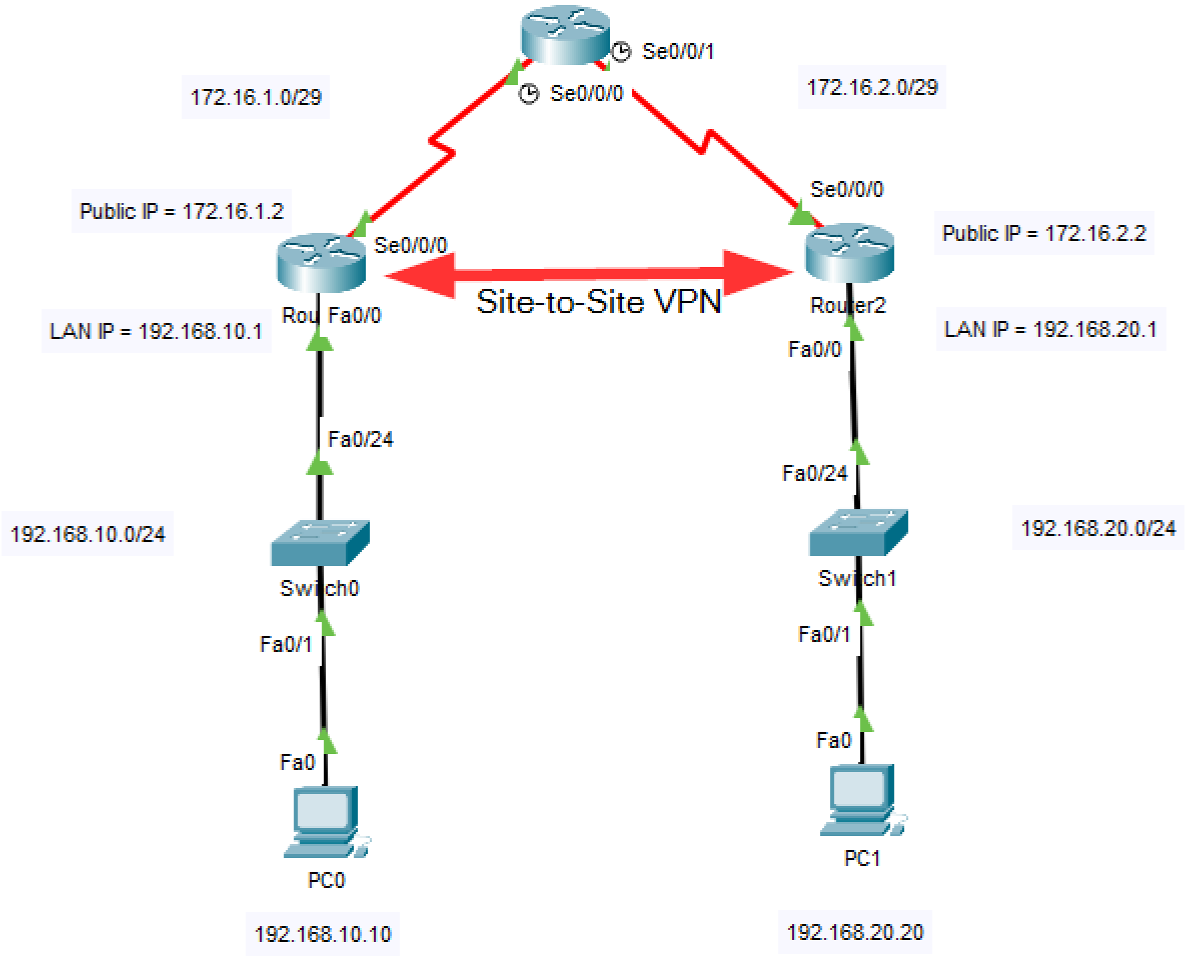
Cisco IOS Site to Site VPN (Router)

Network Topology



In this network configuration a site-to-site VPN between Router1 and Router2 across the link through Router0.

First let's set up the IP and routing information on all three routers as well as the two PCs.

Router0 IP and Routing Configuration Commands

```
Router0>enable
Router0#configure terminal
Router0(config)# interface serial 0/0/0
Router0(config-if)#ip address 172.16.1.1 255.255.255.248
Router0(config-if)#no shutdown
Router0(config-if)#interface serial 0/0/1
Router0(config-if)#ip address 172.16.2.1 255.255.255.248
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#ip route 192.168.10.0 255.255.255.0 172.16.1.2
Router0(config)#ip route 192.168.20.0 255.255.255.0 172.16.2.2
```

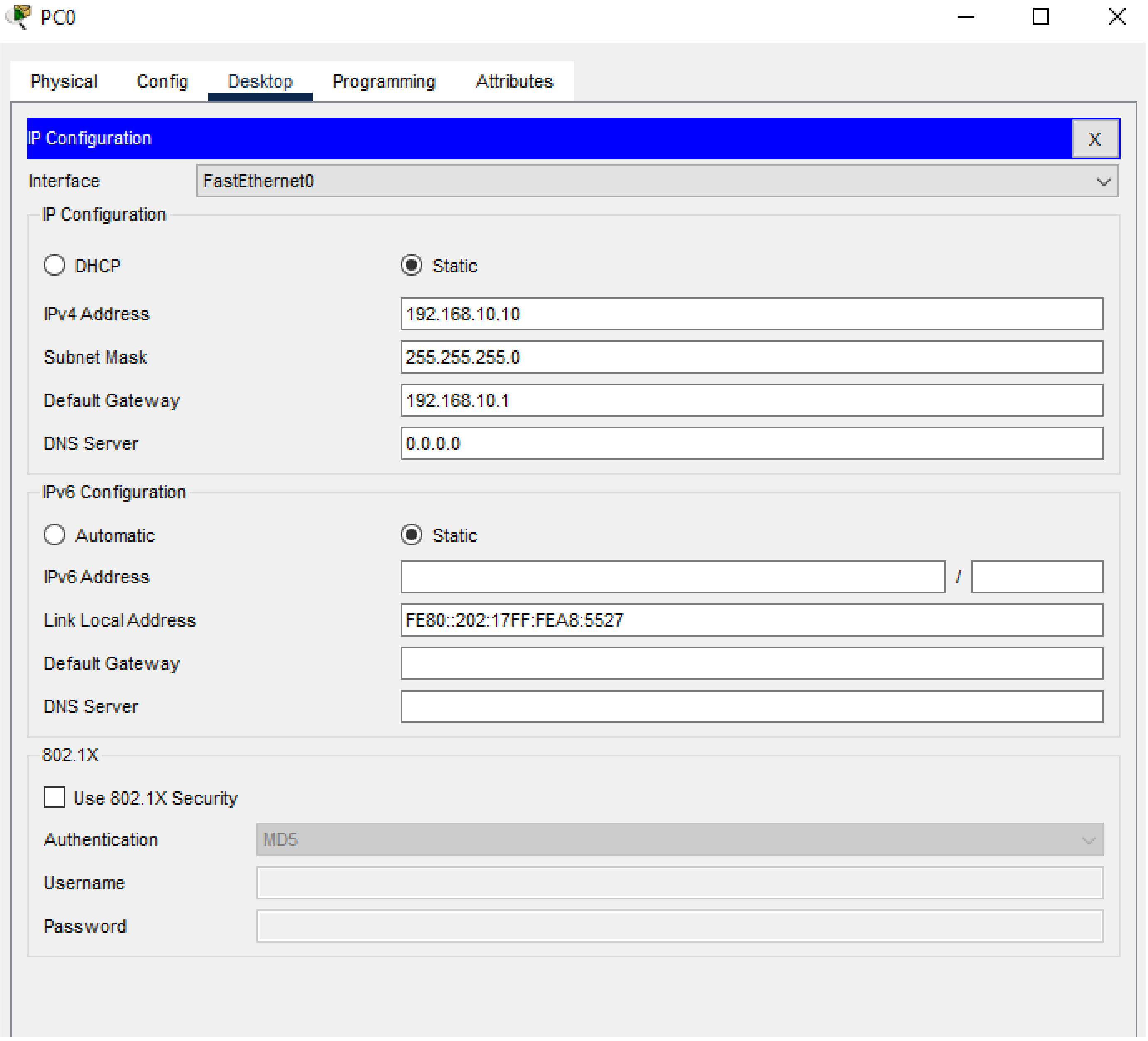
Router1 IP and Routing Configuration Commands

```
Router1>enable
Router1#configure terminal
Router1(config)# interface serial 0/0/0
Router1(config-if)#ip address 172.16.1.2 255.255.255.248
Router1(config-if)#no shutdown
Router1(config-if)#interface fastEthernet 0/0
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

Router2 IP and Routing Configuration Commands

```
Router1>enable
Router1#configure terminal
Router1(config)# interface serial 0/0/0
Router1(config-if)#ip address 172.16.2.2 255.255.255.248
Router1(config-if)#no shutdown
Router1(config-if)#interface fastEthernet 0/0
Router1(config-if)#ip address 192.168.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1
```

PC Computers IP Configuration



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.10.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

IPv6 Configuration

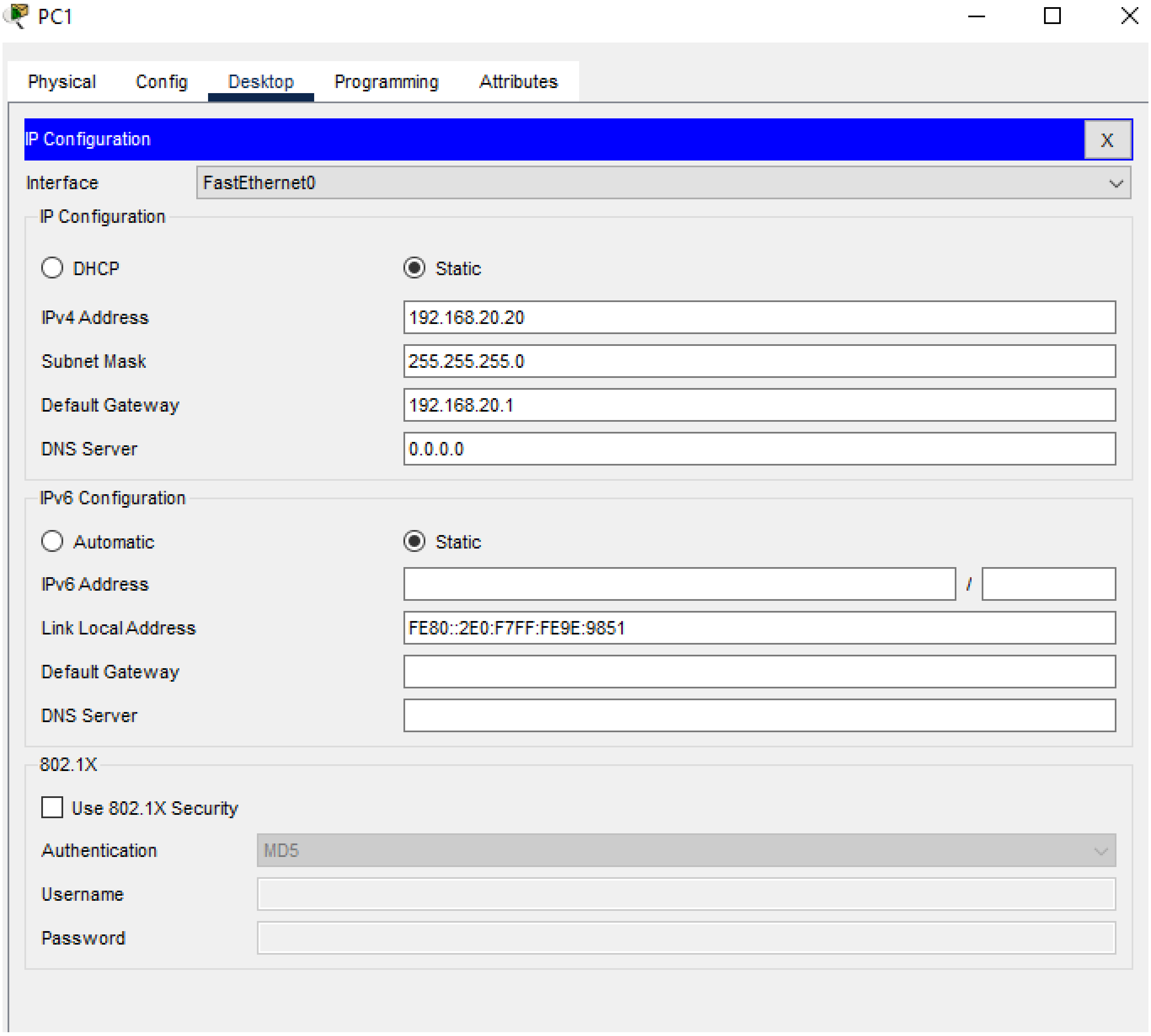
○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::202:17FF:FEA8:5527
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.20.20

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:F7FF:FE9E:9851

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Now that all the routers and PCs have their IP addressing and routing information configured it is time to move on the the specific configuration for enabling the Site-to-Site VPN. This process can be divided into four phases.

Phase 1 - The Key Exchange Setup

Phase 1 Commands	Notes
crypto isakmp enable	
crypto isakmp policy 10	The number can be any number between 1 and 10,000. It identifies the priority of the policy.
encryption aes	this could be 3des but aes is more robust.

hash sha	sha = secure hash algorithm. md5 could be used but sha is more robust.
group 1	Specifies the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. Group 1 is 768-bit
lifetime 3600	Specifies the Security Association (SA) lifetime. The default is 86,400 seconds or 24 hours. As a general rule, a shorter lifetime provides more secure ISAKMP negotiations (up to a point). However, with shorter lifetimes, the security appliance sets up future IPsec SAs more quickly.
authentication pre-share	
crypto isakmp key *ciscokey123* address 172.16.2.2	The italicized text is just a text string that has to match on both sides of the connection. The IP address is the public IP address of our **peer on the other side of the VPN connection**.

Phase 2 - Encrypting the Tunnel

Phase 2 Commands	Notes
crypto ipsec transform-set *vpnset* esp-aes esp-sha-hmac	The italicized text is the set name and can be changed. This could be esp-3des and esp-md5-hmac
crypto map vpnset 10 ipsec-isakmp	The number is any number between 1 and 65,535 that identifies the sequence to insert into the crypto map.
set transform-set vpnset	
match address 100	Match the addresses in the access control list coming up. This will identify the inside-to-inside traffic flow.
set peer 172.16.2.2	This is the other router's outside interface.

Phase 3 - Applying the Crypto Map to the Outside Router Interface

Phase 3 Commands	Notes
int s0/0/0	Whatever the outside interface of the router is (f0/0, g0/2, etc.)
crypto map vpnset	

Phase 4 - Creating an Access List to Identify the Traffic Flow (inside to inside LAN traffic)

Phase 4 Commands	Notes
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255	These are the inside addresses of both routers.

Let's start with Router1

Router1 VPN Configuration Commands

```
Router1>enable
Router1#configure terminal
Router1(config)#crypto isakmp enable
Router1(config)#crypto isakmp policy 10
Router1(config-isakmp)#encryption aes
Router1(config-isakmp)#hash sha
Router1(config-isakmp)#group 1
Router1(config-isakmp)#lifetime 3600
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key ciscokey123 address 172.16.2.2
Router1(config)#crypto map vpnset 10 ipsec-isakmp
Router1(config-crypto-map)#set transform-set vpnset
Router1(config-crypto-map)#match address 100
Router1(config-crypto-map)#set peer 172.16.2.2
Router1(config-crypto-map)#exit
Router1(config)#int serial 0/0/0
Router1(config-if)#crypto map vpnset
Router1(config-if)#exit
Router1(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

Router2 VPN Configuration Commands

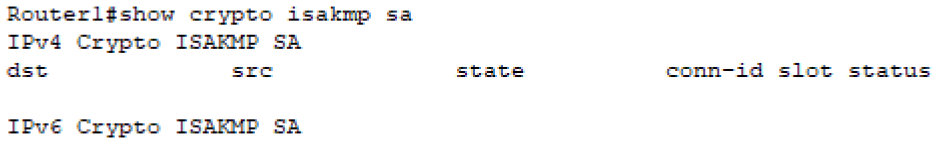
```
Router2>enable
Router2#configure terminal
Router2(config)#crypto isakmp enable
Router2(config)#crypto isakmp policy 10
Router2(config-isakmp)#encryption aes
Router2(config-isakmp)#hash sha
Router2(config-isakmp)#group 1
Router2(config-isakmp)#lifetime 3600
Router2(config-isakmp)#authentication pre-share
Router2(config-isakmp)#exit
Router2(config)#crypto isakmp key ciscokey123 address 172.16.1.2
Router2(config)#crypto map vpnset 10 ipsec-isakmp
Router2(config-crypto-map)#set transform-set vpnset
Router2(config-crypto-map)#match address 100
```

Router2(config-crypto-map)#set peer 172.16.1.2
Router2(config-crypto-map)#exit
Router2(config)#int serial 0/0/0
Router2(config-if)#crypto map vpnset
Router2(config-if)#exit
Router2(config)#access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

Check Status of VPN

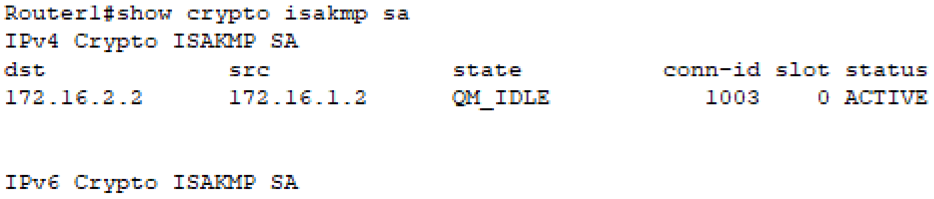
Check the status of the Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs) built between the peers.

Router1#show crypto isakmp sa



```
Router1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

If you run the command right after establishing the VPN you might see a very blank status screen. You can wait for connections to start establishing across the VPN or you can simply do a ping across the VPN. Then when you run the command again you should see a more informative status like this.

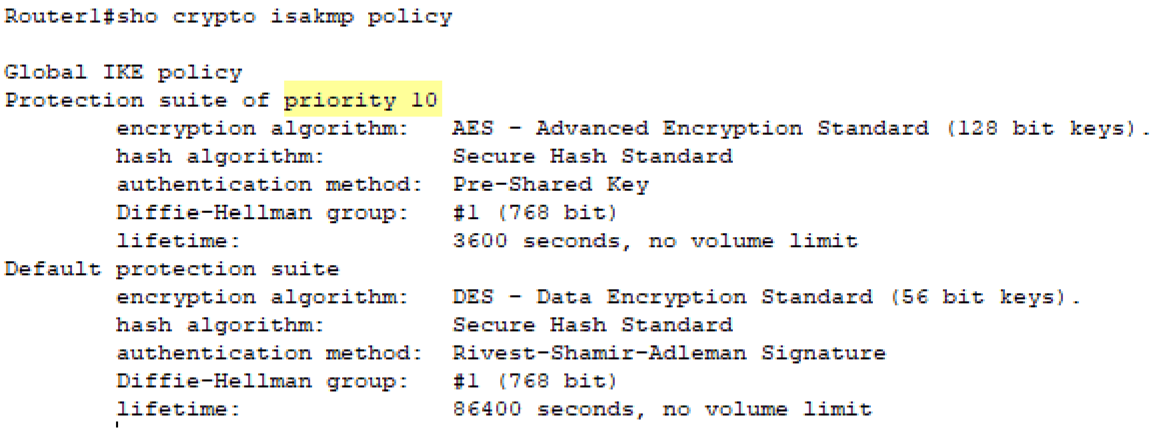


```
Router1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
172.16.2.2      172.16.1.2      QM_IDLE           1003    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

You can see from the output above the destination's (Router2) IP address and the source (Router1). And most importantly the status shows that the security association (link) is ACTIVE.

Check the Internet Security Association Management Protocol (ISAKMP) Policy

Router1#show crypto isakmp policy

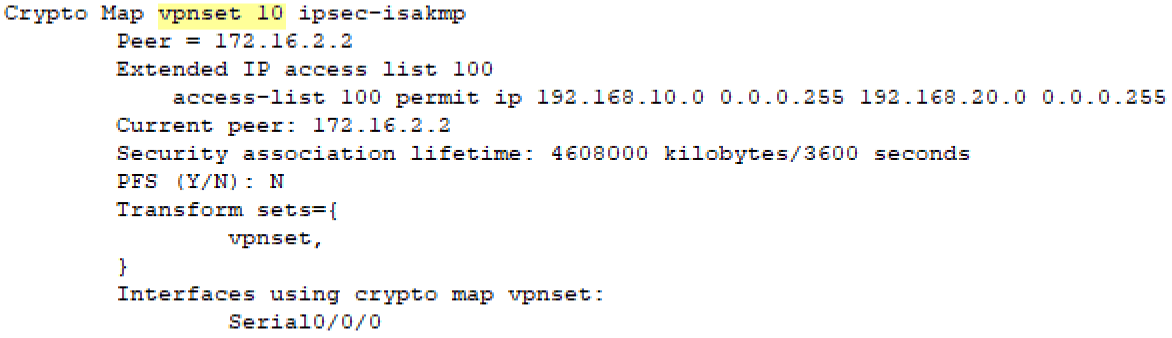


```
Router1#sho crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

As you can see our new ISAKMP policy is at a higher priority than the default protection suite policy. This output shows the priority, the encryption type (AES), the authentication method (pre-shared), the Diffie-Hellman group (1), and the lifetime (3600). These are all the values we set in the configuration.

Check the Crypto Map Settings

Router1#show crypto map

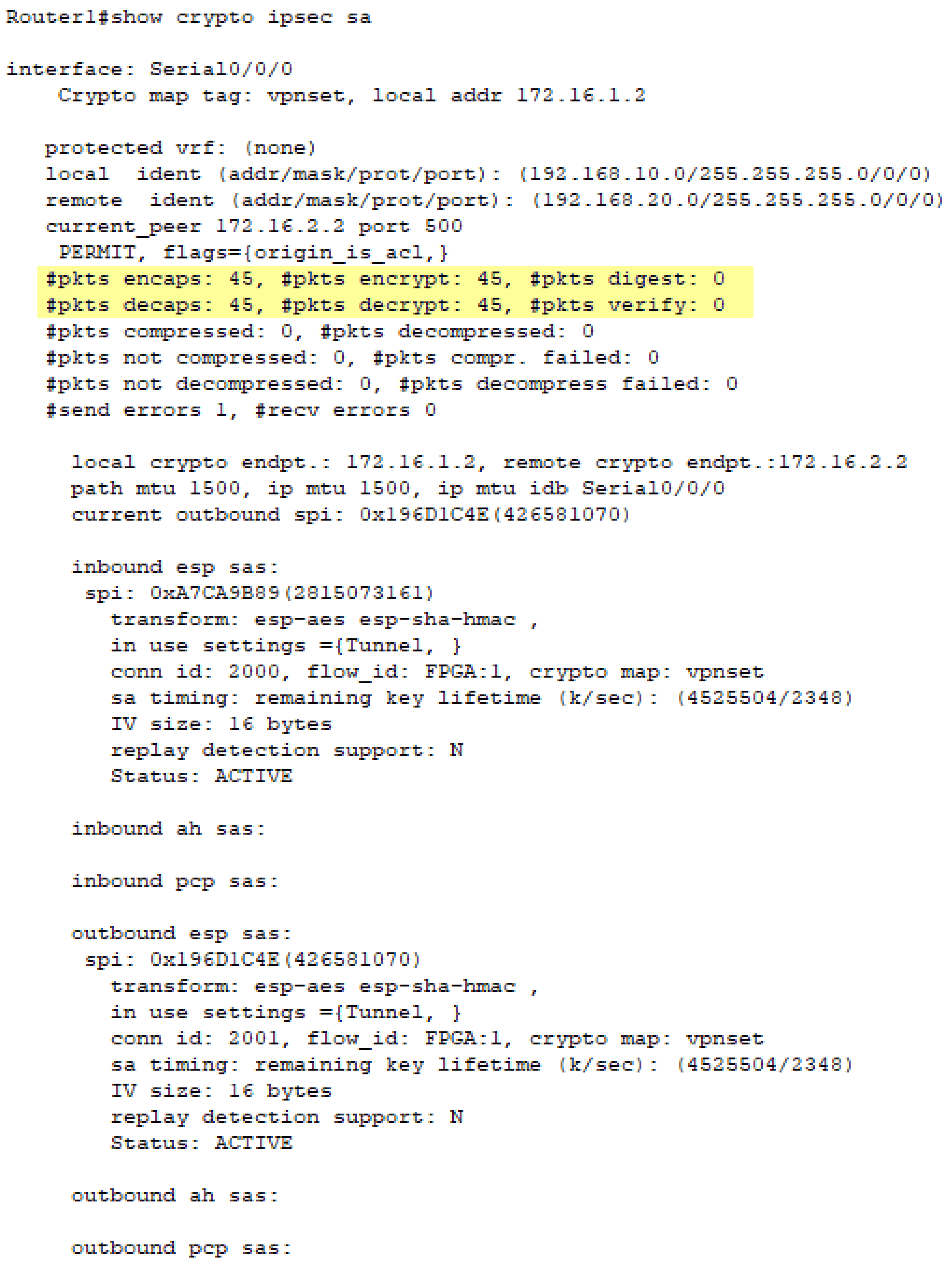


```
Crypto Map vpnset 10 ipsec-isakmp
        Peer = 172.16.2.2
        Extended IP access list 100
            access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
        Current peer: 172.16.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                vpnset,
        }
        Interfaces using crypto map vpnset:
                Serial0/0/0
```

A wealth of information about the configured cryto map including the name and sequence number. The configured peer is visible. The access-list is present as well as the interface that the map is assigned.

Check the IPSEC Security Association

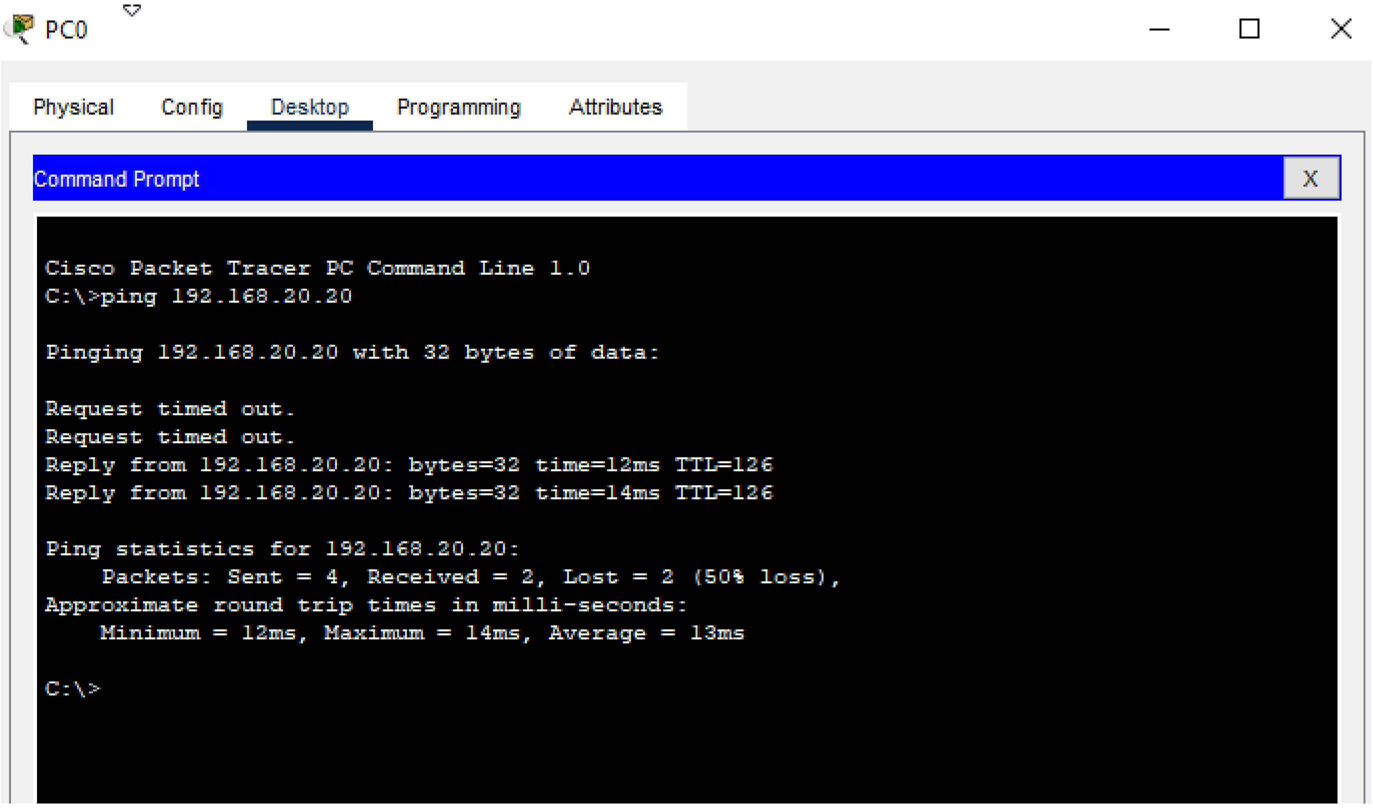
Router1#show crypto ipsec sa



```
Router1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: vpnset, local addr 172.16.1.2

   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 172.16.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 0
   #pkts decaps: 45, #pkts decrypt: 45, #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 1, #recv errors 0

     local crypto endpt.: 172.16.1.2, remote crypto endpt.:172.16.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x196D1C4E(426581070)

     inbound esp sas:
      spi: 0xA7CA9B89(2815073161)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2000, flow_id: FPGA:1, crypto map: vpnset
        sa timing: remaining key lifetime (k/sec): (4525504/2348)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x196D1C4E(426581070)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: FPGA:1, crypto map: vpnset
        sa timing: remaining key lifetime (k/sec): (4525504/2348)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

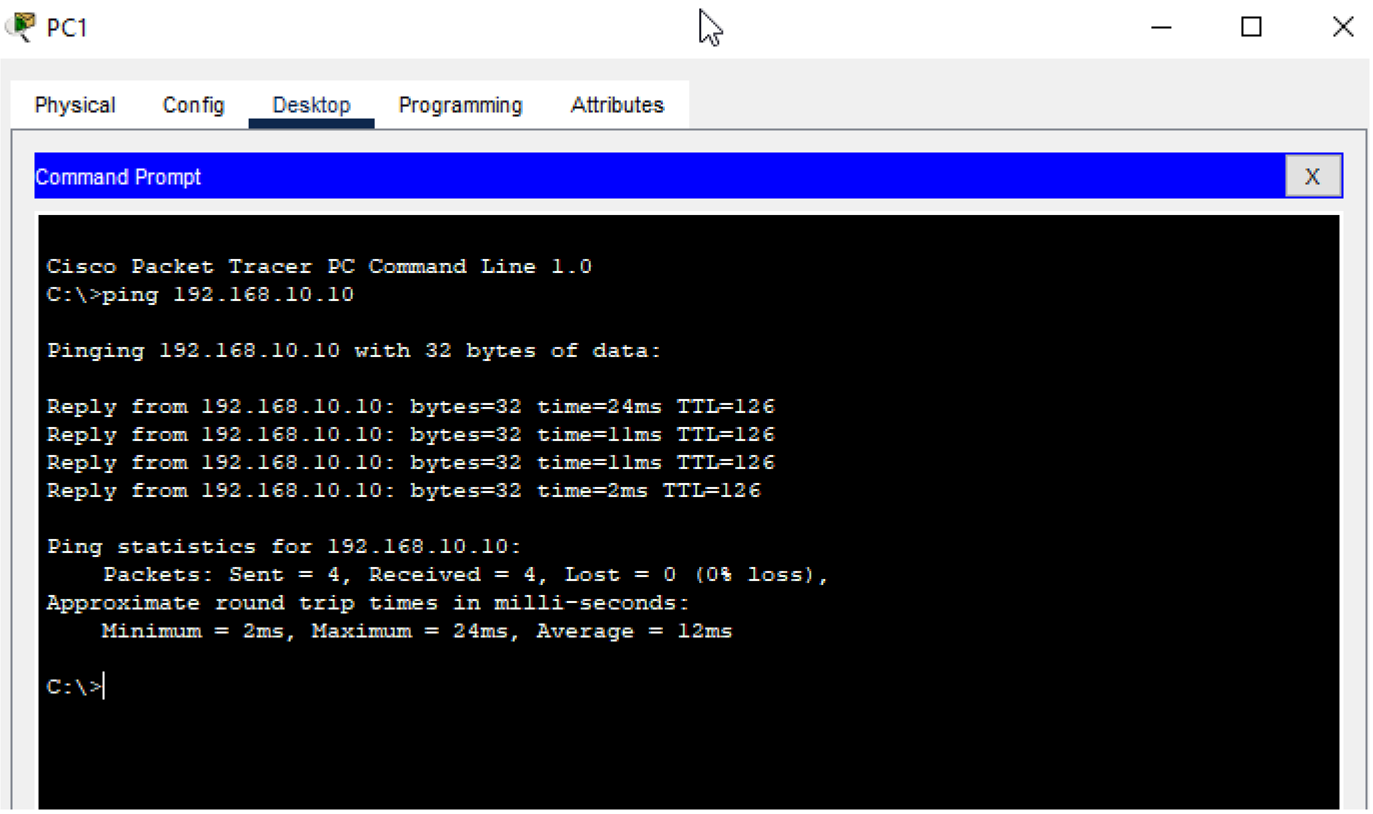
There is a lot of information given in this command but probably the most valuable is the highlighted area above showing that encapsulation and decapsulation is taking place across the VPN. Additionally, you can see status for inbound and outbound tunnel and the configured encryption algorithms.

Check Ping from PC0 to PC1 and visa versa



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.20

Pinging 192.168.20.20 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.20.20: bytes=32 time=12ms TTL=126
Reply from 192.168.20.20: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.20.20:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 14ms, Average = 13ms

C:\>
```

The first ping will most likely lose some packets, but subsequent pings will complete 100%



```
Cisco Packet Tracer PC Command Line 1.0
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=24ms TTL=126
Reply from 192.168.10.10: bytes=32 time=11ms TTL=126
Reply from 192.168.10.10: bytes=32 time=11ms TTL=126
Reply from 192.168.10.10: bytes=32 time=2ms 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 = 24ms, Average = 12ms

C:\>
```

Cisco Packet Tracer File

net13 site to site vpn.pkt

Revision #8
Created 3 January 2023 23:40:00 by Glen Taylor
Updated 24 January 2023 22:45:52 by Glen Taylor