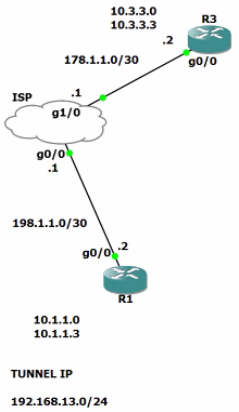
Advance Class-4

VPN



** config the basic ips and loopbacks for all routers

create a default route for R1 and R3

Ip route 0.0.0.0 0.0.0.0 191.1.1.1
Ip route 0.0.0.0 0.0.0.0 178.1.1.1

##Tunnel

#R3

```
R3(config)#int tunnel 1
R3(config-if)#ip add
*Sep 23 20:26:08.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state
to down
R3(config-if)#ip add 192.168.1.3 255.255.255.0
R3(config-if)#tunnel source 178.1.1.2
R3(config-if)#tunnel destination 198.1.1.2
R3(config-if)#exit
*Sep 23 20:26:35.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state
to up
R3(config-if)#exit
R3(config)#
R3(config)#
```

** config the tunnel same on R1 and change destination 171.1.1.2

##create a static-route for tunnel

#R1

```
R1(config)#
R1(config)#ip route 10.3.3.0 255.255.255.252 tunnel 1
R1(config)#
```

```
R1(config)#do ping 10.3.3.3 source 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.2
.....
Success rate is 0 percent (0/5)
R1(config)#
```

** we can’t ping using user [loopbacks]

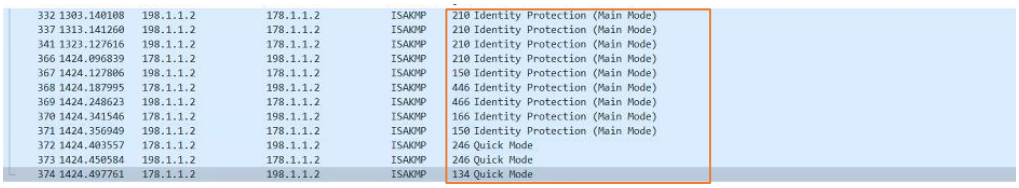
#R3

```
R3(config)#
R3(config)#ip route 10.1.1.0 255.255.255.252 tunnel 1
R3(config)#
R3(config)#dop
```

IP-sec over gre tunnel

```
> Frame 411: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface -, id 0
> Ethernet II, Src: ca:01:31:1c:00:08 (ca:01:31:1c:00:08), Dst: ca:02:22:80:00:08 (ca:02:22:80:
v Internet Protocol Version 4, Src: 198.1.1.2, Dst: 178.1.1.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 180
    Identification: 0x0024 (36)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: Encap Security Payload (50)
    Header Checksum: 0x40ed [validation disabled]
```

** our ip traffic will carried by ESP protocol



332	1303.140108	198.1.1.2	178.1.1.2	ISAKMP	210 Identity Protection (Main Mode)
337	1313.141260	198.1.1.2	178.1.1.2	ISAKMP	210 Identity Protection (Main Mode)
341	1323.127616	198.1.1.2	178.1.1.2	ISAKMP	210 Identity Protection (Main Mode)
366	1424.096839	178.1.1.2	198.1.1.2	ISAKMP	210 Identity Protection (Main Mode)
367	1424.127806	198.1.1.2	178.1.1.2	ISAKMP	150 Identity Protection (Main Mode)
368	1424.187995	178.1.1.2	198.1.1.2	ISAKMP	446 Identity Protection (Main Mode)
369	1424.248623	198.1.1.2	178.1.1.2	ISAKMP	466 Identity Protection (Main Mode)
370	1424.341546	178.1.1.2	198.1.1.2	ISAKMP	166 Identity Protection (Main Mode)
371	1424.356949	198.1.1.2	178.1.1.2	ISAKMP	150 Identity Protection (Main Mode)
372	1424.403557	178.1.1.2	198.1.1.2	ISAKMP	246 Quick Mode
373	1424.450584	198.1.1.2	178.1.1.2	ISAKMP	246 Quick Mode
374	1424.497761	178.1.1.2	198.1.1.2	ISAKMP	134 Quick Mode

**we are having two modes on Phase-1

remove all the things [crypto, tunnel, static-route from R1 and R3]

```
R1(config)#no crypto ipsec profile ABC
R1(config)#no crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
R1(config)#no crypto isakmp key 6 NH address 178.1.1.2
R1(config)#no crypto isakmp policy 30
R1(config)#
R1(config)#
R1(config)#do sh run | sec crypto
R1(config)#
R1(config)#
R1(config)#
R1(config)#do sh run | sec route
ip route 0.0.0.0 0.0.0.0 198.1.1.1
ip route 10.3.3.0 255.255.255.252 Tunnel1
R1(config)#
R1(config)#no ip route 10.3.3.0 255.255.255.252 Tunnel1
R1(config)#
R1(config)#
```

##Directly apply IP-sec without GRE tunnel

#R3

```
access-list 130 permit ip 10.3.3.0 0.0.0.3 10.1.1.0 0.0.0.3
crypto isakmp policy 50
encr aes
hash sha384
authentication pre-share
group 5
crypto isakmp key 6 NH address 198.1.1.2
crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
 mode tunnel
crypto map MYMAP 100 ipsec-isakmp
match address 130
set peer 198.1.1.2
set transform-set TSET
exit
int gig0/0
crypto map MYMAP
```

** apply this on R1 and R3 [change the access-list no, change 171.1.1.2, set peer=171.1.1.2, that's all]