Jefe de laboratorio	Ing. Raúl Ortiz Gaona, PhD
Práctica # 12	Servicio NAT Network Address Translation

1. ANTECEDENTES

Se puede diseñar una red y asignar direcciones IP privadas con toda libertad, pero los hosts no pueden navegar en Internet con una dirección IP privada. Para que se lo pueda hacer, es necesario que el enrutador de la red LAN que está conectada a Internet, le asigne al host una dirección IP pública. Esta tarea se lo hace a través del servicio NAT Network Address Translation.

2. OBJETIVO

El objetivo de la práctica es el siguiente:

1. Configurar en el enrutador el servicio NAT.

3. EQUIPO Y MTERIALES

2 ruteadores

2 switches

4 PCs

6 cables directos

1 cable cruzado

1 cable de consola

4. DISEÑO DE LA RED CON MÁSCARA DE SUBRED DE LONGITUD FIJA

Datos:
Se tiene una red LAN con dirección de red IP privada 192.168.0.0
El servidor al que se desea acceder y que está en Internet tiene la dirección pública 172.100.0.2

5. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

1. Conectar los equipos como se indica en la Figura 1.
2. Configurar las PCs.
3. Configurar las interfaces de red de los enrutadores.
4. Configurar enrutamiento dinámico RIP en los enrutadores
5. Configurar el servicio NAT en el enrutador R1

```
Router(config)# access-list 1 permit 192.168.0.0  0.0.0.255
Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
```

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

6. Comprobar en las PCs si se asignaron dinámicamente las direcciones IP
7. Comprobar la conectividad entre PCs

Luego, los estudiantes configurarán NAT con dos redes LAN conectadas al enrutador R1, con direcciones de red privadas clase A y B respectivamente.

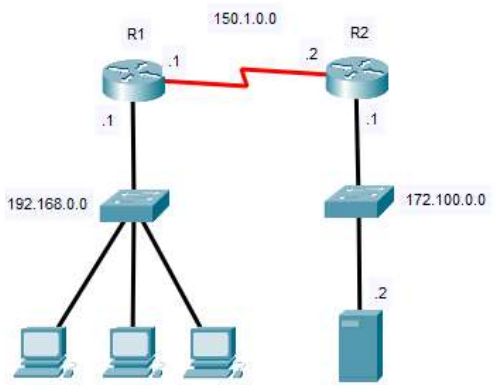

Figura 1. Topología de la red

6. RESULTADOS OBTENIDOS

7. CONCLUSIONES

8. RECOMENDACIONES

9. FUENTES DE INFORMACIÓN

Jefe de laboratorio	Ing. Raúl Ortiz Gaona, PhD
Práctica # 13	Listas de Control de Acceso

1. ANTECEDENTES

Muchas veces se necesita negar a permitir el acceso a ciertos recursos que existen en una red. Una forma de hacerlo es utilizando listas de control de acceso ACL (Access Control List)

2. OBJETIVO

El objetivo de la práctica es el siguiente:

1. Impedir que una red tenga acceso a otra red.

3. EQUIPO Y MTERIALES

2 ruteadores

2 switches

4 PCs

9 cables directos

1 cable cruzado

1 cable de consola

4. DISEÑO DE LA RED CON MÁSCARA DE SUBRED DE LONGITUD FIJA

Datos:
Se desea que la red con dirección 192.168.0.0 no pueda acceder a la red con dirección 172.16.0.0, y que la red con dirección 192.168.1.0 sí pueda acceder a la red 172.16.0.0

5. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

1. Conectar los equipos como se indica en la Figura 1.
2. Configurar las PCs.
3. Configurar las interfaces de red de los enrutadores.
4. Configurar enrutamiento dinámico RIP en los enrutadores
5. Impedir que la red 192.168.0.0 no pued acceder a la red 172.16.0.0
   Router(config)# access-list 101 deny ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.0.0
   Router(config)# interface gigabitEthernet 0/0
   Router(config-if)# ip access-group 101 out

6. Comprobar conectividad

7. Permitir que la red 192.168.1.0 sí pueda acceder a la red 172.16.0.0

Router(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255

8. Volver a probar la conectividad

Luego, los estudiantes configurarán NAT con dos redes LAN conectadas al enrutador R1, con direcciones de red privadas clase A y B respectivamente.

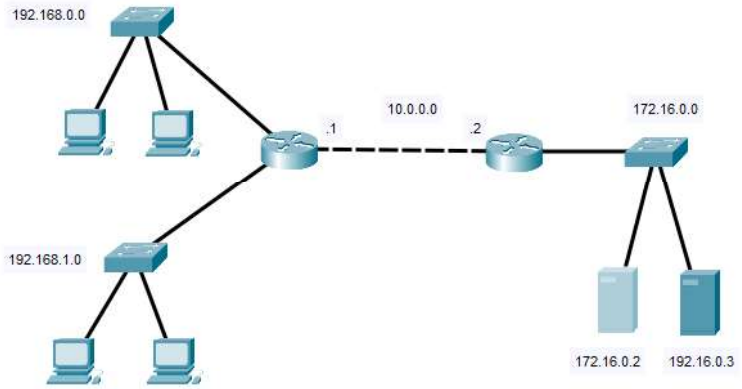

Figura 1. Topología de la red

6. RESULTADOS OBTENIDOS

7. CONCLUSIONES

8. RECOMENDACIONES

9. FUENTES DE INFORMACIÓN