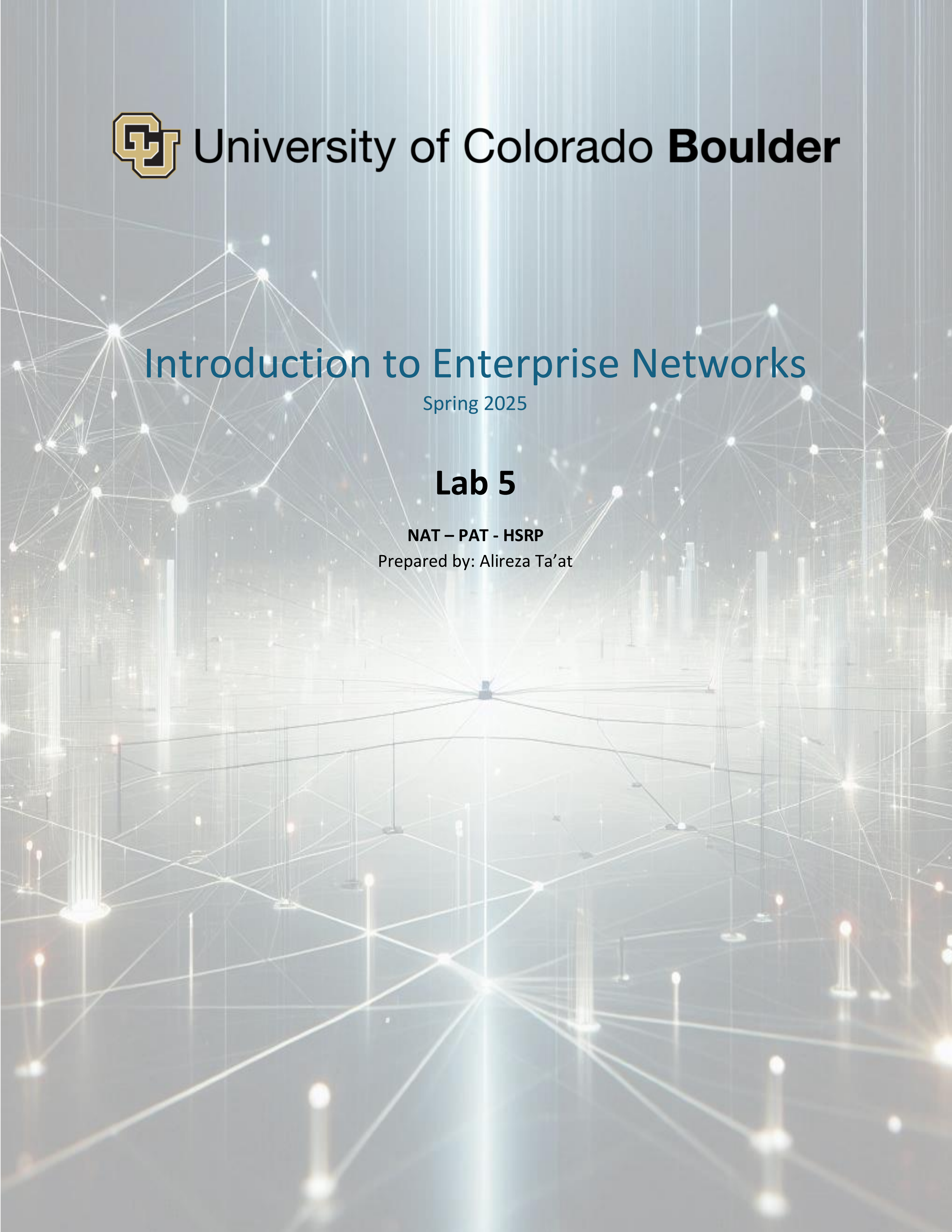


University of Colorado Boulder

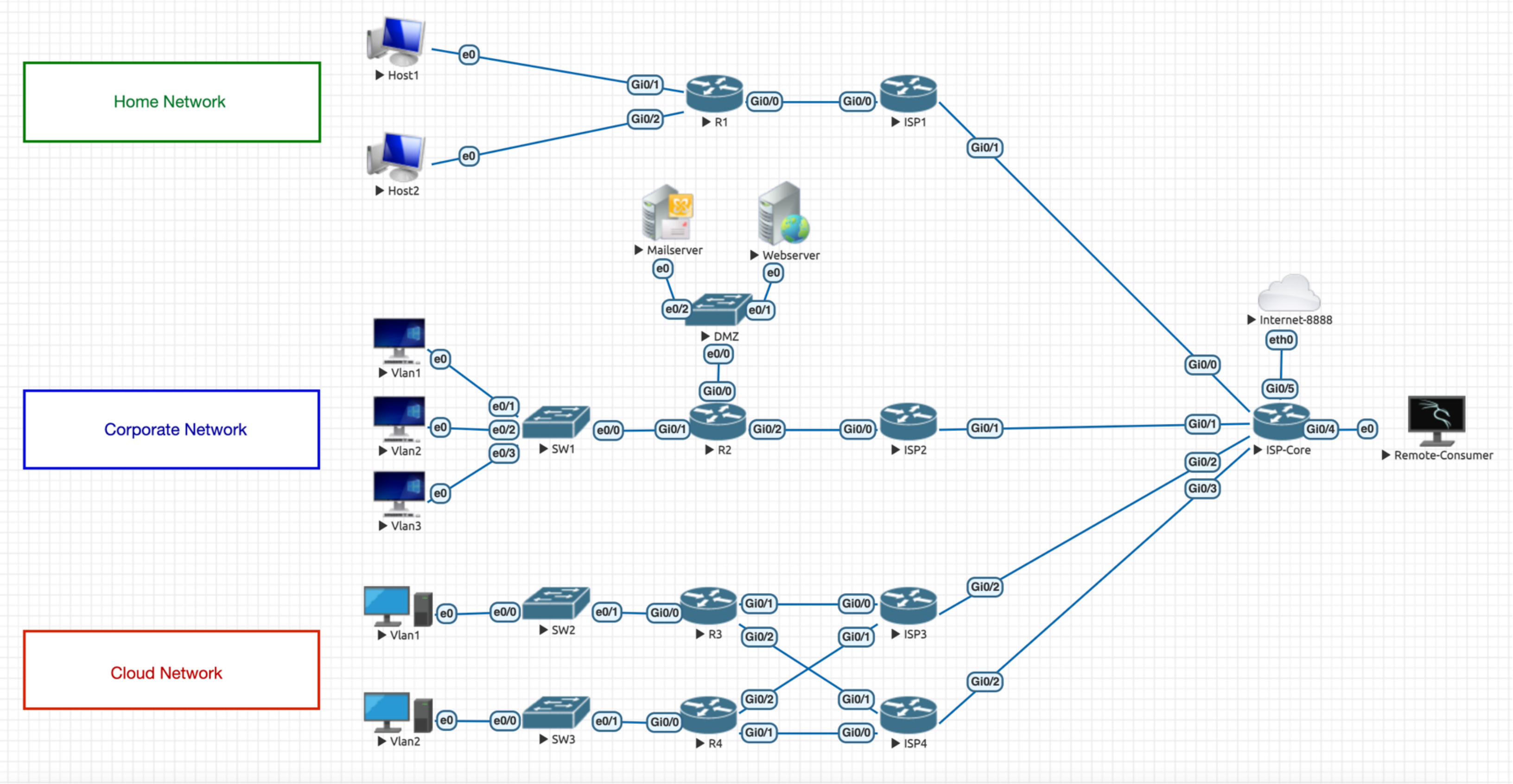
Introduction to Enterprise Networks

Spring 2025

Lab 5

NAT – PAT - HSRP

Prepared by: Alireza Ta’at



Lab Instructions:

The goal of this lab is to use Network Address Translation to give public access to private networks and private networks to public (Internet). You can do each objective separately.

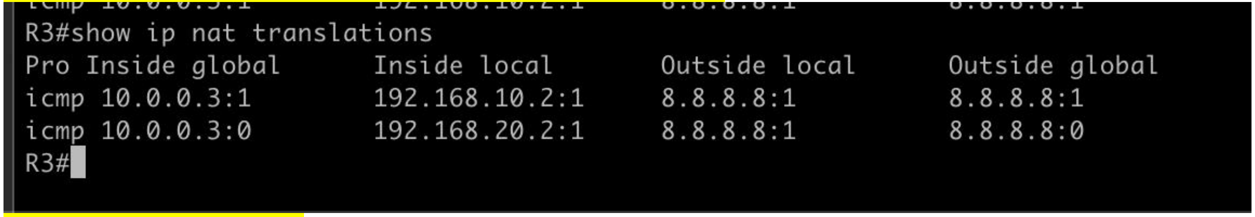
*** Use /31 for the point-to-point networks between routers (ISP access link in all scenarios).

Objective 1:

To give the two hosts in our home network access to the Internet, we need to translate the private IP addresses to a single public Ip address.

- Configure PAT (NAT Overload) on R1 using your physical interface, allowing Host1 and Host2 to access the internet. The ISP-Core has a loopback address of 8.8.8.8. Additionally, both hosts should be able to ping each other.

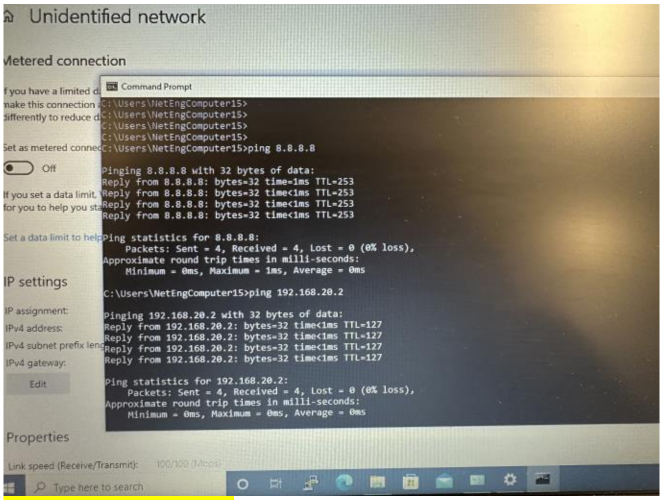
Evidence of Host1 and Host2 being able ping 8.8.8.8 via PAT:



```
icmp 10.0.0.3:1       192.168.10.2:1     8.8.8.8:1          8.8.8.8:1
R3#show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 10.0.0.3:1       192.168.10.2:1     8.8.8.8:1          8.8.8.8:1
icmp 10.0.0.3:0       192.168.20.2:1     8.8.8.8:1          8.8.8.8:0
R3#
```

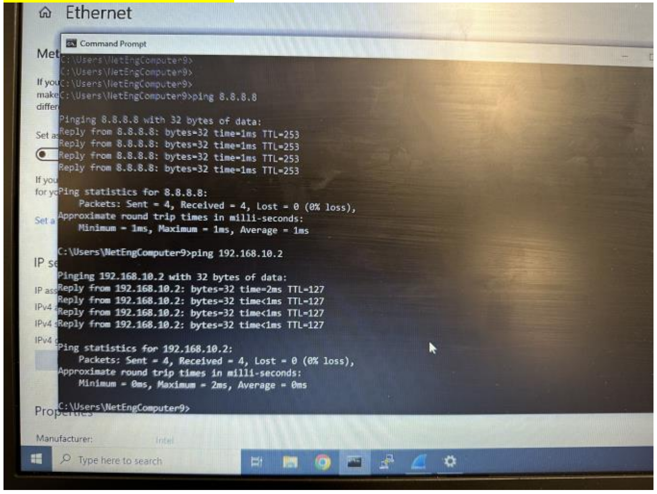
Commands used for PAT:
interface GigabitEthernet0/1
ip address 10.0.0.3 255.255.255.254
ip nat outside
interface FastEthernet1/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
interface FastEthernet1/1
ip address 192.168.10.1 255.255.255.0
ip nat inside
ip nat inside source list 1 interface GigabitEthernet0/1 overload
!
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255

Host connectivity:



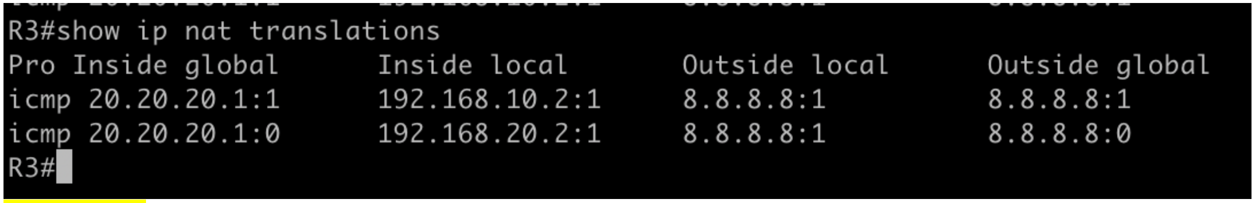
```
C:\Users\NetEngComputer15>
C:\Users\NetEngComputer15>
C:\Users\NetEngComputer15>
C:\Users\NetEngComputer15>
C:\Users\NetEngComputer15>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253

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:\Users\NetEngComputer15>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Host2 connectivity:



```
C:\Users\NetEngComputer9>
C:\Users\NetEngComputer9>
C:\Users\NetEngComputer9>
C:\Users\NetEngComputer9>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=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\NetEngComputer9>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=2ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\NetEngComputer9>
```

- Repeat the process but now use a PAT pool of 1 address (IP address used should be different than the subnet assigned on your point-to-point link)



```
R3#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 20.20.20.1:1      192.168.10.2:1     8.8.8.8:1          8.8.8.8:1
icmp 20.20.20.1:0      192.168.20.2:1     8.8.8.8:1          8.8.8.8:0
R3#
```

Commands:
ip nat pool PAT_POOL 20.20.20.1 20.20.20.1 netmask 255.255.255.252
ip nat inside source list 1 pool PAT_POOL overload
!
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
!

Here we see that the inside global is different from the P2P link, the only problem is there is no connectivity back because 8.8.8.8 does not have the route.

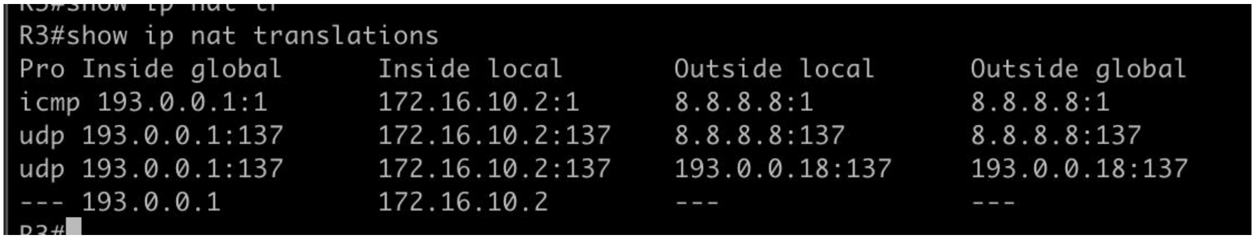
Paste Screenshots showing successful ping from private to public (Internet) + IP/PAT translations + commands used for this objective.

Objective 2:

The Corporate Network has servers accessible from the Internet on its DMZ, as well as employees that can both reach the DMZ and public Internet

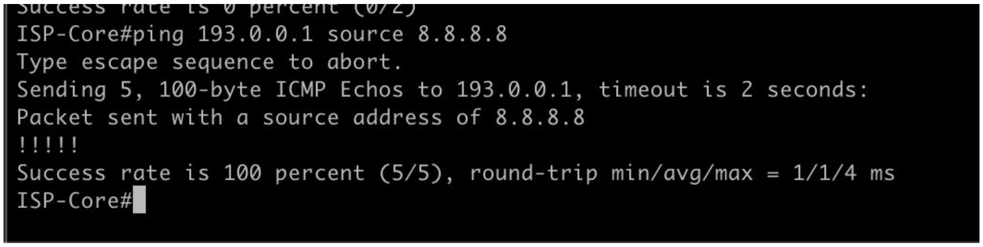
- Use a public /27 address block for public access, for all corporate connectivity needs.
- Both DMZ servers and employees have a private IP address assigned to their systems
- Use 1:1 Static NAT to map public consumer IP addresses to private DMZ servers. Allocate a /29 from your public block subnet for this purpose to ensure public consumers can reach the DMZ servers.
- Each VLAN (1, 2, and 3) should have its own public IP address block for outbound communication. Use a 1:1 NAT pool with a /29 per VLAN to achieve this.

Paste Screenshots showing successful ping from public to private and from private to public (Internet) + IP translations + commands used for this objective.



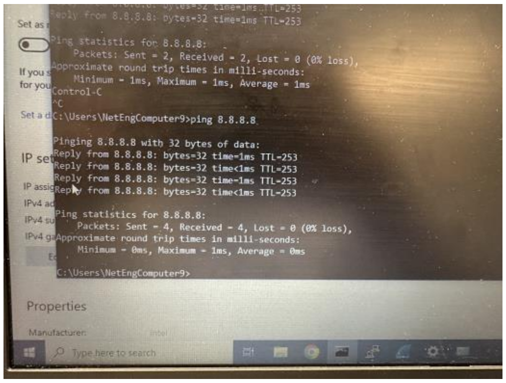
```
R3#show ip nat tr
R3#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 193.0.0.1:1       172.16.10.2:1      8.8.8.8:1          8.8.8.8:1
udp 193.0.0.1:137      172.16.10.2:137    8.8.8.8:137        8.8.8.8:137
udp 193.0.0.1:137      172.16.10.2:137    193.0.0.18:137     193.0.0.18:137
--- 193.0.0.1          172.16.10.2        ---                ---
R3#
```

Above is showing static 1:1 NAT for web server.



```
Success rate is 0 percent (0/2)
ISP-Core#ping 193.0.0.1 source 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
ISP-Core#
```

Here is showing the ping from public to private or NAT ip.

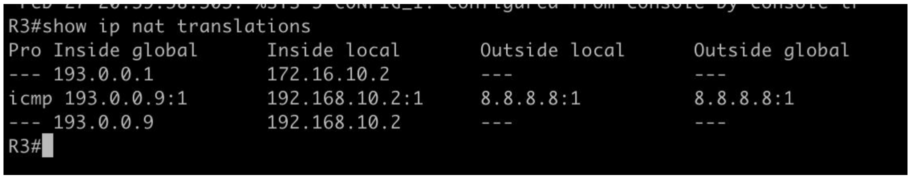


```
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253

Ping statistics for 8.8.8.8:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Users\NetEngComputer9>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=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253

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:\Users\NetEngComputer9>
```

Successful ping from web server to public ip.

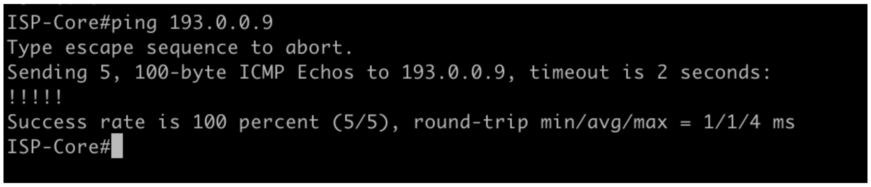
Config:
ip nat inside source static 172.16.10.2 193.0.0.1
interface FastEthernet1/1
ip address 172.16.10.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/1
ip address 193.0.0.17 255.255.255.248
ip nat outside

NOW FOR VLAN 1,2,3:



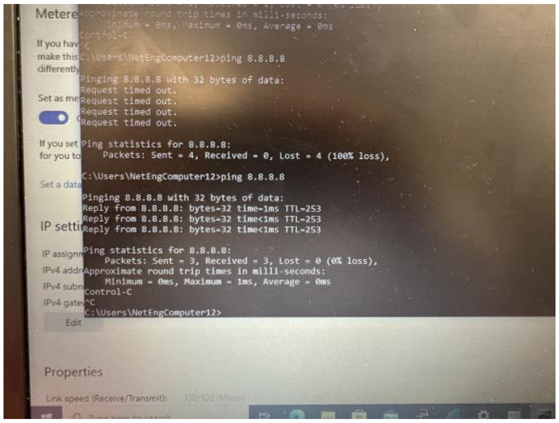
```
R3#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 193.0.0.1          172.16.10.2        ---                ---
icmp 193.0.0.9:1       192.168.10.2:1     8.8.8.8:1          8.8.8.8:1
--- 193.0.0.9          192.168.10.2       ---                ---
R3#
```

Showing that VLAN1 has translation within the pool



```
ISP-Core#ping 193.0.0.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.0.0.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
ISP-Core#
```

Proving public can ping outside interface for NAT pool.



```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\NetEngComputer12>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:\Users\NetEngComputer12>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=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253

Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\NetEngComputer12>
```

Connectivity to 8.8.8.8 via VLAN1

Config:
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/1
ip address 193.0.0.17 255.255.255.248
ip nat outside
ip nat pool MYPOOL 193.0.0.9 193.0.0.14 prefix-length 29

```
ip nat inside source list 1 pool MYPOOL
ip nat inside source static 172.16.10.2 193.0.0.1
```

Objective 3:

The corporate network has two VLANs 1 and 2. In this objective, you will:

- Configure HSRP for gateway redundancy between two routers.
- Implement NAT with:
  - PAT Pool (NAT Overload) for VLAN 1 using a /28 pool
  - 1:1 Static NAT for VLAN 2 using a /28 pool
- Implement SNAT (Stateful NAT) along HSRP to permit traffic/connection survivability after link or device failure (on Enterprise or ISP side)

Task 1: Configure HSRP on R3 and R4

1. Assign HSRP virtual IPs as the default gateways.
2. Configure HSRP tracking for uplink failure detection.

HSRP config on both R3 and R4:

```
interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.10.2 255.255.255.0

standby 10 ip 192.168.10.1

!

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.20.2 255.255.255.0

standby 20 ip 192.168.20.1

!

interface GigabitEthernet0/0.10

encapsulation dot1Q 10
```

ip address 192.168.10.3 255.255.255.0

standby 10 ip 192.168.10.1

!

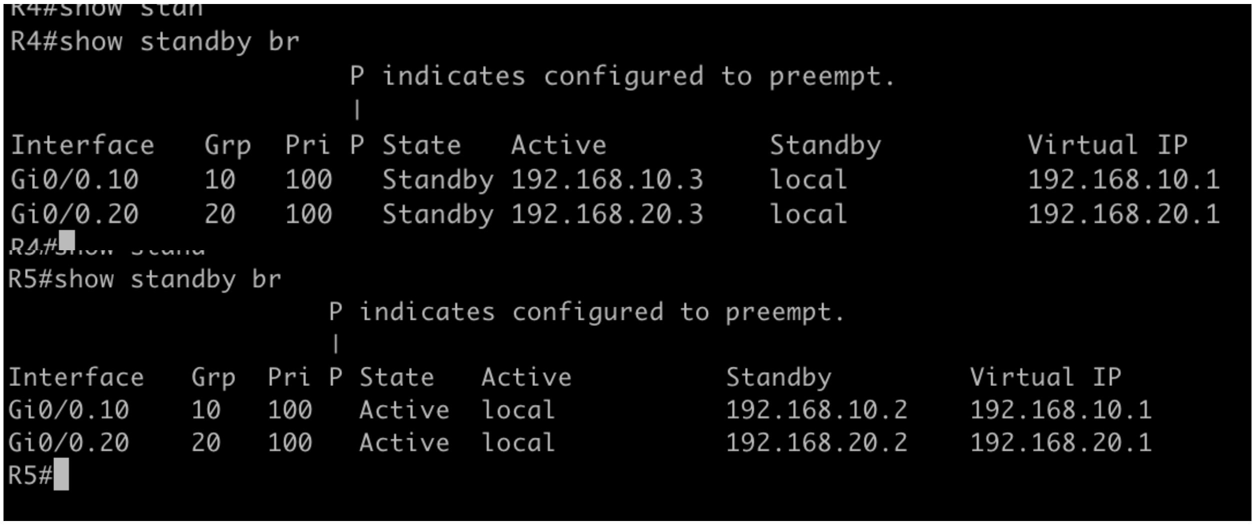
interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.20.3 255.255.255.0

standby 20 ip 192.168.20.1

!

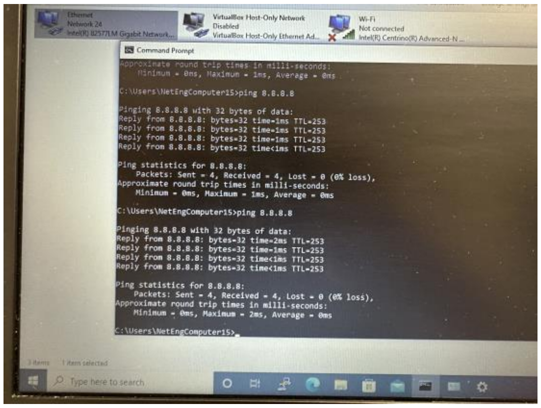


```
R4#show stan
R4#show standby br
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0.10     10   100   Standby 192.168.10.3    local           192.168.10.1
Gi0/0.20     20   100   Standby 192.168.20.3    local           192.168.20.1
R4#
R5#show standby br
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0.10     10   100   Active  local           192.168.10.2    192.168.10.1
Gi0/0.20     20   100   Active  local           192.168.20.2    192.168.20.1
R5#
```

Task 2: Implement NAT

1. Configure PAT (NAT Overload) for VLAN 1 with a /28 public IP pool.

Proof of connectivity:


Ethernet
Network 24
Intel(R) 82577LM Gigabit Network...
VirtualBox Host-Only Network
Disabled
VirtualBox Host-Only Ethernet Ad...
Wi-Fi
Not connected
Intel(R) Centrino(R) Advanced-N ...
Command Prompt
Type here to search

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetEngComputer15>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=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253

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:\Users\NetEngComputer15>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=2ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253

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 = 2ms, Average = 0ms

C:\Users\NetEngComputer15>
```

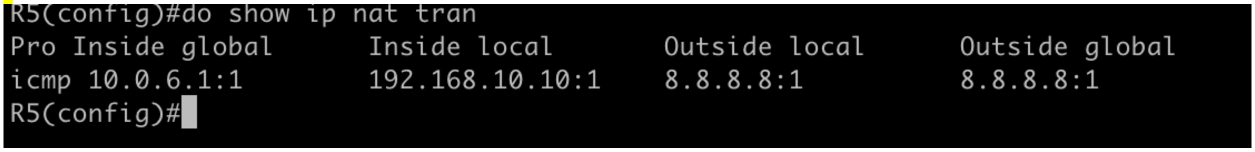
R3 and R4 config:

R3:

```
ip nat inside source route-map ISP3 interface GigabitEthernet0/1 overload

ip nat inside source route-map ISP4 interface FastEthernet1/0 overload

route-map ISP3 permit 10

match ip address 10

match interface GigabitEthernet0/1

!

route-map ISP4 permit 10
match ip address 10
match interface FastEthernet1/0
!
```

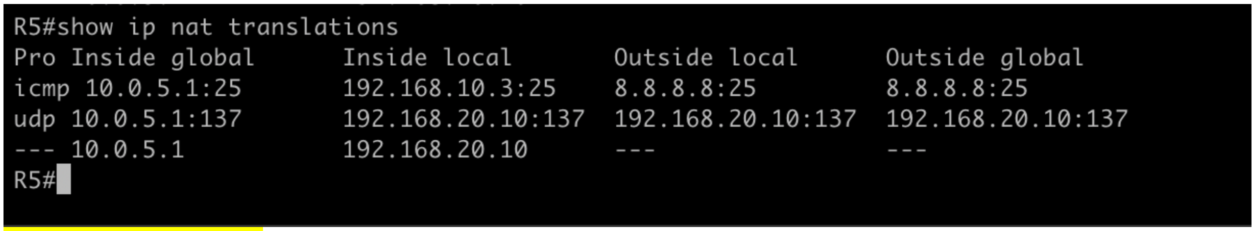
R4:

```
ip nat inside source route-map ISP3 interface FastEthernet2/0 overload
ip nat inside source route-map ISP4 interface GigabitEthernet0/1 overload
route-map ISP3 permit 10
match ip address 10
match interface FastEthernet2/0
!
route-map ISP4 permit 10
match ip address 10
match interface GigabitEthernet0/1
!
```



```
R5(config)#do show ip nat tran
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.0.6.1:1        192.168.10.10:1    8.8.8.8:1          8.8.8.8:1
R5(config)#
```

2. Configure 1:1 Static NAT for VLAN 2 using a /28 public block.



```
R5#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.0.5.1:25       192.168.10.3:25    8.8.8.8:25         8.8.8.8:25
udp 10.0.5.1:137       192.168.20.10:137  192.168.20.10:137  192.168.20.10:137
--- 10.0.5.1           192.168.20.10      ---                ---
R5#
```

Configs on R3 and R4:

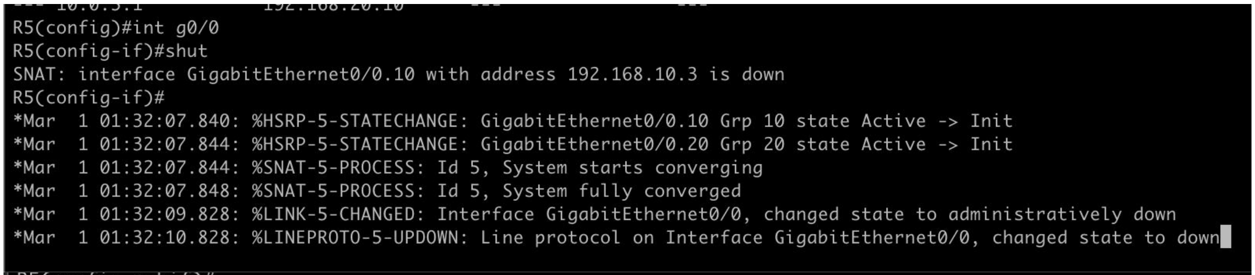
ip nat inside source static 192.168.20.10 interface FastEthernet1/0

ip nat inside source static 192.168.20.10 interface GigabitEthernet0/1

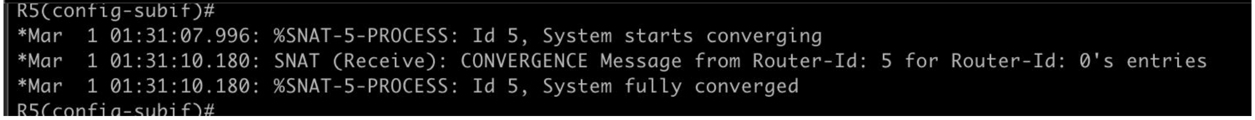
Task 3: Configure SNAT for Failover

1. Implement NAT Stateful Failover between R3 and R4.
2. Test session persistence after failover.

As you can see, when I enabled the NAT Stateful failover between R3 and R4, I turned off R4 interface to switch, and we see messages here for the failover. On the computer, I noticed no dropped packets



```
--- 10.0.5.1           192.168.20.10      ---                ---
R5(config)#int g0/0
R5(config-if)#shut
SNAT: interface GigabitEthernet0/0.10 with address 192.168.10.3 is down
R5(config-if)#
*Mar  1 01:32:07.840: %HSRP-5-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Active -> Init
*Mar  1 01:32:07.844: %HSRP-5-STATECHANGE: GigabitEthernet0/0.20 Grp 20 state Active -> Init
*Mar  1 01:32:07.844: %SNAT-5-PROCESS: Id 5, System starts converging
*Mar  1 01:32:07.848: %SNAT-5-PROCESS: Id 5, System fully converged
*Mar  1 01:32:09.828: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
*Mar  1 01:32:10.828: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
```



```
R5(config-subif)#
*Mar  1 01:31:07.996: %SNAT-5-PROCESS: Id 5, System starts converging
*Mar  1 01:31:10.180: SNAT (Receive): CONVERGENCE Message from Router-Id: 5 for Router-Id: 0's entries
*Mar  1 01:31:10.180: %SNAT-5-PROCESS: Id 5, System fully converged
R5(config-subif)#
```

Here is the config for stateful failover, it is the same for both routers:

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.10.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

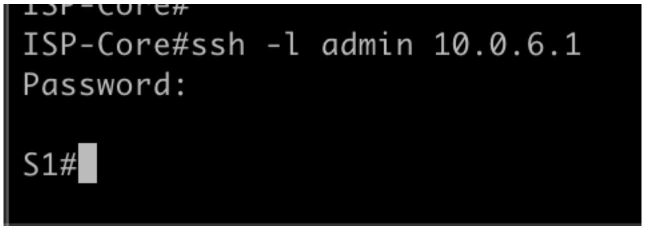
```
standby 10 ip 192.168.10.1

standby 10 name HSRP10

!

ip nat Stateful id 5

 redundancy HSRP10

  mapping-id 10

  protocol   udp
```

Paste commands used for this objective + Screenshots showing IP translations and HSRP status.

Objective 3 Extra Credit:

Enable SSH in your Cloud Network Switches. Configure PAT Port Forwarding on your Edge routers (corporate), such as when the remote consumer SSHs to the public IP address of the Edge Routers (R3 or R4), it redirects the SSH connection to the respective internal switch (i.e you SSH to the public IP address of R3, you should get the SW2 login prompt. Similarly, when you connect to public IP address of R4, you should get the SW3 login prompt)

```
ip nat inside source static tcp 192.168.10.69 22 10.0.6.1 22 extendable
```



```
ISP-Core#
ISP-Core#ssh -l admin 10.0.6.1
Password:

S1#
```

It was quite simple to do, just configured that one command and it worked!

Questions:

1. What command can you use to check the current HSRP active router?

   Issuing the command “show standby brief” and looking at the Active column, you will see either local or the IP of the main HSRP router.

2. If R1 fails, what should happen to the default gateway for VLAN 1 and VLAN 2?

If we are thinking about the HSRP setup for R1, then there should be a failover to R2, and R2 will become the active router for HSRP. There should be no packet drop unless NAT stateful failover isn't configured. If it is not configured, then host will either get instant connectivity to R2 or if R1 has failed routes, it will have to wait for R1's NAT translation to expire.

3. How does HSRP tracking improve network reliability?

   It improves network reliability because it is tracking each time there is a failure and can decrease the actual priority of HSRP on that router. So over time if there is an unreliable link, HSRP can determine which device to use based on calculated priority.

4. How does SNAT ensure session persistence when failover occurs?

   SNAT ensures session persistence by maintaining a constant source IP address for outbound traffic when the failover occurs. If the source IP is the same when one device fails, returning traffic will still have a path back.

5. How can you verify that NAT translations are working correctly?

   By checking show ip nat translations on the device, we can see inside local, inside global, outside local, and outside global IP addresses to make sure we are translating the right IP addresses. For the inside local, you can see the host that is trying to communicate to public space. With inside global, you can see what IP it was translated to and how the public network sees the host. Outside global and outside local are the destination public IPs that the host wants to go to.

6. What is the purpose of **HSRP**, and how does it provide redundancy?

   The purpose of HSRP is to have a host that has multiple ways to get out of the network instead of just one. It provides redundancy by letting the host have its default gateway as the virtual IP, and HSRP will handle which physical IP/port it goes to base on priority.

7. Explain the difference between **PAT (NAT Overload)** and **1:1 Static NAT**.

   PAT is translating many private IPs to one public IP but changing the actual port in the translation table. 1:1 static NAT only maps 1 private IP address to one private IP address.

8. Why is **SNAT important** in a failover scenario?

   SNAT is important because it keeps the same source IP and maintains the actual session to avoid dropped packets. Returning SNAT traffic is always routed through the active router which prevents packet drops on a failed router.

9. What other flavors of First-Hop Redundancy Protocol do you know of? Can you briefly explain how they work?

VRRP is just another version of HSRP, but it is multi-vendor. You can set a virtual IP and priority. GLBP is a cisco proprietary protocol that basically is HSRP but can have multiple active routers for load balancing and increased redundancy.

10. What is the difference between Static and Dynamic NAT.

    Static NAThas a direct relationship with private IP to public IP, these values don’t change, and it should always be an exact match. Dynamic NAT takes from a pool of public IPs and assigns it to a private IP. Once that NAT translation expires, the public IP is put back into the pool.

11. Explain how NAT/PAT works in IPv6 networks? What types of NAT do we have in an IPv6 network?!

    NAT works in IPv6 networks to translate to a different prefix for multi home institutions or it is used for NAT64. NAT64 allows for IPv6 IPs to interface with IPv4 servers.