



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Administración de servicios en red



Práctica 5:

Configuración NAT y DHCP

Alumnos:

Meza Vargas Brandon David
Romero Angeles Abraham

Equipo:

ADR

Grupo:

4CM13

Profesor:

Gaspar Medina Fabian

INTRODUCCIÓN

NAT

Network Address Translation o Direcciones de Red (NAT, por sus siglas en inglés) es una técnica utilizada en redes informáticas para permitir la comunicación entre dispositivos con direcciones IP privadas y la red pública de Internet. NAT actúa como un intermediario entre la red interna y externa, traduciendo las direcciones IP privadas en direcciones IP públicas.

Cuando un dispositivo con una dirección IP privada desea comunicarse con un dispositivo en Internet, el router NAT reescribe la dirección IP privada en el encabezado del paquete y la reemplaza por una dirección IP pública asignada por el proveedor de servicios de Internet (ISP). De esta manera, los dispositivos internos pueden compartir una única dirección IP pública para acceder a Internet.

La traducción de direcciones se realiza a nivel de red o transporte, y puede implicar la traducción de direcciones IP y/o de números de puerto. Existen diferentes tipos de NAT, como NAT estático, NAT dinámico y PAT (Port Address Translation), cada uno con sus propias características y usos.

El NAT ofrece ventajas como la conservación de direcciones IP públicas, ya que permite que múltiples dispositivos utilicen una única dirección IP pública. También proporciona una capa de seguridad adicional al ocultar las direcciones IP internas detrás de una dirección IP pública.

Definición de NAT.

es un proceso mediante el cual las direcciones IP privadas, que son únicas dentro de una red privada, se traducen en direcciones IP públicas, que son reconocibles en Internet. Esto permite que varios dispositivos en una red privada compartan una única dirección IP pública.

Funcionamiento de NAT.

Funciona interceptando los paquetes de datos que se envían desde una red interna hacia Internet y reescribiendo las direcciones IP de origen y destino en el encabezado de los paquetes. Los dispositivos dentro de la red interna se identifican mediante direcciones IP privadas, mientras que el router NAT utiliza una dirección IP pública para comunicarse con el mundo exterior.

Tipos de NAT.

- NAT Estático: Asocia una dirección IP privada específica con una dirección IP pública fija. Permite una traducción uno a uno de direcciones IP.
- NAT Dinámico: Asocia temporalmente una dirección IP privada con una dirección IP pública de un grupo de direcciones disponibles en un pool. Permite compartir una dirección IP pública entre varios dispositivos.
- PAT (Port Address Translation): Utiliza una única dirección IP pública y traduce las direcciones IP privadas junto con los números de puerto para permitir la comunicación. Permite el uso de múltiples conexiones simultáneas en una dirección IP pública.

Ventajas de NAT:

- Escasez de direcciones IP: NAT permite conservar las direcciones IP públicas al compartir una única dirección IP entre varios dispositivos.
- Seguridad: Al ocultar las direcciones IP privadas detrás de una dirección IP pública, NAT proporciona cierto nivel de seguridad, ya que los dispositivos internos no son directamente accesibles desde Internet.
- Flexibilidad en la asignación de direcciones IP: NAT permite el uso de direcciones IP privadas dentro de una red interna, lo que simplifica la administración de direcciones IP.

Desventajas de NAT:

- Limitaciones en la comunicación peer-to-peer: NAT puede dificultar la comunicación directa entre dispositivos internos y externos en aplicaciones que utilizan conexiones peer-to-peer.
- Complejidad en la configuración: La configuración de NAT puede ser complicada, especialmente en redes grandes o complejas.
- Sobrecarga de recursos: NAT puede generar una sobrecarga de recursos en el router, ya que debe realizar la traducción de direcciones para cada paquete que atraviesa la red.

DHCP

El Protocolo de Configuración Dinámica de Host (DHCP, por sus siglas en inglés) es un protocolo de gestión de redes utilizado para asignar dinámicamente direcciones IP y otros parámetros de configuración de red a dispositivos en una red. DHCP simplifica el proceso de asignación de direcciones IP al automatizar el proceso de configuración.

Aquí tienes una investigación más detallada sobre DHCP, que abarca su definición, funcionamiento, componentes, ventajas y consideraciones:

Definición.

DHCP es un protocolo cliente/servidor en el que un servidor DHCP es responsable de asignar y gestionar direcciones IP dentro de una red. Cuando un dispositivo se conecta a una red, envía una solicitud DHCP y el servidor responde con un contrato de arrendamiento que incluye una dirección IP, una máscara de subred, una puerta de enlace predeterminada y otros parámetros de configuración.

Funcionamiento.

DHCP opera a través de una serie de pasos:

1. Descubrimiento DHCP: El cliente envía un mensaje de difusión para descubrir los servidores DHCP disponibles en la red.
2. Oferta DHCP: El servidor DHCP responde al mensaje de descubrimiento del cliente con una oferta que incluye una dirección IP disponible y detalles de configuración.
3. Solicitud DHCP: El cliente selecciona una de las direcciones IP ofrecidas y envía una solicitud al servidor DHCP para reservarla.
4. Reconocimiento DHCP: El servidor responde con un reconocimiento, confirmando el contrato de arrendamiento y proporcionando al cliente la dirección IP asignada y la configuración de red.

Componentes de DHCP.

- Servidor DHCP: Un servidor o dispositivo de red responsable de gestionar y asignar direcciones IP y parámetros de configuración.
- Cliente DHCP: El dispositivo que solicita la configuración de red al servidor DHCP.
- Agente de retransmisión DHCP: Un dispositivo de red que reenvía mensajes DHCP entre clientes y servidores en diferentes segmentos de red.
- Ámbito DHCP: Un rango de direcciones IP que el servidor DHCP puede asignar a los clientes.
- Tiempo de arrendamiento: La duración durante la cual un cliente puede utilizar la dirección IP asignada antes de que deba renovarse.

Ventajas de DHCP.

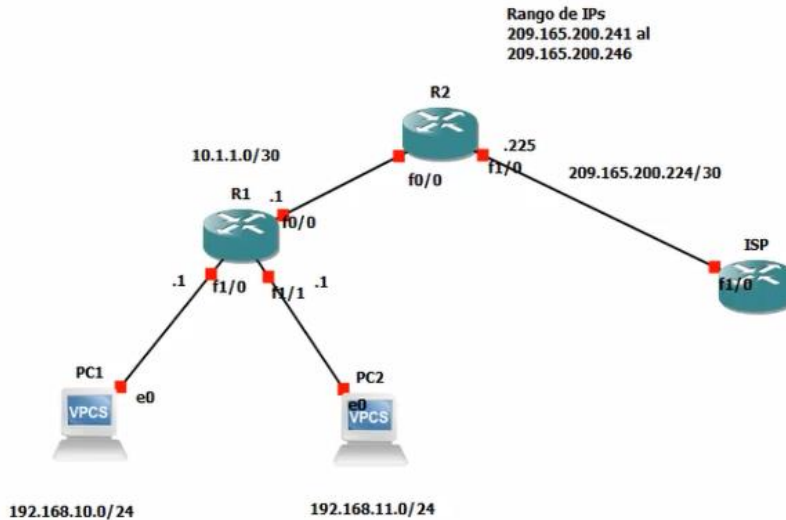
- Administración de red simplificada: DHCP elimina la configuración manual de direcciones IP, lo que facilita la gestión y el mantenimiento de una red.
- Centralización de direcciones IP: DHCP permite un control y una gestión centralizados de la asignación de direcciones IP.
- Utilización eficiente de direcciones: DHCP asigna dinámicamente direcciones IP según sea necesario, evitando el desperdicio de direcciones disponibles.
- Configuración simplificada de dispositivos: DHCP también puede proporcionar parámetros de configuración adicionales, como direcciones de servidores DNS y nombres de dominio, a los clientes.

Consideraciones para DHCP.

- Conflictos de direcciones IP: DHCP debe configurarse correctamente para evitar conflictos cuando varios dispositivos solicitan la misma dirección IP.
- Gestión de arrendamientos: Los contratos de arrendamiento DHCP deben configurarse adecuadamente para garantizar una asignación eficiente de direcciones y evitar el agotamiento de direcciones IP.
- Seguridad: Los servidores DHCP deben protegerse para evitar el acceso no autorizado o actividades maliciosas.
- Redundancia: Implementar servidores DHCP redundantes puede garantizar alta disponibilidad y conmutación por error en caso de fallos del servidor.

DESARROLLO

La topología propuesta para armar en esta práctica y configurar NAT y DHCP es la siguiente:



Primeramente, vamos a configurar las interfaces de los routers como se indica en la imagen.

Para el router 1 tenemos:

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface f1/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface f0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface f1/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*May 25 23:15:35.231: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
R1(config-if)#
*May 25 23:15:35.231: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa1/1 Physical Port Administrative State D
*May 25 23:15:36.231: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed st
R1(config-if)#exit
R1(config)#exit
R1#wr
Building configuration...
```

Verificamos esta configuración

```

R1#sh ip int br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          10.1.1.1        YES manual  up          up
FastEthernet1/0          192.168.10.1    YES manual  up          up
FastEthernet1/1          192.168.11.1    YES manual  up          up
FastEthernet2/0          unassigned      YES unset   administratively down down
FastEthernet2/1          unassigned      YES unset   administratively down down
FastEthernet3/0          unassigned      YES unset   administratively down down
FastEthernet3/1          unassigned      YES unset   administratively down down
Serial4/0                unassigned      YES unset   administratively down down
Serial4/1                unassigned      YES unset   administratively down down
Serial4/2                unassigned      YES unset   administratively down down
Serial4/3                unassigned      YES unset   administratively down down
R1#

```

Ahora vamos con el router 2.

```

R2(config)#interface f1/0
R2(config-if)#ip address 209.165.200.225 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#
*May 25 23:29:02.719: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
R2(config-if)#
*May 25 23:29:02.719: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa1/0 Physical Port Administrat
*May 25 23:29:03.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
R2(config-if)#exit
R2(config)#exi
R2#wr
Building configuration...

*May 25 23:29:31.955: %SYS-5-CONFIG_I: Configured from console by console[OK]
R2#

```

Ahora vamos a excluir las direcciones asignadas estáticamente en el router 1:

```

R1(config)#
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
R1(config)#

```

De igual manera configuramos la alberca de direcciones

```

R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
R1(config)#
R1(config)#ip dhcp pool R1F1_0
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool R1F1_1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool R1F1_0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns
% Incomplete command.

R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#exit
R1(config)#ip dhcp pool R1F1_1
R1(dhcp-config)#default-router 192.168.11.1
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#exit
R1(config)#exit
R1#wr
Building configuration...

```

Algo importante a mencionar en la parte anterior es que el servidor dns 192.168.11.5 no existe y solo fue usado para la práctica.

Ahora verificamos la configuración del pool dhcp en el router 1.

```

R1#
R1#show ip dhcp pool

Pool R1F1_0 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)          : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 0
  Pending event                     : none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  192.168.10.1       192.168.10.1 - 192.168.10.254    0

Pool R1F1_1 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)          : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 0
  Pending event                     : none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  192.168.11.1       192.168.11.1 - 192.168.11.254    0
R1#

```

Ahora procedemos a verificar si nuestra configuración fue exitosa y si funciona en la PC1.

```
PC1> show ip
```

```
NAME           : PC1[1]
IP/MASK         : 0.0.0.0/0
GATEWAY         : 0.0.0.0
DNS             :
MAC             : 00:50:79:66:68:00
LPORT          : 10020
RHOST:PORT      : 127.0.0.1:10021
MTU:            : 1500
```

```
PC1> dhcp
```

```
DDORA IP 192.168.10.11/24 GW 192.168.10.1
```

```
PC1> show ip
```

```
NAME           : PC1[1]
IP/MASK         : 192.168.10.11/24
GATEWAY         : 192.168.10.1
DNS             : 192.168.11.5
DHCP SERVER     : 192.168.10.1
DHCP LEASE      : 86390, 86400/43200/75600
MAC             : 00:50:79:66:68:00
LPORT          : 10020
RHOST:PORT      : 127.0.0.1:10021
MTU:            : 1500
```

```
PC1> █
```

Podemos ver que funcionó correctamente.

Ahora haremos lo mismo con la PC2.

```
PC2> show ip

NAME           : PC2[1]
IP/MASK        : 0.0.0.0/0
GATEWAY        : 0.0.0.0
DNS            :
MAC            : 00:50:79:66:68:01
LPORT         : 10022
RHOST:PORT     : 127.0.0.1:10023
MTU:           : 1500

PC2> dhcp
DDORA IP 192.168.11.11/24 GW 192.168.11.1

PC2> show ip

NAME           : PC2[1]
IP/MASK        : 192.168.11.11/24
GATEWAY        : 192.168.11.1
DNS            : 192.168.11.5
DHCP SERVER    : 192.168.11.1
DHCP LEASE     : 86393, 86400/43200/75600
MAC            : 00:50:79:66:68:01
LPORT         : 10022
RHOST:PORT     : 127.0.0.1:10023
MTU:           : 1500

PC2> █
```

De igual manera fue satisfactorio. Ahora vamos a proceder a configurar NAT en el router 2 comenzando por el proveedor de servicios ISP configurando un enrutamiento estático.

```
ISP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 209.165.200.240 255.255.255.240 209.165.200.225
```

Ahora configuramos OSPF y un enrutamiento estático y determinado en el router 2.

```
Gateway of last resort is not set

    209.165.200.0/30 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, FastEthernet1/0
    10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#exit
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

    209.165.200.0/30 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, FastEthernet1/0
    10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 209.165.200.226
R2#
```

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#default-information originate always
R2(config-router)#exit
R2(config)#exit
```

Ahora procedemos a configurar la NAT estática

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
R2(config)#
*May 25 23:52:46.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to u
R2(config)#ip nat pool MI_NAT_POOL 209.165.200.241 209.165.200.246 net
% Incomplete command.

R2(config)#$OL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
R2(config-ext-nacl)#exit
R2(config)#ip nat inside source list NAT pool MI NAT POOL
```

Se utiliza la dirección IP 209.165.200.254 en el comando de NAT estática para permitir que los dispositivos de la red interna accedan a recursos en Internet utilizando esa dirección IP pública específica, aunque no esté dentro del pool de direcciones IP definido en la práctica.

Especificamos la NAT externa e interna.

```
R2(config)#inter fa1/0
R2(config-if)#ip nat out
R2(config-if)#ip nat outside
R2(config-if)#inter fa0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#end
R2#wr
Building configuration...
[OK]
R2#
```

Y verificamos.

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.254    192.168.20.254    ---                ---
R2#
```

Ahora vamos a verificar la configuración haciendo ping desde la PC1 al ISP y para eso terminamos de configurar ospf en los routers.

En router 1.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.11.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#end
R1#wr
*May 26 00:01:42.555: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
```

En router 2.

```
R2#
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 209
*May 26 00:01:00.691: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on FastEthernet0/24, State Change from Init to 2-Way, Adjacency Done
R2(config-router)#network 209.165.200.224 0.0.0.3 area 0
R2(config-router)#end
R2#
*May 26 00:01:22.051: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Building configuration...
[OK]
R2#
```

Y en el ISP.

```
ISP#confi t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 209.165.200.240 255.255.255.240 209.165.200.225
ISP(config)#end
ISP#wr
Building configuration...
```

Y ahora si hacemos el ping desde PC1 al ISP

```
PC1> ping 209.165.200.226
209.165.200.226 icmp_seq=1 timeout
84 bytes from 209.165.200.226 icmp_seq=2 ttl=253 time=74.797 ms
84 bytes from 209.165.200.226 icmp_seq=3 ttl=253 time=76.627 ms
84 bytes from 209.165.200.226 icmp_seq=4 ttl=253 time=77.119 ms
84 bytes from 209.165.200.226 icmp_seq=5 ttl=253 time=77.206 ms
```

Como vemos ya tenemos comunicación en la red, ahora verificaremos como el servidor NAT realiza la traducción de las ip privadas en ip pública.

Primero verificamos la ip que tiene la PC1 antes de pasar por el servidor NAT.

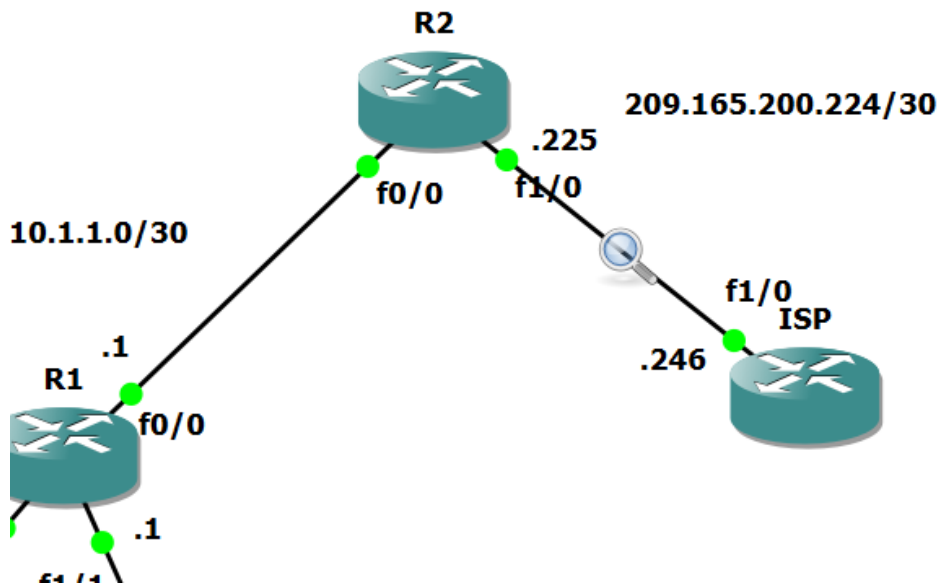
```
NAME : PC1[1]
IP/MASK : 192.168.10.11/24
```

Y comenzamos una captura con wireshark para ver la interacción antes del servidor NAT, filtrando por ICMP y hacemos el ping de nuevo

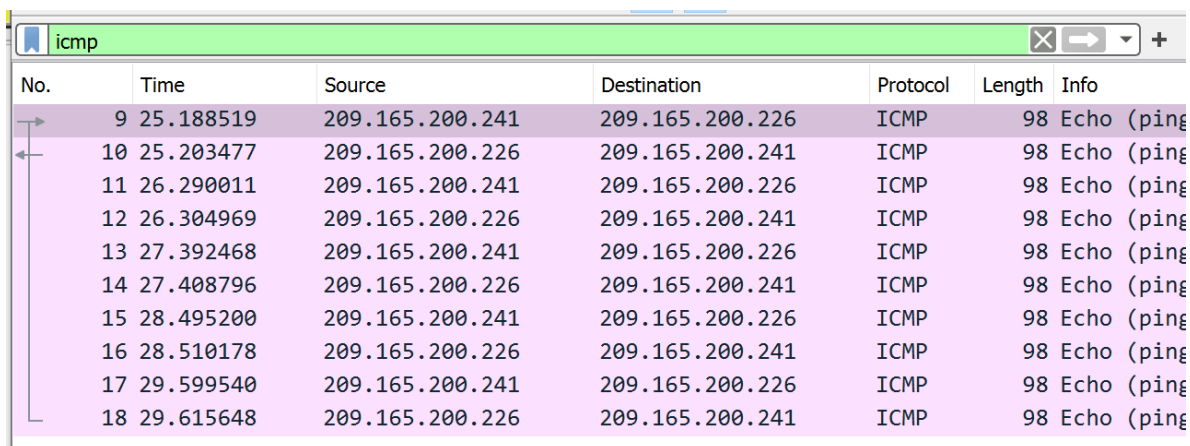
| No. | Time | Source | Destination | Protocol | Length |
|-----|-----------|-----------------|-----------------|----------|--------|
| 9 | 18.276181 | 192.168.10.11 | 209.165.200.226 | ICMP | 9 |
| 10 | 18.321274 | 209.165.200.226 | 192.168.10.11 | ICMP | 9 |
| 11 | 19.368816 | 192.168.10.11 | 209.165.200.226 | ICMP | 9 |
| 12 | 19.415989 | 209.165.200.226 | 192.168.10.11 | ICMP | 9 |
| 14 | 20.464078 | 192.168.10.11 | 209.165.200.226 | ICMP | 9 |
| 15 | 20.510107 | 209.165.200.226 | 192.168.10.11 | ICMP | 9 |
| 16 | 21.545702 | 192.168.10.11 | 209.165.200.226 | ICMP | 9 |
| 17 | 21.591487 | 209.165.200.226 | 192.168.10.11 | ICMP | 9 |
| 18 | 22.639451 | 192.168.10.11 | 209.165.200.226 | ICMP | 9 |
| 19 | 22.685847 | 209.165.200.226 | 192.168.10.11 | ICMP | 9 |

Podemos ver como las ips que interactúan son las que asignamos originalmente.

Ahora vamos a filtrar después del ISP para ver cómo cambian las ips.



Y ahora vemos en wireshark.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------------|-----------------|----------|--------|-------------|
| 9 | 25.188519 | 209.165.200.241 | 209.165.200.226 | ICMP | 98 | Echo (ping) |
| 10 | 25.203477 | 209.165.200.226 | 209.165.200.241 | ICMP | 98 | Echo (ping) |
| 11 | 26.290011 | 209.165.200.241 | 209.165.200.226 | ICMP | 98 | Echo (ping) |
| 12 | 26.304969 | 209.165.200.226 | 209.165.200.241 | ICMP | 98 | Echo (ping) |
| 13 | 27.392468 | 209.165.200.241 | 209.165.200.226 | ICMP | 98 | Echo (ping) |
| 14 | 27.408796 | 209.165.200.226 | 209.165.200.241 | ICMP | 98 | Echo (ping) |
| 15 | 28.495200 | 209.165.200.241 | 209.165.200.226 | ICMP | 98 | Echo (ping) |
| 16 | 28.510178 | 209.165.200.226 | 209.165.200.241 | ICMP | 98 | Echo (ping) |
| 17 | 29.599540 | 209.165.200.241 | 209.165.200.226 | ICMP | 98 | Echo (ping) |
| 18 | 29.615648 | 209.165.200.226 | 209.165.200.241 | ICMP | 98 | Echo (ping) |

De esta manera vemos que nuestro servidor NAT fue configurado correctamente y hace su tarea de traducir ips privadas en ips públicas.

Ahora vamos a configurar una NAT dinámica:

```
%Start and end addresses on different subnets
R2(config)# 209.165.200.241 209.165.200.246 netmask 255.255.255.192
R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R2(config)#ip nat inside source list 1 pool NAT_POOL1
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface fa1/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#exit
```

Y por último una con sobrecarga.

```
R2(config)# 209.165.200.241 209.165.200.246 netmask 255.255.255.192
R2(config)#ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interfa fa1/0
R2(config-if)#ip nat outside
R2(config-if)#exit
```

Y mostramos las estadísticas de las nats configuradas después de mandar un ping de PC1 a ISP

```
R2#show ip nat statistics
Total active translations: 7 (1 static, 6 dynamic; 5 extended)
Outside interfaces:
  FastEthernet1/0
Inside interfaces:
  FastEthernet0/0
Hits: 5 Misses: 4
CEF Translated packets: 8, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 pool NAT-POOL2 refcount 0
  pool NAT-POOL2: netmask 255.255.255.192
    start 209.165.200.241 end 209.165.200.246
    type generic, total addresses 6, allocated 0 (0%), misses 0
[Id: 1] access-list NAT pool MI_NAT_POOL refcount 6
  pool MI_NAT_POOL: netmask 255.255.255.248
    start 209.165.200.241 end 209.165.200.246
    type generic, total addresses 6, allocated 1 (16%), misses 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

CONCLUSIONES

Meza Vargas Brandon David

Esta práctica me sirvió de mucho ya que pude realizar la configuración de NAT y de DHCP, así mismo pude ver como la configuración de DHCP simplificó el proceso de asignación de direcciones IP y parámetros de configuración a los dispositivos en la red y como este proceso es automático.

Romero Angeles Abraham

La práctica me pareció muy interesante ya que pude ver y practicar la configuración y el funcionamiento del DHCP que facilita el trabajo de configuración de IP's, además pude practicar y realizar el procedimiento para mostrar y configurar la NAT estática, dinámica y sobrecarga, además de como se comporta NAT en GNS 3 y a través de los routers y las computadoras.