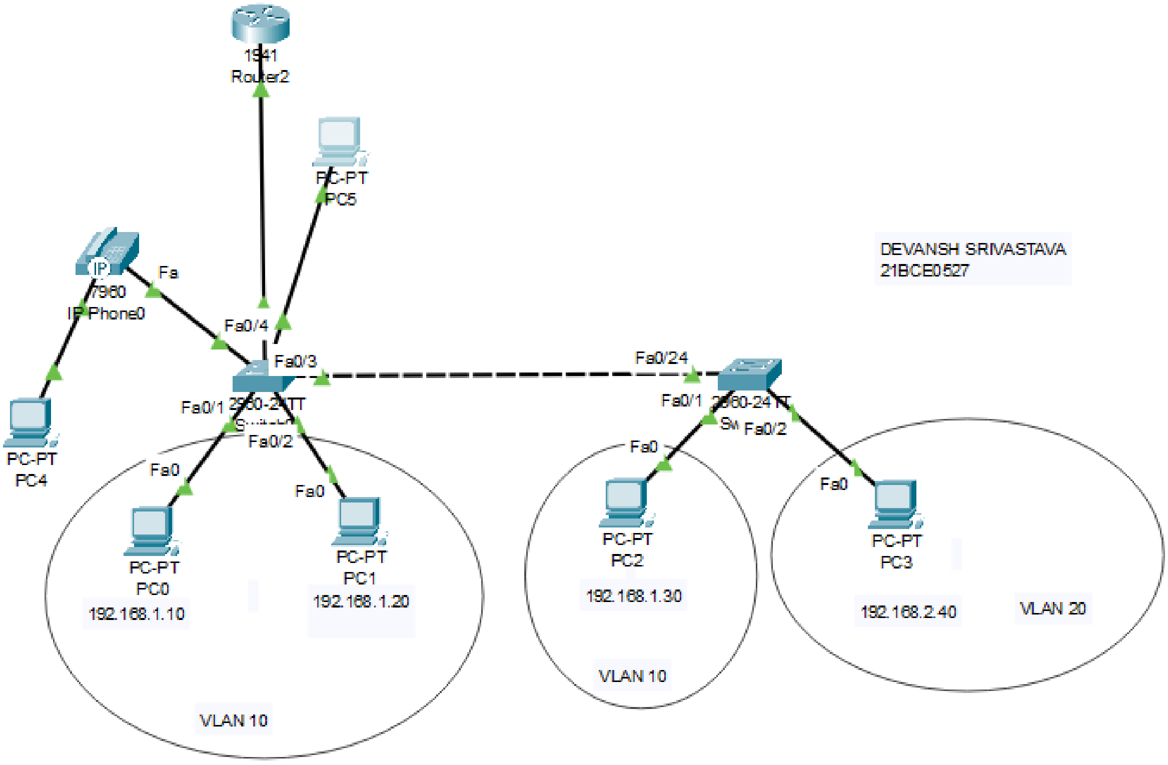
Name: Devansh Srivastava
Registration number: 21BCE0527

Network Training Programme

Module 7 and 8

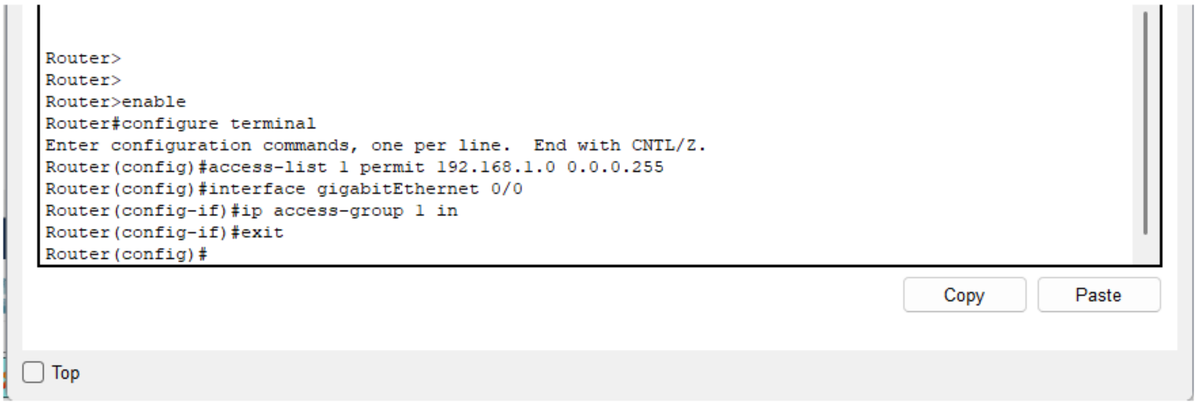
Q11-14. Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic. Configure a standard Access Control List (ACL) on a router to permit traffic from a specific IP range. Test connectivity to verify the ACL is working as intended. Create an extended ACL to block specific applications, such as HTTP or FTP traffic Test the ACL rules by attempting to access blocked services. Try Static NAT, Dynamic NAT and PAT to translate Ips

Network Diagram:



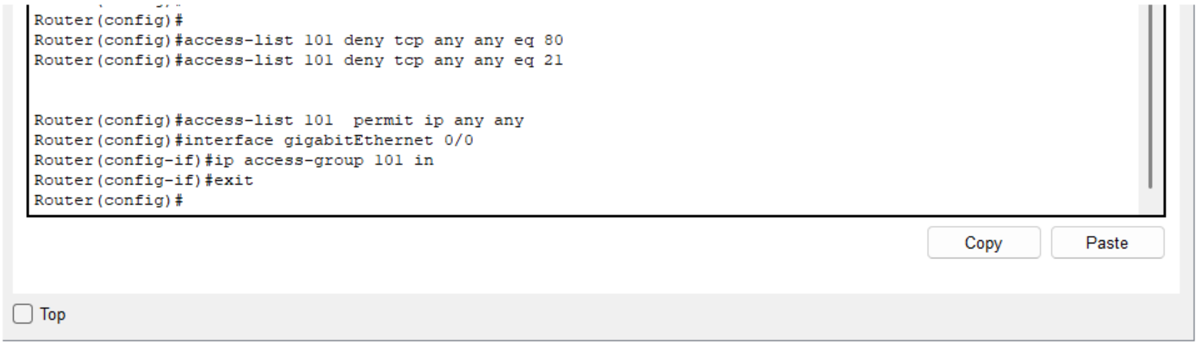
ACL configuration

Configure standard ACL:



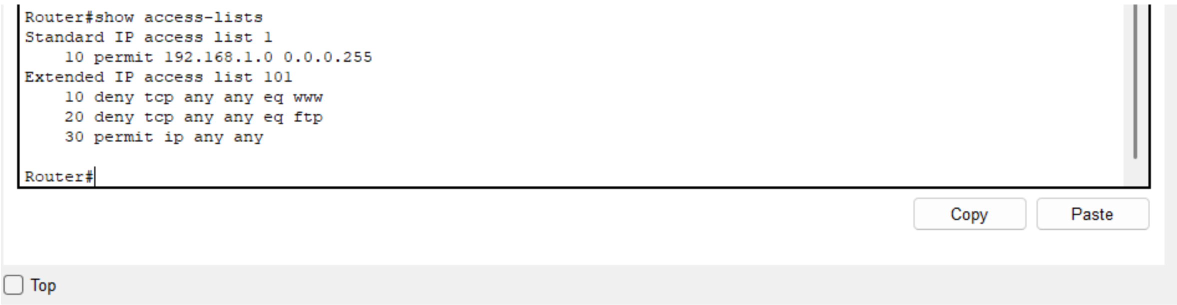
```
Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#
```

Configure extended ACL:



```
Router(config)#
Router(config)#access-list 101 deny tcp any any eq 80
Router(config)#access-list 101 deny tcp any any eq 21


Router(config)#access-list 101  permit ip any any
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#
```

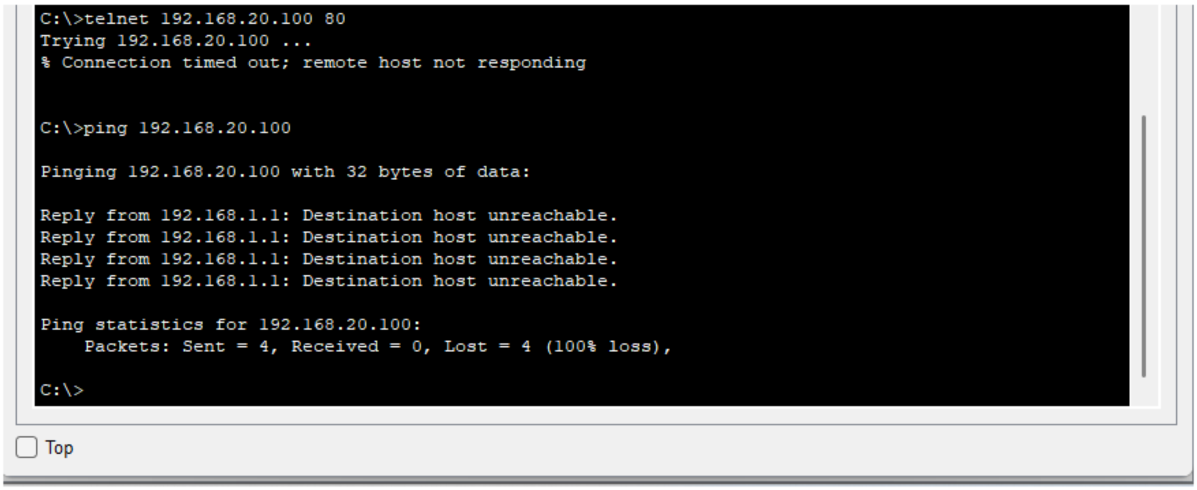
Show Access-Lists



```
Router#show access-lists
Standard IP access list 1
    10 permit 192.168.1.0 0.0.0.255
Extended IP access list 101
    10 deny tcp any any eq www
    20 deny tcp any any eq ftp
    30 permit ip any any

Router#
```

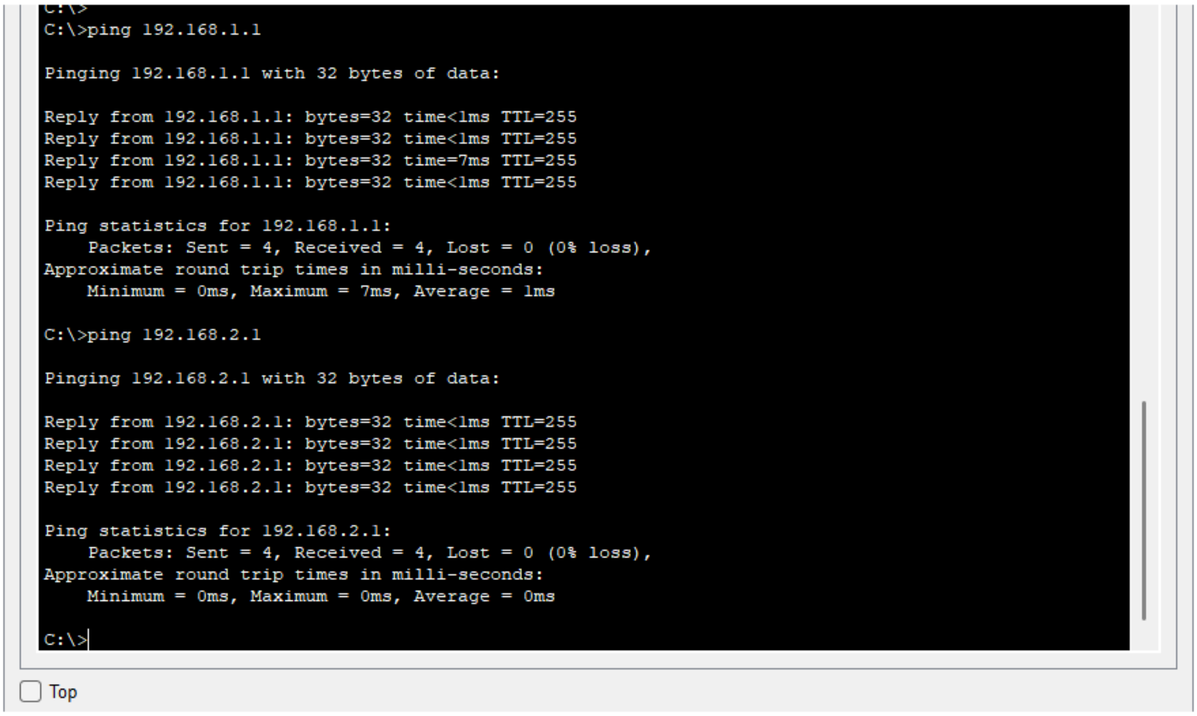
Testing ACLs:

Restricted Access



```
C:\>telnet 192.168.20.100 80
Trying 192.168.20.100 ...
% Connection timed out; remote host not responding


C:\>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

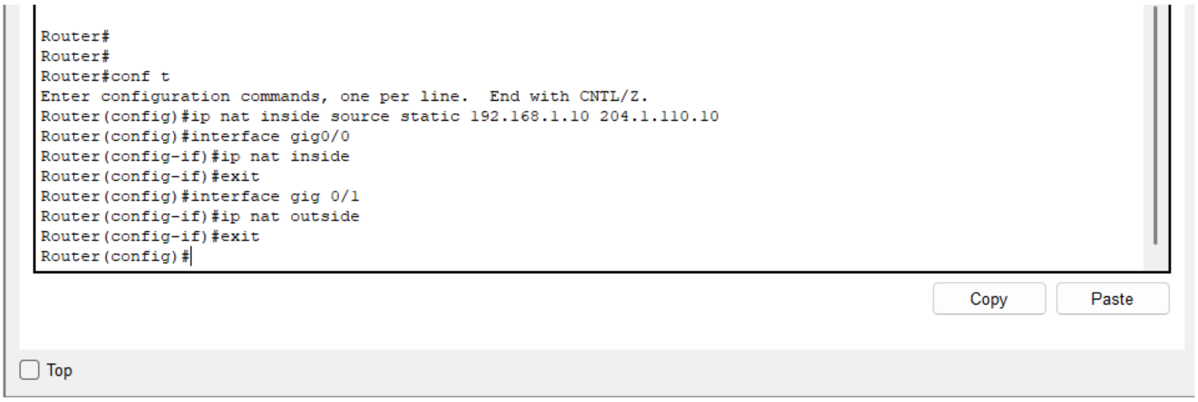
Access Permitted



```
C:\>
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<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=7ms 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 = 7ms, Average = 1ms

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

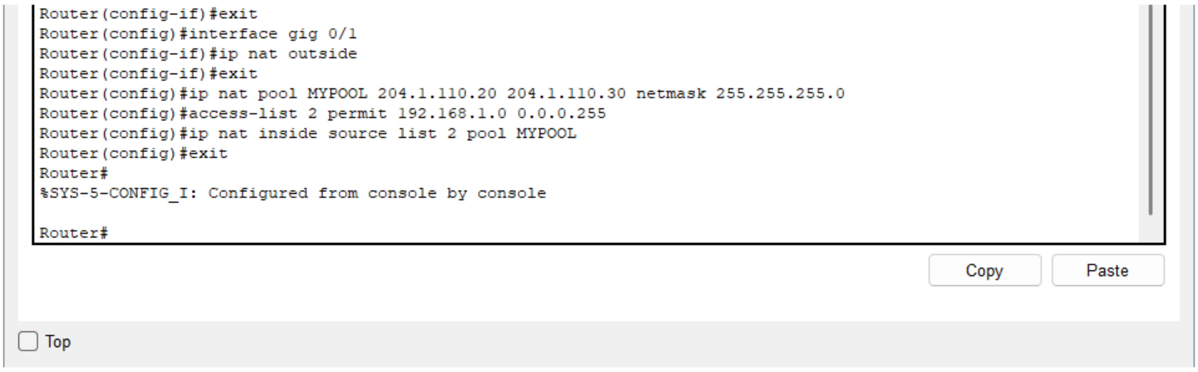
NAT configuration:

Static NAT



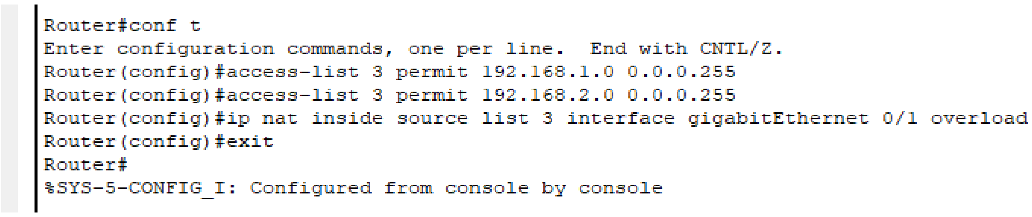
```
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.1.10 204.1.110.10
Router(config)#interface gig0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

Dynamic NAT

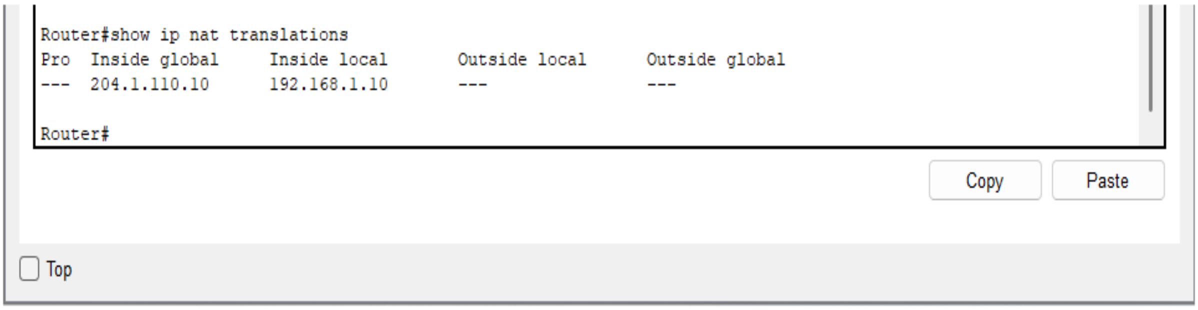


```
Router(config-if)#exit
Router(config)#interface gig 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat pool MYPOOL 204.1.110.20 204.1.110.30 netmask 255.255.255.0
Router(config)#access-list 2 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 2 pool MYPOOL
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Port Addressable Translation



```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 3 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 3 permit 192.168.2.0 0.0.0.255
Router(config)#ip nat inside source list 3 interface gigabitEthernet 0/1 overload
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```



```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  204.1.110.10      192.168.1.10       ---                ---

Router#
```

Key Learnings:

1. Standard ACLs filter traffic based on source IP address only
2. Extended ACLs filter traffic based on source/destination IP, protocol, and port numbers
3. ACLs are processed sequentially, with an implicit "deny all" at the end
4. Static NAT maps one internal IP to one external IP permanently
5. Dynamic NAT uses a pool of external IPs assigned as needed
6. PAT (overload) allows many internal IPs to share one external IP using different ports