INFRAESTRUCTURA I
CONFIGURACIÓN DE NAT (Network Address Traslation)

Nombre: Santiago Valencia García. Código: A00395902.

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.

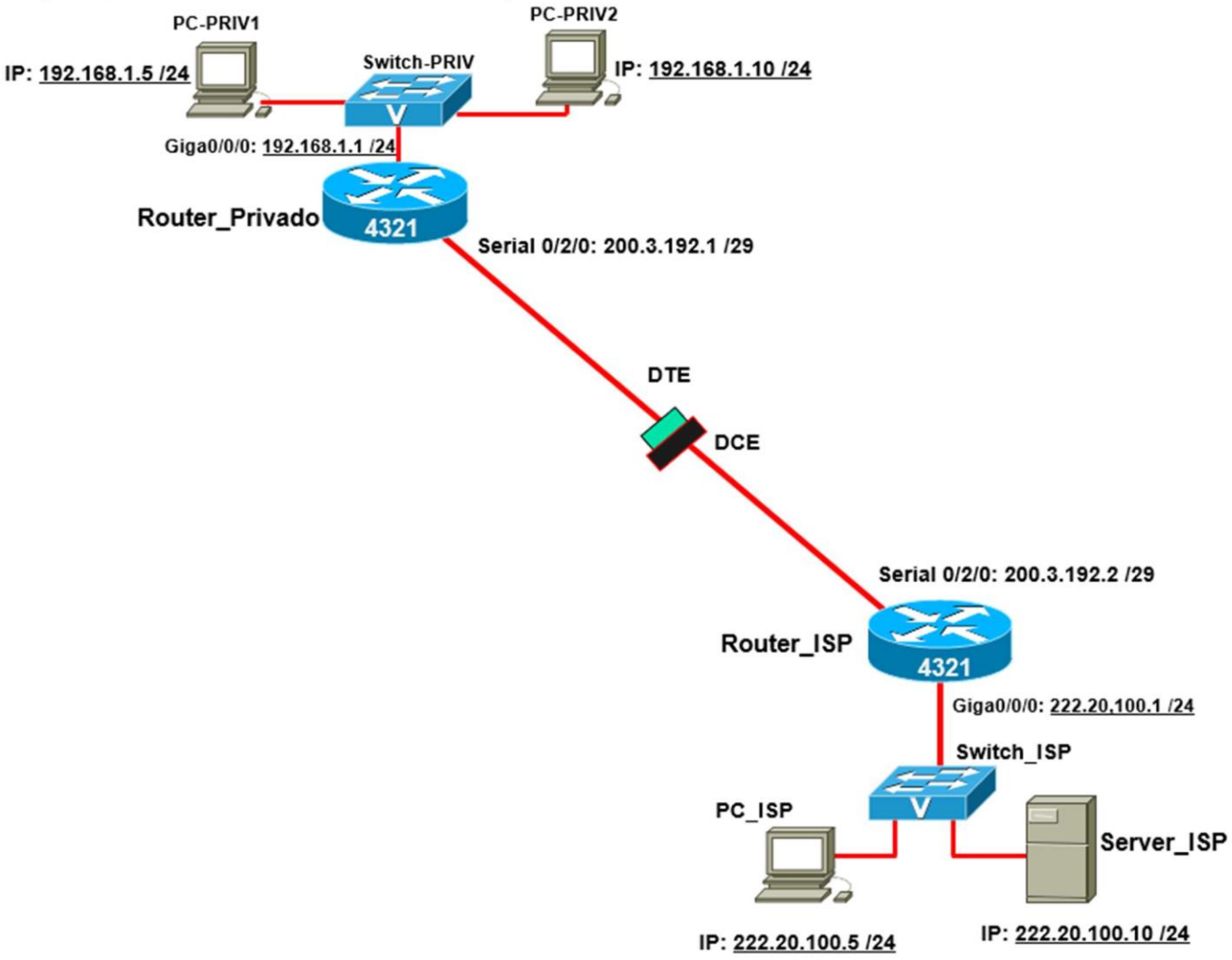


Figura No.1 Esquema a implementar en la práctica.

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`

   En el Router_ISP no configure ningún tipo de enrutamiento.

4. Desde el **PC-ISP** ejecute ping a las siguientes direcciones y verifique que entrega el comando:
   - Ping 200.3.192.2 : Responde ping.
   - Ping 200.3.192.3 : No responde ping. Request timed out.
   - Ping 200.3.192.5 : No responde ping. Request timed out.
   - Ping 192.168.1.5 : No responde ping. Destination host unreachable.
   - Ping 192.168.1.10 : No responde ping. Destination host unreachable.

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 translation
Pro  Inside global     Inside local       Outside local      Outside global
---  200.3.192.3       192.168.1.5        ---                ---
---  200.3.192.5       192.168.1.10       ---                ---
```

Router_Privado# show ip nat statistics

```
Router_Privado#show ip nat statistics
Total translations: 2 (2 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/2/0
Inside Interfaces: GigabitEthernet0/0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

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 : Responde ping.
- Ping 200.3.192.3 : Responde ping.
- Ping 200.3.192.5 : Responde ping.
- Ping 192.168.1.5 : No responde ping. Destination host unreachable.
- Ping 192.168.1.10 : No responde ping. Destination host unreachable.

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?

R/
Al comparar las respuestas obtenidas en el paso 4 con las del paso 7, puedo concluir que las direcciones IP de la red 200.3.192.0/24 ahora responden al ping gracias a la configuración de NAT estático en el Router_Privado.

En el paso 4, la red privada 192.168.1.0/24 no tenía una forma de comunicarse con dispositivos fuera de su red local. El Router_Privado necesitaba una forma de traducir las direcciones privadas a direcciones públicas para que pudieran ser "enrutables" en Internet o en la red pública simulada. Sin esta traducción, los paquetes de ping hacia 192.168.1.5 y 192.168.1.10 desde el PC-ISP no podían ser entregados, y como resultado, se obtenía un mensaje de "Destination host unreachable."

Después de configurar el NAT estático, el Router_Privado traduce las direcciones IP privadas 192.168.1.5 y 192.168.1.10 a las IP públicas 200.3.192.3 y 200.3.192.5, respectivamente. Esto permite que cualquier dispositivo en la red 200.3.192.0/24, como el PC-ISP, vea las IP públicas y pueda comunicarse con los dispositivos de la red 192.168.1.0/24. Por eso, ahora los pings a

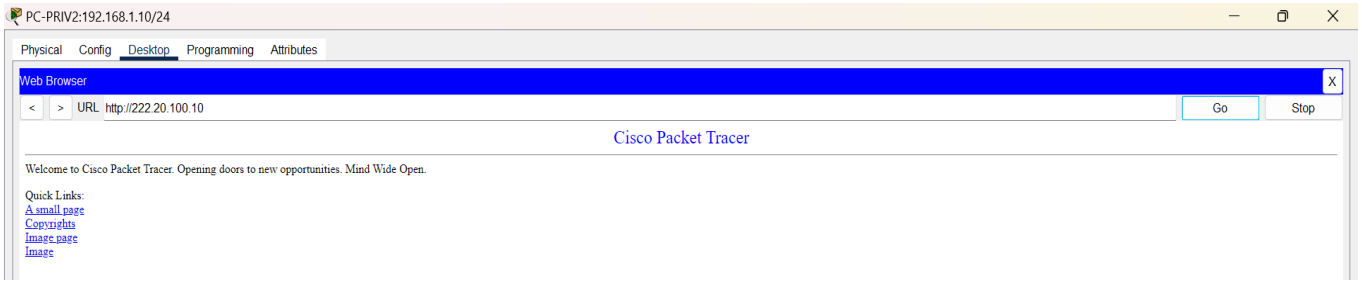
200.3.192.3 y 200.3.192.5 obtienen respuesta.

8. Identifique sobre que **protocolo y puerto** funciona **http y ftp**. Esta información será importante para analizar la información se la siguiente pregunta.
   R/
   HTTP funciona por el protocolo TCP y utiliza el puerto 80 de forma predeterminada. Por su parte, FTP también funciona por el protocolo TCP, y utiliza 2 puertos, el puerto 21 que es usado para control (envío de comandos y configuración de la conexión) y el puerto 20 que es usado para transferencia de datos (envío y recepción de archivos).

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.**
   R/
   Username FTP: cisco
   Password: cisco

```
C:\>ftp 222.20.100.10
Trying to connect...222.20.100.10
Connected to 222.20.100.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

   HTTP:



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?

```
Router_Privado#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  200.3.192.3       192.168.1.5        ---                ---
---  200.3.192.5       192.168.1.10       ---                ---
tcp 200.3.192.3:1026   192.168.1.5:1026   222.20.100.10:21   222.20.100.10:21
tcp 200.3.192.5:1025   192.168.1.10:1025  222.20.100.10:80   222.20.100.10:80
tcp 200.3.192.5:1026   192.168.1.10:1026  222.20.100.10:80   222.20.100.10:80
tcp 200.3.192.5:1027   192.168.1.10:1027  222.20.100.10:80   222.20.100.10:80

Router_Privado#show ip nat statistics
Total translations: 6 (2 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/2/0
Inside Interfaces: GigabitEthernet0/0/0
Hits: 46  Misses: 20
Expired translations: 16
Dynamic mappings:
```

Al comparar los resultados de los comandos en los puntos 6 y 10, se pueden ver cambios importantes en las traducciones NAT y estadísticas en el Router_Privado:

Traducciones de NAT:

En el punto 6, solo estaban las dos traducciones estáticas (200.3.192.3 -> 192.168.1.5 y 200.3.192.5 -> 192.168.1.10) sin tráfico.

En el punto 10, se añaden varias traducciones dinámicas con conexiones TCP a servicios FTP y HTTP, lo que indica tráfico activo de la red interna hacia la externa.

Estadísticas de NAT:

Ahora vemos 46 hits y 20 misses, lo que muestra que ha habido intentos exitosos de acceso a internet, y varias conexiones expiradas (16), evidenciando tráfico continuo y gestión de sesiones por NAT.

Las nuevas entradas y estadísticas confirman que NAT está funcionando para permitir que los dispositivos internos accedan a servicios externos, gestionando múltiples sesiones y conexiones.

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
Router_Privado#show ip nat translation
Router Privado#
```

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`

El comando no muestra nada.

```
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
Router_Privado(config)#exit
Router_Privado#
%SYS-5-CONFIG_I: Configured from console by console

Router_Privado#show ip nat translation
Router_Privado#
```

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

R/

El comando ping utiliza el protocolo ICMP (Internet Control Message Protocol) para verificar la conectividad entre dos dispositivos en una red. A diferencia de otros protocolos como TCP o UDP, ICMP no transporta datos de usuario sino que se utiliza principalmente para enviar mensajes de diagnóstico y control. Cuando ejecutamos un ping, el dispositivo envía paquetes ICMP tipo "Echo Request" al destino, y si este responde, envía un paquete ICMP tipo "Echo Reply" de vuelta.

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

```
C:\>ping 222.20.100.5

Pinging 222.20.100.5 with 32 bytes of data:

Reply from 222.20.100.5: bytes=32 time=1ms TTL=126
Reply from 222.20.100.5: bytes=32 time=1ms TTL=126
Reply from 222.20.100.5: bytes=32 time=1ms TTL=126
Reply from 222.20.100.5: bytes=32 time=1ms TTL=126

Ping statistics for 222.20.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

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

R/

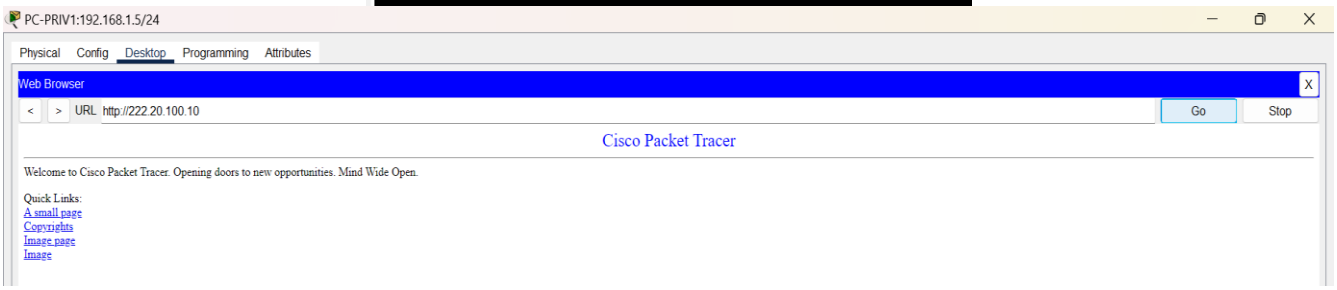
```
Router_Privado#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.3.192.4:10    192.168.1.10:10    222.20.100.5:10    222.20.100.5:10
icmp 200.3.192.4:11    192.168.1.10:11    222.20.100.5:11    222.20.100.5:11
icmp 200.3.192.4:8     192.168.1.10:8     222.20.100.5:8     222.20.100.5:8
icmp 200.3.192.4:9     192.168.1.10:9     222.20.100.5:9     222.20.100.5:9
```

Después del comando, se puede cómo se traducen las direcciones IP gracias a NAT.

18. Identifique sobre que protocolo y puerto funciona http y ftp. Esta información será importante para analizar la información en la pregunta 19.
    R/
    Como ya se mencionó en el punto 8, HTTP funciona por el protocolo TCP y utiliza el puerto 80 de forma predeterminada. Por su parte, FTP también funciona por el protocolo TCP, y utiliza 2 puertos, el puerto 21 que es usado para control (envío de comandos y configuración de la conexión) y el puerto 20 que es usado para transferencia de datos (envío y recepción de archivos).

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

```
C:\>ftp 222.20.100.10
Trying to connect...222.20.100.10
Connected to 222.20.100.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



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?

```
Router_Privado#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 200.3.192.4:1027   192.168.1.5:1027   222.20.100.10:21   222.20.100.10:21
tcp 200.3.192.4:1028   192.168.1.5:1028   222.20.100.10:80   222.20.100.10:80
tcp 200.3.192.5:1028   192.168.1.10:1028  222.20.100.10:21   222.20.100.10:21

Router_Privado#sh ip nat statistics
Total translations: 3 (0 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/2/0
Inside Interfaces: GigabitEthernet0/0/0
Hits: 85  Misses: 35
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool Dir_ISP refCount 3
 pool Dir_ISP: netmask 255.255.255.248
       start 200.3.192.3 end 200.3.192.5
       type generic, total addresses 3 , allocated 2 (66%), misses 0
```

En la captura de los comandos *show ip nat translations* y *show ip nat statistics*, se puede analizar lo siguiente:

Tabla de Traducción: En show ip nat translations, se muestra cómo las direcciones IP internas (192.168.1.5 y 192.168.1.10) han sido traducidas a direcciones globales (200.3.192.4 y 200.3.192.5) para comunicarse con la IP 222.20.100.10 en puertos específicos (21 y 80). Esto confirma que el NAT dinámico está funcionando y permitiendo que los dispositivos internos accedan a servicios externos como FTP y HTTP.

Estadísticas de NAT: En show ip nat statistics, vemos un total de 3 traducciones activas y que todas son dinámicas. Además, muestra una alta cantidad de “hits” (85), lo que indica que muchas conexiones están utilizando las traducciones existentes, mientras que las “misses” (35) reflejan intentos de conexiones que inicialmente no coincidieron con una traducción, lo cual podría ser esperado en tráfico de alta actividad.

Mapeo Dinámico: La sección "Dynamic mappings" confirma que estamos utilizando una lista de acceso (access-list 1) que especifica el rango de direcciones internas permitidas para NAT. El pool "Dir_ISP" está configurado con tres direcciones IP (200.3.192.3 a 200.3.192.5), de las cuales dos ya están asignadas, es decir, está ocupando el 66% de su capacidad.

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`

    El comando no muestra nada:

```
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
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
Router_Privado(config)#exit
Router_Privado#
%SYS-5-CONFIG_I: Configured from console by console

Router_Privado#show ip nat translation
Router_Privado#
```

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

```
C:\>ping 222.20.100.5

Pinging 222.20.100.5 with 32 bytes of data:

Reply from 222.20.100.5: bytes=32 time=16ms TTL=126
Reply from 222.20.100.5: bytes=32 time=1ms TTL=126
Reply from 222.20.100.5: bytes=32 time=1ms TTL=126
Reply from 222.20.100.5: bytes=32 time=1ms TTL=126

Ping statistics for 222.20.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 4ms
```

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

```
C:\>ftp 222.20.100.10
Trying to connect...222.20.100.10
Connected to 222.20.100.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

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

```
Router_Privado#sh ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
tcp 200.3.192.6:1024   192.168.1.5:1029   222.20.100.10:21   222.20.100.10:21
tcp 200.3.192.6:1025   192.168.1.10:1030  222.20.100.10:80   222.20.100.10:80
tcp 200.3.192.6:1029   192.168.1.10:1029  222.20.100.10:21   222.20.100.10:21
tcp 200.3.192.6:1030   192.168.1.5:1030   222.20.100.10:80   222.20.100.10:80
```

Al analizar el comando show ip nat translation, se observa el mapeo de direcciones privadas a públicas, que se realiza mediante NAT. La columna "Inside global" muestra las direcciones IP públicas asignadas por el pool de NAT para que los dispositivos de la red privada accedan a la red externa (en este caso, la red del ISP). La "Inside local" representa las direcciones IP privadas de los dispositivos dentro de la red interna.

Cada línea muestra una conexión específica, con el protocolo TCP. En este caso, veo que los dispositivos 192.168.1.5 y 192.168.1.10 han sido mapeados a la IP pública 200.3.192.6 y están accediendo a recursos en las direcciones externas 222.20.100.10:21 (FTP) y 222.20.100.10:80 (HTTP). Las conexiones se establecen en diferentes puertos, permitiendo múltiples sesiones a través de la misma IP pública.

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.

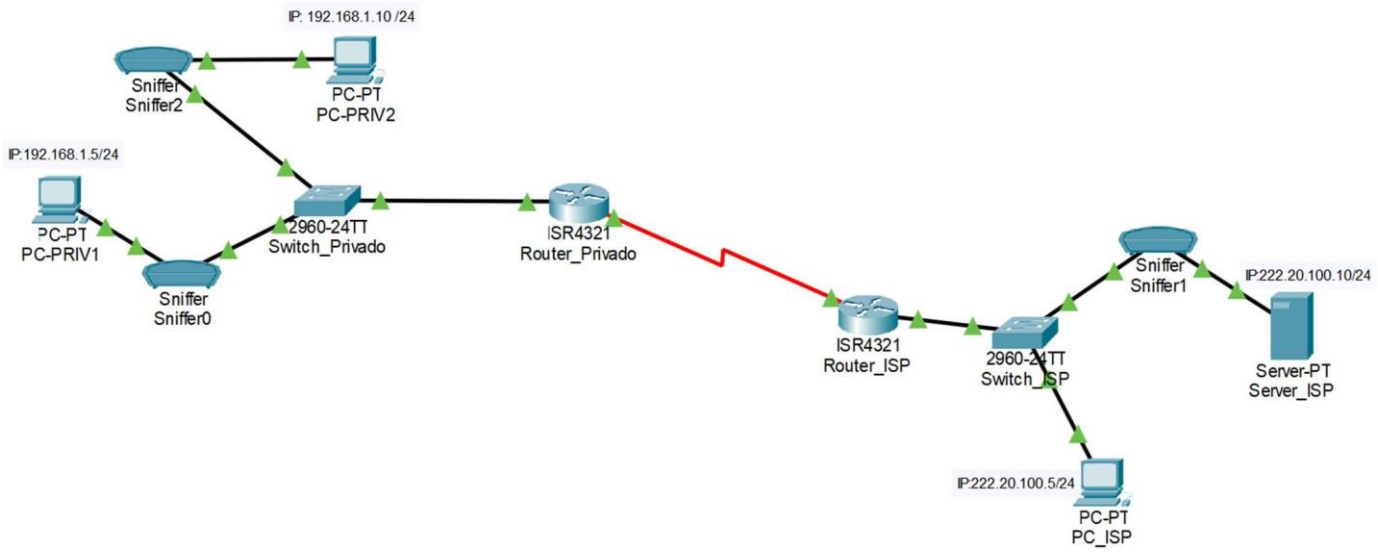
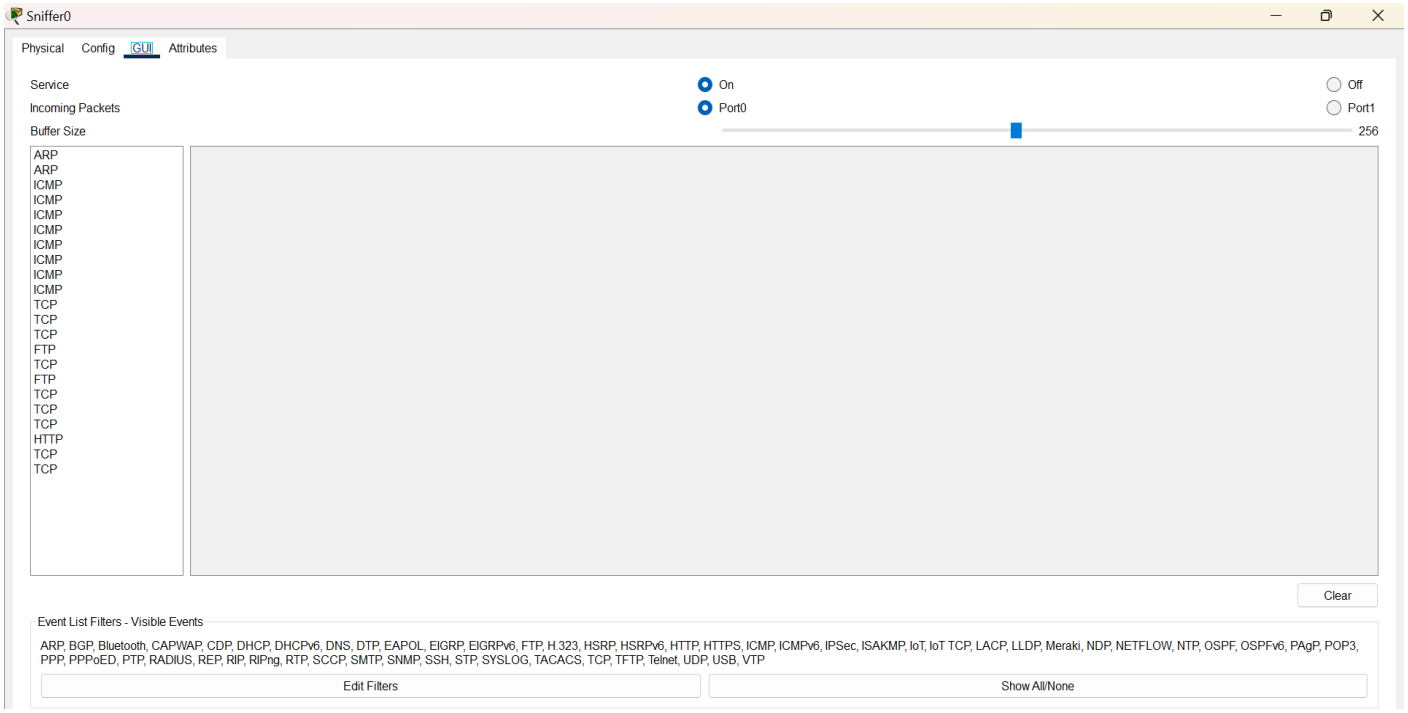
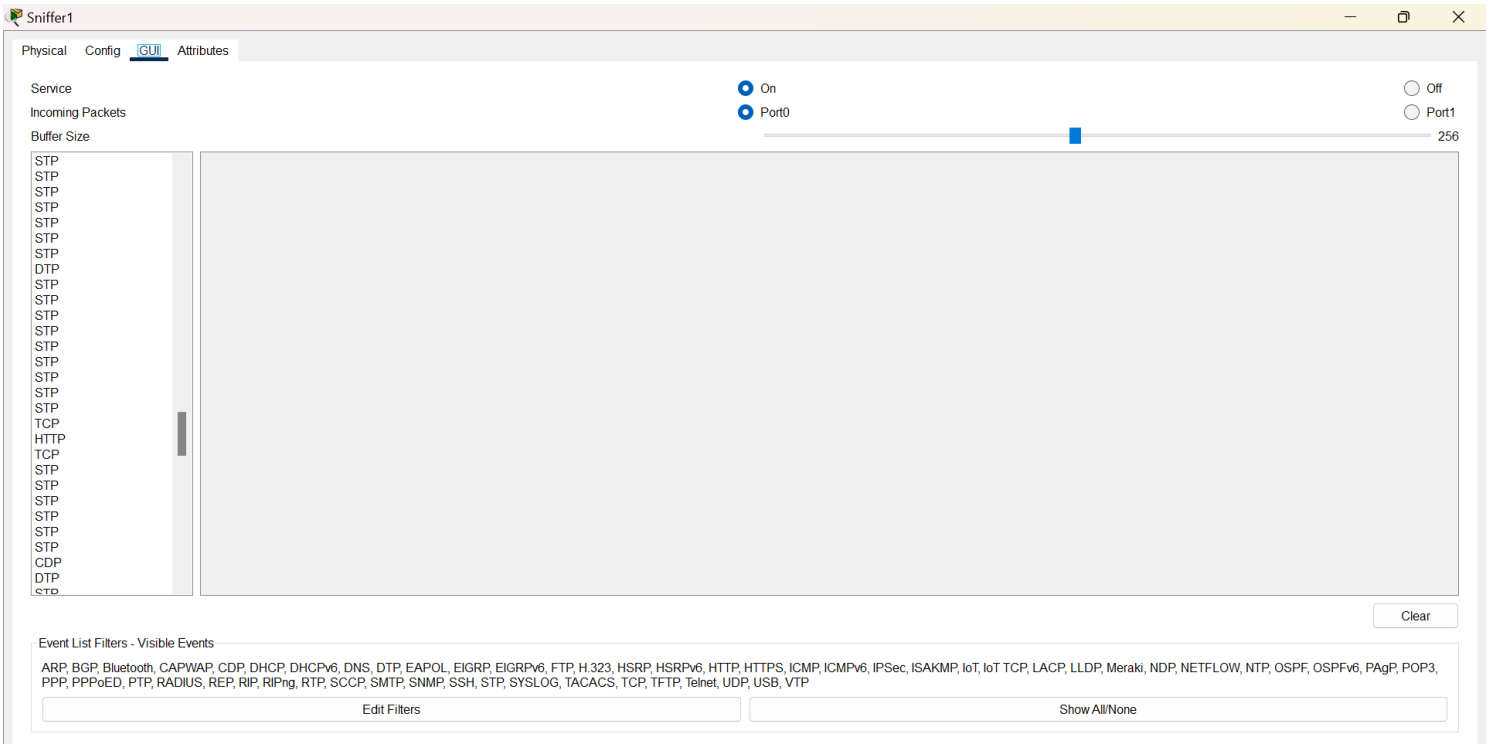


Figura No. 3. Sniffers en el esquema para la captura de tráfico.

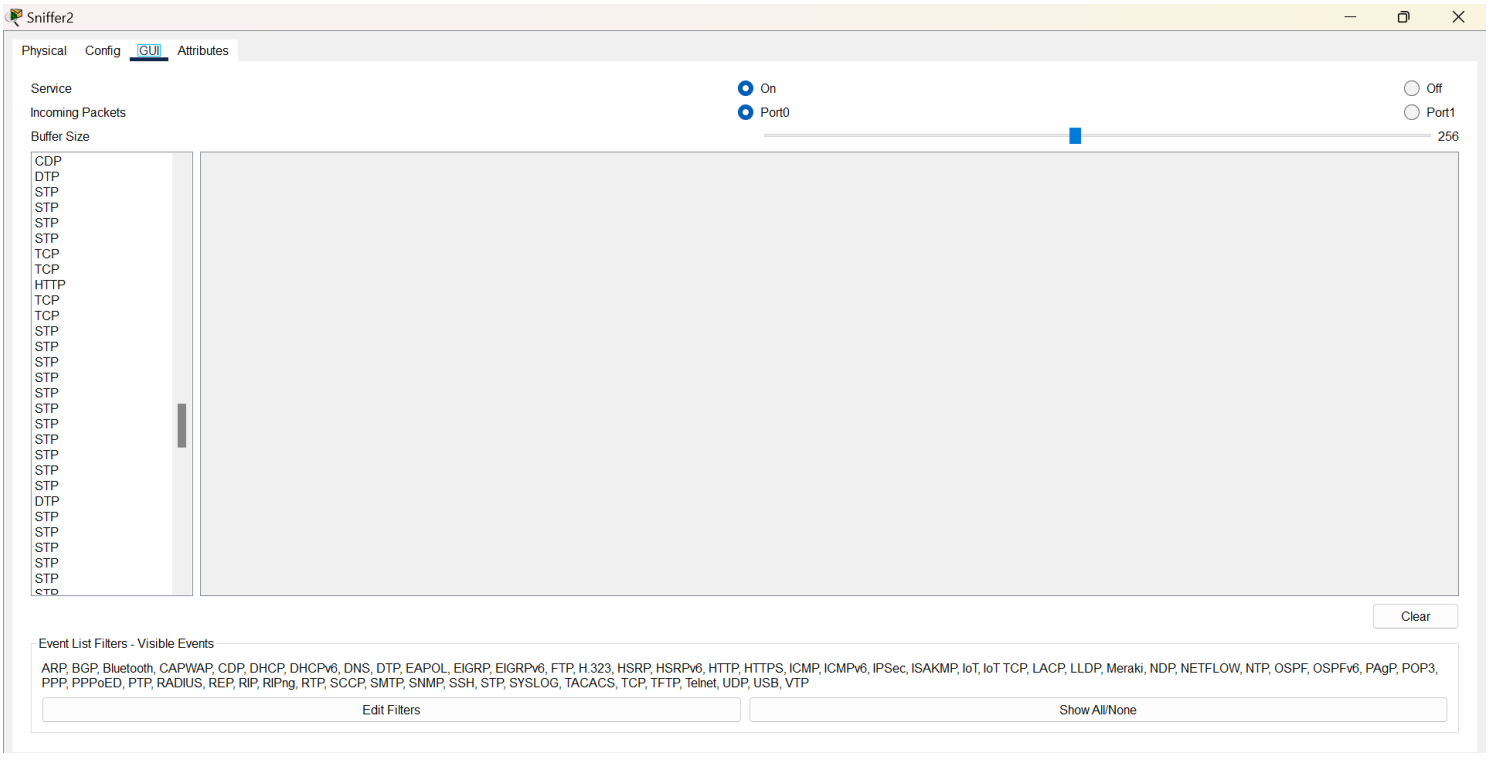
Sniffer 0:

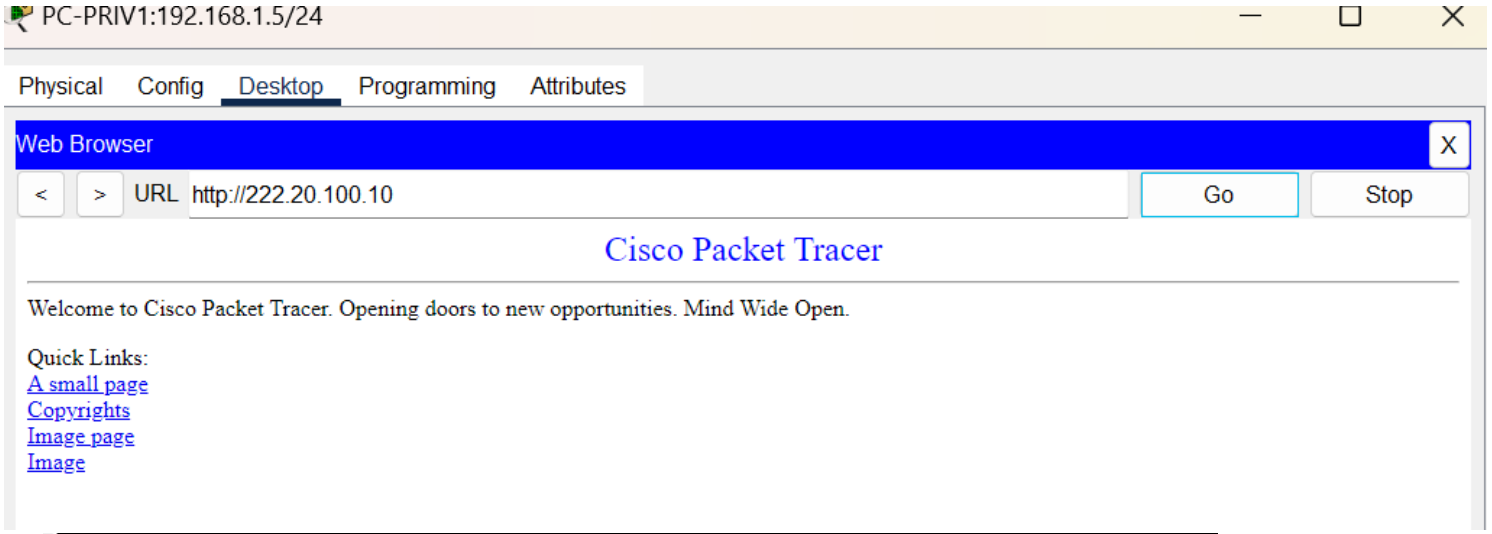


Sniffer 1:

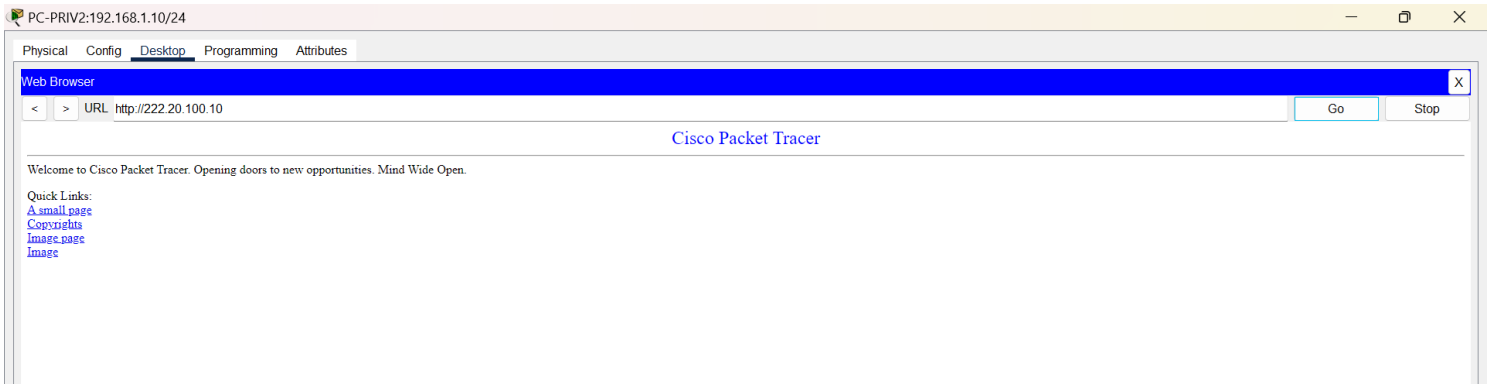

Sniffer1
Physical
Config
GUI
Attributes
Service
On
Off
Incoming Packets
Port0
Port1
Buffer Size
256
STP
STP
STP
STP
STP
STP
STP
DTP
STP
STP
STP
STP
STP
STP
STP
STP
STP
TCP
HTTP
TCP
STP
STP
STP
STP
STP
STP
CDP
DTP
Clear
Event List Filters - Visible Events
ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None

Sniffer 2:

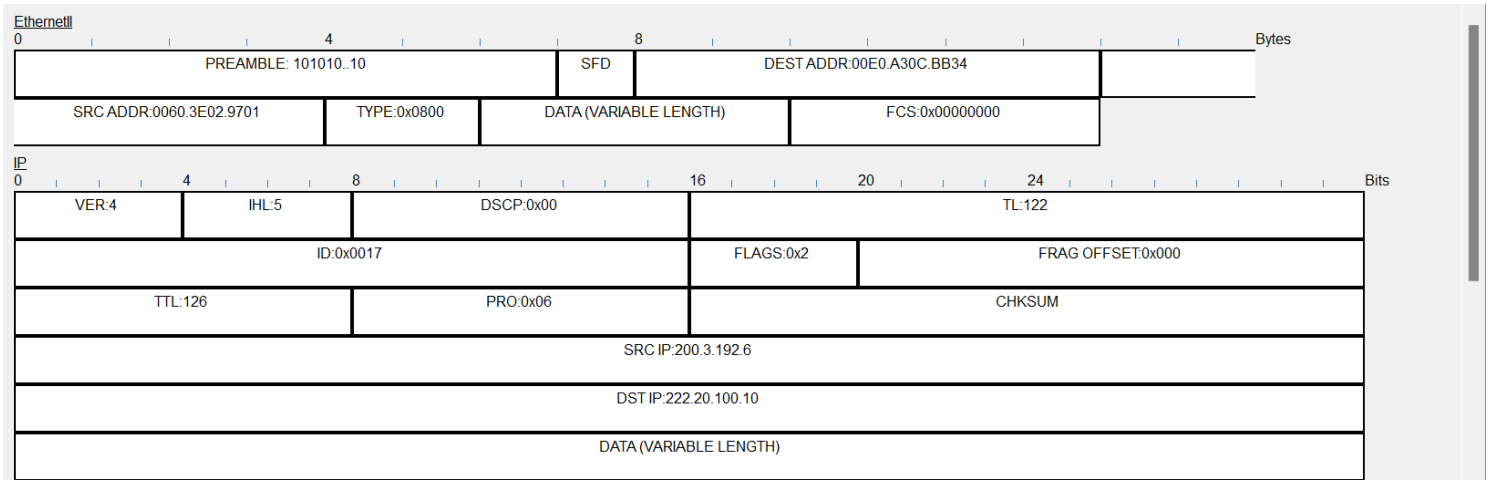

Sniffer2
Physical
Config
GUI
Attributes
Service
On
Off
Incoming Packets
Port0
Port1
Buffer Size
256
CDP
DTP
STP
STP
STP
STP
STP
TCP
TCP
HTTP
TCP
TCP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
DTP
STP
STP
STP
STP
STP
Clear
Event List Filters - Visible Events
ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None

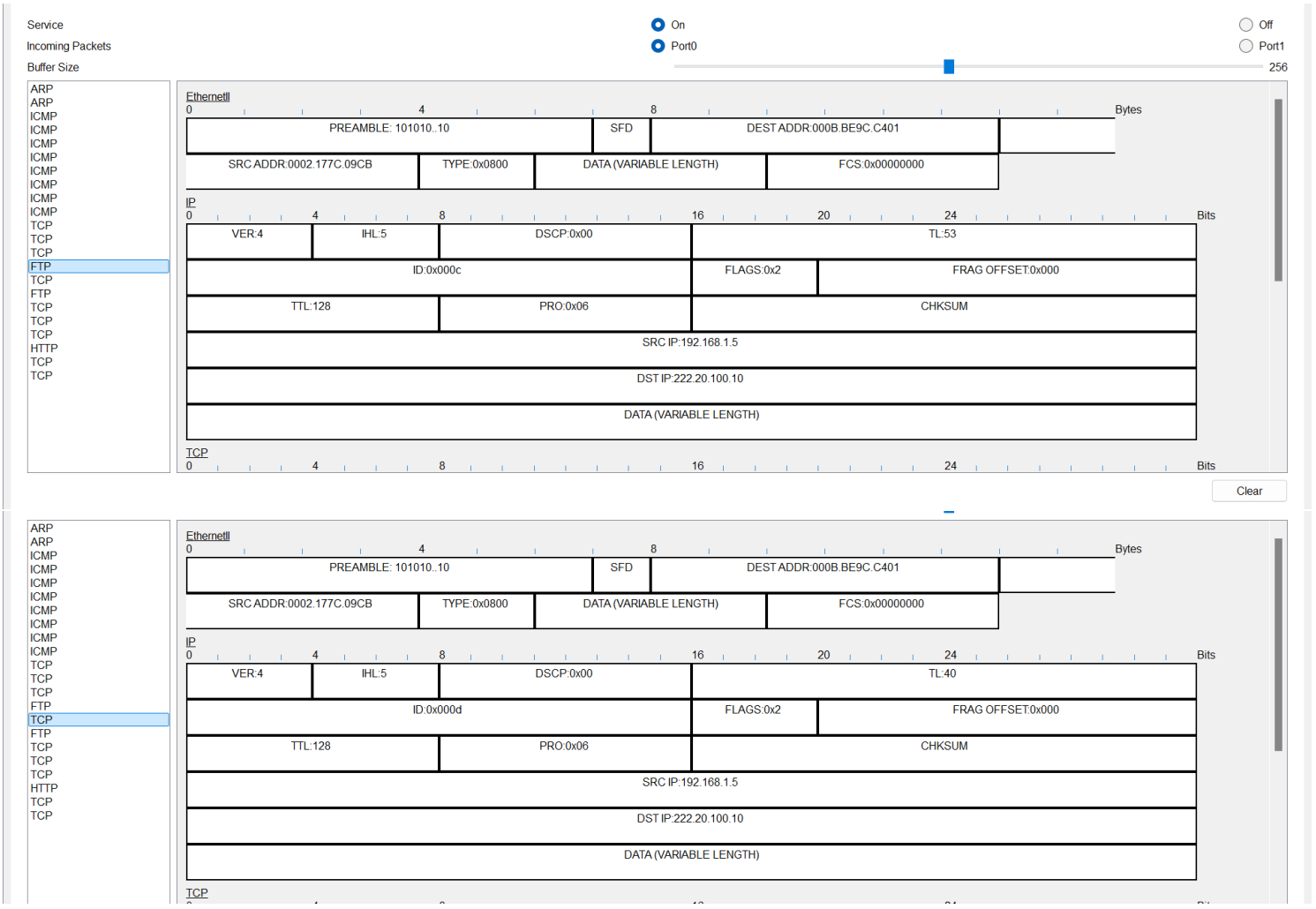



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 222.20.100.10

Pinging 222.20.100.10 with 32 bytes of data:

Request timed out.
Reply from 222.20.100.10: bytes=32 time=1ms TTL=126
Reply from 222.20.100.10: bytes=32 time=15ms TTL=126
Reply from 222.20.100.10: bytes=32 time=3ms TTL=126

Ping statistics for 222.20.100.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 6ms

C:\>ping 222.20.100.10

Pinging 222.20.100.10 with 32 bytes of data:

Reply from 222.20.100.10: bytes=32 time=12ms TTL=126
Reply from 222.20.100.10: bytes=32 time=12ms TTL=126
Reply from 222.20.100.10: bytes=32 time=2ms TTL=126
Reply from 222.20.100.10: bytes=32 time=3ms TTL=126

Ping statistics for 222.20.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 7ms

C:\>ftp 222.20.100.10
Trying to connect...222.20.100.10
Connected to 222.20.100.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```


PC-PRIV2:192.168.1.10/24
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://222.20.100.10
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 222.20.100.10

Pinging 222.20.100.10 with 32 bytes of data:

Reply from 222.20.100.10: bytes=32 time=2ms TTL=126
Reply from 222.20.100.10: bytes=32 time=1ms TTL=126
Reply from 222.20.100.10: bytes=32 time=2ms TTL=126
Reply from 222.20.100.10: bytes=32 time=1ms TTL=126

Ping statistics for 222.20.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 222.20.100.10

Pinging 222.20.100.10 with 32 bytes of data:

Reply from 222.20.100.10: bytes=32 time=13ms TTL=126
Reply from 222.20.100.10: bytes=32 time=2ms TTL=126
Reply from 222.20.100.10: bytes=32 time=3ms TTL=126
Reply from 222.20.100.10: bytes=32 time=24ms TTL=126

Ping statistics for 222.20.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 24ms, Average = 10ms

C:\>ftp 222.20.100.10
Trying to connect...222.20.100.10
Connected to 222.20.100.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```





En las capturas de cada sniffer, se observan los paquetes ICMP, FTP y HTTP generados desde las PCs. Al analizar los encabezados de origen y destino, se verifica que las IP privadas de las PCs se traducen a una IP pública al llegar al Server_ISP, confirmando que NAT está funcionando correctamente.

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*