

CSE3501-Information Security Analysis and Audit Lab

NAME- HRITIK DUBEY REG NO-19BIT0150 SLOT- L41+L42

DIGITAL ASSIGNMENT 1

Faculty : Dr. Priya V

Drive link -

https://drive.google.com/drive/folders/14YZQp8UiSnI3ydqcQSvFREH3Ick_8Jxd?usp=sharing

Question 1.

Changing the name of PC & Router using CLI



```
Router>en
Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#hostname Hritik1
Hritik1(config)#do sh run
Building configuration...

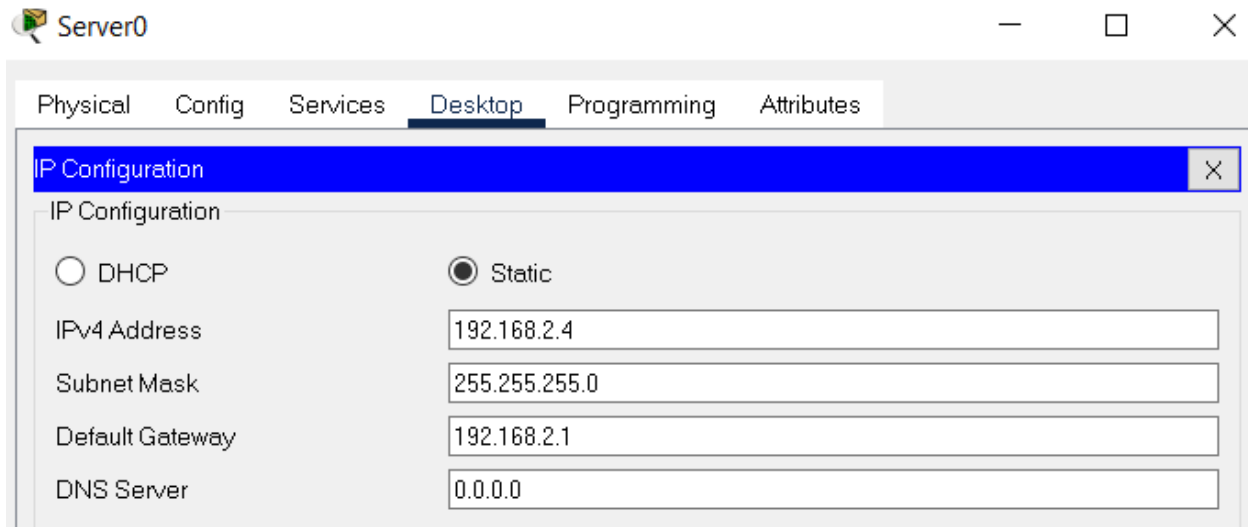
Current configuration : 740 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Hritik1
!
```

```
Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#hostname Hritik2
Hritik2(config)#
Hritik2(config)#
```

Configured DNS server with server

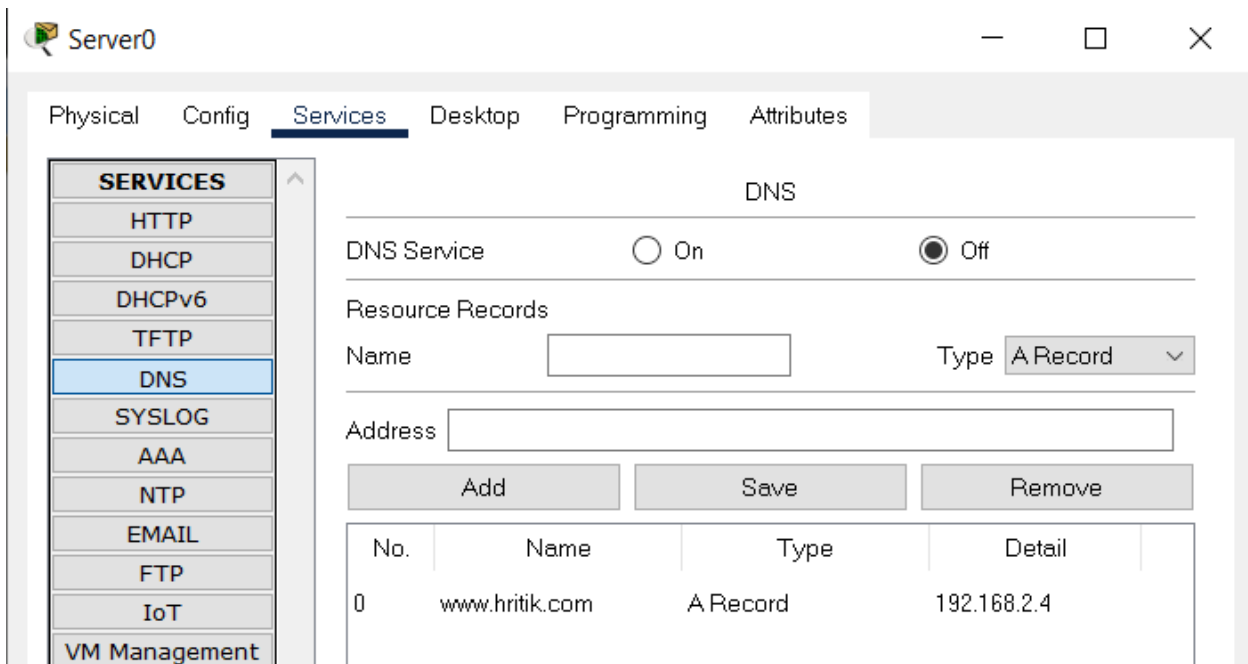
Name : www.hritik.com

IP : 192.168.2.4 Default gateway : 192.168.2.1



The screenshot shows the 'IP Configuration' window for 'Server0'. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Static' radio button is chosen. The fields are filled with: IPv4 Address: 192.168.2.4, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1, and DNS Server: 0.0.0.0.

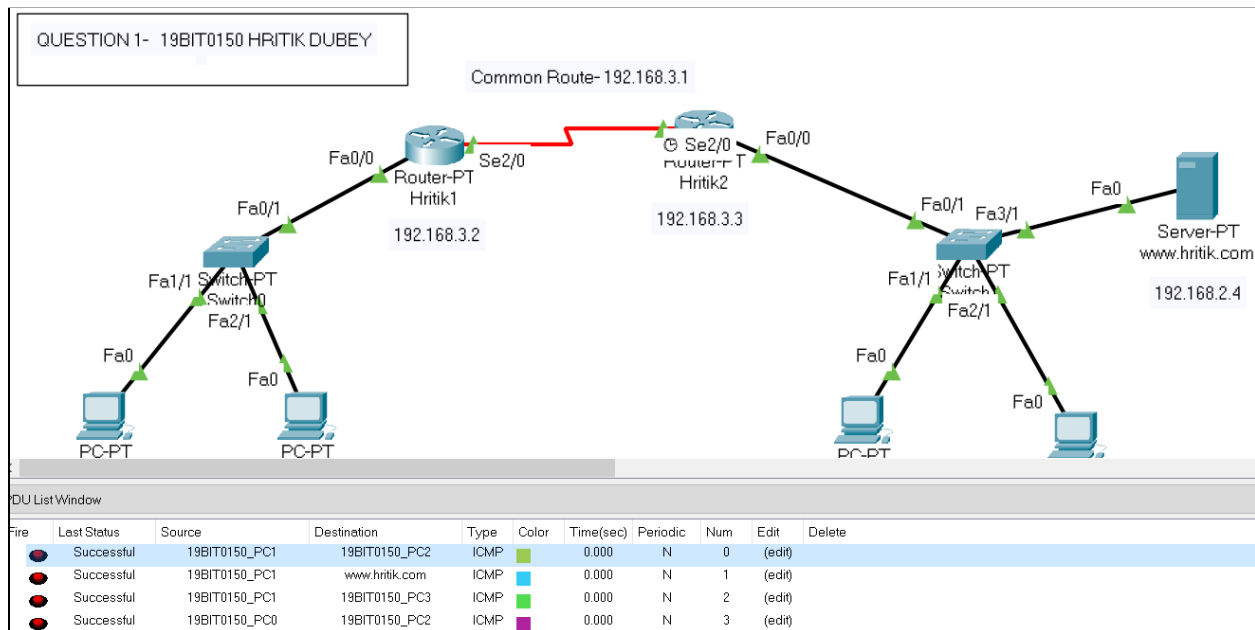
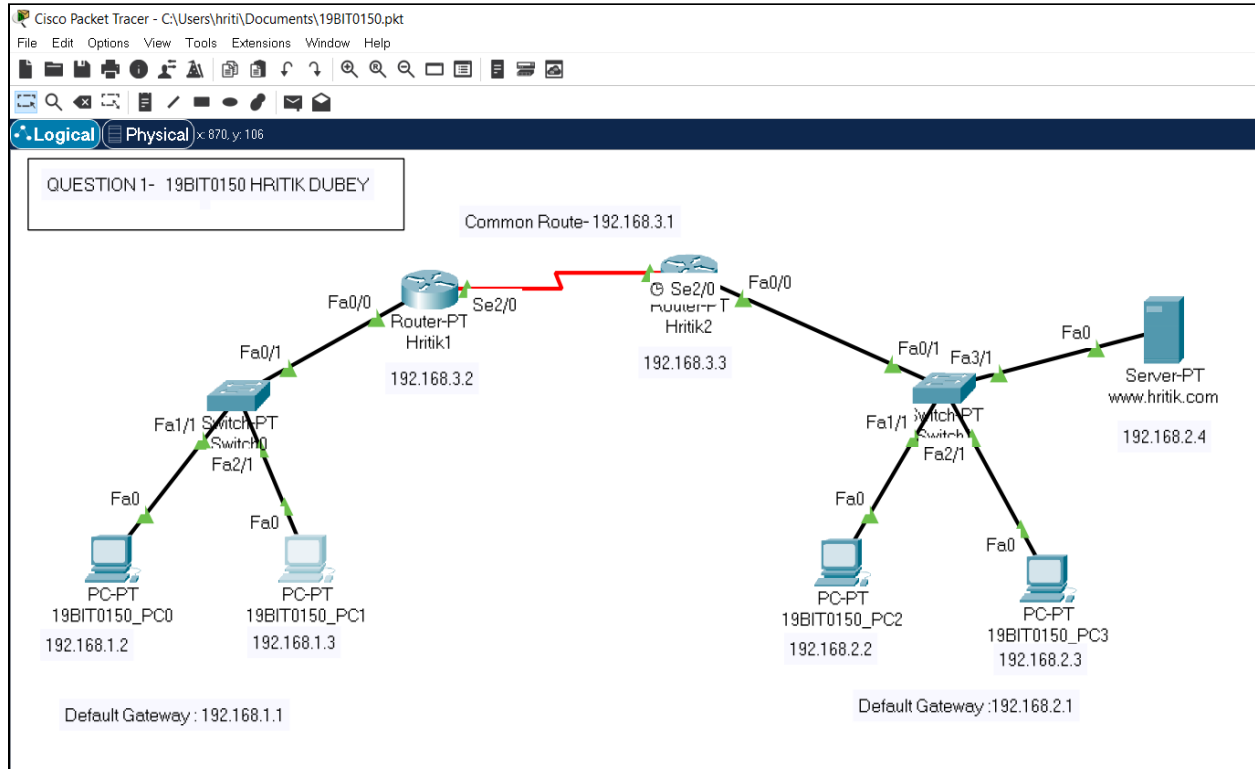
Field	Value
IPv4 Address	192.168.2.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0



The screenshot shows the 'DNS' configuration window for 'Server0'. The 'Services' tab is selected. The 'DNS Service' is set to 'Off'. The 'Resource Records' section shows a table with one record: 'www.hritik.com' of type 'A Record' with address '192.168.2.4'.

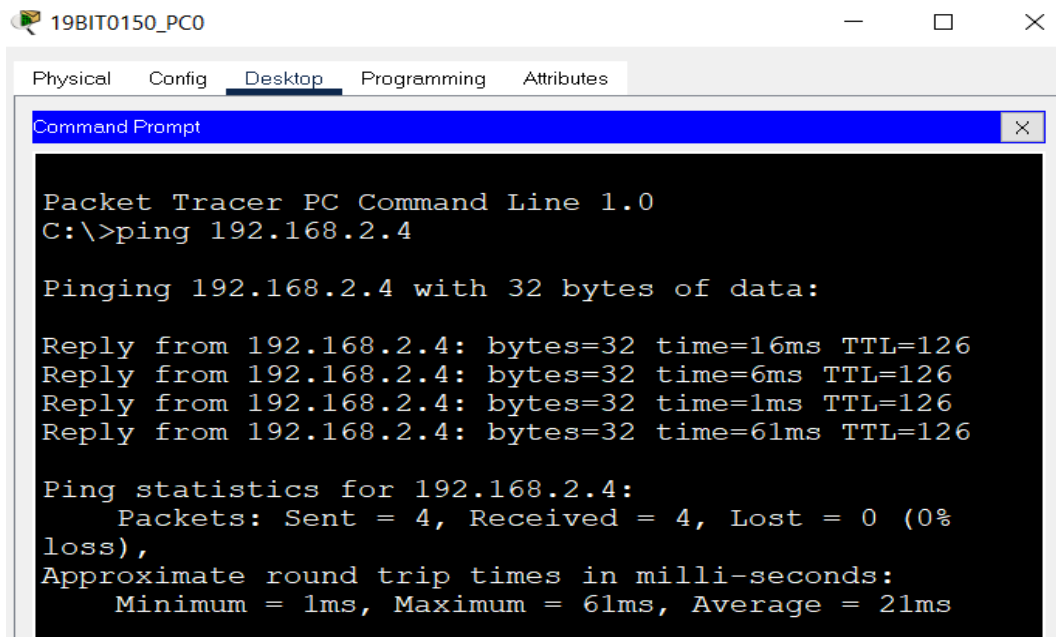
No.	Name	Type	Detail
0	www.hritik.com	A Record	192.168.2.4

Configured Devices, Interface & Routing Service



Configured Extended ACL

Before applying ACL, ping from 19BIT0150_PC0 to server



The screenshot shows a Packet Tracer PC window for 19BIT0150_PC0. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 192.168.2.4, which is successful. The output includes details about the data size (32 bytes), response times (16ms, 6ms, 1ms, 61ms), and TTL (126). Ping statistics show 4 packets sent, 4 received, and 0 lost (0% loss). Approximate round trip times are: Minimum = 1ms, Maximum = 61ms, Average = 21ms.

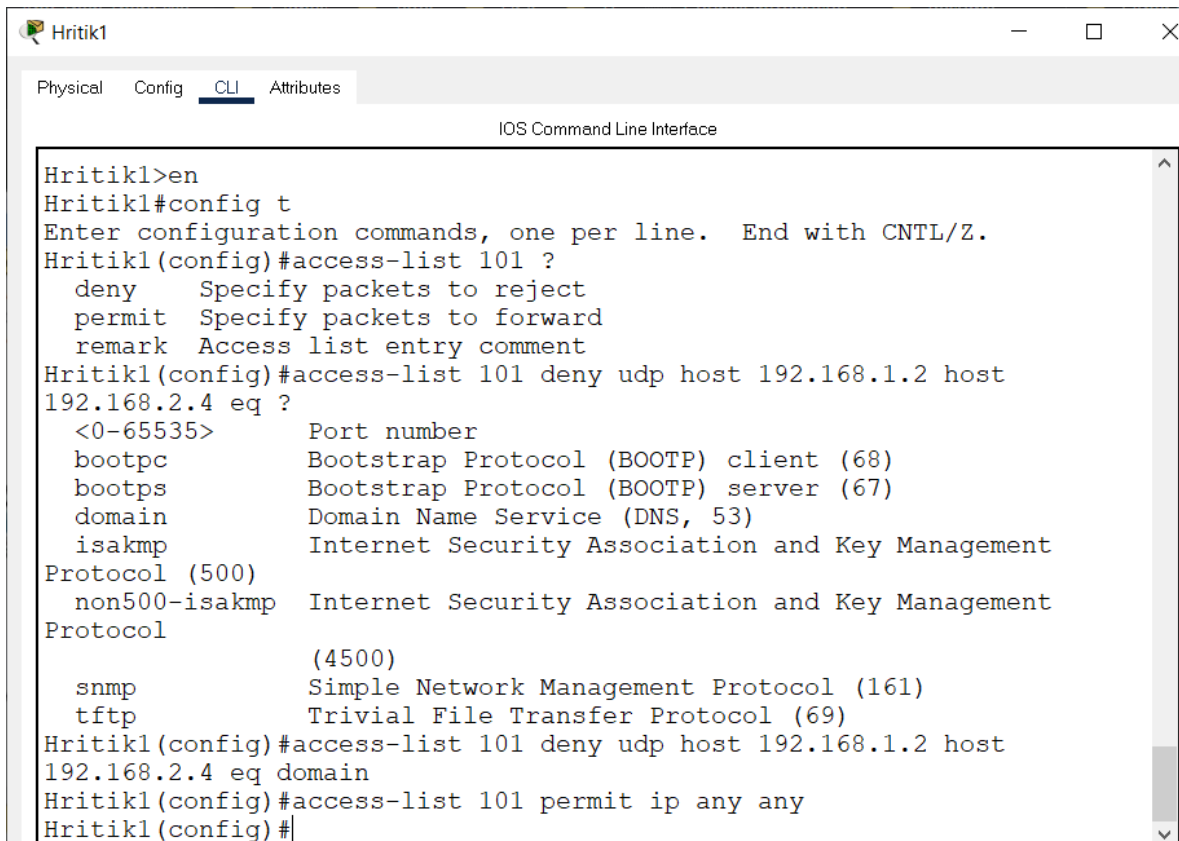
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=16ms TTL=126
Reply from 192.168.2.4: bytes=32 time=6ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=61ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 61ms, Average = 21ms
```

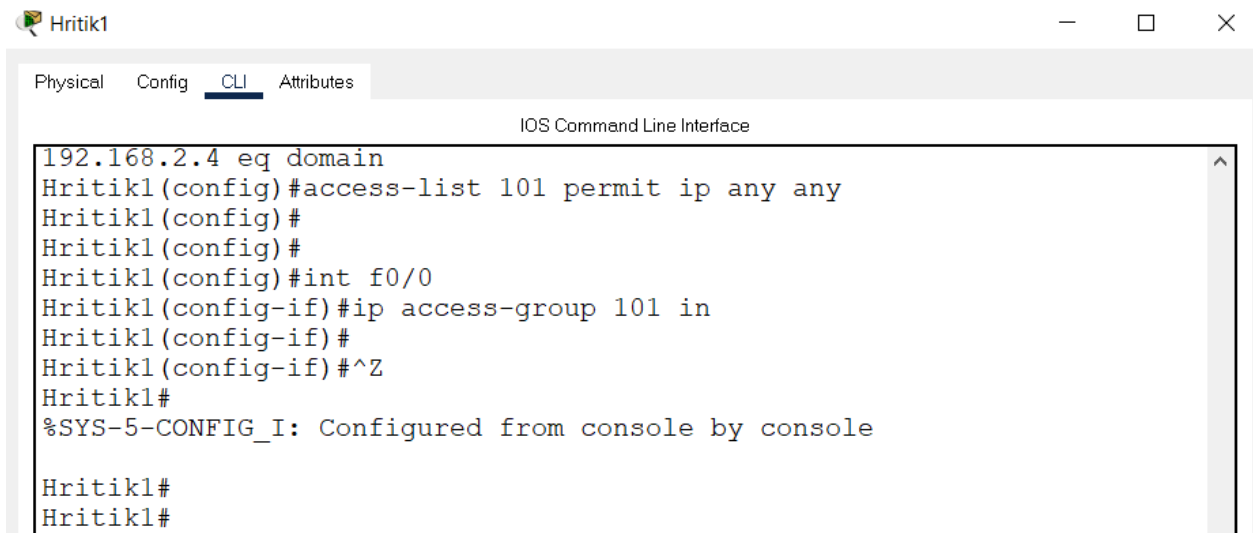
****Extended ACL is placed near the source so we will configure Hritik1 router****



The screenshot shows the CLI of the Hritik1 router. The user enters 'en' to enter enable mode, then 'config t' to enter configuration mode. They then create an extended access list 101, denying UDP traffic from 192.168.1.2 to 192.168.2.4 on port 500. The configuration is shown as it is entered, with a list of available protocols and their port numbers for reference. Finally, the user enters 'access-list 101 permit ip any any' to allow all other traffic.

```
Hritik1>en
Hritik1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Hritik1(config)#access-list 101 ?
    deny      Specify packets to reject
    permit    Specify packets to forward
    remark    Access list entry comment
Hritik1(config)#access-list 101 deny udp host 192.168.1.2 host
192.168.2.4 eq ?
    <0-65535>  Port number
    bootpc    Bootstrap Protocol (BOOTP) client (68)
    bootps    Bootstrap Protocol (BOOTP) server (67)
    domain    Domain Name Service (DNS, 53)
    isakmp    Internet Security Association and Key Management
Protocol (500)
    non500-isakmp Internet Security Association and Key Management
Protocol
                  (4500)
    snmp      Simple Network Management Protocol (161)
    tftp      Trivial File Transfer Protocol (69)
Hritik1(config)#access-list 101 deny udp host 192.168.1.2 host
192.168.2.4 eq domain
Hritik1(config)#access-list 101 permit ip any any
Hritik1(config)#
```

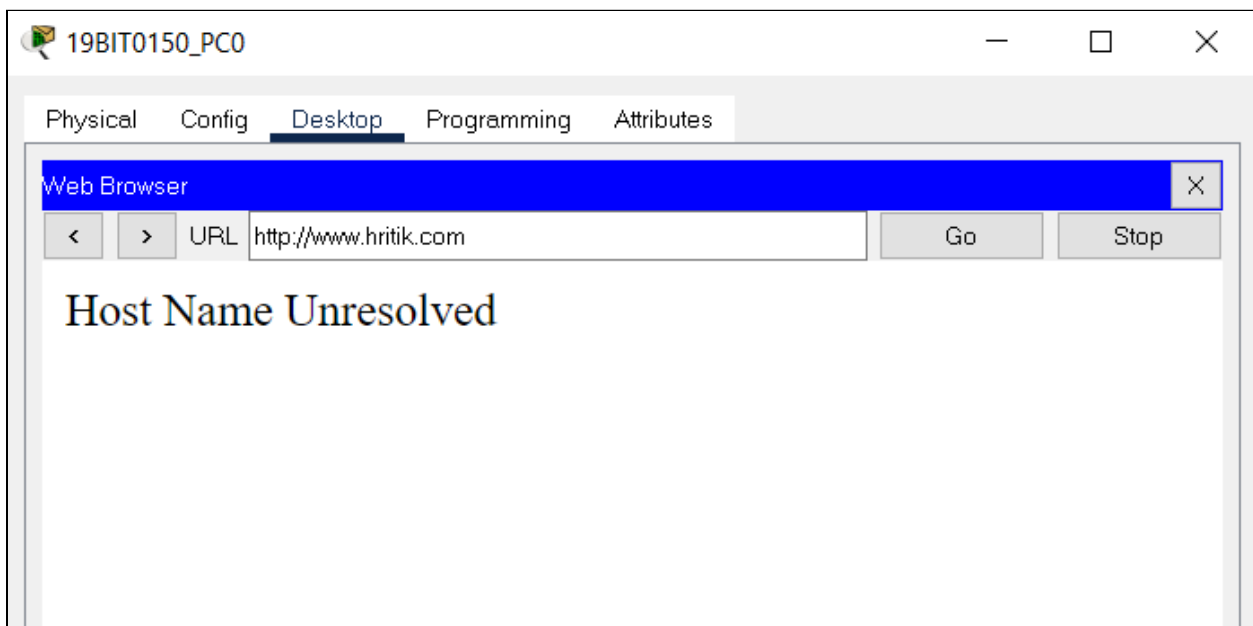
****Extended ACL start with access list 101** To interface f0/0**



The screenshot shows a terminal window titled 'Hritik1' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The following commands are entered:

```
192.168.2.4 eq domain
Hritik1(config)#access-list 101 permit ip any any
Hritik1(config)#
Hritik1(config)#
Hritik1(config)#int f0/0
Hritik1(config-if)#ip access-group 101 in
Hritik1(config-if)#
Hritik1(config-if)#^Z
Hritik1#
%SYS-5-CONFIG_I: Configured from console by console
Hritik1#
Hritik1#
```

Connecting the server...



Question 2.

Configure the routers and rename with your First name using CLI

```
Router#
Router#
Router#
Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#hostname Hritik_R0
Hritik_R0(config)#exit
Hritik_R0#
%SYS-5-CONFIG_I: Configured from console by console

Hritik R0#

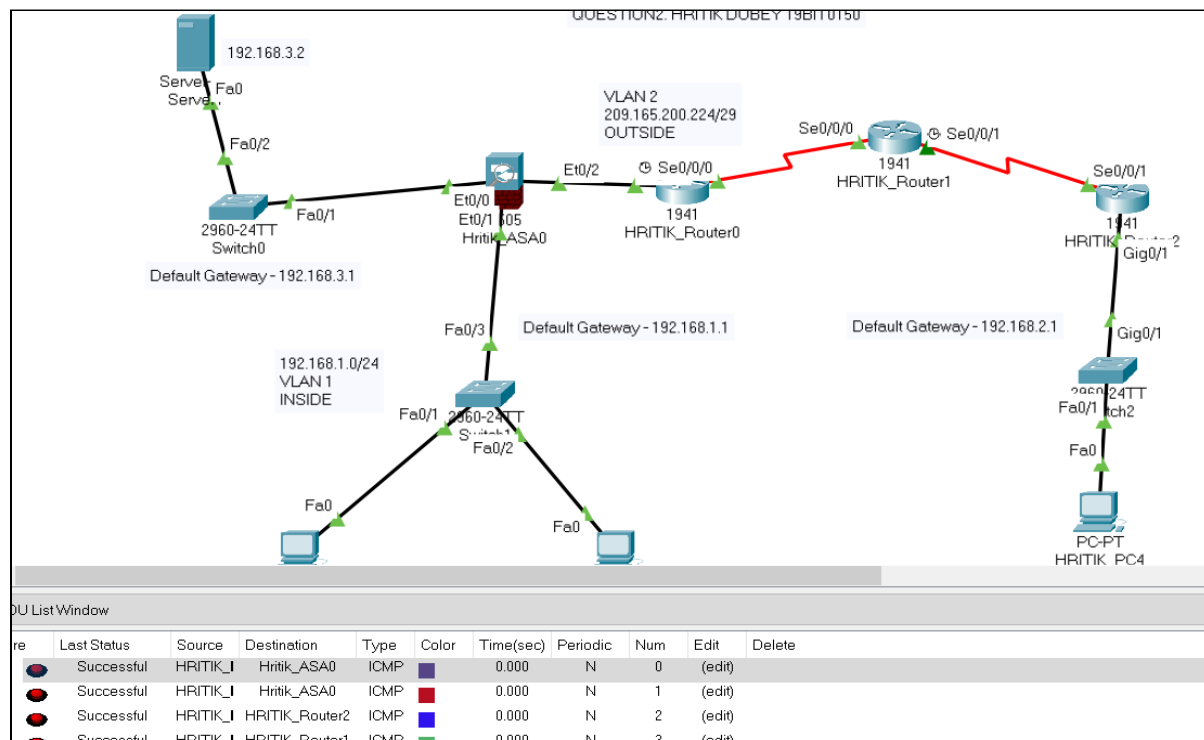
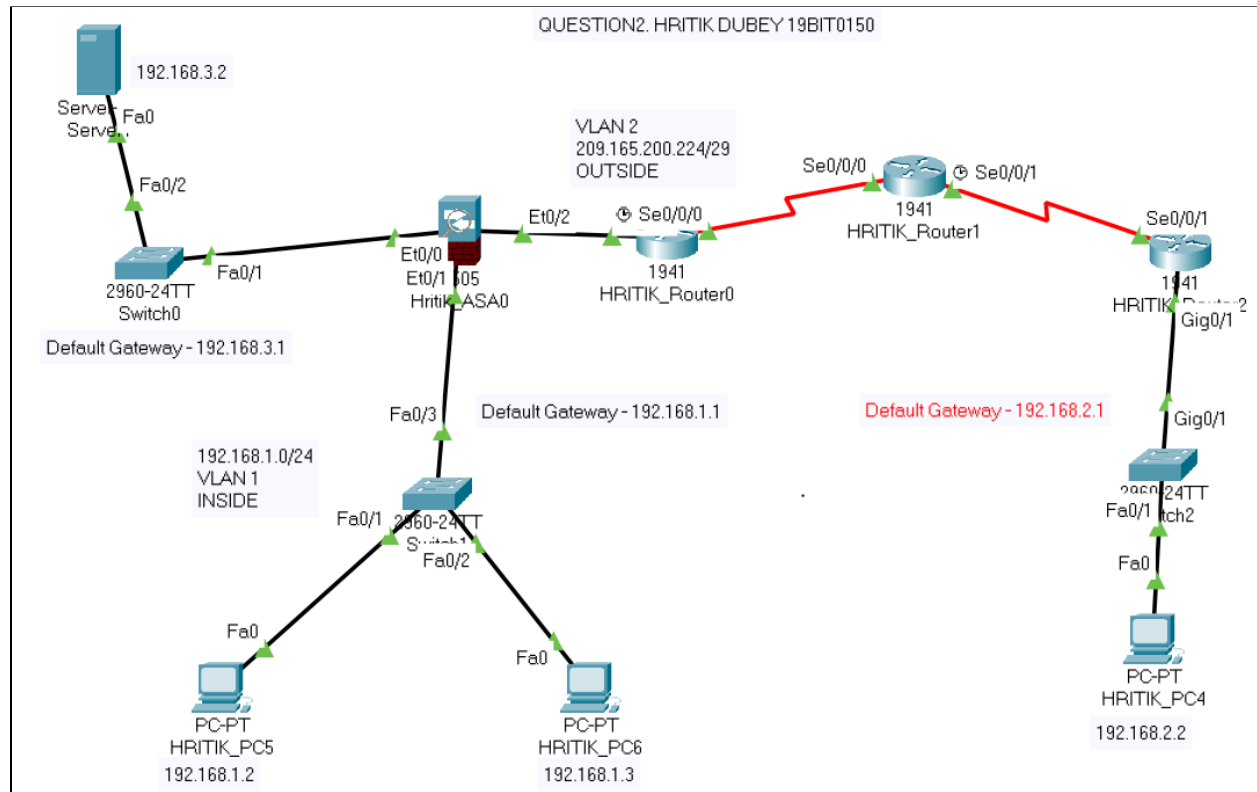
Router>en
Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#hostname Hritik_R1
Hritik_R1(config)#exit
Hritik_R1#
%SYS-5-CONFIG_I: Configured from console by console

Hritik R1#

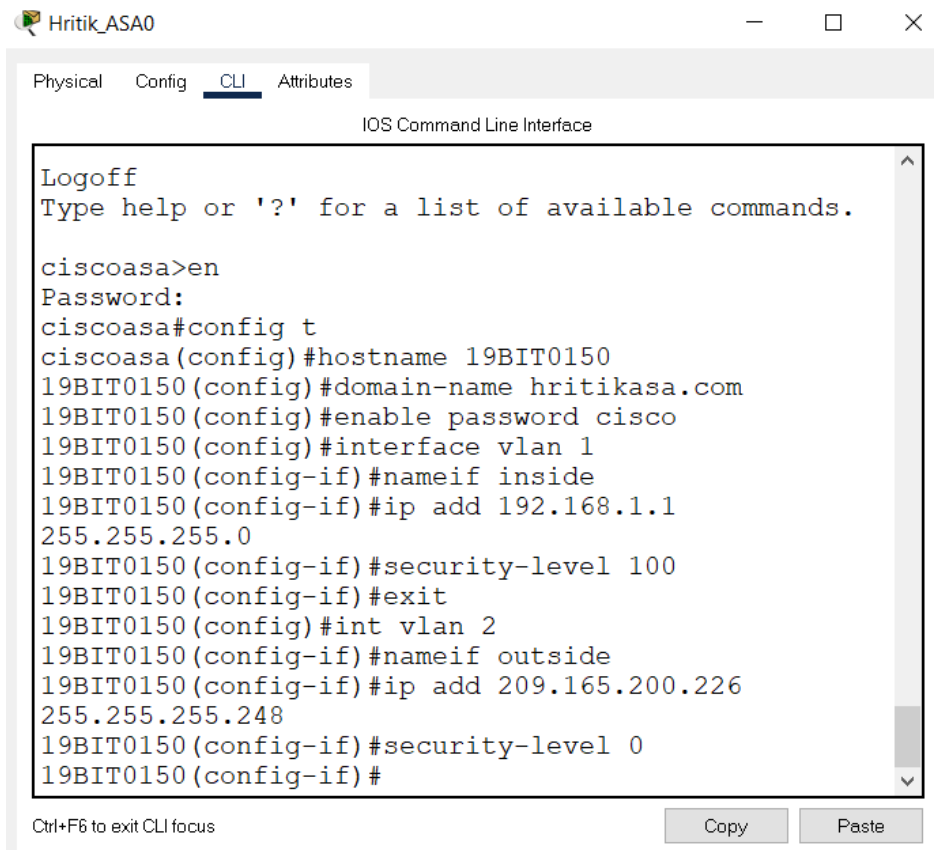
Router>en
Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#hostname Hritik_R2
Hritik_R2(config)#exit
Hritik_R2#
%SYS-5-CONFIG_I: Configured from console by console

Hritik R2#
```

Configure the devices, interfaces & servers



Configure basic ASA settings

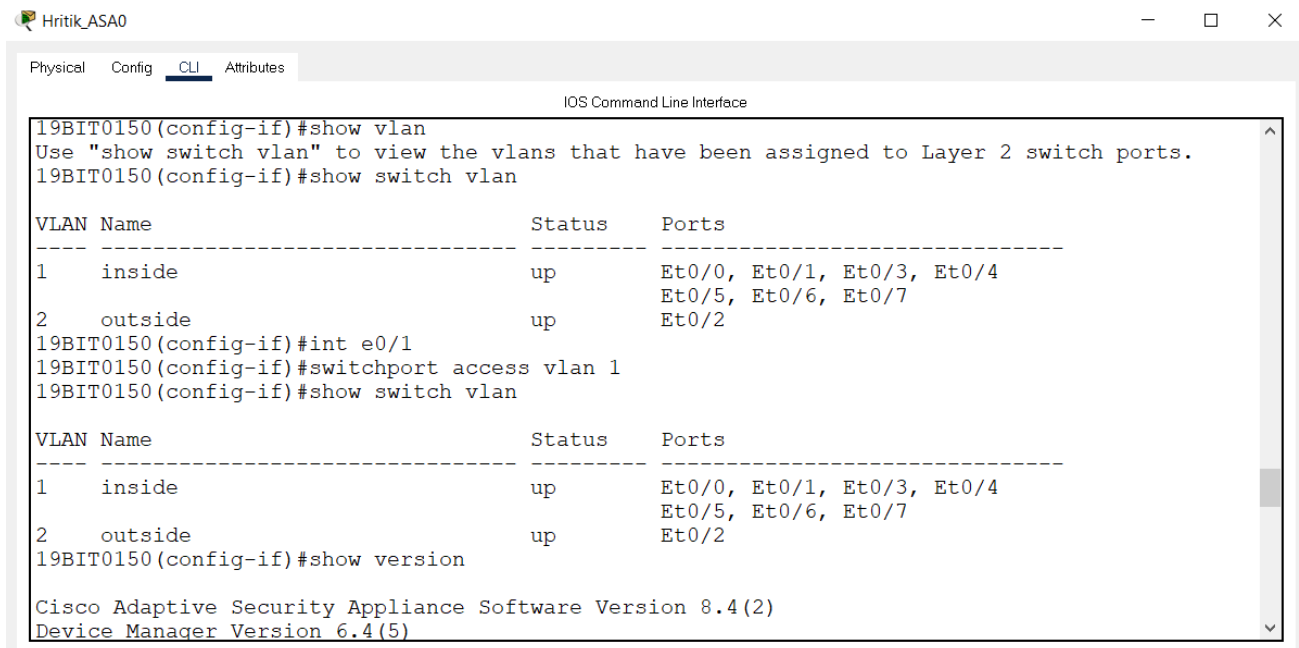


Logoff
Type help or '?' for a list of available commands.

```
ciscoasa>en
Password:
ciscoasa#config t
ciscoasa(config)#hostname 19BIT0150
19BIT0150(config)#domain-name hritikasa.com
19BIT0150(config)#enable password cisco
19BIT0150(config)#interface vlan 1
19BIT0150(config-if)#nameif inside
19BIT0150(config-if)#ip add 192.168.1.1
255.255.255.0
19BIT0150(config-if)#security-level 100
19BIT0150(config-if)#exit
19BIT0150(config)#int vlan 2
19BIT0150(config-if)#nameif outside
19BIT0150(config-if)#ip add 209.165.200.226
255.255.255.248
19BIT0150(config-if)#security-level 0
19BIT0150(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste



```
19BIT0150(config-if)#show vlan
Use "show switch vlan" to view the vlans that have been assigned to Layer 2 switch ports.
19BIT0150(config-if)#show switch vlan
```

VLAN	Name	Status	Ports
1	inside	up	Et0/0, Et0/1, Et0/3, Et0/4 Et0/5, Et0/6, Et0/7
2	outside	up	Et0/2

```
19BIT0150(config-if)#int e0/1
19BIT0150(config-if)#switchport access vlan 1
19BIT0150(config-if)#show switch vlan
```

VLAN	Name	Status	Ports
1	inside	up	Et0/0, Et0/1, Et0/3, Et0/4 Et0/5, Et0/6, Et0/7
2	outside	up	Et0/2

```
19BIT0150(config-if)#show version

Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)
```



```

19BIT0150(config-if)#show int ip brief
Interface          IP-Address      OK? Method
Status             Protocol

Ethernet0/0        unassigned      YES unset
up                 up

Ethernet0/1        unassigned      YES unset
up                 up

Ethernet0/2        unassigned      YES unset
up                 up

Ethernet0/3        unassigned      YES unset
down              down

Ethernet0/4        unassigned      YES unset
down              down

Ethernet0/5        unassigned      YES unset
down              down

Ethernet0/6        unassigned      YES unset
down              down

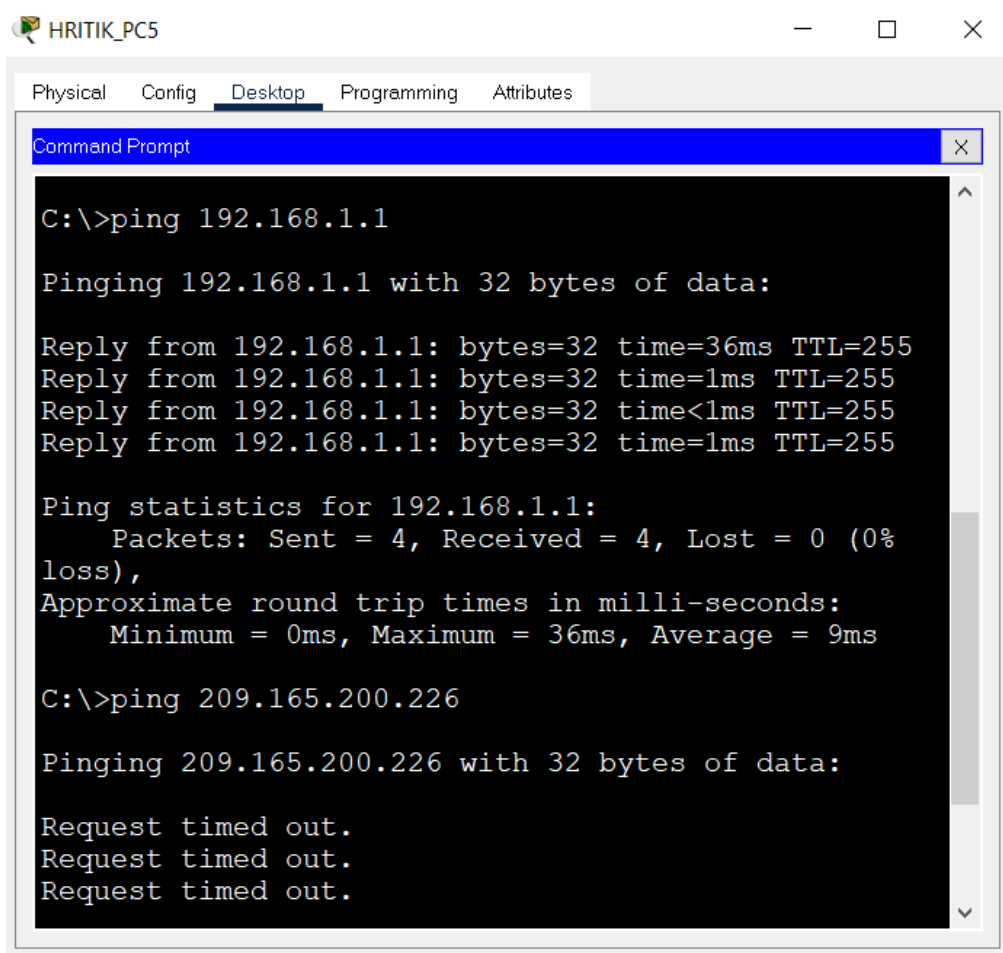
Ethernet0/7        unassigned      YES unset
down              down

Vlan1              192.168.1.1     YES manual
up                 up

Vlan2              209.165.200.226 YES manual
up                 up
19BIT0150(config-if)#

```

Ping snapshots from HRITIK PC to Firewall



HRITIK_PC5

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

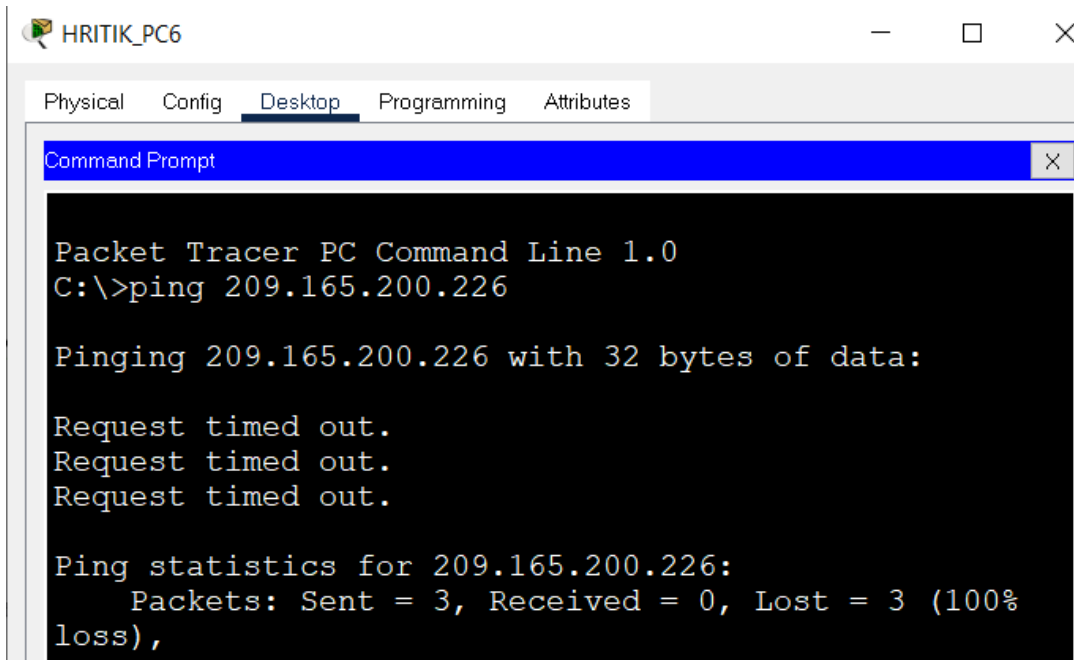
Reply from 192.168.1.1: bytes=32 time=36ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms

C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```



HRITIK_PC6

Physical Config Desktop Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.226:
    Packets: Sent = 3, Received = 0, Lost = 3 (100%
loss),
```