VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

DIGITAL ASSIGNMENT 1- WINTER SEMESTER 2023-24

Course: Information Security Management Lab

Marks: 10 Course

Code: BCSE354E

Slot: L33+L34 Deadline: 12-Jan-2024

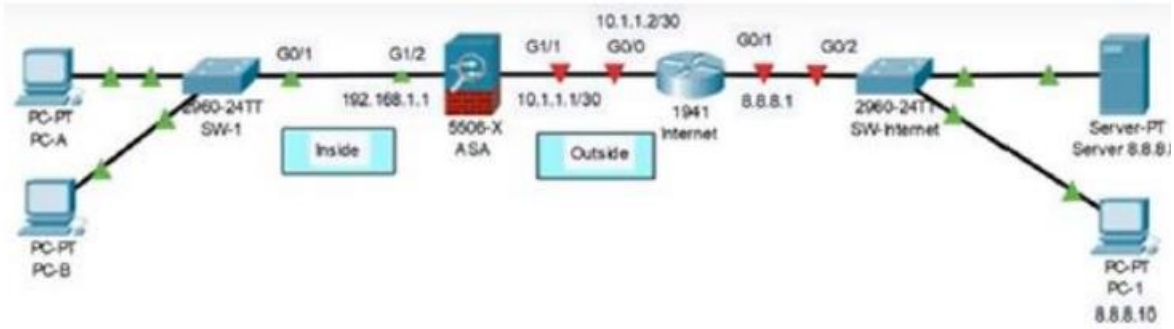
GROUP

Poli Vardhini Reddy- 21BIT0382

Kaushal .M- 21BIT0506

Question 1 [5 Marks]

Configure an ASA firewall according to the topology given below.

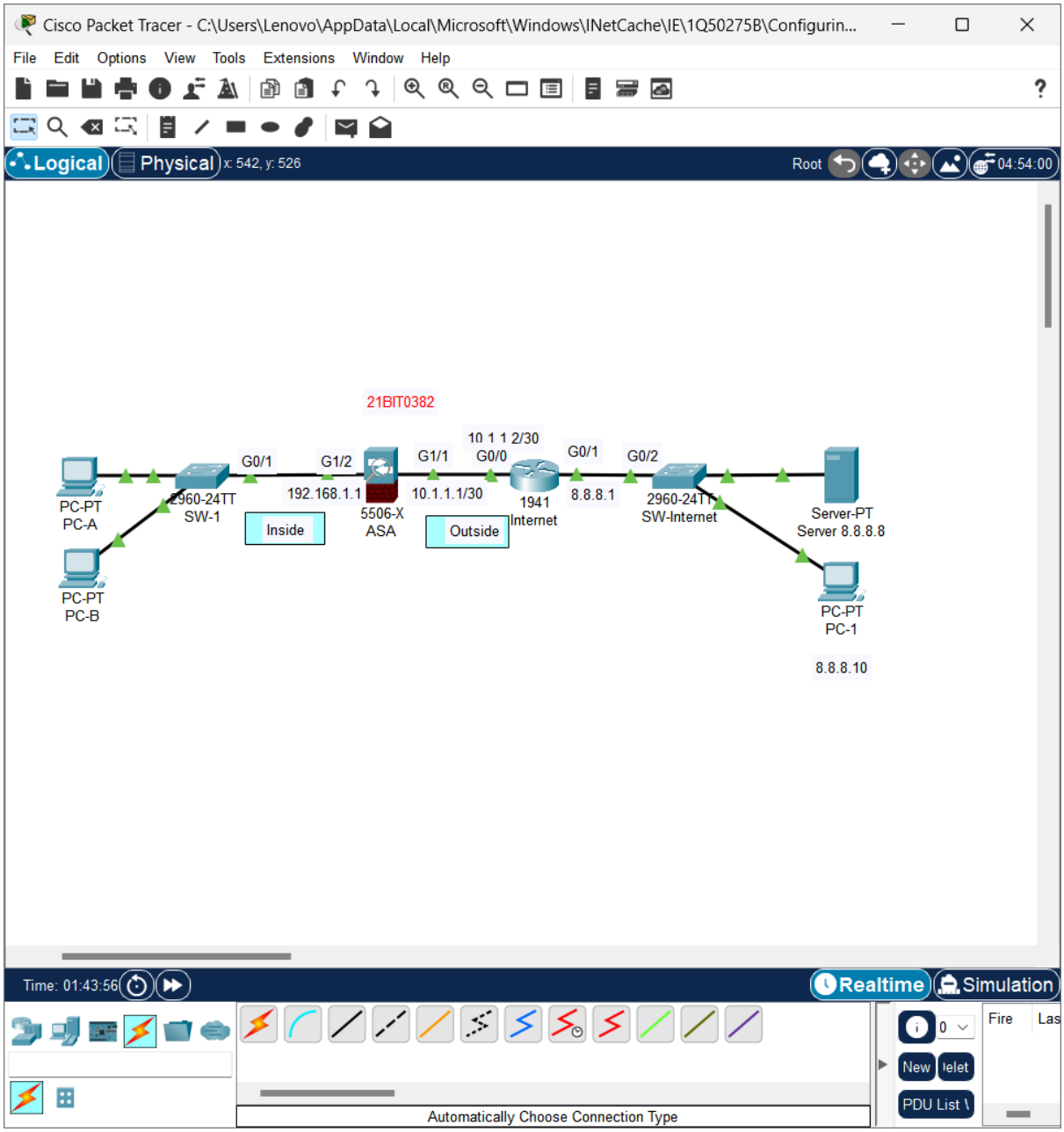


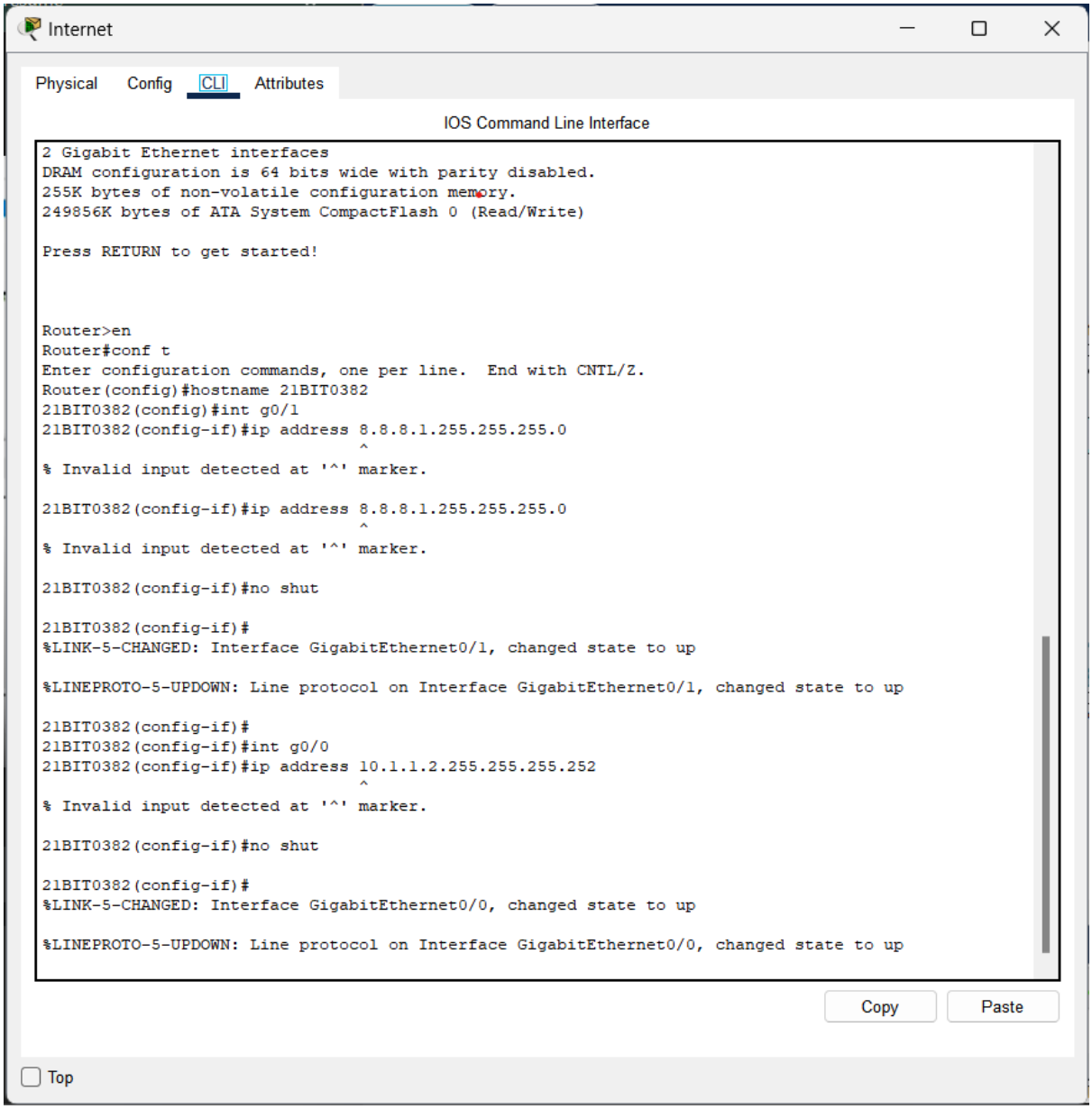
ASA should be named with your registration number and also screenshots for all subdivisions given below. Perform the following on the ASA whose host name should be configured as your registration number.

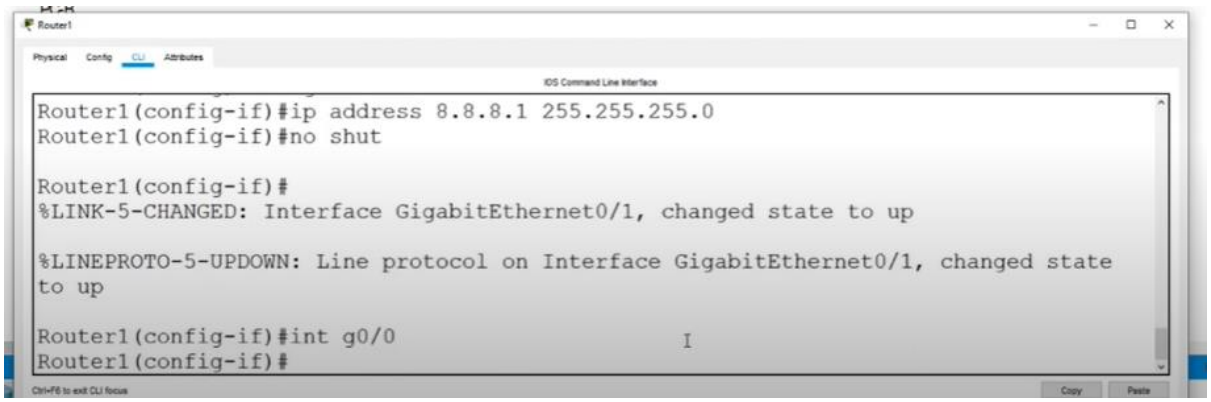
(i) **Verify connectivity of ASA • Configure interface security levels using CLI • Configure routing, address translation, and inspection policy on ICMP, FTP and HTTP using the CLI • Configure DHCP**

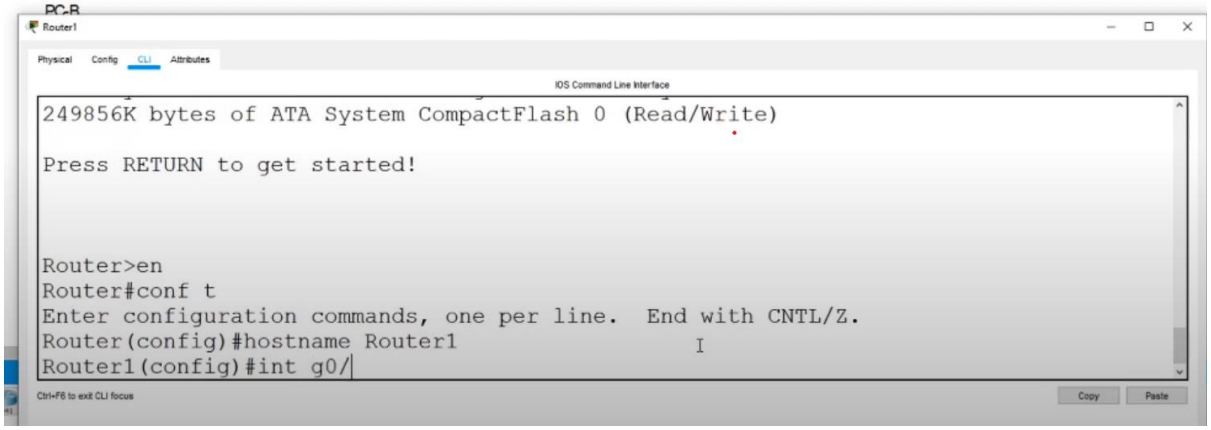
(ii) **(ii) Configure ACLs. ACL should filter traffic based on the following • PC-A can send ICMP and DNS traffic but not FTP and web traffic • PC- B cannot send ICMP and DNS traffic but can send web and FTP traffic**

CONNECTIVITY OF ASA


Cisco Packet Tracer - C:\Users\Lenovo\AppData\Local\Microsoft\Windows\INetCache\IE\1Q50275B\Configurin...
File Edit Options View Tools Extensions Window Help
Logical Physical x: 542, y: 526
Root 04:54:00
21BIT0382
PC-PT PC-A
PC-PT PC-B
2960-24TT SW-1
G0/1
G1/2
192.168.1.1
Inside
5506-X ASA
G1/1
10.1.1.1/30
Outside
10 1 1 2/30
G0/0
1941 Internet
G0/1
8.8.8.1
G0/2
2960-24TT SW-Internet
Server-PT Server 8.8.8.8
PC-PT PC-1
8.8.8.10
Time: 01:43:56
Realtime
Simulation
Automatically Choose Connection Type
Fire
New
PDU List

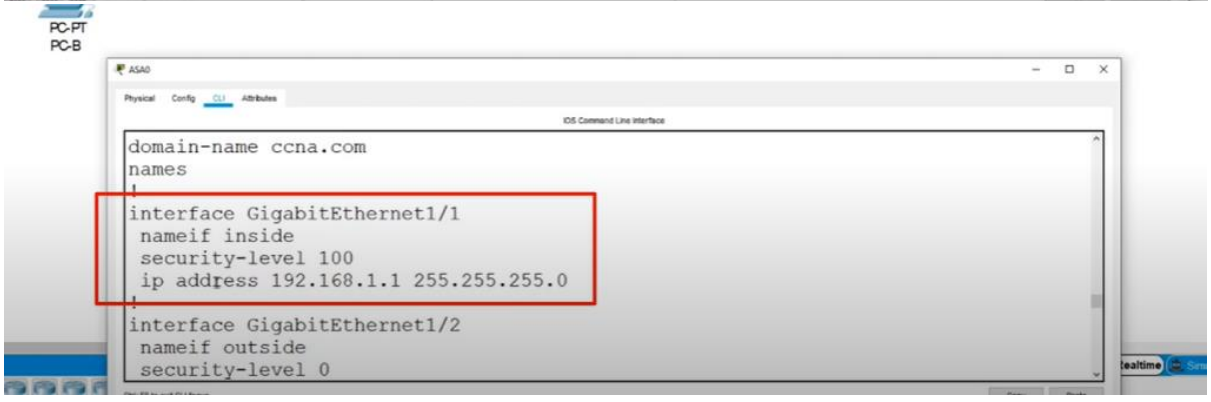

Internet
Physical
Config
CLI
Attributes
IOS Command Line Interface
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname 21BIT0382
21BIT0382(config)#int g0/1
21BIT0382(config-if)#ip address 8.8.8.1.255.255.255.0
% Invalid input detected at '^' marker.
21BIT0382(config-if)#ip address 8.8.8.1.255.255.255.0
% Invalid input detected at '^' marker.
21BIT0382(config-if)#no shut
21BIT0382(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
21BIT0382(config-if)#
21BIT0382(config-if)#int g0/0
21BIT0382(config-if)#ip address 10.1.1.2.255.255.255.252
% Invalid input detected at '^' marker.
21BIT0382(config-if)#no shut
21BIT0382(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Copy
Paste
Top


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router1(config-if)#ip address 8.8.8.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Router1(config-if)#int g0/0
Router1(config-if)#

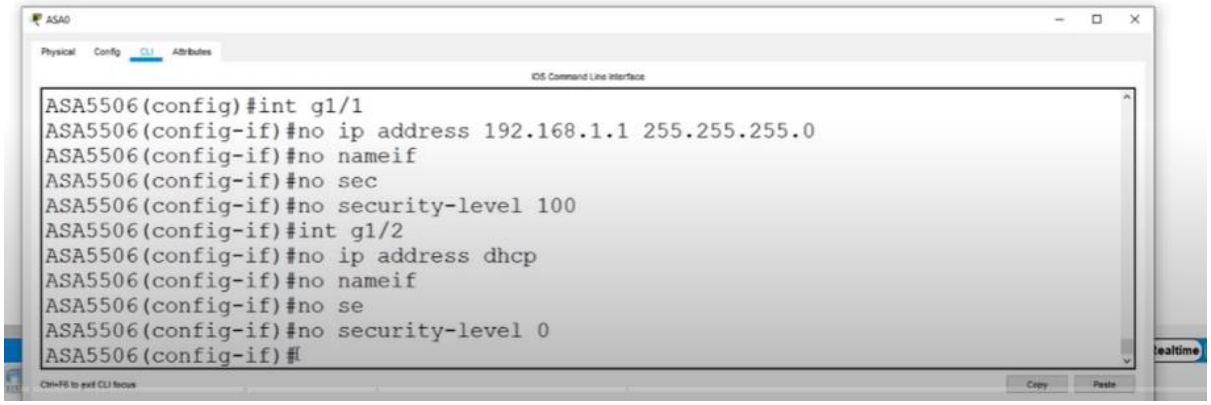

PC-B
Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#int g0/
Ctrl+F6 to exit CLI focus
Copy
Paste

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Type help or '?' for a list of available commands.
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname ASA5506
ASA5506(config)#

PC-PT
PC-B
ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address dhcp
!
interface GigabitEthernet1/3
no nameif
Ctrl+F6 to exit CLI focus
Copy
Paste


PC-PT
PC-B
ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
domain-name ccna.com
names
!
interface GigabitEthernet1/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif outside
security-level 0

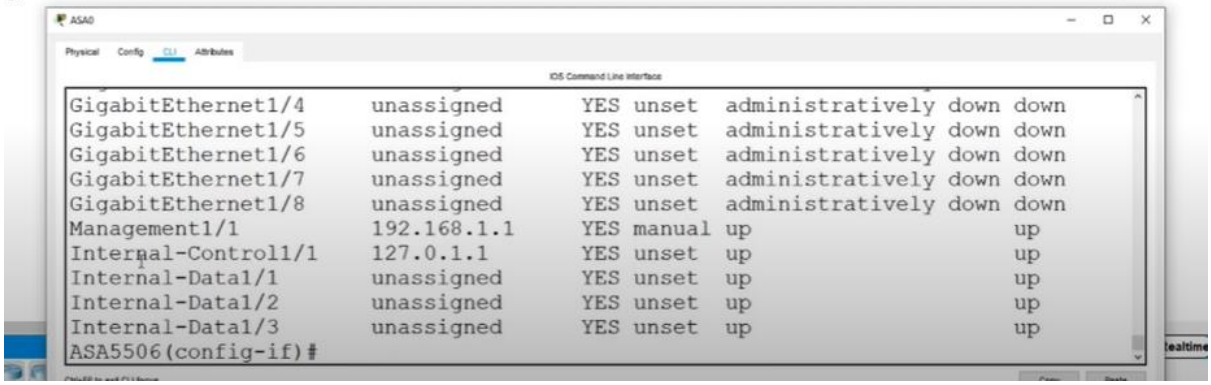
ASA0
Physical Config CLI Attributes
IOS Command Line Interface
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address dhcp
!
interface GigabitEthernet1/3
no nameif
Ctrl+F6 to exit CLI focus
Copy
Paste

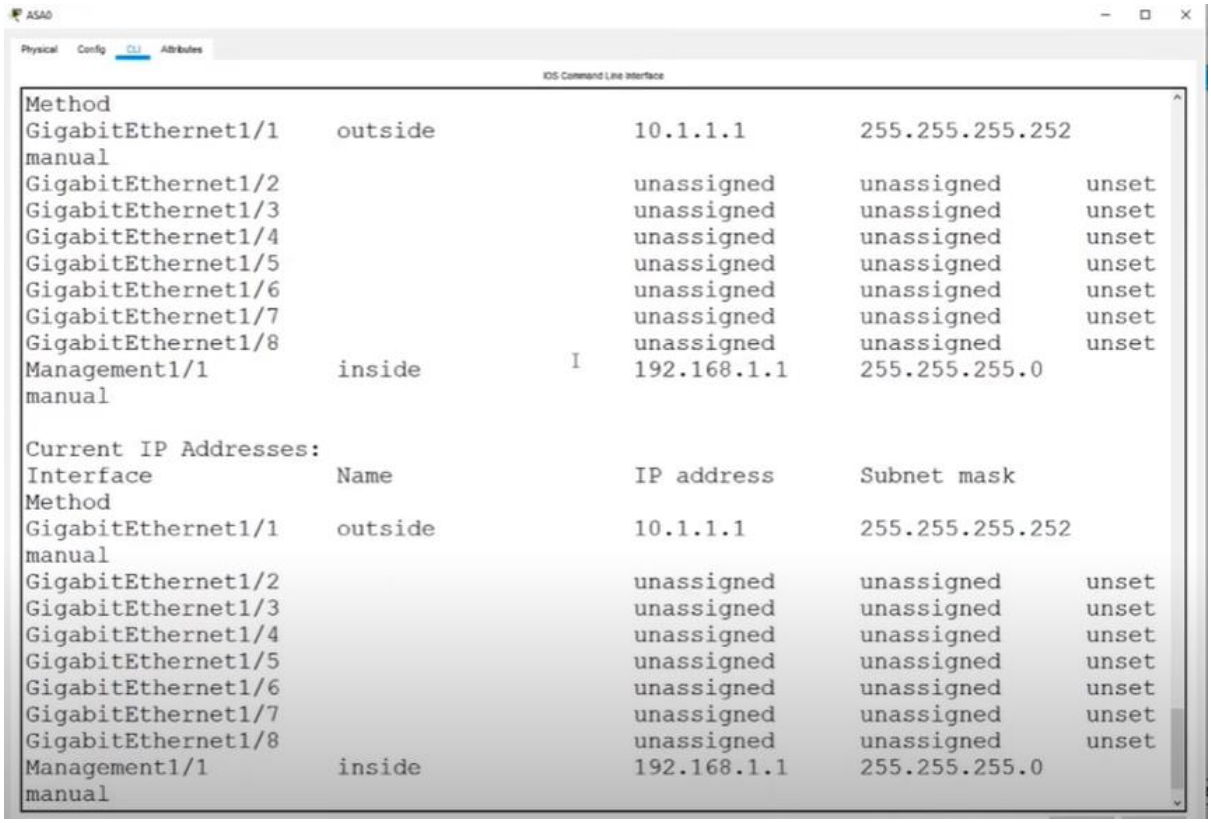

ASA0
Physical Config CLI Attributes
IOS Command Line Interface
ASA5506(config)#int g1/1
ASA5506(config-if)#no ip address 192.168.1.1 255.255.255.0
ASA5506(config-if)#no nameif
ASA5506(config-if)#no sec
ASA5506(config-if)#no security-level 100
ASA5506(config-if)#int g1/2
ASA5506(config-if)#no ip address dhcp
ASA5506(config-if)#no nameif
ASA5506(config-if)#no se
ASA5506(config-if)#no security-level 0
ASA5506(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste

PC-PT
PC-B

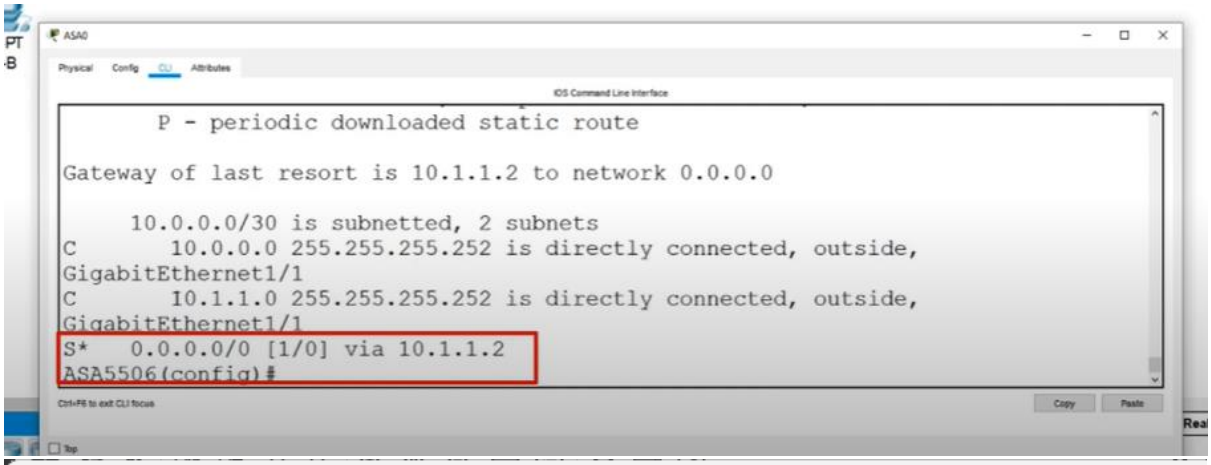
ASA0
Physical Config CLI Attributes
IOS Command Line Interface
!
interface Management1/1
management-only
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
!
!
!
!

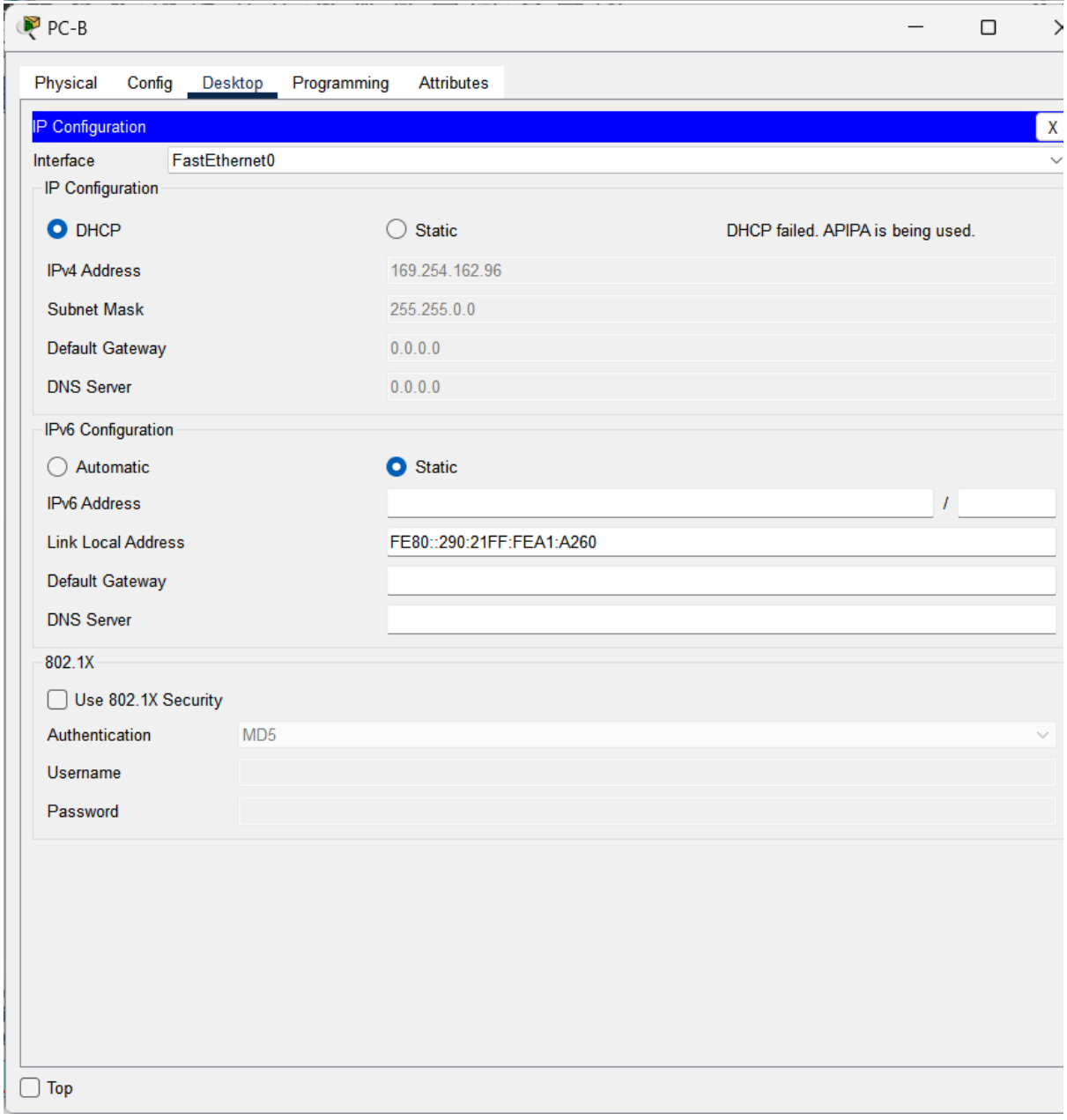
-B

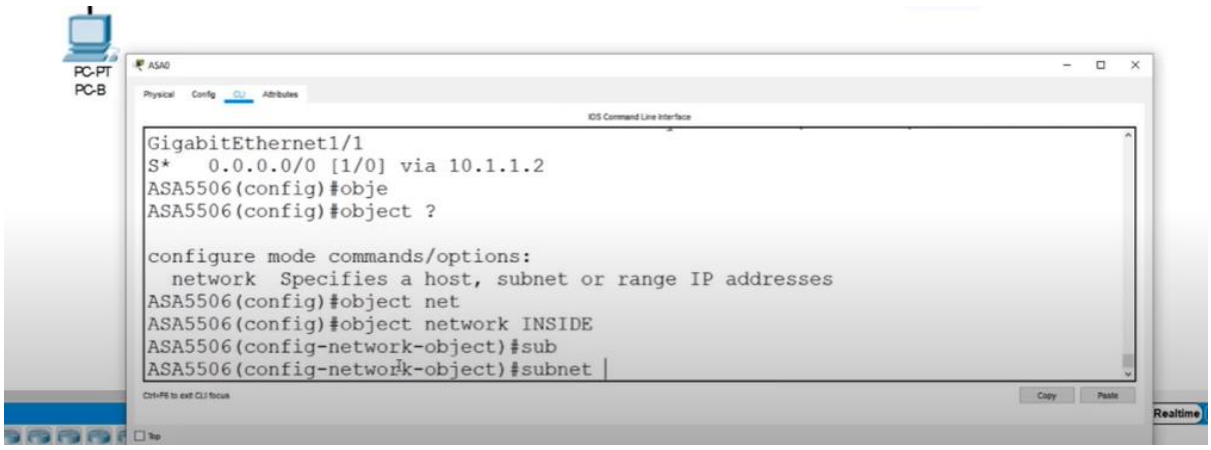

ASA0
Physical Config CLI Attributes
IOS Command Line Interface
GigabitEthernet1/4 unassigned YES unset administratively down down
GigabitEthernet1/5 unassigned YES unset administratively down down
GigabitEthernet1/6 unassigned YES unset administratively down down
GigabitEthernet1/7 unassigned YES unset administratively down down
GigabitEthernet1/8 unassigned YES unset administratively down down
Management1/1 192.168.1.1 YES manual up up
Internal-Control1/1 127.0.1.1 YES unset up up
Internal-Data1/1 unassigned YES unset up up
Internal-Data1/2 unassigned YES unset up up
Internal-Data1/3 unassigned YES unset up up
ASA5506(config-if)#

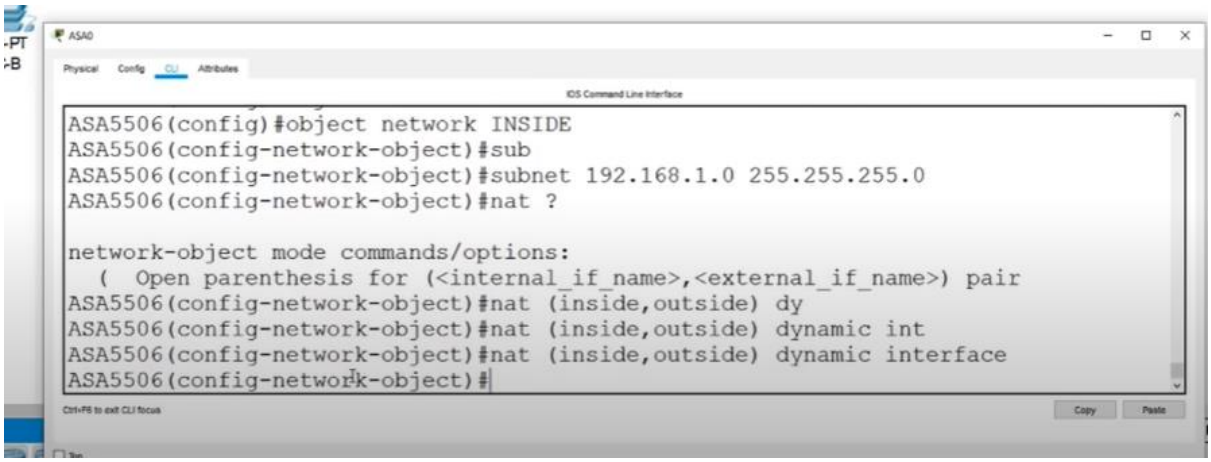

ASA0
Physical Config CLI Attributes
IOS Command Line Interface
Method
GigabitEthernet1/1 outside 10.1.1.1 255.255.255.252
manual
GigabitEthernet1/2 unassigned unassigned unset
GigabitEthernet1/3 unassigned unassigned unset
GigabitEthernet1/4 unassigned unassigned unset
GigabitEthernet1/5 unassigned unassigned unset
GigabitEthernet1/6 unassigned unassigned unset
GigabitEthernet1/7 unassigned unassigned unset
GigabitEthernet1/8 unassigned unassigned unset
Management1/1 inside 192.168.1.1 255.255.255.0
manual
Current IP Addresses:
Interface Name IP address Subnet mask
Method
GigabitEthernet1/1 outside 10.1.1.1 255.255.255.252
manual
GigabitEthernet1/2 unassigned unassigned unset
GigabitEthernet1/3 unassigned unassigned unset
GigabitEthernet1/4 unassigned unassigned unset
GigabitEthernet1/5 unassigned unassigned unset
GigabitEthernet1/6 unassigned unassigned unset
GigabitEthernet1/7 unassigned unassigned unset
GigabitEthernet1/8 unassigned unassigned unset
Management1/1 inside 192.168.1.1 255.255.255.0
manual

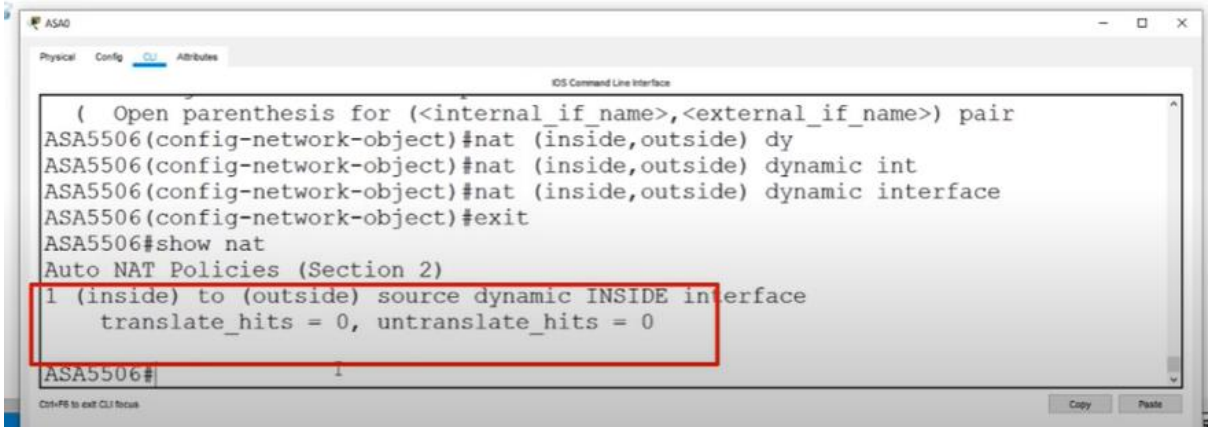
ASA0
Physical Config CLI Attributes
IOS Command Line Interface
ASA5506(config)#dhcp address 192.168.1.10-192.168.1.20 inside
ASA5506(config)#dhcp dns 8.8.8.8
ASA5506(config)#dhcp option 3 ip 192.168.1.1
ASA5506(config)#dhcp en
ASA5506(config)#dhcp enable ?
configure mode commands/options:
outside Name of interface GigabitEthernet1/1
inside Name of interface Management1/1
ASA5506(config)#dhcp enable inside
ASA5506(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste

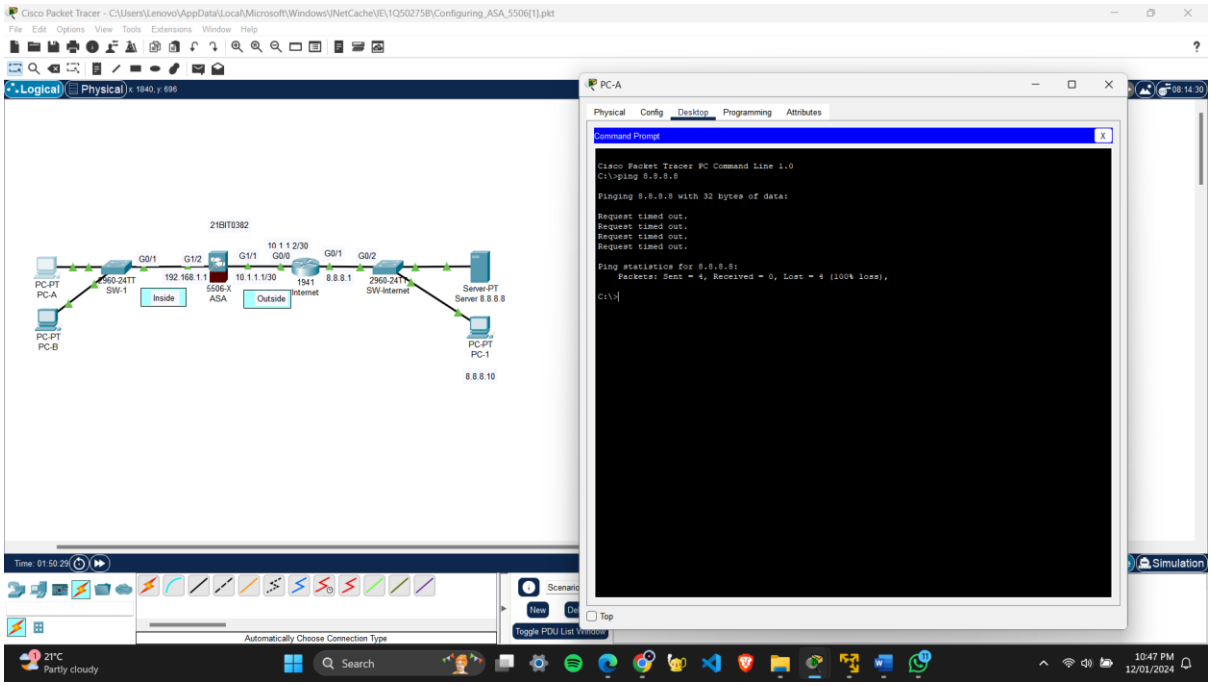

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
P - periodic downloaded static route
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
10.0.0.0/30 is subnetted, 2 subnets
C 10.0.0.0 255.255.255.252 is directly connected, outside,
GigabitEthernet1/1
C 10.1.1.0 255.255.255.252 is directly connected, outside,
GigabitEthernet1/1
S* 0.0.0.0/0 [1/0] via 10.1.1.2
ASA5506(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste


PC-B
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP failed. APIPA is being used.
IPv4 Address
169.254.162.96
Subnet Mask
255.255.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::290:21FF:FEA1:A260
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

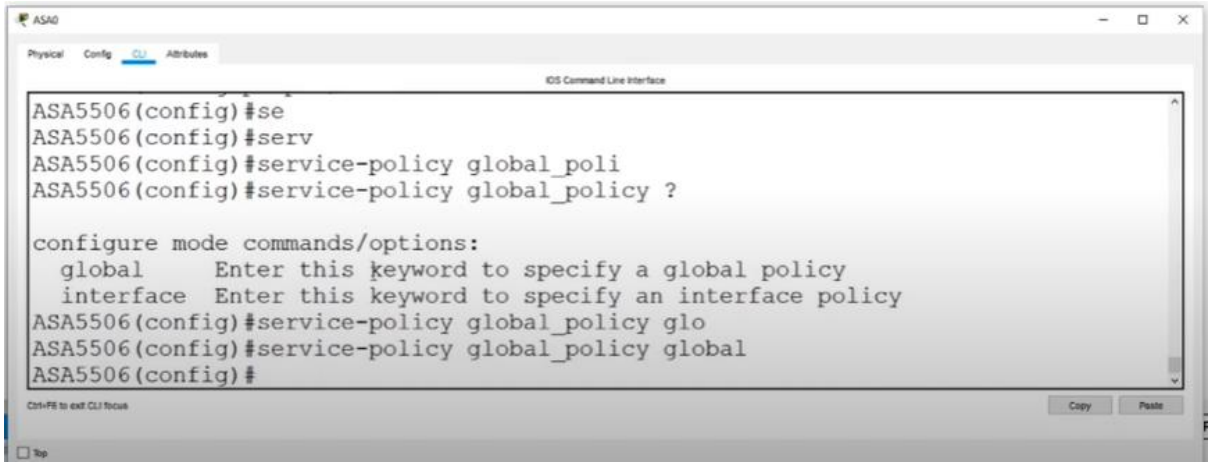

PC-PT
PC-B
ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
GigabitEthernet1/1
S*   0.0.0.0/0 [1/0] via 10.1.1.2
ASA5506(config)#obje
ASA5506(config)#object ?
configure mode commands/options:
  network Specifies a host, subnet or range IP addresses
ASA5506(config)#object net
ASA5506(config)#object network INSIDE
ASA5506(config-network-object)#sub
ASA5506(config-network-object)#subnet
Ctrl+F6 to exit CLI focus
Copy
Paste
Realtime

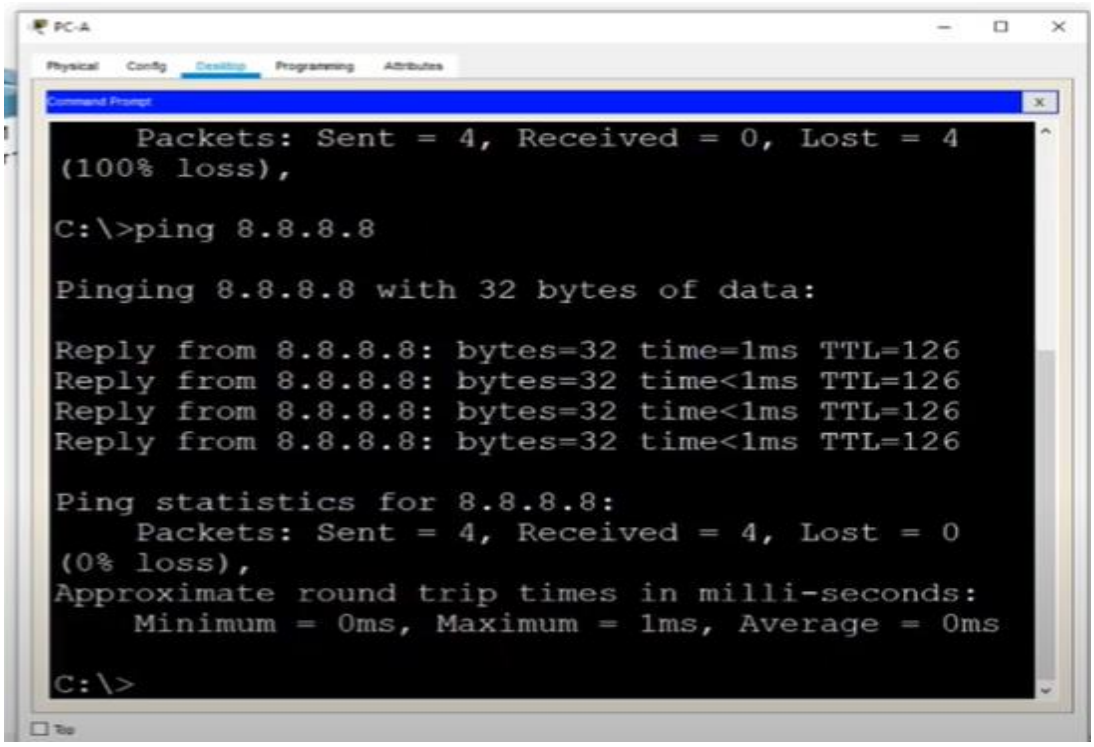

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ASA5506(config)#object network INSIDE
ASA5506(config-network-object)#sub
ASA5506(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA5506(config-network-object)#nat ?
network-object mode commands/options:
  (Open parenthesis for (<internal_if_name>,<external_if_name>) pair
ASA5506(config-network-object)#nat (inside,outside) dy
ASA5506(config-network-object)#nat (inside,outside) dynamic int
ASA5506(config-network-object)#nat (inside,outside) dynamic interface
ASA5506(config-network-object)#
Ctrl+F6 to exit CLI focus
Copy
Paste

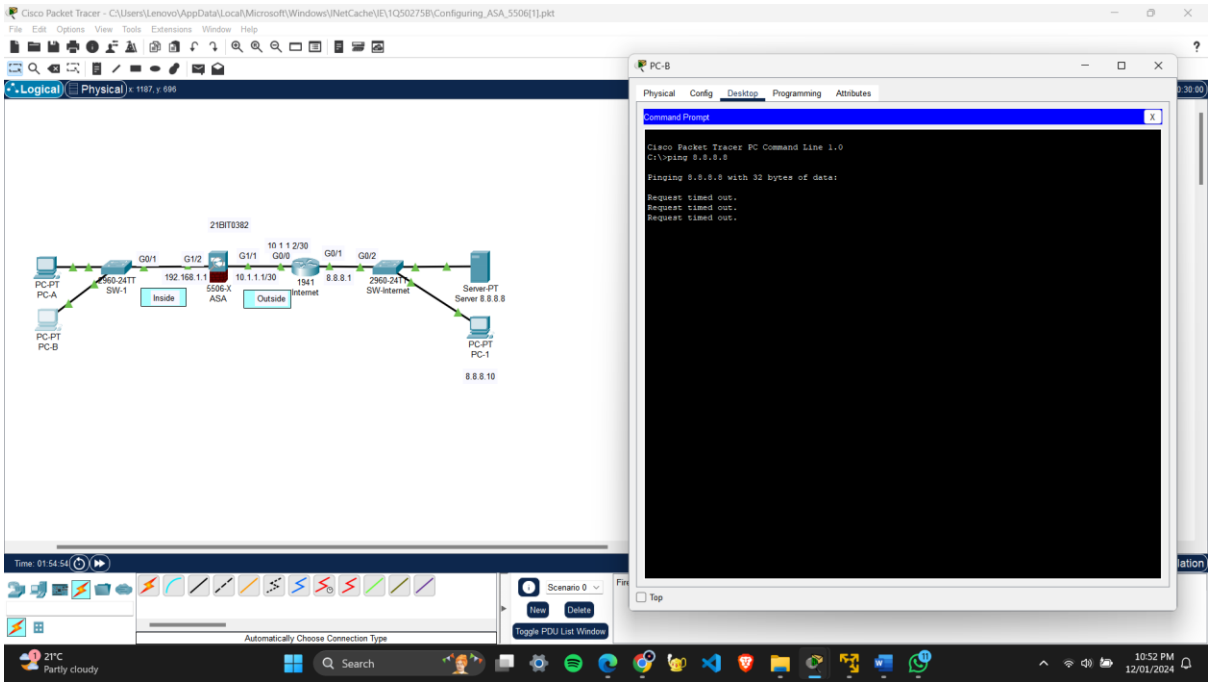

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
  (Open parenthesis for (<internal_if_name>,<external_if_name>) pair
ASA5506(config-network-object)#nat (inside,outside) dy
ASA5506(config-network-object)#nat (inside,outside) dynamic int
ASA5506(config-network-object)#nat (inside,outside) dynamic interface
ASA5506(config-network-object)#exit
ASA5506#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE interface
    translate_hits = 0, untranslate_hits = 0
ASA5506#
Ctrl+F6 to exit CLI focus
Copy
Paste

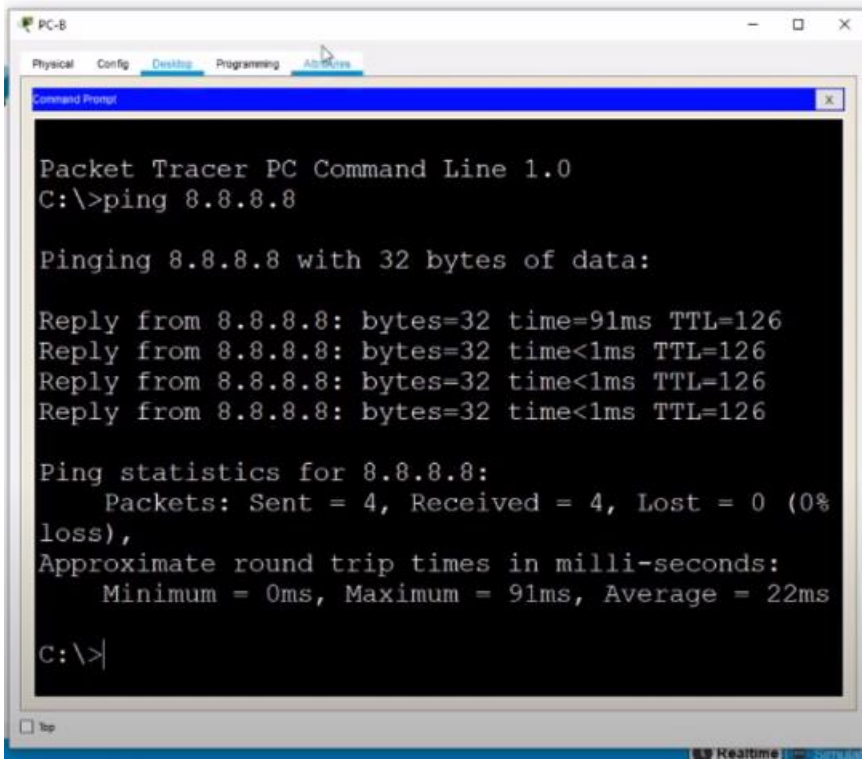

Cisco Packet Tracer - C:\Users\Lenovo\AppData\Local\Microsoft\Windows\INetCache\IE\1Q50275B\Configuring_ASA_5506[1].pkt
Logical
Physical
21BIT0382
PC-PT PC-A
PC-PT PC-B
2960-24TT SW-1
Inside
5506-X ASA
Outside
1941 Internet
2960-24TT SW-Internet
Server-PT Server 8.8.8.8
PC-PT PC-1
8.8.8.10
192.168.1.1
10.1.1.1/30
10.1.1.2/30
8.8.8.1
PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Automatically Choose Connection Type
Simulation
21°C
Partly cloudy
Search
10:47 PM
12/01/2024

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
translate_hits = 0, untranslate_hits = 0
ASA5506#conf t
ASA5506(config)#cl
ASA5506(config)#clas
ASA5506(config)#class-map inspection_default
ASA5506(config-cmap)#m
ASA5506(config-cmap)#match d
ASA5506(config-cmap)#match default-inspection-traffic
ASA5506(config-cmap)#exit
ASA5506(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste

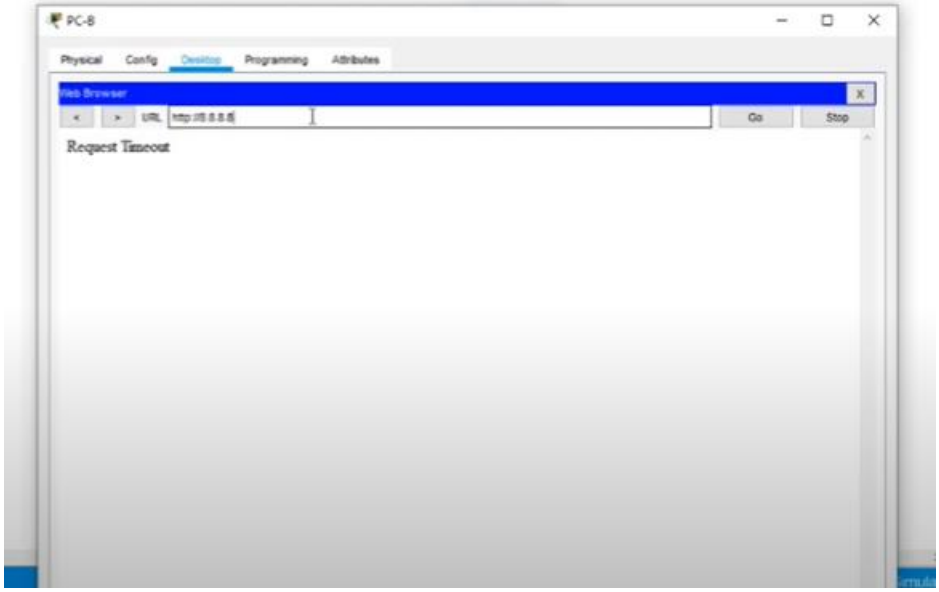

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ASA5506(config)#se
ASA5506(config)#serv
ASA5506(config)#service-policy global_poli
ASA5506(config)#service-policy global_policy ?
configure mode commands/options:
global Enter this keyword to specify a global policy
interface Enter this keyword to specify an interface policy
ASA5506(config)#service-policy global_policy glo
ASA5506(config)#service-policy global_policy global
ASA5506(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4
(100% loss),
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0
(0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

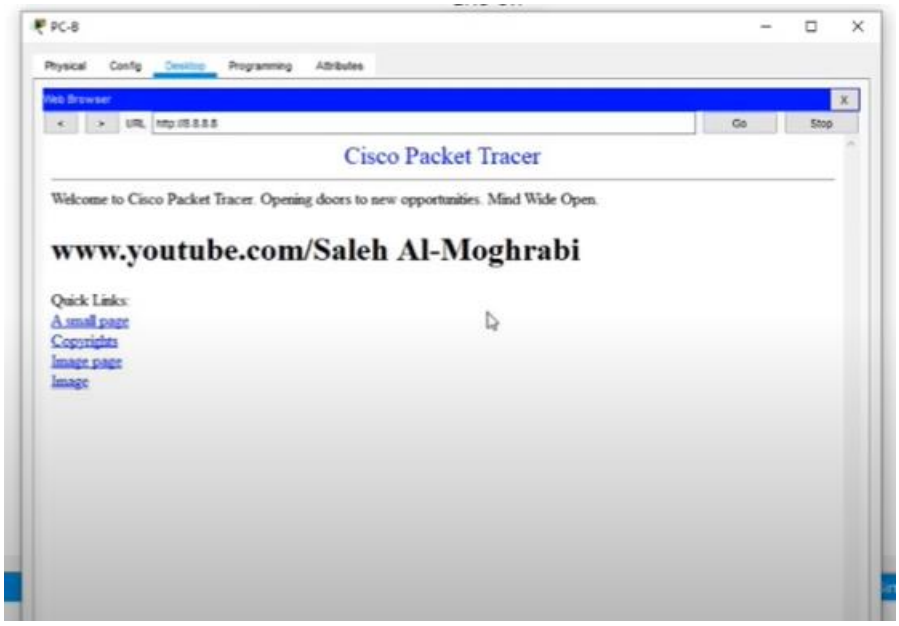

Cisco Packet Tracer
Logical
Physical
21BIT0382
PC-PT PC-A
PC-PT PC-B
2960-24TT SW-1
G0/1
G1/2
192.168.1.1
Inside
5506-X ASA
G1/1
10.1.1.1/30
Outside
10.1.1.2/30
G0/0
1941 Internet
G0/1
8.8.8.1
G0/2
2960-24TT SW-Internet
Server-PT Server 8.8.8.8
PC-PT PC-1
8.8.8.10
PC-B
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Top
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
21°C
Partly cloudy
Search
10:52 PM
12/01/2024

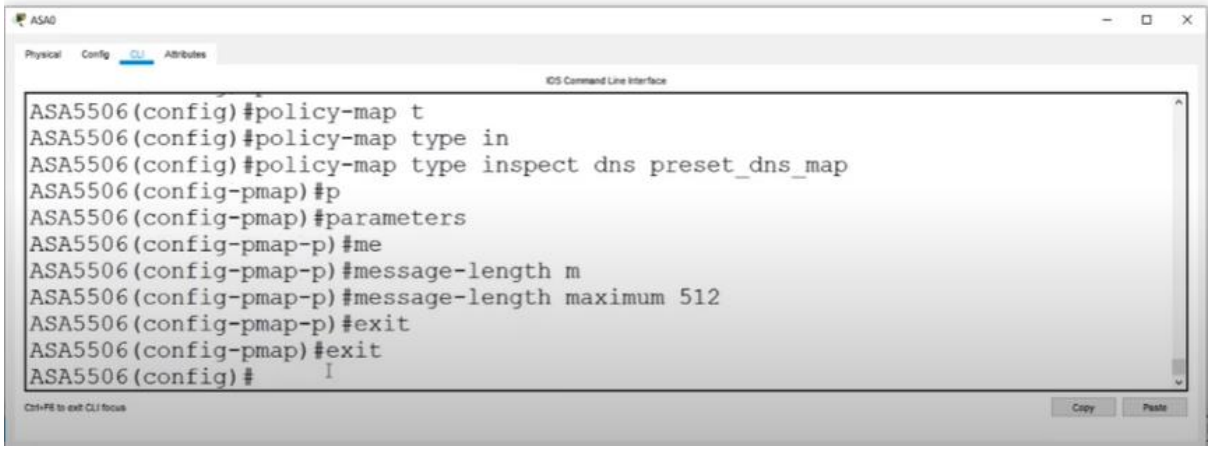


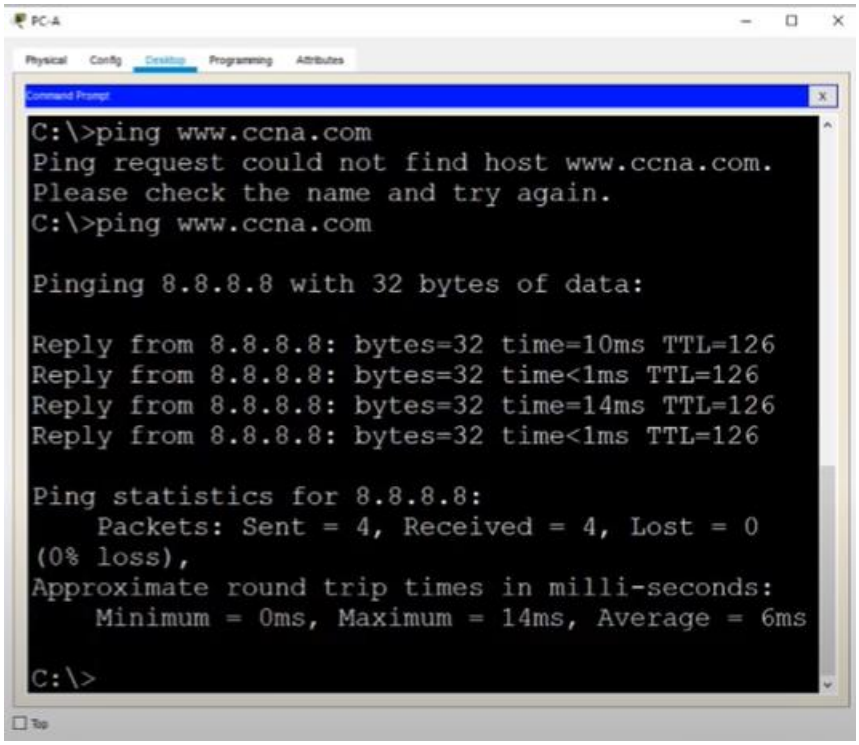
Router1 SW-2 Server-PT DNS-Svr

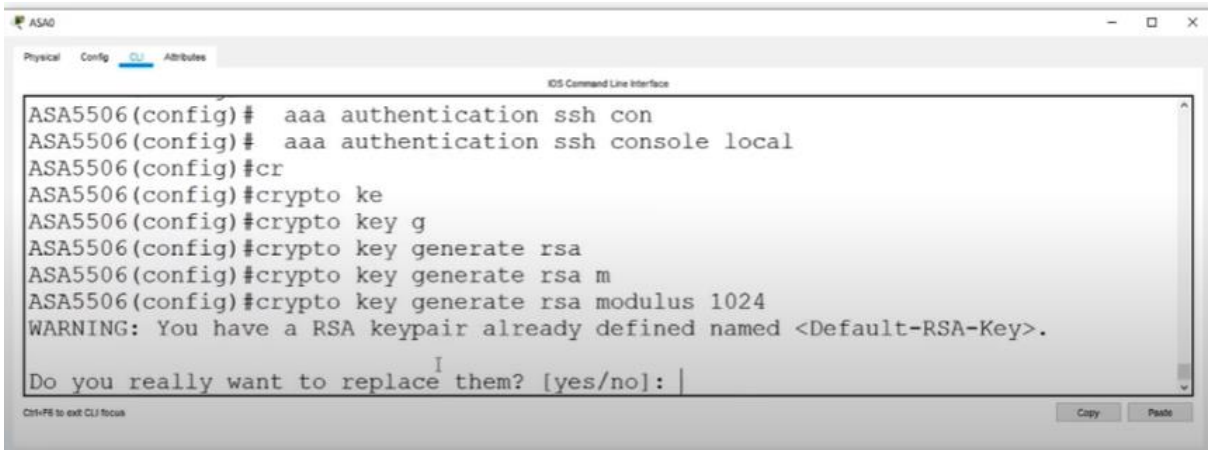


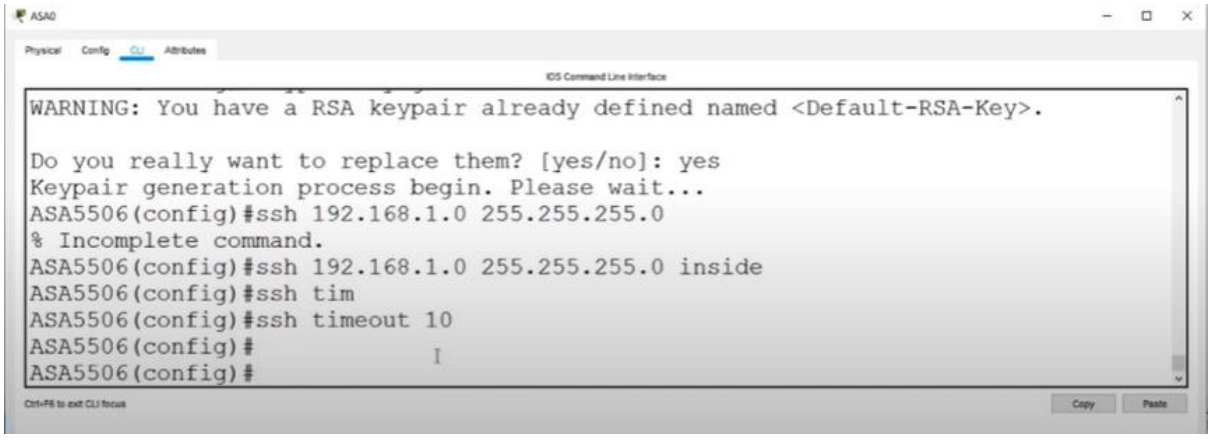
ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
match default-inspection-traffic
!
policy-map global_policy
class inspection_default
inspect http
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
Ctrl+F6 to exit CLI focus
Copy
Paste
Realtime
Top

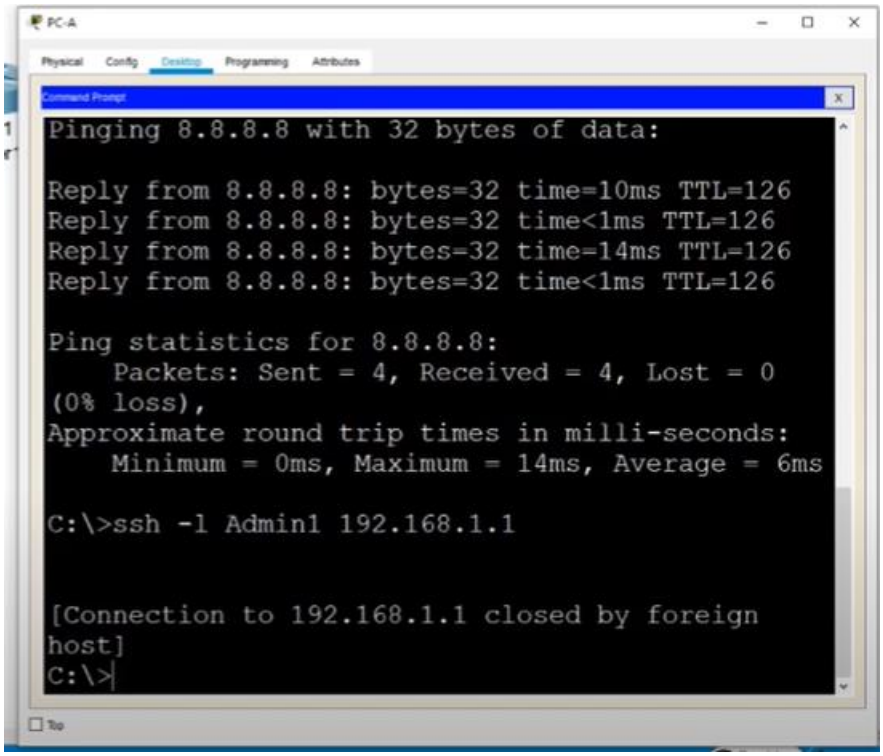

PC-B
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
www.youtube.com/Saleh Al-Moghrabi
Quick Links:
A small page
Copyrights
Image page
Image


ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ASA5506(config)#policy-map t
ASA5506(config)#policy-map type in
ASA5506(config)#policy-map type inspect dns preset_dns_map
ASA5506(config-pmap)#p
ASA5506(config-pmap)#parameters
ASA5506(config-pmap-p)#me
ASA5506(config-pmap-p)#message-length m
ASA5506(config-pmap-p)#message-length maximum 512
ASA5506(config-pmap-p)#exit
ASA5506(config-pmap)#exit
ASA5506(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste


PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping www.ccna.com
Ping request could not find host www.ccna.com.
Please check the name and try again.
C:\>ping www.ccna.com
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=14ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0
(0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 6ms
C:\>
Top


ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ASA5506(config)# aaa authentication ssh con
ASA5506(config)# aaa authentication ssh console local
ASA5506(config)#cr
ASA5506(config)#crypto ke
ASA5506(config)#crypto key g
ASA5506(config)#crypto key generate rsa
ASA5506(config)#crypto key generate rsa m
ASA5506(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
Do you really want to replace them? [yes/no]:
Ctrl+F6 to exit CLI focus
Copy
Paste

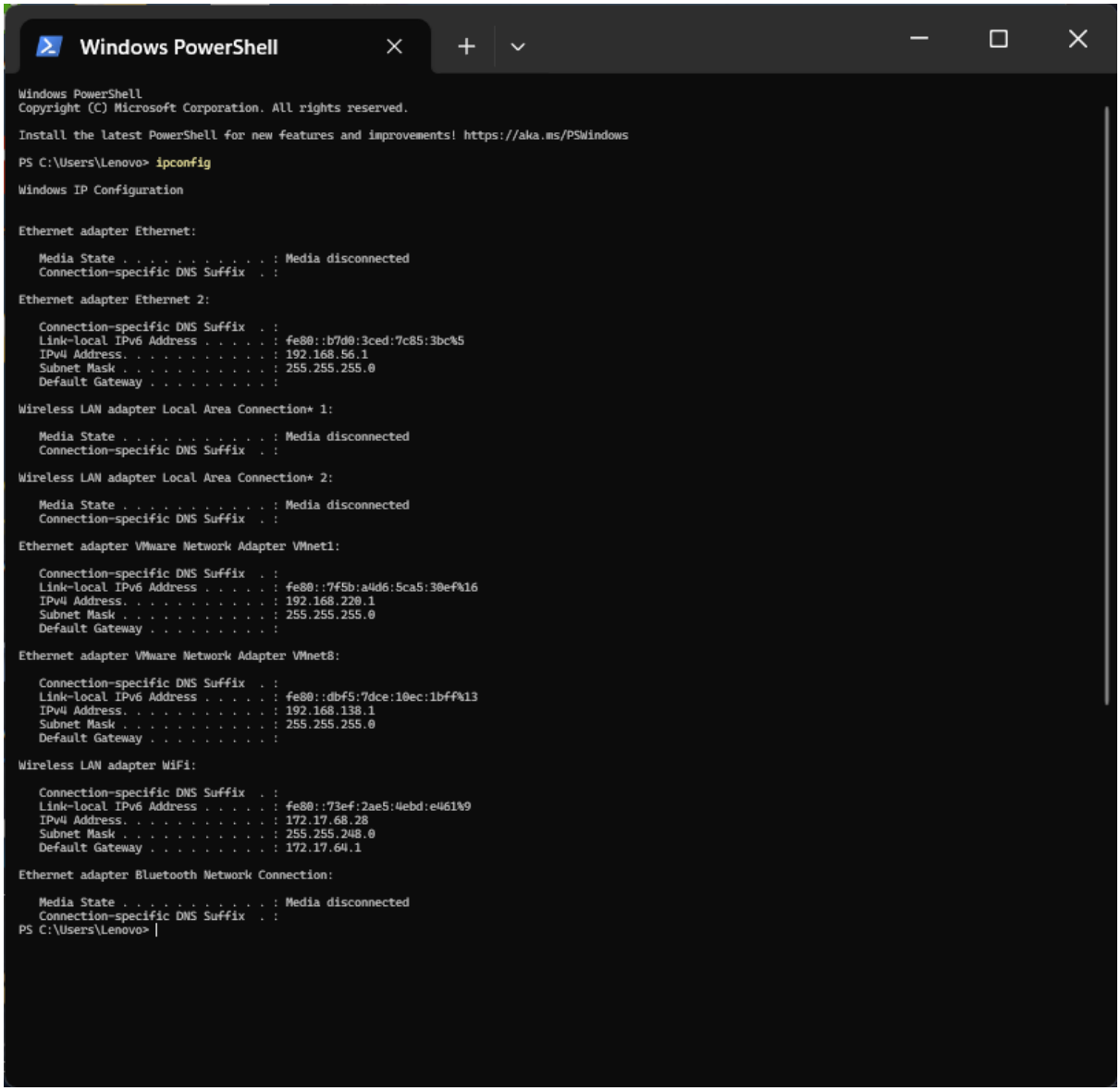

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
ASA5506(config)#ssh 192.168.1.0 255.255.255.0
% Incomplete command.
ASA5506(config)#ssh 192.168.1.0 255.255.255.0 inside
ASA5506(config)#ssh tim
ASA5506(config)#ssh timeout 10
ASA5506(config)#
ASA5506(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste

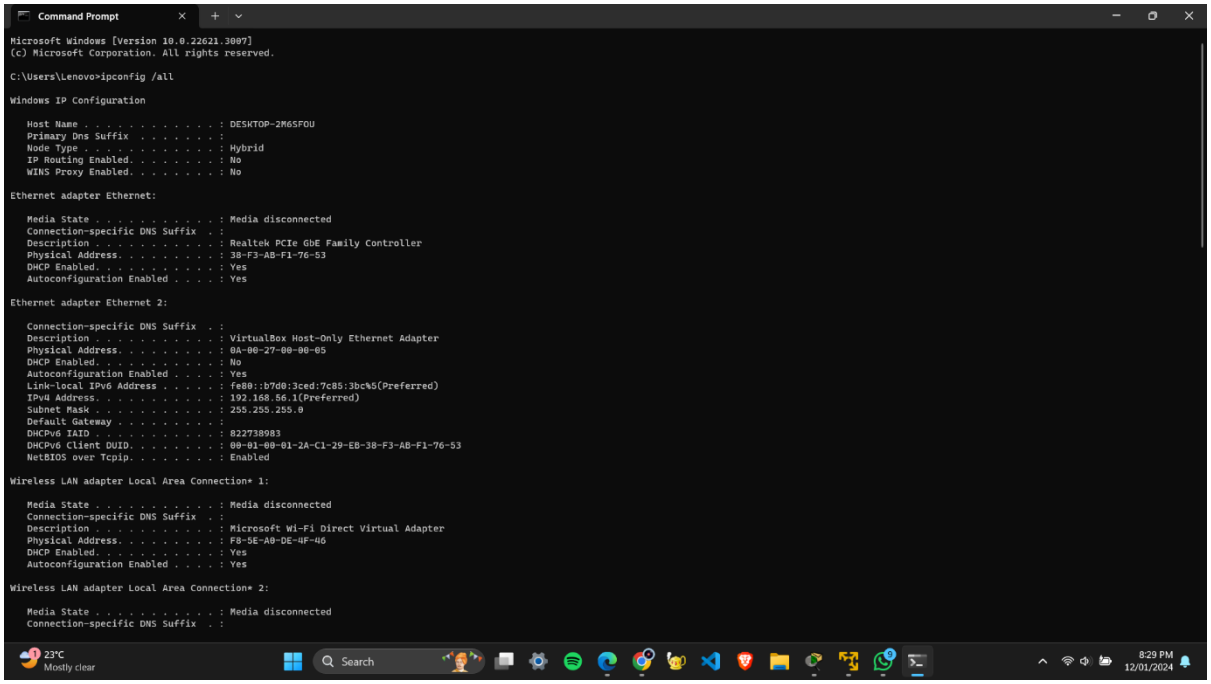


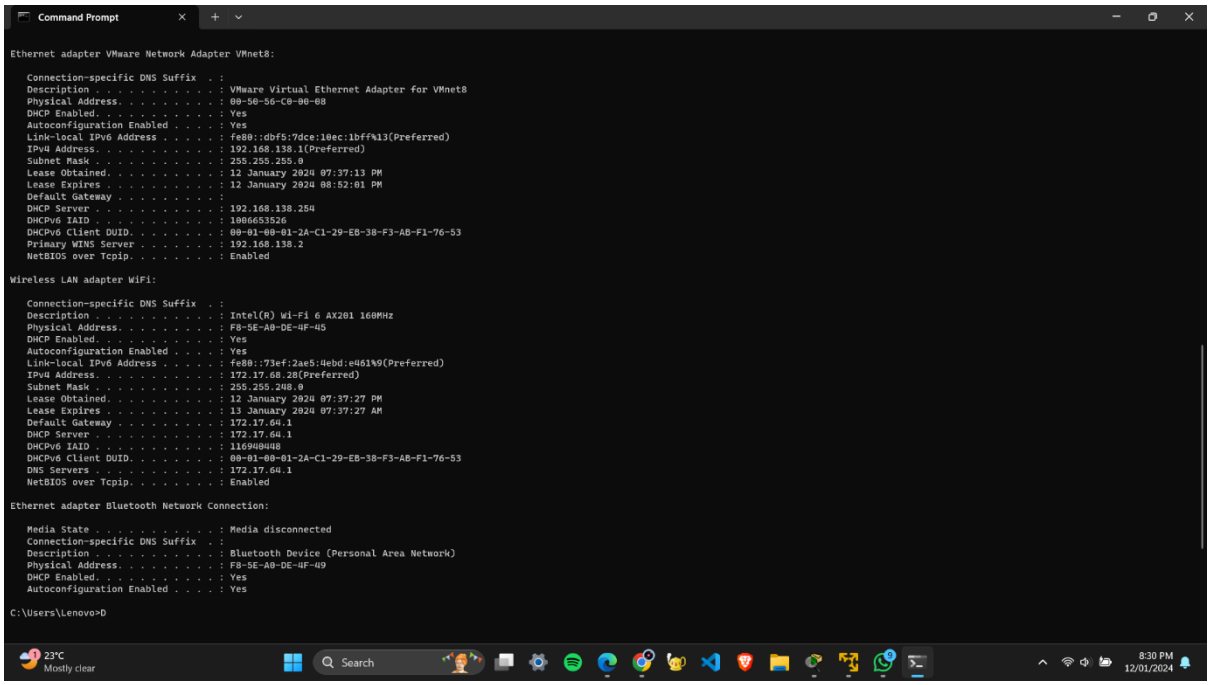
Question 2 [5 Marks]

i. Give screenshot of System IP, Kali Linux IP and Metasploitable IP (3 Marks)

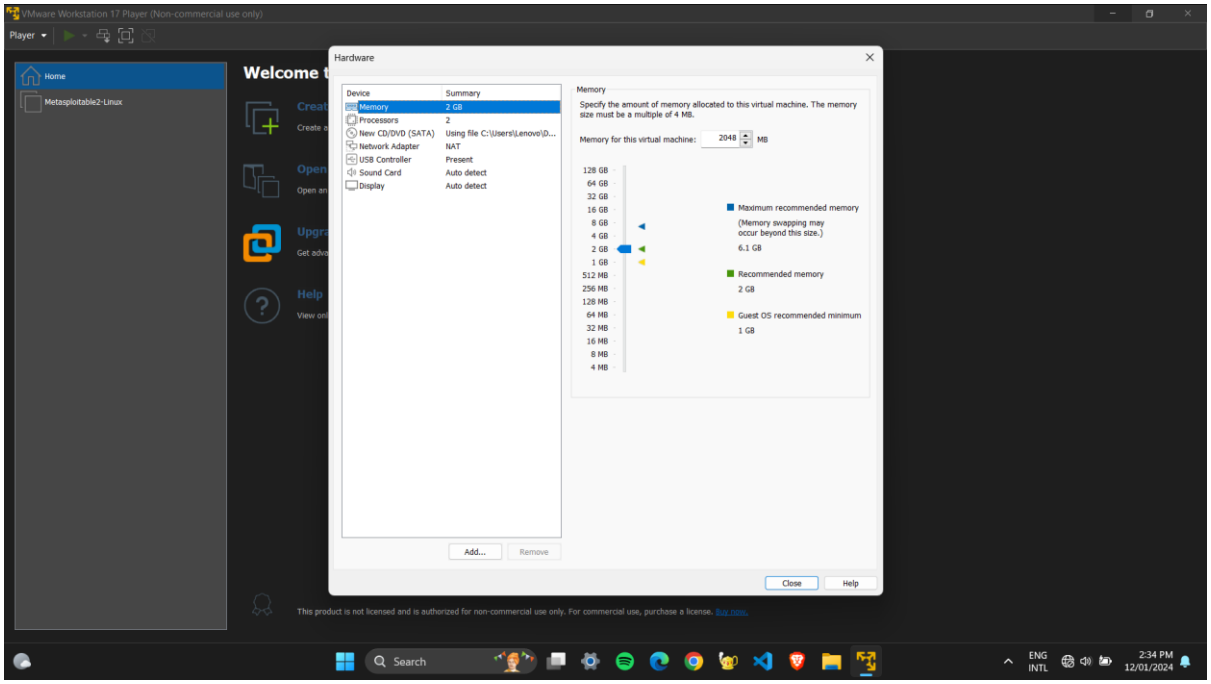
SYSTEM IP

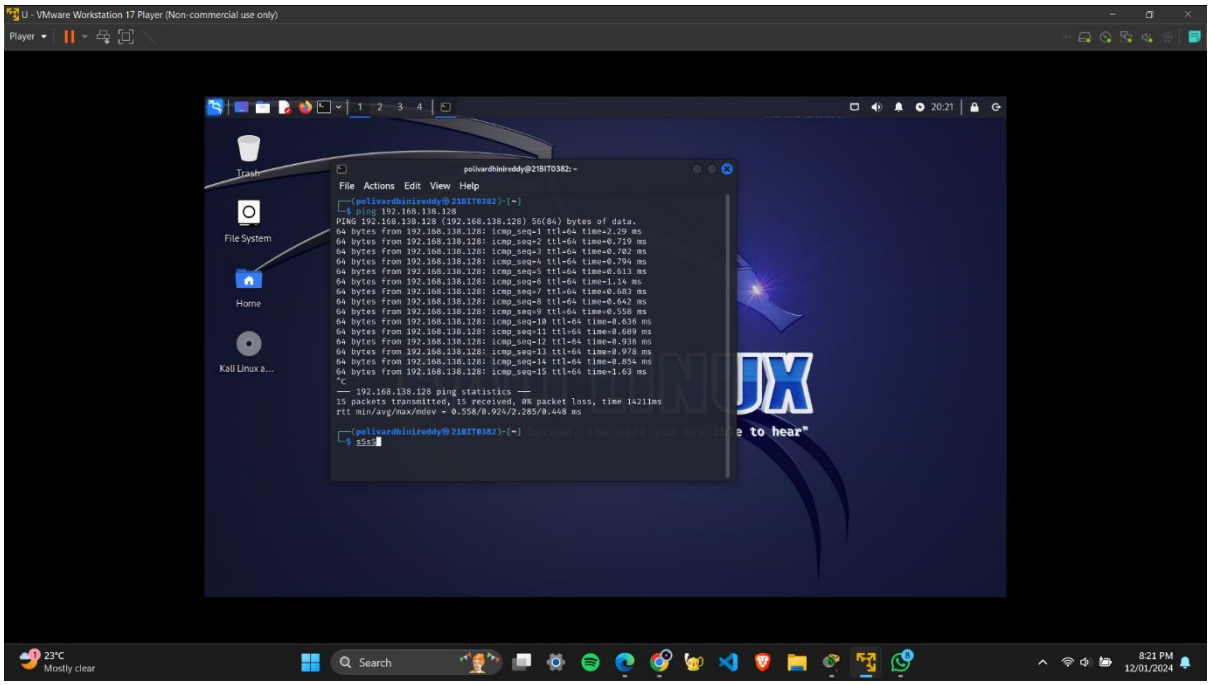

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Lenovo> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b7d0:3ced:7c85:3bc%5
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::7f5b:a4d6:5ca5:30ef%16
IPv4 Address. . . . . : 192.168.220.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::dbf5:7dce:10ec:1bff%13
IPv4 Address. . . . . : 192.168.138.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter WiFi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::73ef:2ae5:4ebd:e461%9
IPv4 Address. . . . . : 172.17.68.28
Subnet Mask . . . . . : 255.255.248.0
Default Gateway . . . . . : 172.17.64.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
PS C:\Users\Lenovo>



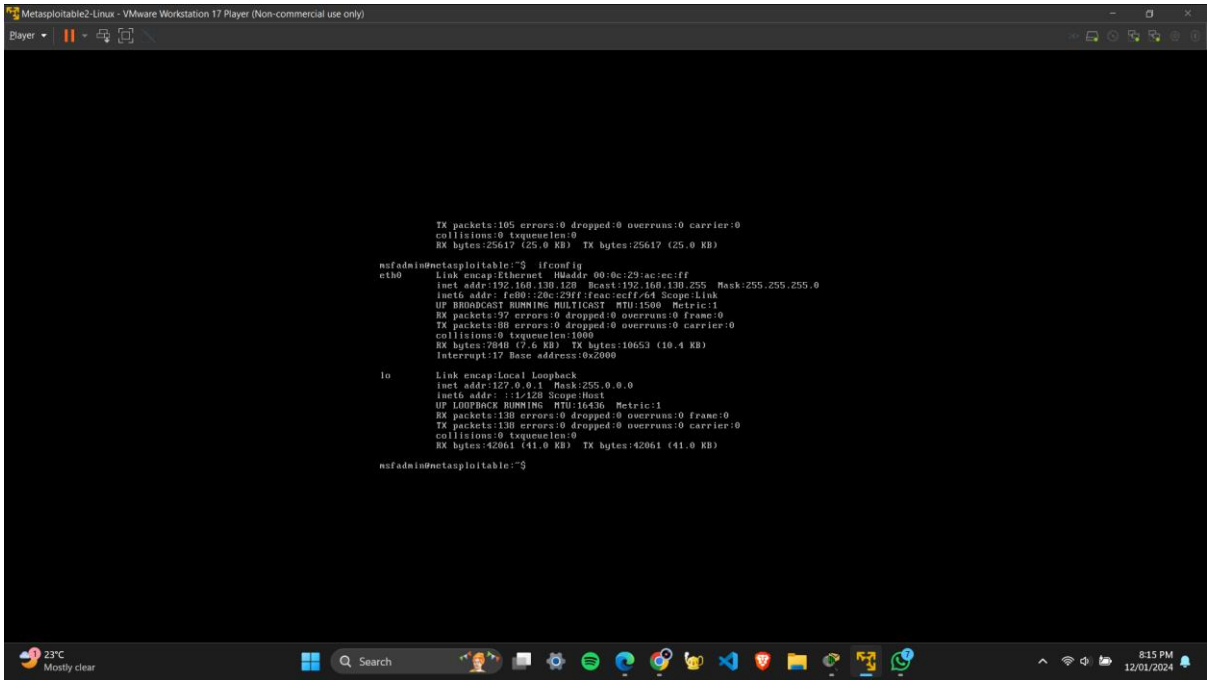
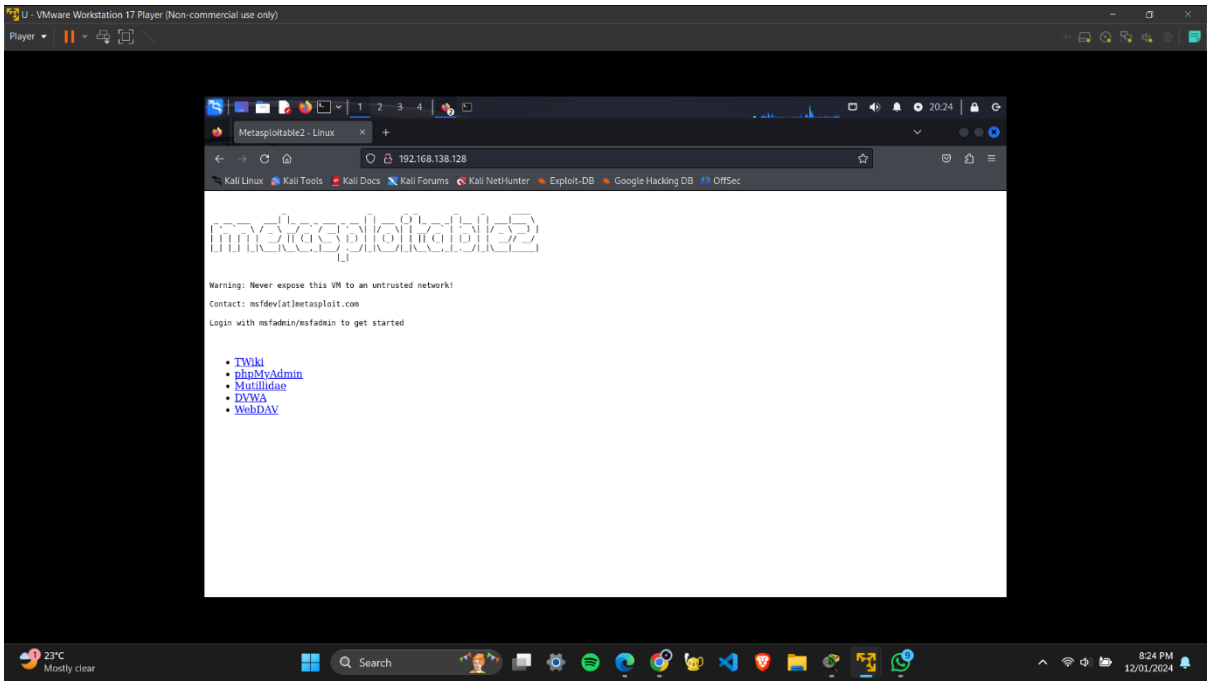


KALI LINUX IP





Metasploitable IP



ii. ii. Run Metasploitable IP in firefox browser of Kali. Give Screenshot (2 Marks)