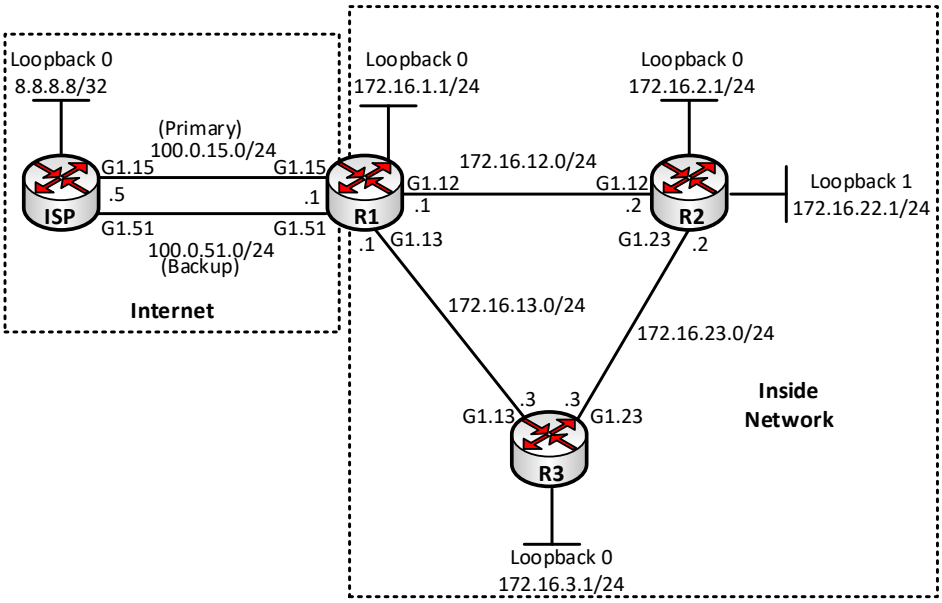
Lab – Network Address Translation

Sơ đồ:



Hình 1 – Sơ đồ bài lab

Mô tả:

- Bài lab gồm 5 router được kết nối với nhau theo sơ đồ hình 1.
- Các router R1 đến R4 đóng vai trò các router của một mạng doanh nghiệp.
- Router ISP giả lập môi trường Internet. Mạng doanh nghiệp giả lập ở trên sử dụng hai đường kết nối Internet cho mục đích dự phòng lẫn nhau (multihoming).
- Trong bài lab này, học viên sẽ khảo sát một số kỹ thuật NAT nâng cao trên router.

Yêu cầu:

1. Cấu hình ban đầu:

- Học viên thực hiện cấu hình các địa chỉ IP trên các interface của các router như được chỉ ra trên hình 1.
- Trên phần mạng Inside Network, thực hiện cấu hình OSPF Area 0 đảm bảo mọi địa chỉ trong mạng Inside có thể đi đến được nhau.
- Hiệu chỉnh OSPF đảm bảo R1 đi đến R2 theo đường link nối giữa hai cổng G1.12 của R1 và R2 nhưng R2 đi về R1 theo đường trung chuyển qua router R3.
- Trên R1 thực hiện cấu hình hai static defaut – route trỏ đến ISP:
    - Trong đó, đảm bảo R1 sẽ sử dụng đường link G1.15 làm đường chính đi Internet,

đường G1.51 chỉ sử dụng để dự phòng.

- Thực hiện cơ chế track bằng IP SLA để đảm bảo hoạt động dự phòng diễn ra.

Cấu hình:

Cấu hình OSPF trên Inside Network:

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.1 0.0.0.0 area 0
R1(config-router)#network 172.16.12.1 0.0.0.0 area 0
R1(config-router)#network 172.16.13.1 0.0.0.0 area 0

R2(config)#router ospf 1
R2(config-router)#network 172.16.2.1 0.0.0.0 area 0
R2(config-router)#network 172.16.12.2 0.0.0.0 area 0
R2(config-router)#network 172.16.22.1 0.0.0.0 area 0
R2(config-router)#network 172.16.23.2 0.0.0.0 area 0

R3(config)#router ospf 1
R3(config-router)#network 172.16.3.1 0.0.0.0 area 0
R3(config-router)#network 172.16.13.3 0.0.0.0 area 0
R3(config-router)#network 172.16.13.3 0.0.0.0 area 0
R3(config-router)#network 172.16.23.3 0.0.0.0 area 0
```

Hiệu chỉnh đường đi với OSPF theo yêu cầu đặt ra:

```
R2(config)#int g1.12
R2(config-subif)#ip ospf cost 3
```

Cấu hình defaut – route trên R1 cho hoạt động đi Internet:

```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 100.0.15.5 source-interface g1.15
R1(config-ip-sla-echo)#frequency 5
R1(config-ip-sla-echo)#exit

R1(config)#ip sla schedule 1 start-time now life forever

R1(config)#track 1 ip sla 1
R1(config-track)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 100.0.15.5 5 track 1
R1(config)#ip route 0.0.0.0 0.0.0.0 100.0.51.5 10
```

Sau khi cấu hình xong default – route, thực hiện lan truyền default – route này vào mạng bên trong:

```
R1(config)#router ospf 1
R1(config-router)#default-information originate
R1(config-router)#exit
```

Kiểm tra:

Định tuyến OSPF đã hội tụ trong Inside Network:

```
R1#show ip route ospf
```

```
  172.16.0.0/16 is variably subnetted, 11 subnets, 2 masks
O   172.16.2.1/32  [110/2] via 172.16.12.2, 00:23:52, GigabitEthernet1.12
O   172.16.3.1/32  [110/2] via 172.16.13.3, 00:23:21, GigabitEthernet1.13
O   172.16.22.1/32 [110/2] via 172.16.12.2, 00:23:53, GigabitEthernet1.12
O   172.16.23.0/24 [110/2] via 172.16.13.3, 00:23:11, GigabitEthernet1.13
                  [110/2] via 172.16.12.2, 00:23:11, GigabitEthernet1.12

R2#show ip route ospf
O*E2  0.0.0.0/0 [110/1] via 172.16.23.3, 00:03:08, GigabitEthernet1.23
  172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
O   172.16.1.1/32  [110/3] via 172.16.23.3, 00:11:27, GigabitEthernet1.23
O   172.16.3.1/32  [110/2] via 172.16.23.3, 00:23:14, GigabitEthernet1.23
O   172.16.13.0/24 [110/2] via 172.16.23.3, 00:23:14, GigabitEthernet1.23

R3#show ip route ospf
O*E2  0.0.0.0/0 [110/1] via 172.16.13.1, 00:03:18, GigabitEthernet1.13
   172.16.0.0/16 is variably subnetted, 11 subnets, 2 masks
O   172.16.1.1/32 [110/2] via 172.16.13.1, 00:23:24, GigabitEthernet1.13
O   172.16.2.1/32 [110/2] via 172.16.23.2, 00:23:24, GigabitEthernet1.23
O   172.16.12.0/24[110/2] via 172.16.13.1, 00:23:24, GigabitEthernet1.13
O   172.16.22.1/32[110/2] via 172.16.23.2, 00:23:26, GigabitEthernet1.23
```

R1 đi đến R2 theo link G1.12:

```
R1#traceroute 172.16.2.1
Type escape sequence to abort.
Tracing the route to 172.16.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.12.2 5 msec *  1 msec
```

R2 đi đến R1 theo đường trung chuyển qua R3:

```
R2#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.23.3 4 msec 4 msec 4 msec
  2 172.16.13.1 3 msec *  3 msec
```

Hiện tại, R1 đang đi Internet theo cổng output G1.15 (next – hop IP 100.0.15.5):

```
R1#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 5, metric 0, candidate default path
  Routing Descriptor Blocks:
* 100.0.15.5
      Route metric is 0, traffic share count is 1
```

Nếu link G1.15 nối đến ISP down (giả lập bằng cách shutdown cổng G1.15 phía ISP), link dự phòng được sử dụng:

```
ISP(config)#int g1.15
ISP(config-subif)#shutdown
R1#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
```

```
  Known via "static", distance 10, metric 0, candidate default path
  Routing Descriptor Blocks:
* 100.0.51.5
      Route metric is 0, traffic share count is 1
```

Sau khi kiểm tra xong, nhớ no shutdown cổng G1.15 của ISP lại như cũ.

2. Dự phòng với NAT (1):

- Cấu hình NAT trên R1 đảm bảo server 172.16.22.1 bên trong Inside Network sẽ được NAT thành địa chỉ public 100.0.15.22 khi đường đi Internet chính của mạng doanh nghiệp đang được sử dụng.
- Bên cạnh đó, cũng thực hiện cấu hình NAT trên R1 đảm bảo server 172.16.22.1 sẽ được NAT thành địa chỉ public 100.0.51.22 khi đường Internet chính down và đường Internet dự phòng của mạng doanh nghiệp được sử dụng.

Cấu hình:

Trong câu lab này, yêu cầu đặt ra là cần phải NAT địa chỉ Inside local 172.16.22.1 thành hai địa chỉ outside global bên ngoài để đảm bảo mục đích dự phòng. Tuy nhiên, nếu thực hiện static NAT theo cách thức thông thường, IOS trên router sẽ báo lỗi:

```
R1(config)#ip nat inside source static 172.16.22.1 100.0.15.22
R1(config)#ip nat inside source static 172.16.22.1 100.0.51.22
%NAT: 172.16.4.1 already mapped (172.16.22.1 -> 100.0.15.4)

R1#show run | inc ip nat
ip nat inside source static 172.16.22.1 100.0.15.22
```

Kết quả thực hiện ở trên cho thấy chỉ một dòng cấu hình static NAT khai báo trước mới được ghi nhận vào cấu hình NAT của router, dòng khai báo sau không được cập nhật.

Để thực hiện yêu cầu đặt ra, cần phải thực hiện static NAT ở trên tham chiếu đến các route – map:

```
R1(config)#access-list 1 permit 172.16.22.1

R1(config)#route-map PRIMARY
R1(config-route-map)#match ip address 1
R1(config-route-map)#match interface g1.15
R1(config-route-map)#exit

R1(config)#route-map BACKUP
R1(config-route-map)#match ip address 1
R1(config-route-map)#match interface g1.51
R1(config-route-map)#exit

R1(config)#ip nat inside source static 172.16.22.1 100.0.15.22 route-map
PRIMARY
R1(config)#ip nat inside source static 172.16.22.1 100.0.51.22 route-map BACKUP

R1(config)#interface g1.12
R1(config-subif)#ip nat inside
R1(config-subif)#exit
```

```
R1(config)#interface g1.13
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#interface g1.15
R1(config-subif)#ip nat outside
R1(config-subif)#exit
R1(config)#interface g1.51
R1(config-subif)#ip nat outside
R1(config-subif)#exit
```

Trong cấu hình ở trên, các route – map PRIMARY và BACKUP đã giúp phân biệt giữa hai mệnh đề NAT được khai báo.

Kiểm tra:

Bảng NAT của R1 đã ghi nhận hai dòng thông tin NAT đã khai báo:

```
R1#show ip nat translations
Pro  Inside globalInside local       Outside local      Outside global
---  100.0.15.22172.16.22.1          ---                ---
---  100.0.51.22172.16.22.1          ---                ---
Total number of translations: 2
```

Địa chỉ 172.16.22.1 có thể truy nhập được Internet, được NAT thành IP Inside global 100.0.15.22:

```
R2#ping 8.8.8.8 source 172.16.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 172.16.22.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms

R1#show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
---  100.0.15.22        172.16.22.1          ---                ---
---  100.0.51.22        172.16.22.1          ---                ---
icmp 100.0.15.22:3      172.16.22.1:3        8.8.8.8:3          8.8.8.8:3
Total number of translations: 3
```

Thực hiện shutdown cổng G1.15 của ISP để kiểm tra hoạt động dự phòng:

```
ISP(config)#interface g1.15
ISP(config-subif)#shutdown
```

Khi link chính down, server 172.16.4.1 vẫn có thể truy nhập được Internet thông qua link backup và IP public dự phòng 100.0.51.4:

```
R2#ping 8.8.8.8 source 172.16.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 172.16.22.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/5/6 ms

R1#show ip nat translations
Pro  Inside global    Inside local     Outside local      Outside global
```

```
---  100.0.15.4        172.16.22.1          ---                ---
---  100.0.51.4        172.16.22.1          ---                ---
icmp 100.0.51.22:4     172.16.22.1:4        8.8.8.8:4          8.8.8.8:4
Total number of translations: 3
```

Như vậy, hoạt động dự phòng cho việc NAT server 172.16.22.1 ra Internet đã diễn ra đúng theo yêu cầu đặt ra.

Sau khi kiểm tra xong, nhớ no shutdown cổng G1.15 của ISP lại như cũ.

3. Dự phòng với NAT (2):

- Cấu hình NAT overload trên R1 đảm bảo mọi địa chỉ còn lại trong mạng Inside sẽ được NAT thành địa chỉ trên cổng G1.15 của R1 để có thể truy nhập Internet.
- Khi đường Internet chính down và đường dự phòng được sử dụng, các địa chỉ trong mạng Inside sẽ được NAT thành địa chỉ trên cổng G1.51 của R1 để có thể truy nhập Internet.

Cấu hình:

Để thực hiện yêu cầu 3, một access – list bao hàm các địa chỉ cần đi Internet phải được NAT overload thành địa chỉ trên cổng G1.15 và cổng G1.51. Tuy nhiên, tương tự như trên, Cisco IOS sẽ không cho phép NAT một source thành nhiều destination cùng một lúc nếu như không có yếu tố phân biệt giữa hai mệnh đề NAT này:

```
R1(config)#access-list 2 deny 172.16.22.1
R1(config)#access-list 2 permit 172.16.0.0 0.0.255.255

R1(config)#ip nat inside source list 2 interface g1.15 overload
R1(config)#ip nat inside source list 2 interface g1.51 overload
Cannot change mapping's interface name; remove mapping first
```

Do đó, cần phải tham chiếu đến các route – map để thực hiện yêu cầu này:

```
R1(config)#route-map OVERLOAD_PRIMARY
R1(config-route-map)#match ip address 2
R1(config-route-map)#match interface g1.15
R1(config-route-map)#exit
R1(config)#route-map OVERLOAD_BACKUP
R1(config-route-map)#match ip address 2
R1(config-route-map)#match interface g1.51
R1(config-route-map)#exit

R1(config)#ip nat inside source route-map OVERLOAD_PRIMARY interface g1.15
overload
R1(config)#ip nat inside source route-map OVERLOAD_BACKUP interface g1.51
overload
```

Kiểm tra:

Thực hiện ping đi Internet từ một địa chỉ bất kỳ ngoại trừ địa chỉ 172.16.4.1:

```
R3#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/9 ms
```

Bảng NAT trên R1:

```
R1#show ip nat translations
Pro  Inside global     Inside local   Outside local      Outside global
---  100.0.15.22       172.16.22.1          ---                ---
---  100.0.51.22       172.16.22.1          ---                ---
icmp 100.0.15.1:1      172.16.23.3:1    8.8.8.8:1          8.8.8.8:1
Total number of translations: 3
```

Có thể thấy địa chỉ 172.16.23.3 của R3 đã được NAT thành địa chỉ trên cổng G1.15 của R1 khi R3 truy nhập Internet.

Shutdown cổng G1.15 của ISP để kiểm tra hoạt động dự phòng:

```
ISP(config)#interface g1.15
ISP(config-subif)#shutdown
```

Từ Inside Network vẫn có thể đi được Internet dù link chính đã down:

```
R3#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/15 ms
```

Bảng NAT trên R1 cho thấy lúc này địa chỉ 100.0.51.1 trên cổng G1.51 của R1 đã được sử dụng cho hoạt động NAT:

```
R1#show ip nat translations
Pro  Inside global       Inside local   Outside local   Outside global
---  100.0.15.4          172.16.4.1           ---            ---
---  100.0.51.4          172.16.4.1           ---            ---
icmp 100.0.51.1:1        172.16.23.3:2     8.8.8.8:2      8.8.8.8:1
Total number of translations: 3
```

Như vậy, hoạt động NAT dự phòng đã diễn ra đúng theo yêu cầu đặt ra.

Sau khi kiểm tra xong, nhớ no shutdown cổng G1.15 của ISP trở lại như cũ.