NetSecMon – Network Operation Project

Configuring the Topology:

* 1 Router, 6 Switches, 8 PC’s

To simulate an enterprise’s network with the security needs we added 3 switches for STP to prevent looping, closed off ports, sticky mac addresses

Commands:

R1: enable -> config terminal -> interface gig0/0/0 -> ip address 192.168.1.1 255.255.255.0 -> no shutdown -> exit -> interface gig0/0/1 -> ip address 192.168.2.1 255.255.255.0 -> no shutdown -> exit // interface gig0/0/2 -> ip address 192.168.3.1 255.255.255.0 -> no shutdown -> exit

R1: ACL Commands:

access-list 110 deny icmp any any

(Blocks all ICMP traffic (such as ping, echo request/reply, etc.) from any source to any destination.) this is done to block DOS attacks

access-list 110 permit ip any any

(Allows all remaining IP traffic (from any source to any destination) that hasn’t been matched by previous ACL rules.)

(we will apply same logic to VLAN 30 and VLAN 40)

PC’s Divided onto VLANS based on IP’s:

* PC1 192.168.10.2 // 255.255.255.0 // 192.168.10.1
* PC2 192.168.10.3 // 255.255.255.0 // 192.168.10.1
* PC3 192.168.20.2 // 255.255.255.0 // 192.168.20.1
* PC4 192.168.20.3 // 255.255.255.0 // 192.168.20.1
* PC5 192.168.30.2 // 255.255.255.0 // 192.168.30.1
* PC6 192.168.30.3 // 255.255.255.0 // 192.168.30.1
* PC7 192.168.40.2 // 255.255.255.0 // 192.168.40.1
* PC8 192.168.40.3 // 255.255.255.0 // 192.168.40.1

For switches we did:  
interface fa0/1

switchport mode access

switchport access vlan 10 or 20 or 30 or 40

spanning-tree portfast

for switches facing PCS and  
  
interface gi0/1

switchport mode trunk

switchport trunk allowed vlan 10 or 20 or 30 or 40

for switches facing other Switches

**Switch 5:**

enable

config t

interface Fe/0/1

VLAN 10

name left1

**Switch 6:**  
enable

config t

interface Fe/0/1

VLAN 20

name left2

**Switch 2:**  
enable

config t

interface Fe/0/1

VLAN 30

name right1

**Switch 4:**  
enable

config t

interface Fe/0/1

VLAN 40

name right2

Switches 1 and 4:  
spanning-tree vlan 1 priority 24576  
(This enabled STP which prevents looping and is only done on those two switches due to the other switches being bridging switches not routing switches)

Between Each Switch and PC there is Port Security by adding Sticky Mac Addresses ex: S5->PC1:  
enable

configure terminal

interface range fa0/1 - 3

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security violation restrict

switchport port-security mac-address sticky

exit

exit

write

For the Server we enabled SYSLOG and in S1 and in S4 we were supposed to do alerts but the switch doesn’t support it:  
  
logging 192.168.3.2

logging trap Alert

As for Logging switch commands:  
S6>en

S6#conf t

S6(config)#int vlan 1

S6(config-if)#ip add

S6(config-if)#ip address 192.168.2.12 255.255.255.0

S6(config-if)#ex

S6(config)#service timestamps log datetime msec

S6(config)#ip default-gateway 192.168.2.1

S6(config)#logging 192.168.3.3

S6(config)#logging 192.168.2.1

S6(config)#int vlan 1

S6(config-if)#no shutdown

S6(config)#hostname H1

H1(config)#ex

H1#

\*Mar 02, 00:17:19.1717: SYS-5-CONFIG\_I: Configured from console by console

H1#conf t

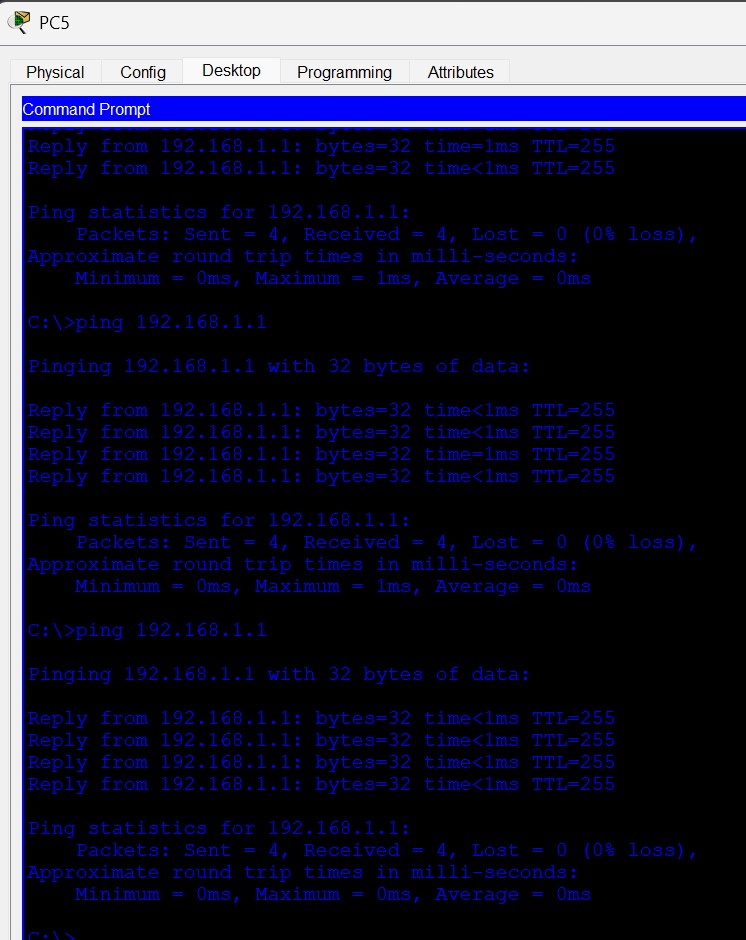
H1(config)#hostname S6

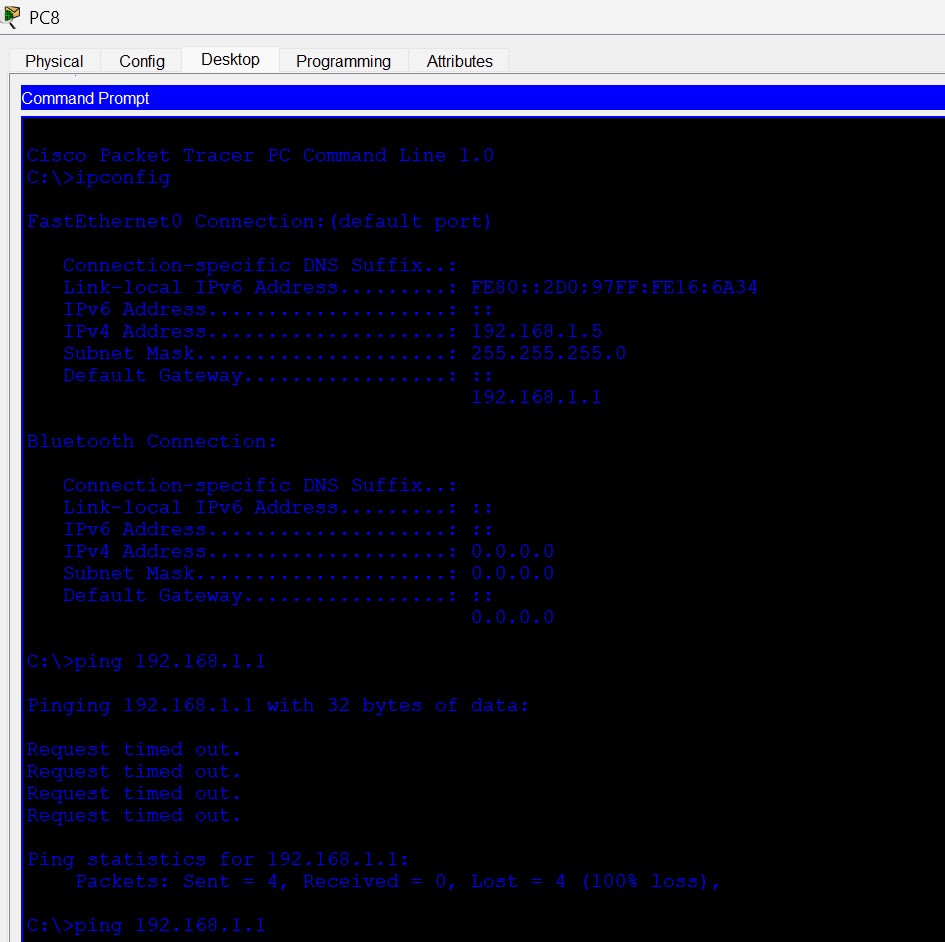
S6(config)#exit

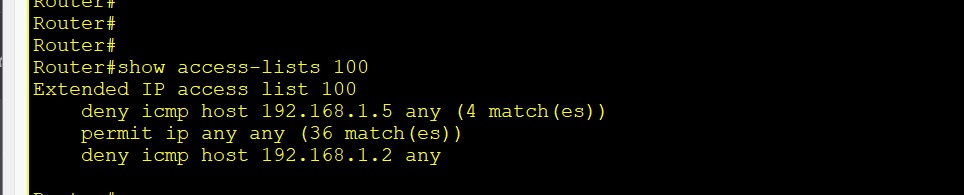
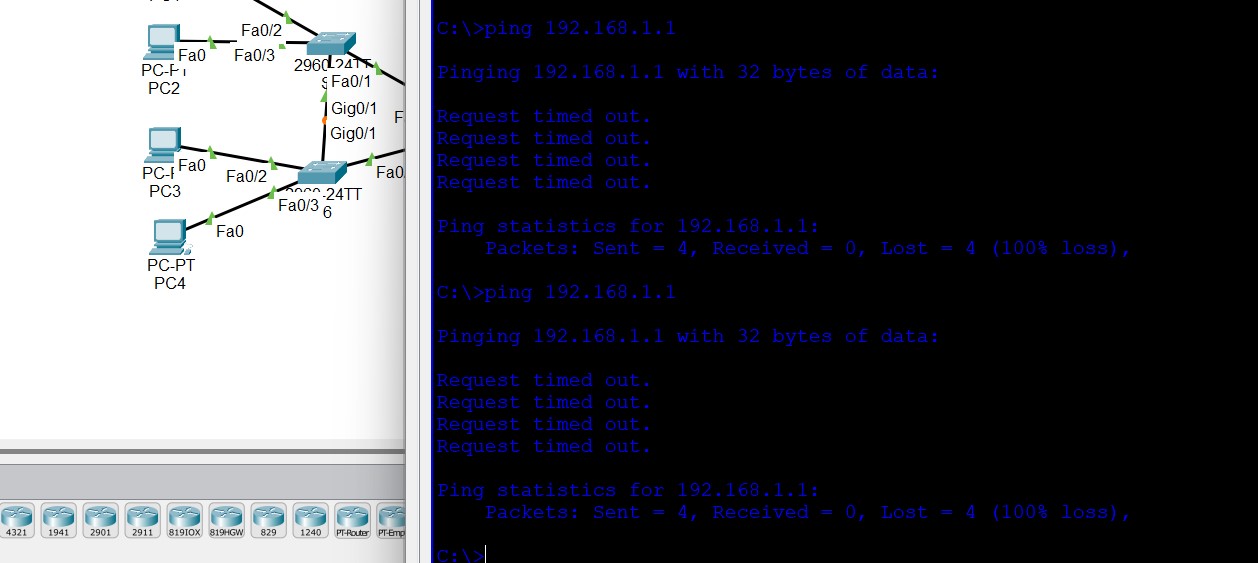
\*Mar 02, 00:17:28.1717: SYS-5-CONFIG\_I: Configured from console by console

**Attacks**

Dos Attack:







Mac Spoofing Attack:  
