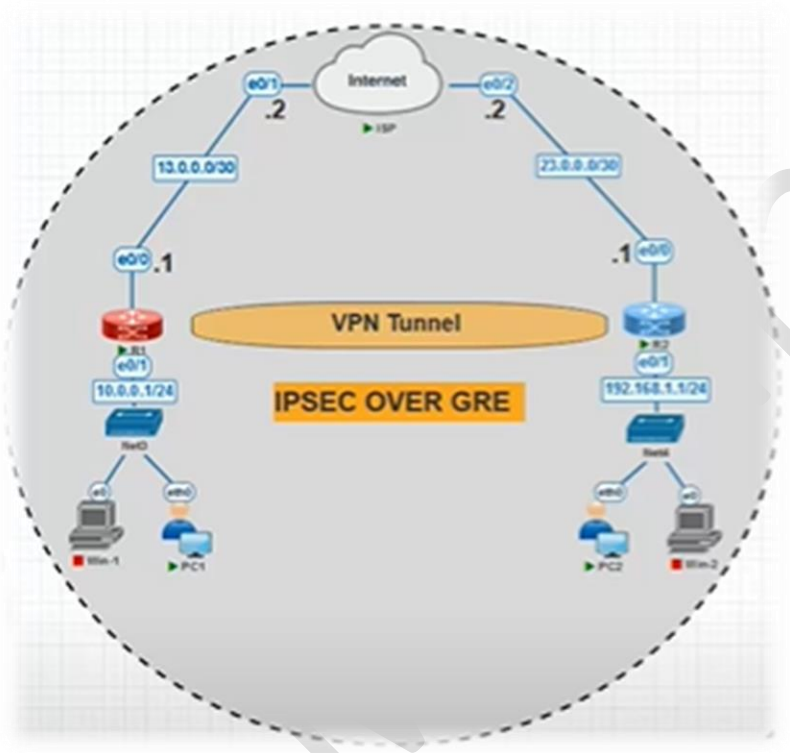
GRE OVER IPsec

Generic Routing Encapsulation



Generic Routing Encapsulation: Its definition simply is running IPsec above GRE

Generic Routing Encapsulation: Create interface tunnel

GRE Vs Legacy vpn

Generic Routing Encapsulation (GRE)	Legacy vpn
GRE is a tunneling protocol used to construct a virtual point-to-point link between two networks, not a security protocol (More than one branch)	Uses site to site
Routing protocol (OSPF-EIGRP- RIP)	The way to work is through Access list

Difference Between IPsec and GRE

IPsec and GRE are two protocols used in computer networking to guarantee data security and privacy. While they have certain similarities, they serve diverse functions and have unique characteristics.

IPsec are used in Virtual Private Networks (VPNs) to offer safe communication over an insecure network like the internet. GRE is a tunneling protocol used to construct a virtual point-to-point link between two networks, not a security protocol.

Read this article to find out more about IPsec and GRE and how they are different from each other.

Fares Mostafa

What is IPsec?

The Internet Protocol Security (IPsec) protocol suite secures IP packets in computer networks. It's often used in virtual private networks (VPNs) to ensure safe communication across an untrustworthy network, like the internet.

IPsec offers three types of security: secrecy, integrity, and authentication. Encryption ensures that data transported across the network is not visible to unauthorized parties, ensuring confidentiality. Integrity is preserved by employing cryptographic methods that prevent data tampering during transmission. Authentication is given via digital certificates or pre-shared keys, which ensure that only authorized parties can access the network.

IPsec has two modes of operation: transport mode and tunnel mode. Transport Mode encrypts only the content of an IP packet, whereas Tunnel Mode encrypts the complete IP packet, including the IP header. Tunnel mode is typically used in VPNs to provide a secure link between two networks, whereas transport mode is used to secure individual hosts or devices.

IPsec is a strong and adaptable protocol suite that ensures the security of IP packets in computer networks. Its use is critical for guaranteeing secure communication in today's linked world, when dangers to data security and privacy abound.

What is GRE?

GRE (Generic Routing Encapsulation) is a computer networking tunneling technology that is used to encapsulate one protocol inside another. It is not a security protocol like IPSEC but rather a versatile protocol for establishing a virtual point-to-point connection between two networks.

GRE encapsulates data packets within IP packets, allowing them to travel through networks that do not support the original protocol. It can encapsulate a variety of protocols, such as IP, IPX, and AppleTalk. This adaptability makes it a popular choice for enterprises with a wide range of networking needs.

GRE works by appending an extra IP header to the original IP packet. The old packet becomes the payload of the new packet, which is subsequently forwarded through the network. The additional IP header is removed when the packet arrives at its destination, and the original packet is transmitted to the receiving host.

GRE is often used in VPNs to establish a secure link between two networks. It enables enterprises to connect geographically scattered networks and provide remote access through a secure tunnel. Because it permits private IP addresses to be contained inside public IP addresses, it can also be utilized in circumstances where network address translation (NAT) is necessary.

GRE is a versatile and extensively used technology that enables the encapsulation of many protocols into IP packets. While it does not offer the same level of security as IPSEC, it is a vital component of many networking solutions and is critical for enterprises with a wide range of networking needs.

Difference between Induction IPsec and GRE

The following table highlights the major differences between IPsec and GRE –

Characteristics	IPsec	GRE
Function	IPsec provides security for IP packets.	GRE encapsulates one protocol inside another protocol.
Encryption	Yes	Optional
Integrity Protection	It provides integrity protection.	It doesn't provide the integrity protection.
Authentication	It provides the authentication.	It doesn't provide the authentication.
Modes of Operation	Tunnel and Transport Mode	It doesn't have any modes of operation.

LAB Configuration

Defuel route R-1

```
R1(config)#ip route
R1(config)#ip route 0.0.0.0 0.0.0.0 13.0.0.2
```

R-2

```
R2(config)#ip route
R2(config)#ip route 0.0.0.0 0.0.0.0 23.0.0.2
R2(config)#
```

R-1

Create interface tunnel & set IP address

```
R1(config)#int tun 0
R1(config-if)#
*Sep 29 13:49:55.628: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
R1(config-if)#ip add 12.0.0.1 255.0.0.0
```

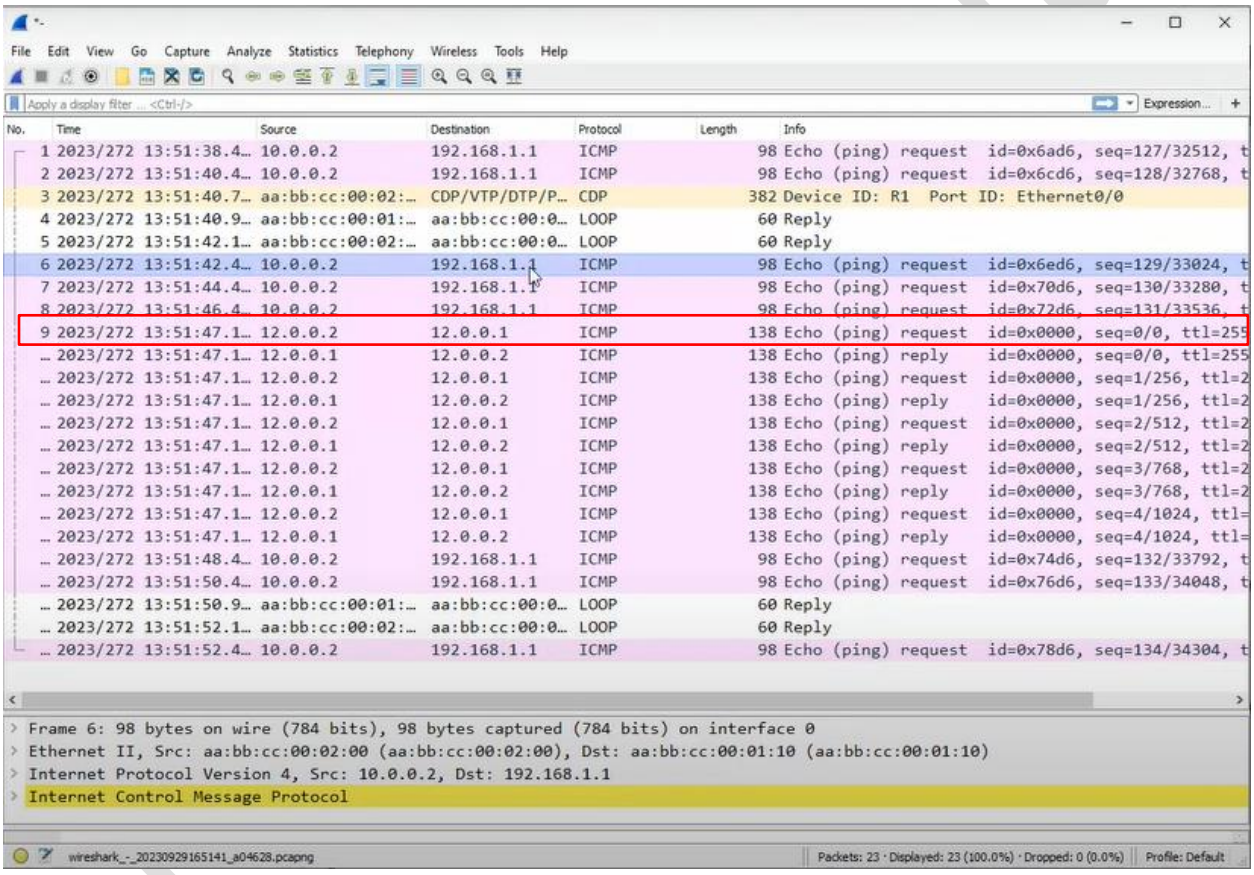
Tunnel source and destination

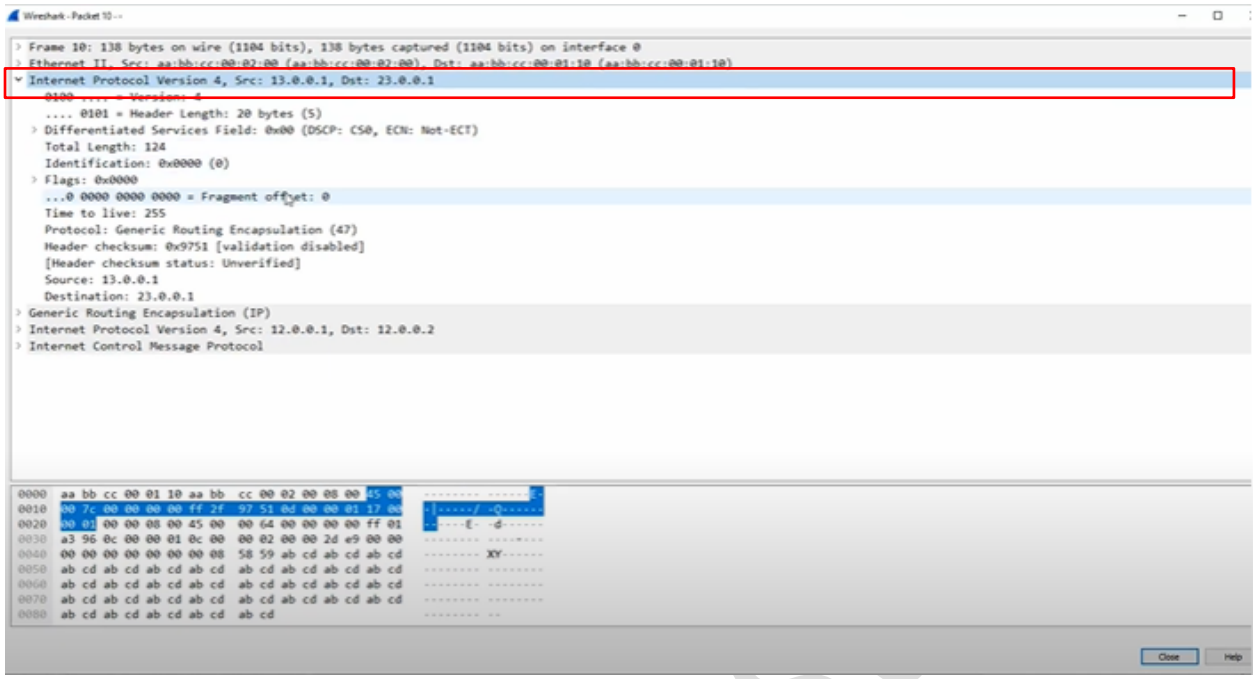
```
R1(config-if)#tun sou e0/0
R1(config-if)#tun des 23.0.0.1
R1(config-if)#
*Sep 29 13:51:01.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
R1(config-if)#
```

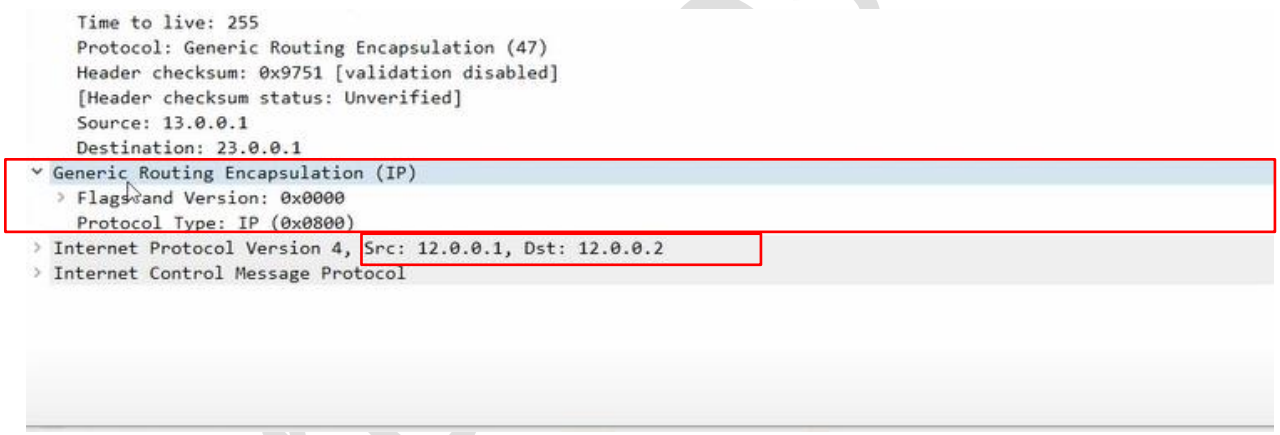
R-2

```
R2(config)#int tun 0
R2(config-if)#ip add 12.0
*Sep 29 13:51:13.917: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
R2(config-if)#ip add 12.0.0.2 255.0.0.0
R2(config-if)#tun sou 23.0.0.1
R2(config-if)#tun des 13.0.0.1
R2(config-if)#
R2(config-if)#
```

```
R2(config-if)#do pin 12.0.0.1 sou 12.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 12.0.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R2(config-if)#
```







R-1

Up routing Protocol

```
R1(config)#router eig 100
R1(config-router)#net 12.0.0.0
R1(config-router)#net 10.0.0.0
R1(config-router)#
```

R-2

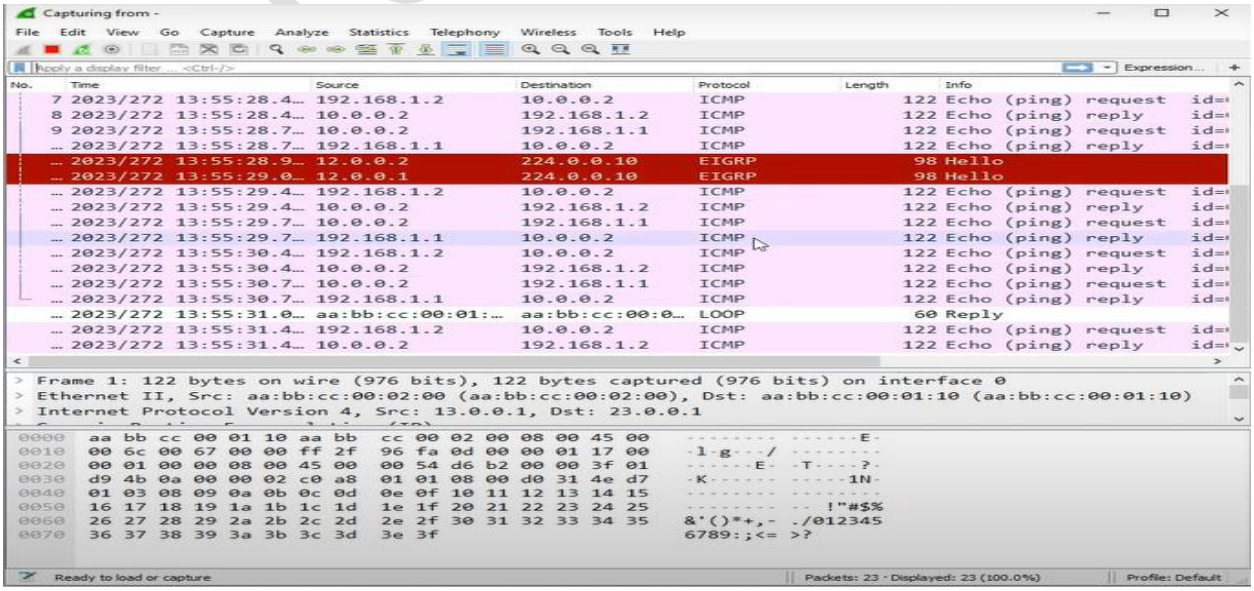
```
R2(config-if)#router eig 100
R2(config-router)#net 12.0.0.0
```

```
R2(config-router)#net 19
*Sep 29 13:54:47.103: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 12.0.0.1 (Tunnel0) is up: new adjacency
R2(config-router)#net 192.168.1.0
R2(config-router)#
R2(config-router)#do sh ip oru eig
                                 ^
% Invalid input detected at '^' marker.

R2(config-router)#do sh ip rou eig
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 23.0.0.2 to network 0.0.0.0

      10.0.0.0/24 is subnetted, 1 subnets
D        10.0.0.0 [90/26905600] via 12.0.0.1, 00:00:10, Tunnel0
R2(config-router)#
```

R-1

```
R1(config-router)#do sh ip rou eig
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 13.0.0.2 to network 0.0.0.0

D      192.168.1.0/24 [90/26905600] via 12.0.0.2, 00:00:16, Tunnel0
R1(config-router)#
```

```
84 bytes from 192.168.1.1 icmp_seq=223 ttl=254 time=1.458 ms
84 bytes from 192.168.1.1 icmp_seq=224 ttl=254 time=2.954 ms
84 bytes from 192.168.1.1 icmp_seq=225 ttl=254 time=1.460 ms
84 bytes from 192.168.1.1 icmp_seq=226 ttl=254 time=1.457 ms
84 bytes from 192.168.1.1 icmp_seq=227 ttl=254 time=1.441 ms
84 bytes from 192.168.1.1 icmp_seq=228 ttl=254 time=1.884 ms
```



Fares Mostafa

Up police IPsec

R-1

```
R1(config)#cry isa pol 1
R1(config-isakmp)#au pre
R1(config-isakmp)#au pre-share
R1(config-isakmp)#en
R1(config-isakmp)#encryption a
R1(config-isakmp)#encryption aes 128
R1(config-isakmp)#hs
R1(config-isakmp)#h
R1(config-isakmp)#hash s
R1(config-isakmp)#hash sha256
R1(config-isakmp)#gr 5
R1(config-isakmp)#ex
```

```
R1(config)#cry isa key cisco123 da
R1(config)#cry isa key cisco123 ad
R1(config)#cry isa key cisco123 address 13.0.0.1
```

```
R1(config)#crypto ip
R1(config)#crypto ipsec tr
R1(config)#crypto ipsec transform-set R1set
R1(config)#crypto ipsec transform-set R1set es
R1(config)#crypto ipsec transform-set R1set esp-3
R1(config)#crypto ipsec transform-set R1set esp-3des ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
  <cr>

R1(config)#crypto ipsec transform-set R1set esp-3des
```

```
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
  <cr>

R1(config)#crypto ipsec transform-set R1set esp-3des esp-sha256-hmac
R1(cfg-crypto-trans)#e
```

```
R1(config)#crypto ip
R1(config)#crypto ipsec pr
R1(config)#crypto ipsec profile prof
R1(config)#crypto ipsec profile prof1
R1(ipsec-profile)#set tr
R1(ipsec-profile)#set transform-set R1set
R1(ipsec-profile)#
R1(ipsec-profile)#
```

```
R1(ipsec-profile)#int tun 0
R1(config-if)#tu
R1(config-if)#tunnel pr
R1(config-if)#tunnel protection ip
R1(config-if)#tunnel protection ipsec p
R1(config-if)#tunnel protection ipsec profile prof1
R1(config-if)#
R1(config-if)#
*Sep 29 13:58:12.026: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
R1(config-if)#
*Sep 29 13:58:12.033: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip) vrf/dest_addr=
 /13.0.0.1, src_addr= 23.0.0.1, prot= 47
R1(config-if)#
*Sep 29 13:58:14.877: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Sep 29 13:58:14.877: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 12.0.0.2 (Tunnel0) is down: interface do
wn
```

R-2

Create police

```
R2(config)#
R2(config)#cry isa pol 1
R2(config-isakmp)#au pre
R2(config-isakmp)#au pre-share
R2(config-isakmp)#en
R2(config-isakmp)#encryption a
R2(config-isakmp)#encryption aes 128
R2(config-isakmp)#hs
R2(config-isakmp)#ha
R2(config-isakmp)#hash s
R2(config-isakmp)#hash sha256
R2(config-isakmp)#gr 5
R2(config-isakmp)#ex
R2(config)#cry ip
R2(config)#cry isa
R2(config)#cry isakmp key
R2(config)#cry isakmp key cisco123 ad
R2(config)#cry isakmp key cisco123 address 13.0.0.1
R2(config)#cry
R2(config)#crypto ip
R2(config)#crypto ipsec tr
R2(config)#crypto ipsec transform-set R2set es
R2(config)#crypto ipsec transform-set R2set esp-
```

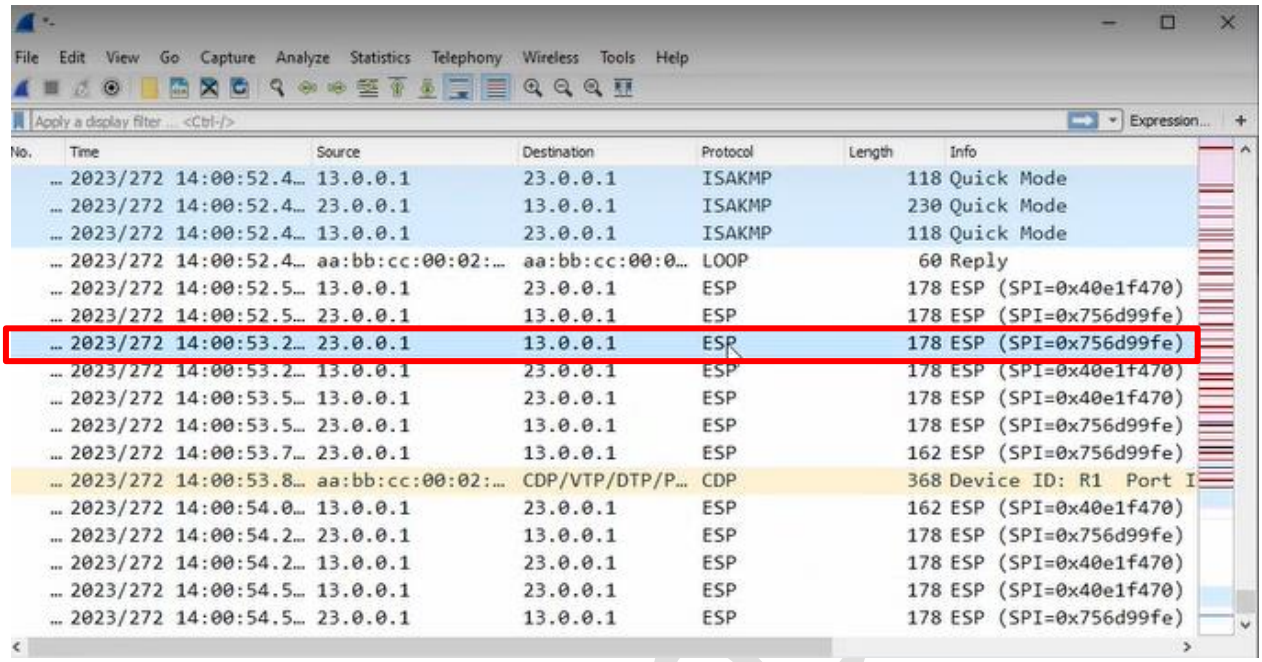
```
R2(config)#crypto ipsec tr
R2(config)#crypto ipsec transform-set R2set es
R2(config)#crypto ipsec transform-set R2set esp-3
R2(config)#crypto ipsec transform-set R2set esp-3des ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
  <cr>

R2(config)#crypto ipsec transform-set R2set esp-3des esp-sha256-hmac
```

```
R2(config)#cry
R2(config)#crypto ip
R2(config)#crypto ipsec p
R2(config)#crypto ipsec profile prof2
R2(ipsec-profile)#set tr
R2(ipsec-profile)#set transform-set R2set
R2(ipsec-profile)#int tun 0
R2(config-if)#tu
R2(config-if)#tunnel pr
R2(config-if)#tunnel protection ip
R2(config-if)#tunnel protection ipsec p
R2(config-if)#tunnel protection ipsec profile prof2
R2(config-if)#
R2(config-if)#
R2(config-if)#
R2(config-if)#
R2(config-if)#ex
*Sep 29 14:00:42.961: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config)#
R2(config)#
```

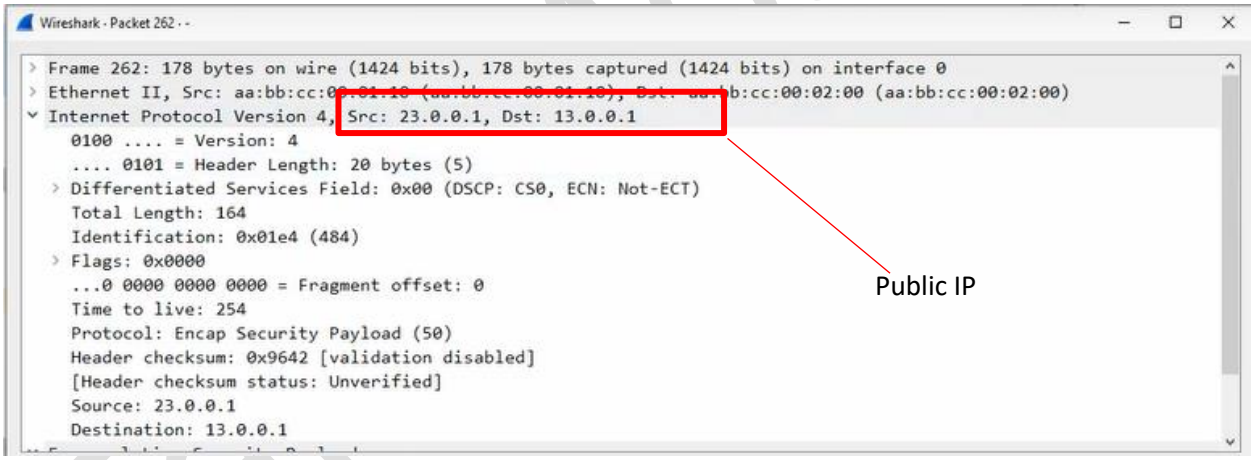
```
R2(config)#
*Sep 29 14:00:44.510: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 12.0.0.1 (Tunnel0) is up: new adjacency
R2(config)#
```

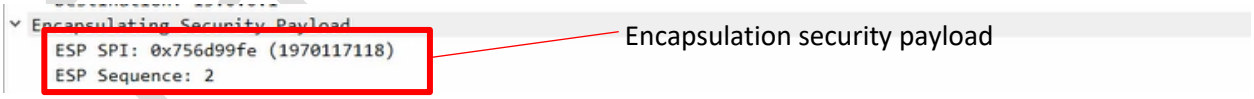
```
84 bytes from 192.168.1.1 icmp_seq=501 ttl=254 time=1.927 ms
84 bytes from 192.168.1.1 icmp_seq=502 ttl=254 time=2.124 ms
84 bytes from 192.168.1.1 icmp_seq=503 ttl=254 time=1.886 ms
84 bytes from 192.168.1.1 icmp_seq=504 ttl=254 time=2.530 ms
84 bytes from 192.168.1.1 icmp_seq=505 ttl=254 time=2.139 ms
84 bytes from 192.168.1.1 icmp_seq=506 ttl=254 time=3.679 ms
```

Encapsulation security payload

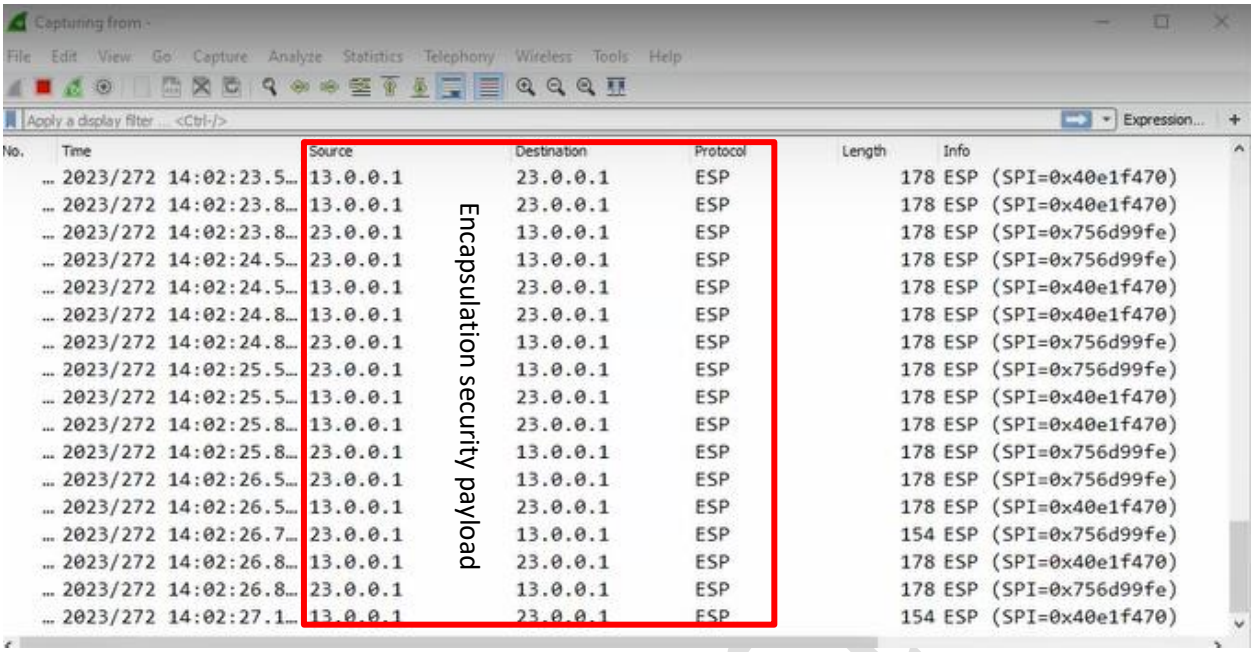


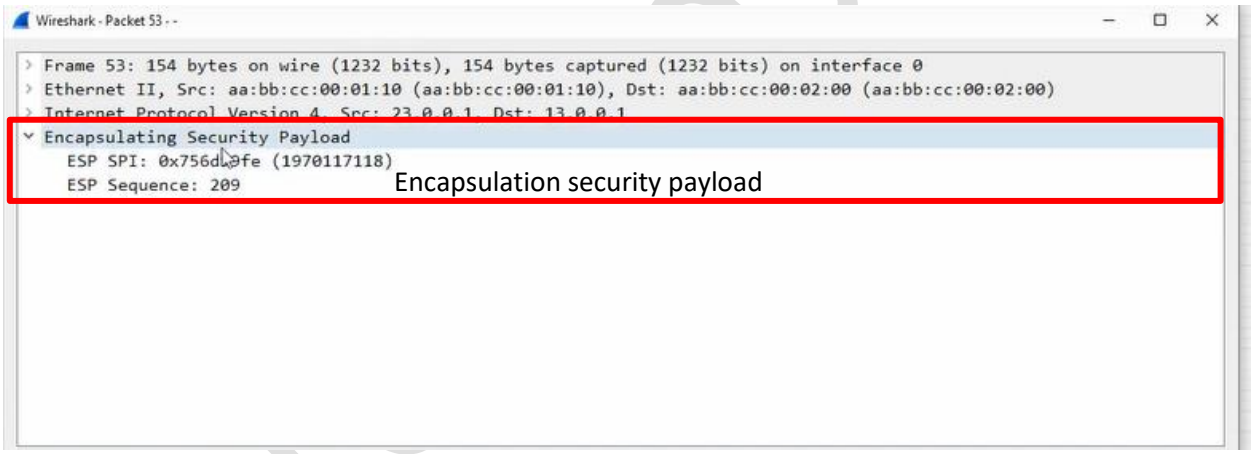
No.	Time	Source	Destination	Protocol	Length	Info
…	2023/272 14:00:52.4…	13.0.0.1	23.0.0.1	ISAKMP	118	Quick Mode
…	2023/272 14:00:52.4…	23.0.0.1	13.0.0.1	ISAKMP	230	Quick Mode
…	2023/272 14:00:52.4…	13.0.0.1	23.0.0.1	ISAKMP	118	Quick Mode
…	2023/272 14:00:52.4…	aa:bb:cc:00:02:…	aa:bb:cc:00:0…	LOOP	60	Reply
…	2023/272 14:00:52.5…	13.0.0.1	23.0.0.1	ESP	178	ESP (SPI=0x40e1f470)
…	2023/272 14:00:52.5…	23.0.0.1	13.0.0.1	ESP	178	ESP (SPI=0x756d99fe)
…	2023/272 14:00:53.2…	23.0.0.1	13.0.0.1	ESP	178	ESP (SPI=0x756d99fe)
…	2023/272 14:00:53.2…	13.0.0.1	23.0.0.1	ESP	178	ESP (SPI=0x40e1f470)
…	2023/272 14:00:53.5…	13.0.0.1	23.0.0.1	ESP	178	ESP (SPI=0x40e1f470)
…	2023/272 14:00:53.5…	23.0.0.1	13.0.0.1	ESP	178	ESP (SPI=0x756d99fe)
…	2023/272 14:00:53.7…	23.0.0.1	13.0.0.1	ESP	162	ESP (SPI=0x756d99fe)
…	2023/272 14:00:53.8…	aa:bb:cc:00:02:…	CDP/VTP/DTP/P…	CDP	368	Device ID: R1 Port I
…	2023/272 14:00:54.0…	13.0.0.1	23.0.0.1	ESP	162	ESP (SPI=0x40e1f470)
…	2023/272 14:00:54.2…	23.0.0.1	13.0.0.1	ESP	178	ESP (SPI=0x756d99fe)
…	2023/272 14:00:54.2…	13.0.0.1	23.0.0.1	ESP	178	ESP (SPI=0x40e1f470)
…	2023/272 14:00:54.5…	13.0.0.1	23.0.0.1	ESP	178	ESP (SPI=0x40e1f470)
…	2023/272 14:00:54.5…	23.0.0.1	13.0.0.1	ESP	178	ESP (SPI=0x756d99fe)

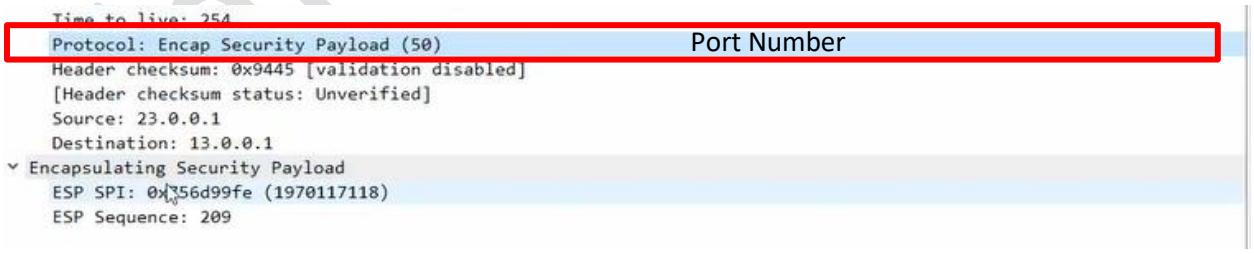




Capture e0/1 ISP







I hope it is useful

Fares Mostafa