.

```
R1(config)# crypto ipsec transform-set mytrans esp-aes 256 esp-sha-hmac ah-
sha-hmac
R1(cfg-crypto-trans)# exit
R1(config)#

R3(config)# crypto ipsec transform-set mytrans esp-aes 256 esp-sha-hmac ah-
sha-hmac
R3(cfg-crypto-trans)# exit
R3(config)#
```

Step 8: Define the Traffic to be Encrypted

On both endpoint routers, define traffic to be encrypted by IPsec to be GRE traffic with the source and destination as the tunnel endpoint addresses. Remember to keep the correct order of these networks on each router.

```
R1(config)# access-list 101 permit gre host 192.168.12.1 host 192.168.23.3

R3(config)# access-list 101 permit gre host 192.168.23.3 host 192.168.12.1
```

Step 9: Create and Apply Crypto Maps

On both endpoint routers, you will need to create and apply an IPsec crypto map to the outgoing interfaces to encrypt the GRE tunnel traffic. The EIGRP neighbor adjacency may “flap” (go down and then come back up) while the crypto map is configured on one router and not the other.


```
R1(config)# crypto map mymap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set peer 192.168.23.3
R1(config-crypto-map)# set transform-set mytrans
R1(config-crypto-map)# exit
R1(config)# interface fastethernet 0/0
R1(config-if)# crypto map mymap
*Jan 22 07:01:30.147: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R3(config)# crypto map mymap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 192.168.12.1
R3(config-crypto-map)# set transform-set mytrans
R3(config-crypto-map)# interface serial 0/0/1
R3(config-if)# crypto map mymap
*Jan 22 07:02:47.726: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

NOTE: On certain older IOS releases, you may also need to apply the crypto map to the tunnel interface.

Step 10: Verify Crypto Operation

Verify that the number of packets is increasing by issuing the command **show crypto ipsec sa**, and monitoring the number of packet differences after issuing the command on a router.

```
R1# show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: mymap, local addr 192.168.12.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.12.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.23.3/255.255.255.255/47/0)
   current_peer 192.168.23.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
...
```

Wait a few seconds, then issue the **show crypto ipsec sa** command again.

```
R1# show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: mymap, local addr 192.168.12.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.12.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.23.3/255.255.255.255/47/0)
   current_peer 192.168.23.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
```


...

Although you have not issued another ping, packets are still being encrypted in the GRE tunnel and in the IPsec VPN.

Based on your knowledge of the configuration on R1 and R3, what packets are causing the packet count to increment as time passes?

For more crypto verification commands, consult Lab 3.5.

Challenge: Use Wireshark to Monitor Encryption of Traffic

You can observe packets on the wire using Wireshark and see how their content looks unencrypted and then encrypted. To do this, first configure a SPAN session on the switch and open up Wireshark on a host attached to the SPAN destination port. You can use the host that you used for SDM because you don't need it anymore to configure the VPNs. If you do not know how to do this, refer to Lab 3.3: Configuring Wireshark and SPAN.

Next, you will remove the **crypto map** statements on R1 and R3. View the current configuration on the FastEthernet0/0 interface on R1 and Serial0/0/1 as shown below.

Then, issue the **no crypto map** *name* command in interface configuration mode to remove the ISAKMP security association. The router may issue a warning that ISAKMP is now off.

```
R1# show run interface fastethernet 0/0
Building configuration...

Current configuration : 120 bytes
!
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
 duplex auto
 speed auto
 crypto map mymap
end

R1# configure terminal
R1(config)# interface fastethernet0/0
R1(config-if)# no crypto map mymap
*Jan 16 06:02:58.999: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF

R3# show run interface serial 0/0/1
Building configuration...

Current configuration : 91 bytes
```



```
!
interface Serial0/0/1
 ip address 192.168.23.3 255.255.255.0
 crypto map mymap
end

R3# configure terminal
R3(config)# interface serial0/0/1
R3(config-if)# no crypto map mymap
*Jan 16 06:05:36.038: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
```

The traffic we want to sniff will be telnet traffic, so enable telnet access and an enable password on R3 if you haven't already.

```
R3(config)# enable secret cisco
R3(config)# line vty 0 4
R3(config-line)# password cisco
R3(config-line)# login
```

Have Wireshark start sniffing packets that it receives via the SPAN session.

Choose **Capture > Interfaces...**. Then click the **Start** button associated with the interface connected to the SPAN destination port. SPAN should start capturing packets on the line, so you can now telnet from R1's loopback to R3's loopback. To send telnet traffic, use the **telnet** *destination* command.

Do you need to use the ***/source*** attribute in the telnet command? Explain.

First, begin capturing packets using Wireshark. Then, begin the telnet session. Once you are connected to R3, issue a command or two and then log out. The packets will be routed through the tunnel interface towards the loopback on R3, so Wireshark will display the GRE packets.

```
R1# telnet 172.16.3.1
Trying 172.16.3.1 ... Open


User Access Verification

Password:
R3> enable
Password:
R3# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES unset  administratively down
down
```



```
FastEthernet0/1            unassigned      YES unset  administratively down
down
Serial0/0/0                unassigned      YES unset  administratively down
down
Serial0/0/1                192.168.23.3    YES manual up                    up
Serial0/1/0                unassigned      YES unset  administratively down
down
Serial0/1/1                unassigned      YES unset  administratively down
down
Loopback0                  172.16.3.1      YES manual up                    up
Tunnel0                    172.16.13.3     YES manual up                    up
R3# exit

[Connection to 172.16.3.1 closed by foreign host]
R1#
```

Now, take a look at the output. Notice that Wireshark is smart enough to classify these packets as telnet traffic, even though the actual packets are GRE. Looking in the middle pane in Wireshark, it will show the multiple layers of encapsulation, including the GRE information. Notice that since you disabled encryption, you can easily read the plaintext strings of the telnet session in Wireshark.

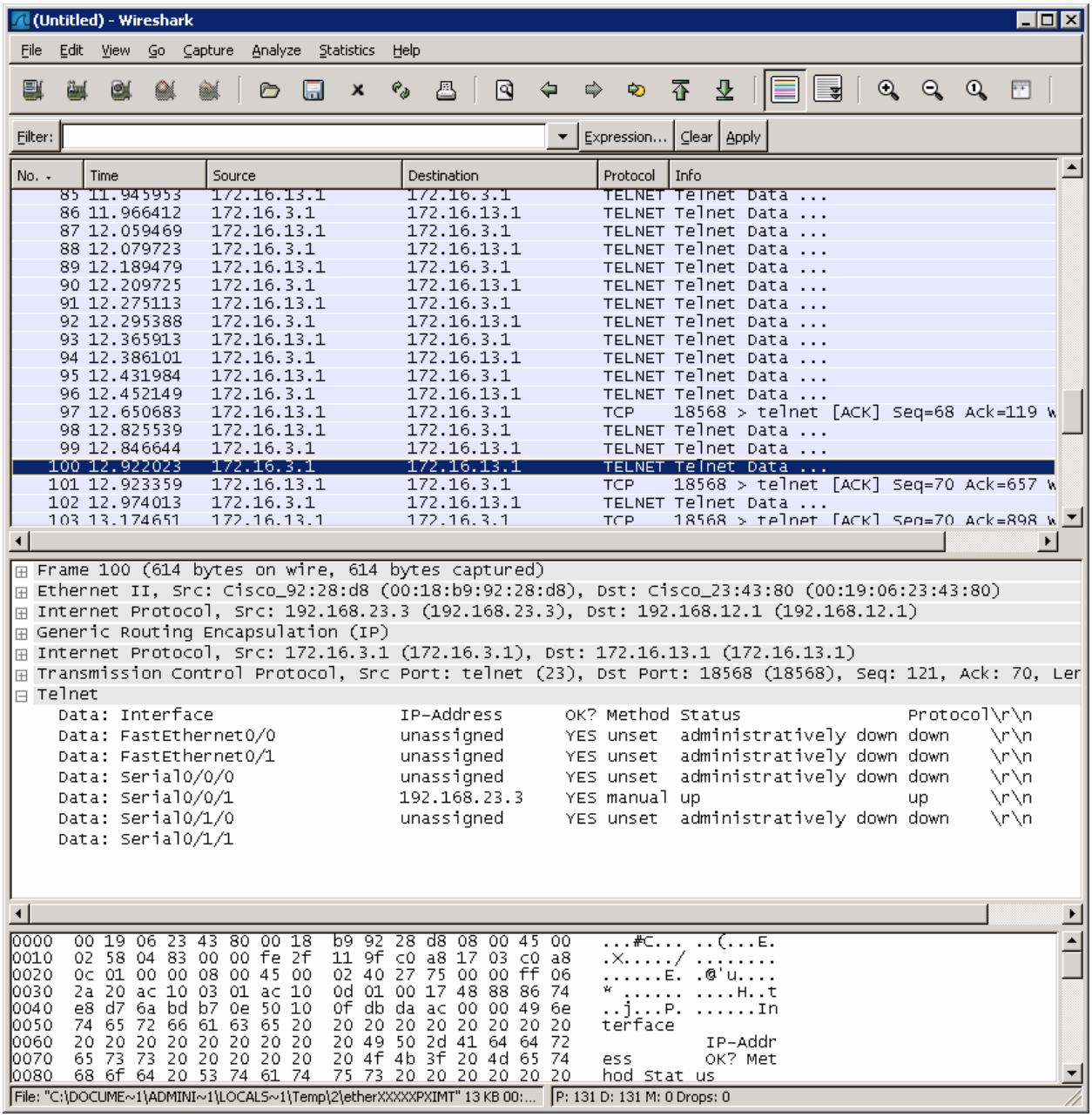


Figure 11-1: Detailed Packet Data on Telnet String Sent From R1

Based on this output, you can see how easy it is for someone who is in the path of sensitive data to view unencrypted or clear text traffic.

Now, you will reapply the cryptography settings on R1 and R3 and begin a telnet session from R1 to R3 as before.

Begin by reapplying the crypto maps you removed earlier on R1 and R3.

```
R1(config)# interface fastethernet 0/0
R1(config-if)# crypto map mymap
```



```
R3(config)# interface serial0/0/1
R3(config-if)# crypto map mymap
```

Start the packet capturing again in Wireshark, and then issue the same telnet sequence that you did previously.

```
R1# telnet 172.16.3.1
Trying 172.16.3.1 ... Open


User Access Verification

Password:
R3> enable
Password:
R3# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES unset  administratively down
down
FastEthernet0/1            unassigned      YES unset  administratively down
down
Serial0/0/0                unassigned      YES unset  administratively down
down
Serial0/0/1                192.168.23.3    YES manual up                    up
Serial0/1/0                unassigned      YES unset  administratively down
down
Serial0/1/1                unassigned      YES unset  administratively down
down
Loopback0                  172.16.3.1      YES manual up                    up
Tunnel0                    172.16.13.3     YES manual up                    up
R3#exit

[Connection to 172.16.3.1 closed by foreign host]
R1#
```

End your Wireshark capture when you are finished with the telnet session.

As far as the user is concerned, the telnet session seems the same with and without encryption. However, the packet capture from Wireshark shows that the VPN is actively encapsulating and encrypting packets.

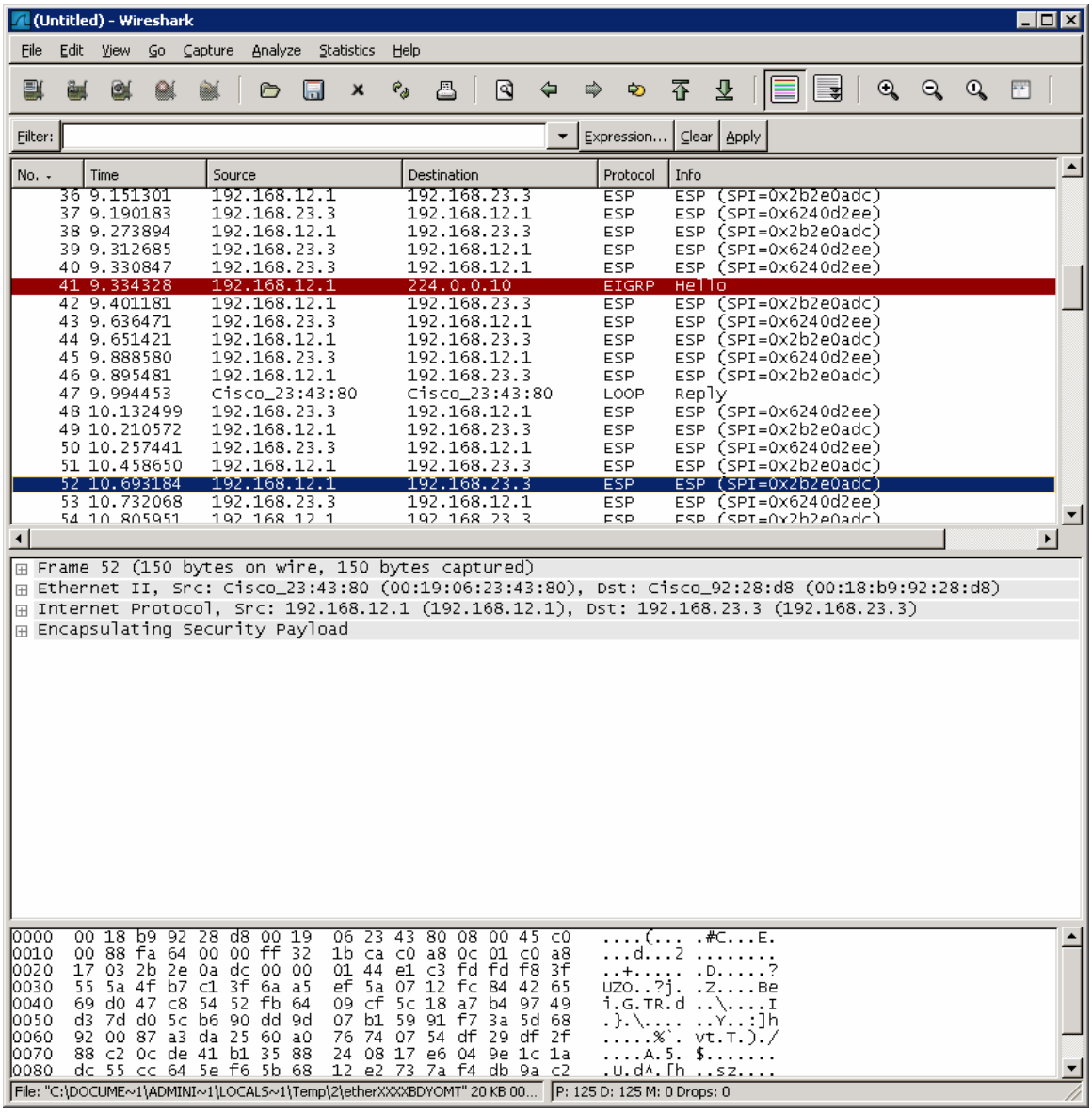


Figure 11-2: Detailed Packet Data on Encrypted Telnet String Sent From R1

Notice that the protocol is not telnet (TCP port 23), but the Encapsulating Security Protocol (ESP, IP protocol number 50). Remember, all traffic here matches the IPSec access list.

Also, notice that the source and destination are not the actual source and destination of the addresses participating in this telnet conversation. Rather, they are the endpoints of the VPN.

Finally, and most important, if you look at the contents of these packets in Wireshark, no matter how you try to format or filter them, you will not be able to see what data was originally inside.

The encryption suite provided by IPSec successfully secures data through authentication, encryption, and data-integrity services.

Final Configurations

```
R1# show run
!
hostname R1
!
crypto isakmp policy 10
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 192.168.23.3
!
crypto ipsec transform-set mytrans ah-sha-hmac esp-aes 256 esp-sha-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 192.168.23.3
 set transform-set mytrans
 match address 101
!
interface Tunnel0
 ip address 172.16.13.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 192.168.23.3
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
 crypto map mymap
 no shutdown
!
router eigrp 1
 network 192.168.12.0
 no auto-summary
!
router eigrp 2
 network 172.16.0.0
 no auto-summary
!
access-list 101 permit gre host 192.168.12.1 host 192.168.23.3
end

R2# show run
hostname R2
!
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 192.168.23.2 255.255.255.0
 clock rate 64000
 no shutdown
!
router eigrp 1
 network 192.168.12.0
 network 192.168.23.0
 no auto-summary
```



```
!
end

R3# show run
hostname R3
!
enable secret 5 $1$kkTj$cIYDuP2yz3vA1ARGVwxd11
!
crypto isakmp policy 10
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 192.168.12.1
!
crypto ipsec transform-set mytrans ah-sha-hmac esp-aes 256 esp-sha-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 192.168.12.1
 set transform-set mytrans
 match address 101
!
interface Loopback0
 ip address 172.16.3.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.13.3 255.255.255.0
 tunnel source Serial0/0/1
 tunnel destination 192.168.12.1
!
interface Serial0/0/1
 ip address 192.168.23.3 255.255.255.0
 crypto map mymap
 no shutdown
!
router eigrp 1
 network 192.168.23.0
 no auto-summary
!
router eigrp 2
 network 172.16.0.0
 no auto-summary
!
access-list 101 permit gre host 192.168.23.3 host 192.168.12.1
!
line vty 0 4
 password cisco
 login
end
```

