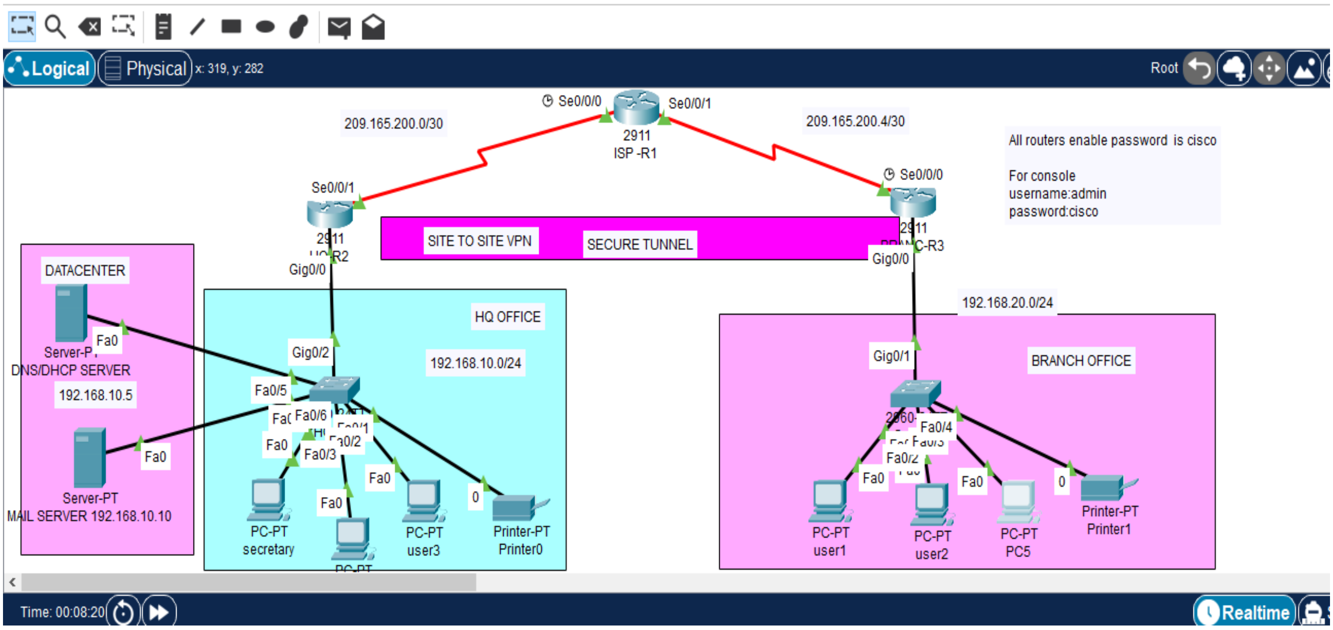
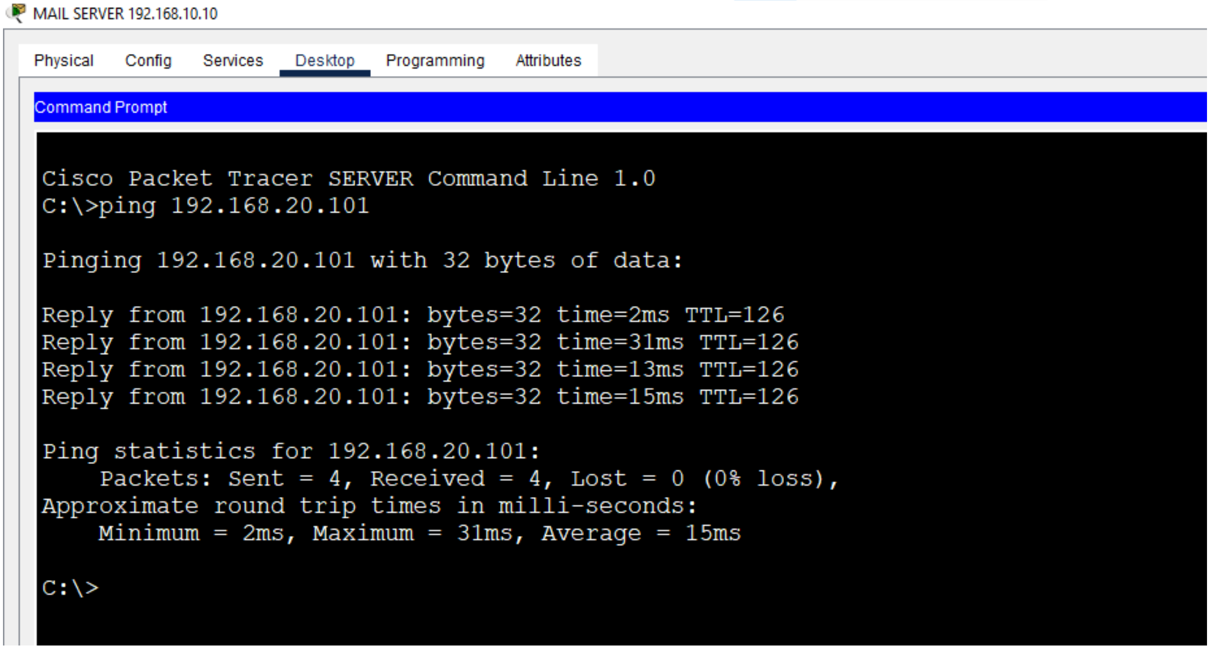
ENTERPRISENETWORK WITH SITE TO SITE VPN

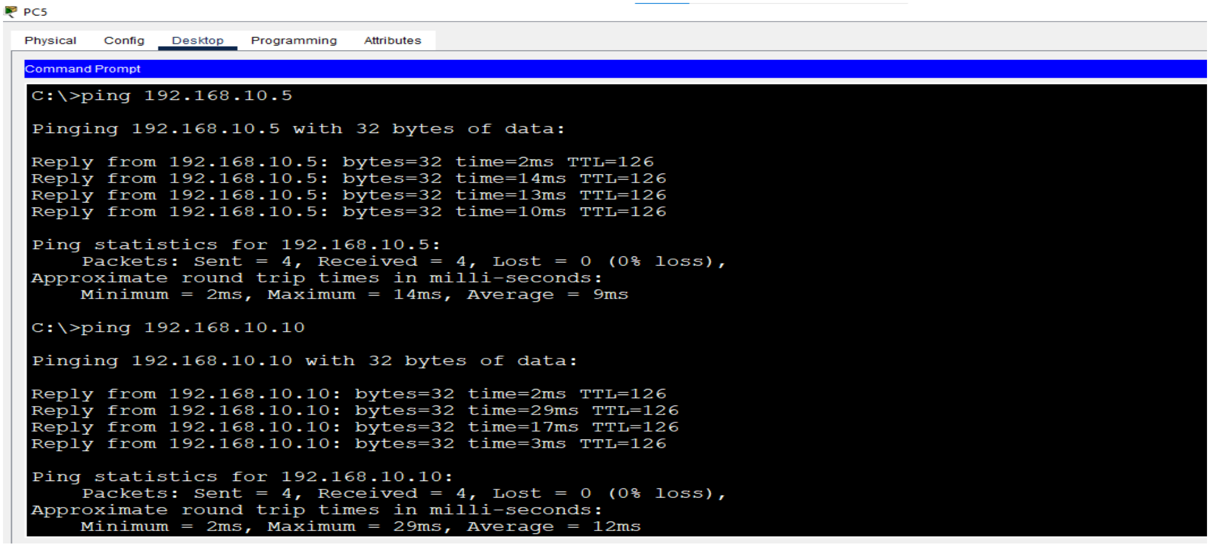


Communication from HQ mail server to Branch LAN



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.20.101

Pinging 192.168.20.101 with 32 bytes of data:

Reply from 192.168.20.101: bytes=32 time=2ms TTL=126
Reply from 192.168.20.101: bytes=32 time=31ms TTL=126
Reply from 192.168.20.101: bytes=32 time=13ms TTL=126
Reply from 192.168.20.101: bytes=32 time=15ms TTL=126

Ping statistics for 192.168.20.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 31ms, Average = 15ms

C:\>
```

LAN pc to Mail server

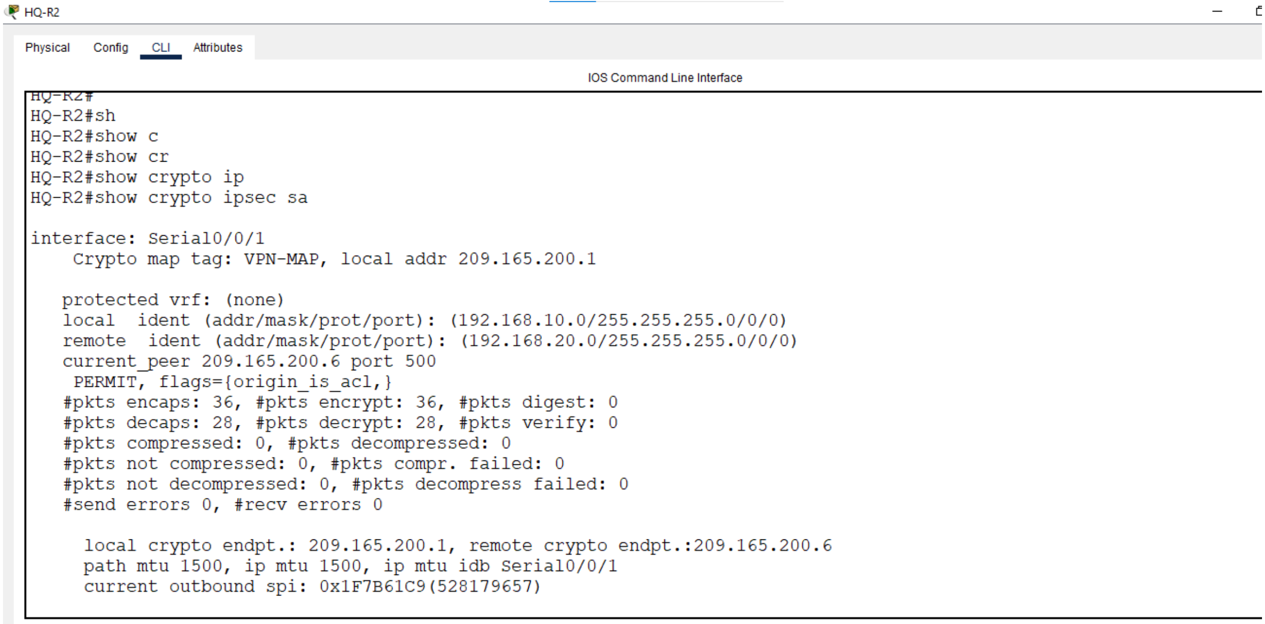


```
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

Reply from 192.168.10.5: bytes=32 time=2ms TTL=126
Reply from 192.168.10.5: bytes=32 time=14ms TTL=126
Reply from 192.168.10.5: bytes=32 time=13ms TTL=126
Reply from 192.168.10.5: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 9ms

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=2ms TTL=126
Reply from 192.168.10.10: bytes=32 time=29ms TTL=126
Reply from 192.168.10.10: bytes=32 time=17ms TTL=126
Reply from 192.168.10.10: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 29ms, Average = 12ms
```

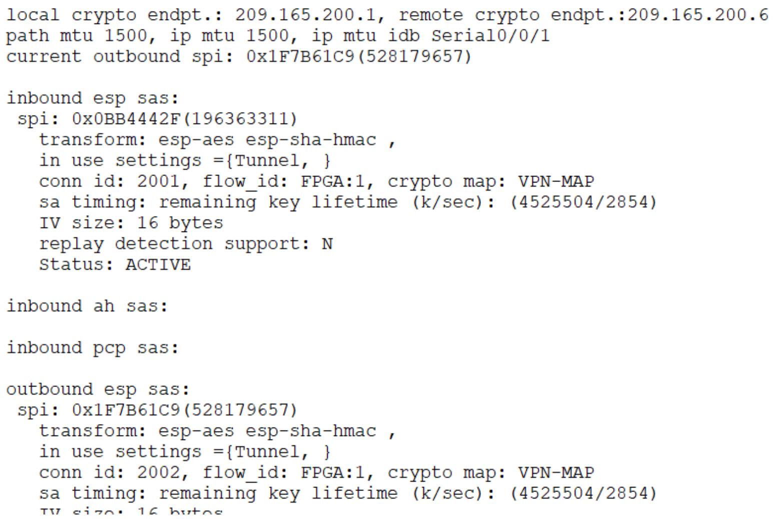
IPSec Vpn Data encryption as from HQ to BRANCH

To verify and see how the Site to site VPN tunnel encrypts data use

Show crypto ipsec sa



```
HQ-R2#
HQ-R2#sh
HQ-R2#show c
HQ-R2#show cr
HQ-R2#show crypto ip
HQ-R2#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: VPN-MAP, local addr 209.165.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   current_peer 209.165.200.6 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 0
   #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.200.1, remote crypto endpt.:209.165.200.6
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x1F7B61C9(528179657)
```



```
local crypto endpt.: 209.165.200.1, remote crypto endpt.:209.165.200.6
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
current outbound spi: 0x1F7B61C9(528179657)

inbound esp sas:
 spi: 0x0BB4442F(196363311)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP
   sa timing: remaining key lifetime (k/sec): (4525504/2854)
   IV size: 16 bytes
   replay detection support: N
   Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x1F7B61C9(528179657)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
   sa timing: remaining key lifetime (k/sec): (4525504/2854)
   IV size: 16 bytes
```