INFRAESTRUCTURA I
CONFIGURACIÓN DE NAT (Network Address Traslation)

Objetivos

- Revisar los conceptos de configuración básica de los enrutadores Cisco analizados en las simulaciones anteriores haciendo énfasis en la configuración de NAT.
- Que el estudiante con ayuda del material visto en clase y la guía de laboratorio, sea capaz de configurar los diferentes tipos NAT en el packet tracer.
- Verificar la operación de NAT mediante la captura de tráfico del sniffer del packet tracer.

Procedimiento

El esquema a implementar es el de la figura No.1, por favor respete las conexiones, nombres de enrutadores y direcciones IP ahí asignadas para el buen funcionamiento y resultados de la guía.

Al final de la práctica debe entregar en un archivo las capturas de los comandos que se le indiquen y el archivo de simulación en packet tracer.

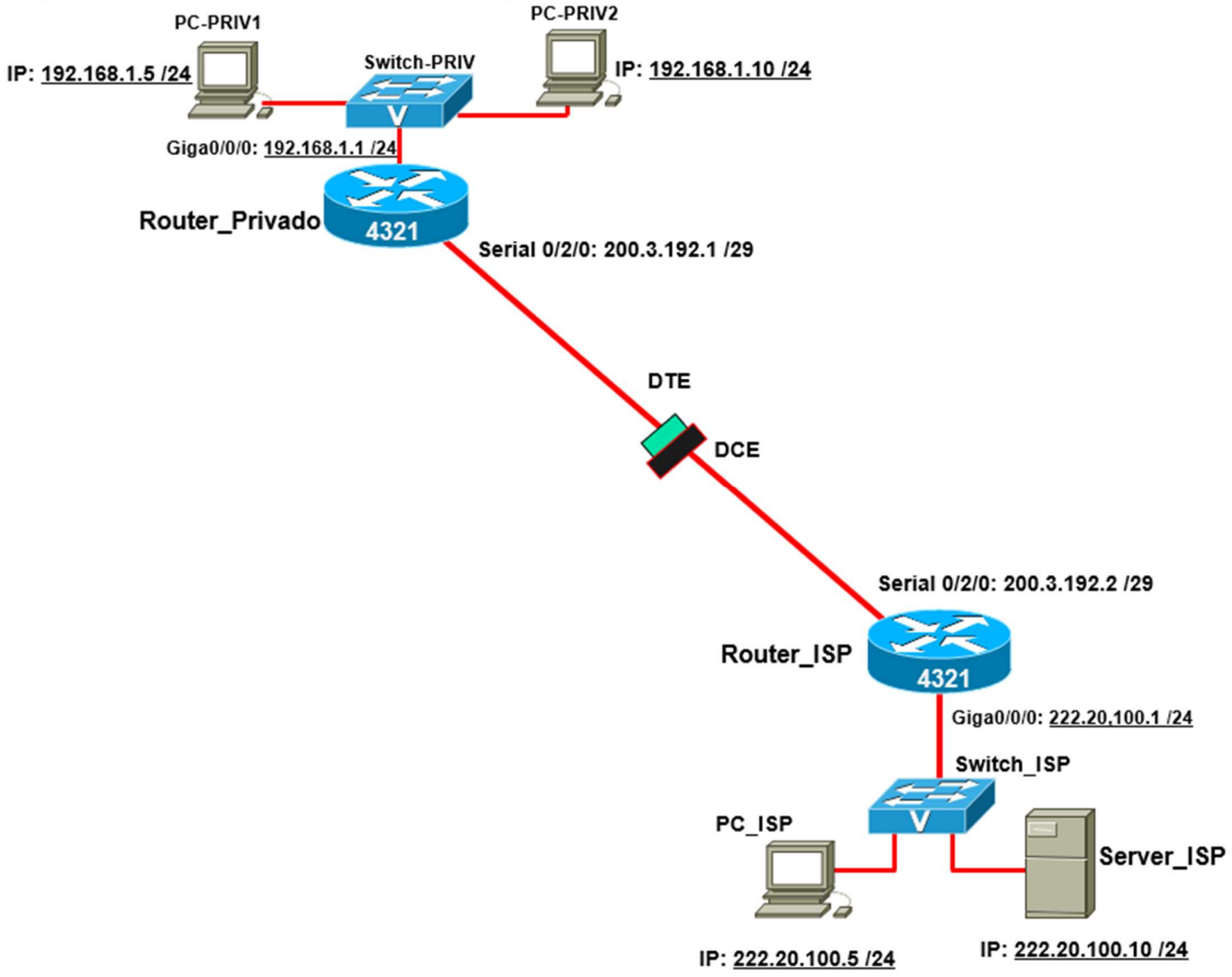

Figura No.1 Esquema a implementar en la práctica.

1. Configure el esquema de la figura No.1 con las direcciones ahí planteadas (en PC´s, puertos LAN y WAN), coloque de nombre a los enrutadores los que aparecen en el esquema y configure lo necesario para hacer gestión remota. Para utilizar los nombres de las interfaces que se presentan en la guía la tarjeta de puertos seriales en los enrutadores 4321 se debe colocar como se aprecia en la figura 1. Si no lo hace de esta manera cambie los nombres de las interfaces de acuerdo a su montaje.
   Nota: Para los switches todos los puertos deben estar en la VLAN1.

Figura 2. Ubicación de la tarjeta de puertos seriales en los enrutadores 4321.

2. Verifique que los equipos (PC y Router) de cada red respondan ping entre sí al igual que con las interfaces seriales locales.

3. Configure una ruta estática por default en el **Router_Privado** de la siguiente manera:
   `Router_Privado(config)#ip route 0.0.0.0 0.0.0.0 200.3.192.2`

   <u>En el Router_ISP no configure ningún tipo de enrutamiento.</u>

4. Desde el **PC-ISP** ejecute ping a las siguientes direcciones y verifique que entrega el comando:
   - Ping 200.3.192.2 :_____
   - Ping 200.3.192.3 :_____
   - Ping 200.3.192.5 :_____
   - Ping 192.168.1.5 :_____
   - Ping 192.168.1.10 :_____

5. Ahora configure NAT estático bajo las siguientes características:

- En el **Router_Privado** la interfaz **GigabitEthernet 0/0/0** va a ser **inside**, y la interfaz **Serial 0/2/0** va a ser **outside**.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
interface Serial0/2/0
 ip address 200.3.192.1 255.255.255.248
 ip nat outside
```

- Ahora termine de configurar el **NAT estático** con los siguientes comandos:

```
Router_Privado(config)# ip nat inside source static 192.168.1.5 200.3.192.3
Router_Privado(config)# ip nat inside source static 192.168.1.10 200.3.192.5
```

6. Verifique la configuración realizada con los siguientes comandos, y realice una captura de la información que entregan para que la compare posteriormente después de generar tráfico:

```
Router_Privado# show ip nat translation

Router_Privado# show ip nat statistics
```

7. Ejecute de nuevo desde el **PC-ISP** a las siguientes direcciones y verifique que entrega el comando, compare las respuestas obtenidas aquí con las obtenidas en el punto No.4:

- Ping 200.3.192.2 :_____
- Ping 200.3.192.3 :_____
- Ping 200.3.192.5 :_____
- Ping 192.168.1.5 :_____
- Ping 192.168.1.10 :_____

Pregunta para analizar:
¿Comparando las respuestas obtenidas en la pregunta No. 4, por qué considera que las direcciones IP de la red 200.3.192.0/24 ahora si contestan al ping?

8. Identifique sobre que **protocolo y puerto** funciona **http y ftp**. Esta información será importante para analizar la información se la siguiente pregunta.

9. Verifique que desde los equipos **PC-PRIV1 y PC-PRIV2** pueda hacer **http y ftp** al **Server_ISP**. Para hacer ftp, por favor entre al servicio ftp del servidor e identifique usuario y password para poder acceder al servicio en el servidor. Para hacer ftp lo debe hacer desde una ventana de **comand prompt.**

10. Ejecute de nuevo los siguientes comandos y analice lo que entregan, con respecto a los comandos ejecutados en el punto 6.

```
Router_Privado# show ip nat translation

Router_Privado# show ip nat statistics
```

Realice captura de lo que muestra el comando anterior. ¿Qué puede identificar en dicha captura?

11. Para configurar NAT dinámico se debe deshabilitar el NAT estático de la siguiente manera:

```
Router_Privado(config)# no ip nat inside source static 192.168.1.5 200.3.192.3
Router_Privado(config)# no ip nat inside source static 192.168.1.10 200.3.192.5
```

12. Verifique que ya no está configurado el NAT con el siguiente comando:

```
Router_Privado show ip nat translation
```

13. Configure **NAT dinámico** con ayuda de los siguientes comandos:

```
Router_Privado(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Router_Privado(config)# ip nat pool Dir_ISP 200.3.192.3 200.3.192.5 netmask 255.255.255.248
Router_Privado(config)# ip nat inside source list 1 pool Dir_ISP
```

14. Verifique que información entrega el siguiente comando en este momento, después de configurar el NAT dinámico:

```
Router_Privado show ip nat translation
```

15. Identifique o investigue sobre que protocolo funciona ping. Esta información será importante para analizar la pregunta 16.

16. Realice ping desde los equipos **PC-PRIV1** y **PC-PRIV2** al equipo **PC-ISP**.

17. Ejecute el comando `sh ip nat translations` y analice la información que entrega.
    Realice captura de lo que muestra el comando anterior.

18. Identifique sobre que protocolo y puerto funciona http y ftp. Esta información será importante para analizar la información en la pregunta 19.

19. Verifique que desde los equipos PC-PRIV1 y PC-PRIV2 pueda hacer, http y ftp al Server_ISP.

20. Ejecute el comando `sh ip nat translations y show ip nat statistics.` Analice la información que entrega.
    Realice captura de lo que muestra el comando anterior. ¿Qué puede analizar de dicha captura?

21. Para configurar **NAT overload** debe deshabilitar solamente los siguientes comandos del NAT dinámico:
    - **Nota**: En caso de que aparezca un mensaje indicando que no se puede remover el mapeo dinámico utilice el siguiente comando:
      `Router_Privado#clear ip nat translation *`

```
Router_Privado(config)# no ip nat inside source list 1 pool Dir_ISP
Router_Privado(config)#no   ip   nat   pool   Dir_ISP   200.3.192.3   200.3.192.5   netmask
                       255.255.255.248
```

22. Para configurar **NAT overload** ejecute los siguientes comandos:

```
Router_Privado(config)# ip nat pool Dir_ISP 200.3.192.6 200.3.192.6 netmask 255.255.255.248
Router_Privado(config)# ip nat inside source list 1 pool Dir_ISP overload
```

23. Verifique que información entrega el siguiente comando en este momento, después de configurar el NAT overload:
    `Router_Privado#show ip nat translation`

24. Realice ping desde los equipos **PC-PRIV1** y **PC-PRIV2** al equipo **PC-ISP**.

25. Verifique que desde los equipos **PC-PRIV1** y **PC-PRIV2** pueda hacer **http y ftp al Server_ISP.**

26. Ejecute el comando `sh ip nat translation` analice la información que entregan.
    Realice captura de lo que muestra el comando anterior.

27. Ahora instale un sniffer en cada PC de **la red privada** (PC-PRIV21 y PC-PRIV2) y otro sniffer para capturar el **tráfico del Server_ISP**.
    Empiece a capturar tráfico realizando un ping, ftp y http desde el equipo PC-PRIV1 y PC-PRIV2 al Server_ISP, Analice con detenimiento lo que observa en cada sniffer.
    El esquema le debe quedar como se muestra en la figura No. 3.

Entregue captura de lo que visualiza en todos sniffers (una trama por cada tipo de tráfico y PC), donde se permita demostrar que NAT está funcionando, pero discuta/pregúntele a su profesor al momento de hacer esta captura.

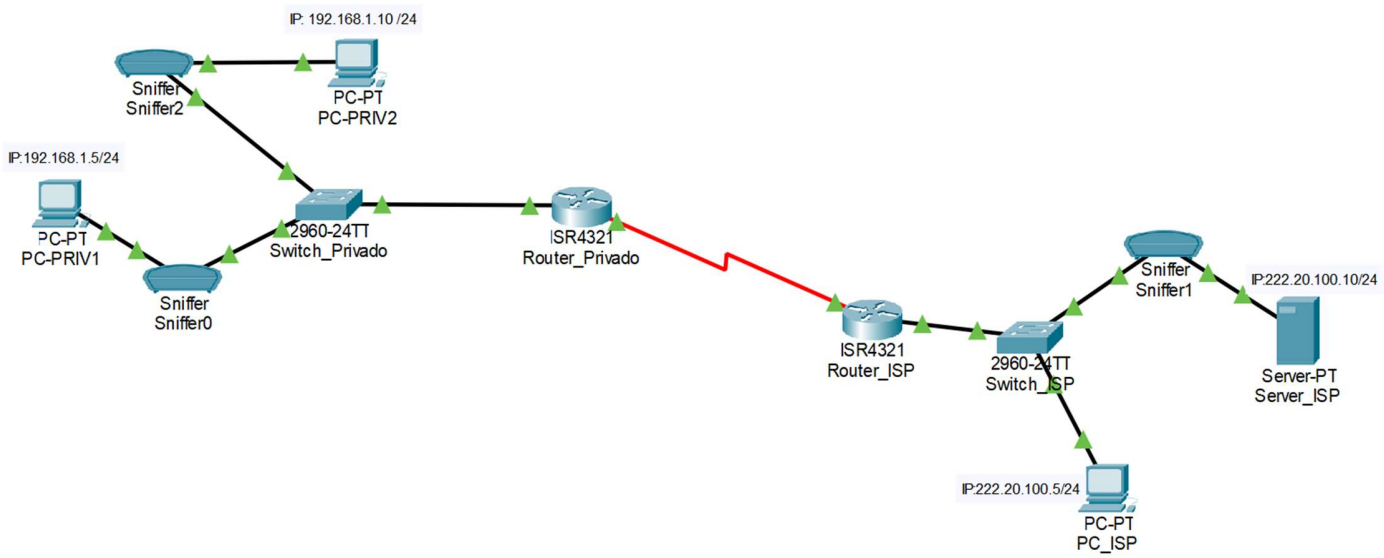

Figura No. 3. Sniffers en el esquema para la captura de tráfico.

28. Al finalizar la práctica debe entregar archivo con las capturas realizadas y sus respectivos análisis explicando que es lo que se observa en cada captura y el archivo de la simulación en packet tracer. Recuerde seguir el esquema para nombrar los archivos: *Apellido_Nombre.pdf* – *Apellido_Nombre.pkt*