Configuración de NAT
Taller

Edwar Diaz Ruiz
Cód. 20141020004

Daissi Bibiana Gonzalez Roldan
Cód. 20152020108

11 de junio de 2019

Índice general

Introducción **2**

Objetivos **3**
Objetivo General 3
Objetivos Específicos 3

Desarrollo **4**
NAT *(Network Address Translation)* 4
Tipos de NAT 6
NAT Dinámico 6
NAT Estático 7
PAT *(Port Address Translation)* 8
PAT con múltiples IP 9
Ventajas y Desventajas 9
Practica 12
Preguntas 24

Conclusiones **28**

Introducción

Las redes como herramienta básica para la transmisión de información de forma masiva son elementos que poseen alta capacidad de soporte referente a los diferentes formatos y/o dispositivos emisores inmersos en una red determinada, que con los diversos avances tecnológicos dados en la diversidad de contenidos y funcionalidades propias de los dispositivos, enriquece la distribución de información a través de redes complejas como internet, establecimiento nuevas instancias y retos en la transmisión de la información, de igual forma con las tecnologías orientadas a garantizar el acceso a las redes partiendo inherentemente de la diferenciación de los diversos protocolos a través de los cuales se da el proceso de direccionamiento, como elementos básicos para la definición de dicho transporte de información a través de la red referente a la recepción y emisión de datos, teniendo así el protocolo IP inicialmente propuesto en la creación del proyecto que involucro el desarrollo de las redes como lo fue Ipv4, que si bien permite la transmisión eficiente de información presenta como dificultad el agotamiento de direcciones ip con el progresivo aumento de dispositivos relacionados a la conexión en la red, hecho por el cual se proponen diversas técnicas para la optimización de las mismas, teniendo así la proposición de vlsm, no obstante dicha optimización se puede trasladar a la configuración y transmisión de información entre las redes públicas y privadas respectivamente proponiéndose así la NAT*(Network Address Translation)* o también denominada *Traducción de Direcciones de Red.*

Objetivos

Objetivo General

Definir una topología de red que permita el análisis y la aplicación del proceso de traducción de datos inmerso en la transformación de información desde una red privada a una red publica, teniendo en cuenta el proceso inverso que pudiera darse en el uso de la red.

Objetivos Específicos

- Comprensión de los aspectos referentes a la definición de las NAT *(Network Address Translation)* o también denominadas *Traducción de Direcciones de Red*.
- Definir la diferenciación inmersas en lo diferentes tipos de NAT que e pueden dar en el proceso de implementación de un proceso de traducción determinado dentro de una red, destacando así el papel de los NAT *Estaticos* y *Dinámicos* respectivamente.
- Estructurar topología básica entre dos departamentos que permita ver la distribución que eventualmente se daría con la definición de una red configurada con el protocolo RIP v2, que incluya NAT de diferentes tipos.
- Configurar red teniendo en cuenta las NAT, las subredes y la conexión privada y publica que se incluyan dentro del proceso de transmisión de datos.

Desarrollo

De forma inicial la implementación relacionada con lo procesos de enrutamiento e Internet no fue pensada para ser una red tan extensa, sino como una herramienta que permitiera la conexión entre universidades estadounidenses, por lo cual se reservaron "sólo" 32 bits para direcciones, el equivalente a 4.294.967.296 direcciones únicas; hecho que con el desarrollo progresivo de la transmisión de información se ha constituido como un limitante fundamental debido al masivo aumento de dispositivos conectados a Internet, así como la implementación de diversas tecnologías que hacen uso de la misma como la IoT o el aumento de redes de diferentes características alrededor del mundo, por lo cual se dio que las direcciones IP se agotaban, hecho por el cual surgió la *NAT* o *Network Address Translation.*[1]

NAT *(Network Address Translation)*

Dentro del proceso de estructuración de la de redes se tiene que a definición de IP's que permitan el enrutamiento de paquetes de información a través de la red, como un proceso básico fundamental para el adecuado funcionamiento de las mismas, de esta manera se tiene el planteamiento de las NAT *(Network Address Translation)* o *Traducción de Direcciones de red*, la cual consiste en el proceso de volver a asignar un espacio de dirección IP a otro modificando la información de direccionamiento de red en los paquetes de encabezado IP. Este proceso ocurre mientras los paquetes están en tránsito a través de un dispositivo de enrutamiento de tráfico y se usó originalmente como un acceso directo en lugar de que cada host individual se redirigiera cada vez que se movía una red. Sin embargo, desde entonces, especialmente gracias al agotamiento de las direcciones IPv4, NAT se ha convertido en una herramienta popular y esencial para conservar el espacio global de direcciones. Esto se debe a que incluso una sola dirección IP enrutable de Internet

de una puerta de enlace NAT se puede usar para una red privada completa; si bien la NAT se ha vuelto popular y común debido a lo bueno que es para conservar el espacio de direcciones, conlleva serias consecuencias para la calidad de la conexión a Internet. Como tal, se necesita mucha atención al detalle cuando se implementa para garantizar que no se convierta en un detrimento. Esto se debe a que la implementación de NAT puede variar en el comportamiento de direccionamiento y su efecto en el tráfico de red.[2] De esta manera partiendo de la estructura de las redes locales tienen varias direcciones IP privadas que pertenecen a dispositivos específicos de la red. A través de un sistema NAT, estas direcciones privadas se traducen en una dirección IP pública cuando las peticiones salientes de los dispositivos de red se envían a Internet. Un proceso inverso ocurre cuando los datos entrantes, normalmente como respuesta a peticiones específicas, se envían a una red local. En este caso, el NAT cambia la dirección IP pública por la dirección IP privada del dispositivo específico al que se dirige el paquete de datos. La dirección IP pública es utilizada repetidamente por el enrutador que conecta los ordenadores a Internet.[3]

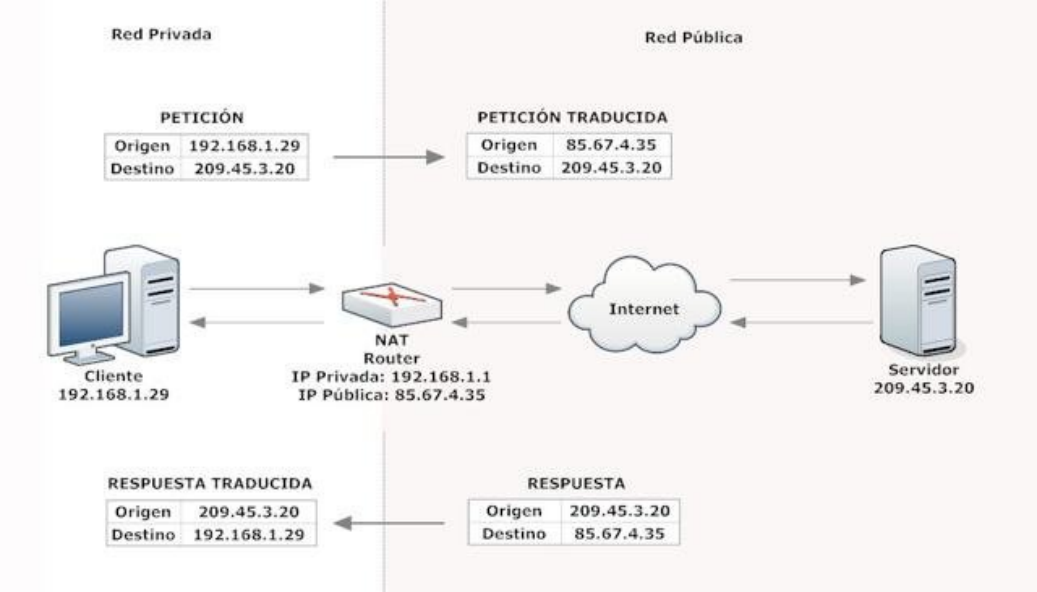

Figura 1: Proceso de NAT [1]

Así se tiene que el flujo interno en la red se da de forma que cuando los usuarios inician el tráfico a la dirección IP global del servidor, el tráfico

llega al router NAT y se desvía al servidor, pero cuando el tráfico regresa al router NAT, el router no lo reenvía, porque el servidor 192.168.1.1 está adjunto/reconocido en la interfaz interna, por lo cual para corregir esta situación, se enmascara (NAT) el tráfico de origen externo cuando atraviese el router NAT, teniendo en cuanta que la NAT tiene que estar habilitada en las interfaces internas y externas.[4] De esta manera se tiene que NAT es uno de los mecanismos utilizados en la Internet actual para hacer frente a la escacez de direcciones IPv4 públicas junto con el enrutamiento sin clase CIDR (Classless Interdomain Routing) y la utilización de máscaras variables VLSM (Variable Lenght Subnet Mask). Hoy en día solamente queda cerca de un 5 % de direcciones IPv4 públicas, con lo cual se hace cada vez más necesario comenzar con la implementación de IPv6. Sin embargo aún son muchas las organizaciones que no cuentan con IPv6 en sus redes y deben trabajar con las limitaciones de IPv4. Es ahí donde entra a funcionar NAT.[5]

Tipos de NAT

Este proceso de traducción puede darse de diferente maneras de esta manera se hace posible ver diferentes tipos de configuracion NAT, teniendo así:

NAT Dinámico

El NAT dinámico es el más básico de todos los métodos de traducción de direcciones privadas a públicas, el cual consiste en tener un bloque IP público e ir asignando dinámicamente una de esas IP a cada máquina de la LAN interna para que salga a Internet, de esta manera se hacen necesaria la definición de una cantidad adicional de IP públicas aparte de la necesaria en la interfaz WAN del router para lograr conectividad. En este tipo de NAT, las IP reservadas para el bloque público se van utilizando y se crea un mapping 1:1 entre las IP internas y las externas, Asociándose de forma dinámica.

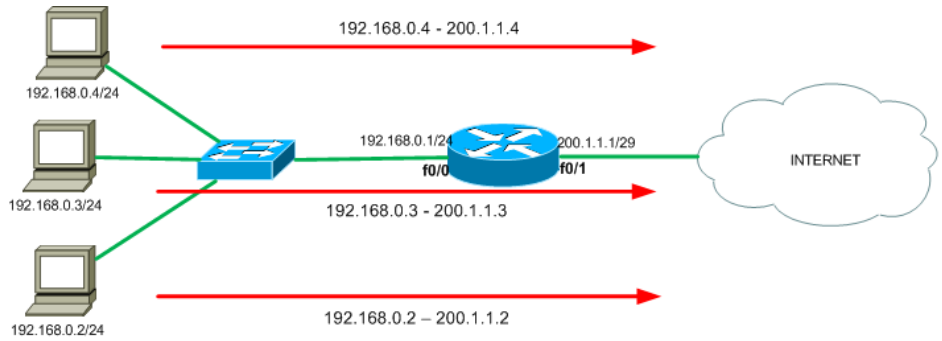

Figura 2: NAP Dinámico [5]

La desventaja de implementar NAT dinámico es que se debe contar con una IP pública para cada PC de la LAN interna que se quiera conectar a Internet. En un entorno con más de 100 equipos, que es lo habitual, esto encarecería enormemente los costos mensuales del acceso a Internet. Por esta razón no es muy fácil encontrar NAT dinámico actualmente.[5]

NAT Estático

Es el más simple de configurar y permite asociar estáticamente una dirección pública a una dirección IP privada. Es ideal para permitir el acceso desde Internet a un servidor que alojamos en una DMZ(demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet, por ejemplo o en la red LAN institucional.

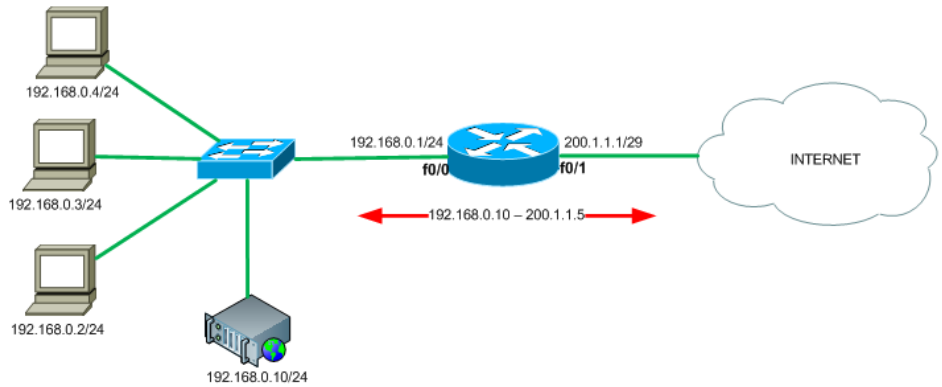

Figura 3: NAP Estático[5]

Para proveer un acceso publico de forma que se pueda acceder exteriomente a un servidor en una LAN, se hace necesaria la configuración de forma que se de asocie una dirección IP pública única al servidor, donde se tiene que esta IP no puede ser utilizada en otro NAT al mismo tiempo ya que queda reservada para la IP privada del mismo; es de destacar que en otros sistemas, como OpenBSD, se suele utilizar el nombre de NAT 1:1 (one-to-one).[5]

PAT *(Port Address Translation)*

Es el método de NAT más utilizado probablemente. A diferencia de los dos métodos anteriores donde cada IP privada se mapea en forma directa con una única IP pública, en el PAT se asocian dinámicamente todas las conexiones originadas en la LAN con una única IP pública, identificando cada sesión con un puerto de dicha IP (Por eso se llama Port Address Translation). Habitualmente PAT se conoce también como "Sobrecarga" u "Overload", ya que se le da todo el trabajo de traducción a una sola IP o interfaz de red.

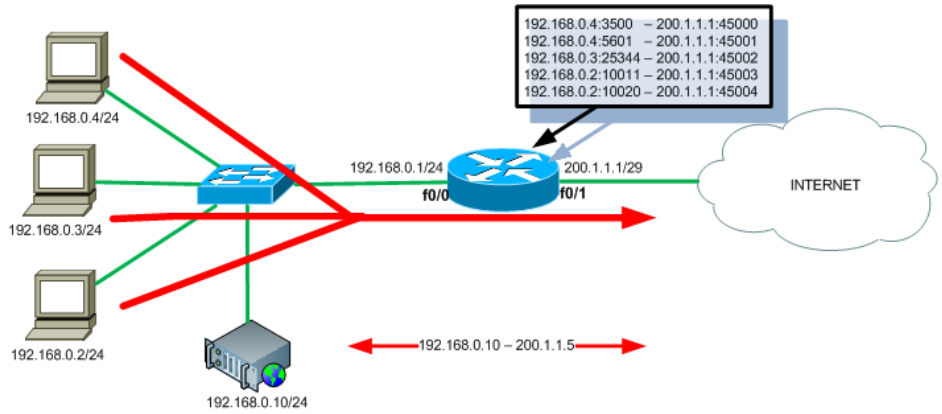

Figura 4: PAT *(Port Address Translation)*[5]

Este es el tipo de NAT que más se usa, además de venir implementado de manera predeterminada en los routers de tipo SOHO (domésticos); de igual forma se tiene que si se encuentra un servidor privado el acceso al mismo se daría como en el caso del NAT Estático, asignándole una dirección publica especifica a la IP privada del servidor, sin incluir dicha dirección privada en la asociación dinámica de puertos.[5]

PAT con múltiples IP

A pesar de que PAT es el mecanismo más ampliamente configurado en las redes actuales, lo cierto es que tiene una tremenda limitación en entornos donde la cantidad de máquinas en la LAN es de gran tamaño.Conduciendo a la asociación de una nueva IP pública a la sobrecarga o un rango de ellas, multiplicando las cantidades de sesiones simultáneas que se permitan en la traducción de puertos, para evitar los ataques DoS por el agotamiento de peticiones que dichas redes podrían atender simultáneamente.

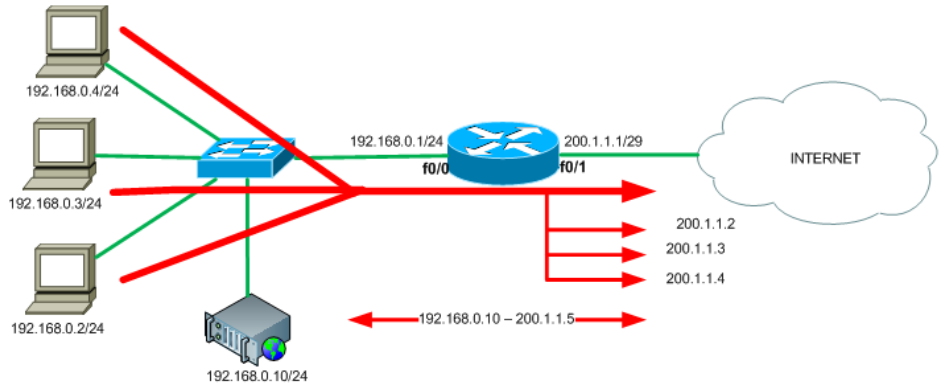

Figura 5: PAT con múltiples IP[5]

Es de destacar que hay otras implementaciones más complejas como NAT-T que por lo general se utiliza para resolver problemas de conectividad con VPNs y acceso a redes detrás de un NAT.[5]

Ventajas y Desventajas

Es de evidenciar que el uso de las NAT es un método utilizado por las múltiples ventajas que este proporciona en cuanto a la conexión que este permite, no obstante es de recalar los diferentes aspectos que dicha tecnología abarca, teniendo así:

Ventajas	***Desventajas***
Ayuda a mitigar el agotamiento del espacio de direcciones IP públicas globales.	Los protocolos de tunelización se complican a medida que el NAT cambia los valores en las cabeceras de los paquetes, lo que afectará a las comprobaciones de integridad de estos protocolos.
Las redes ahora pueden utilizar internamente el espacio de direcciones privado RFC 1918 sin dejar de tener acceso a Internet.	Dado que las direcciones internas están ocultas detrás de una única dirección de acceso público, sería imposible que un host externo inicie la comunicación con un host interno sin una configuración especial en el cortafuegos que lo permita.
Aumenta el nivel de seguridad al ocultar el esquema de direccionamiento y la topología interna de la red.	La NAT dinámica (también DNAT), como la NAT estática (utilizada por WatchGuard), no es común en redes pequeñas, sino en redes grandes que se usan en corporaciones con redes complejas. Si bien la NAT estática proporciona una asignación de direcciones IP estáticas internas a públicas, la NAT dinámica difiere al no hacer que la asignación sea estática y utiliza un conjunto de direcciones IP públicas disponibles.

Cuadro 1: Ventajas y desventajas [2][3]

Ventajas	***Desventajas***
	Los hosts privados detrás de un enrutador habilitado para NAT no pueden usar comunicación de extremo a extremo y por lo tanto; No se pueden usar algunos protocolos IP. Por ejemplo, los servicios que requieren conexiones TCP desde fuera de la red y conexiones sin estado como UDP pueden interrumpirse. Esto significa que el propio enrutador debe hacer un esfuerzo para admitir estos protocolos, ya que los paquetes entrantes que los utilizan nunca alcanzarán a su destinatario. Algunos protocolos pueden admitir una instancia de NAT entre hosts, como el Protocolo de transferencia de archivos (FTP) cuando se encuentra en modo pasivo, pero a veces necesitarán ayuda de una puerta de enlace de nivel de aplicación y fallarán cuando los sistemas estén separados de Internet por NAT. Otra limitación es que los protocolos de tunelización también son complicados a medida que el NAT cambia los valores en los encabezados de los paquetes, lo que afectará las verificaciones de integridad de estos protocolos.
	Las aplicaciones que utilizan Voz sobre IP (VoIP), videoconferencias y otras funciones peer-to-peer deben utilizar técnicas transversales NAT para que funcione; debido a que las direcciones internas están ocultas detrás de una única de acceso público, es imposible que un host externo inicie la comunicación con un host interno sin alguna configuración especial en el firewall para permitir esto.

Cuadro 2: Ventajas y desventajas [2][3]

Es de destacar igualmente que NAT no se usa comúnmente en IPv6, ya que uno de los objetivos de IPv6 es restaurar la conectividad de red de extremo a extremo. Esto significa que el loopback NAT no es necesario y, aunque es posible, el gran espacio de direccionamiento de IPv6 disminuye la necesidad de conservar las direcciones.[2]

Practica

De forma inicial se construye la topología sin la adición respectiva de una configuración, así se tiene:

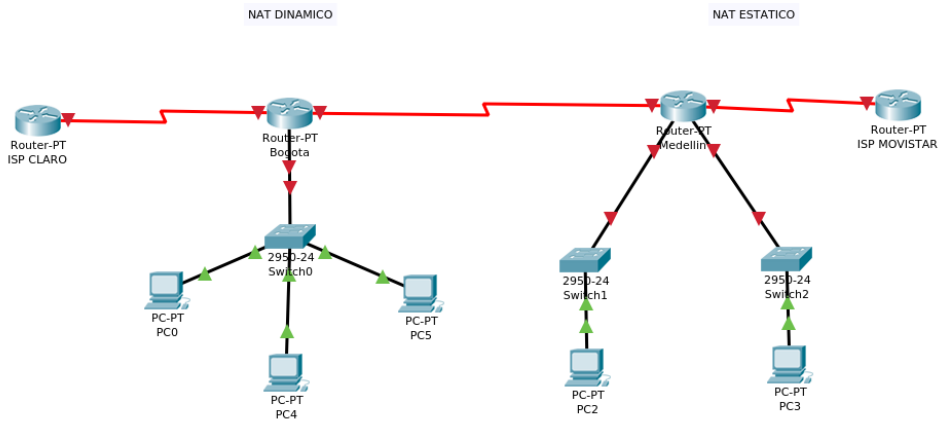

Figura 6: Topología Básica

Teniendo en cuenta la configuración propuesta, teniendo:

Cantidad de Host Requeridas	***Dirección de Red***	***Mascara de Subred***	***Cantidad máxima de host posibles***	***Nombre de la red***	***Dirección Inicial***	***Dirección Final***	***Broadcast***
240	172.17.0.0	255.255.255.0	254	Bogota	172.17.0.1	172.14.0.254	172.14.0.255
264	172.17.2.0	255.255.255.0	254	Medellín	172.17.2.1	172.17.2.254	172.17.2.255
	172.17.3.0	255.255.255.240	14	Medellín	172.17.3.1	172.17.3.14	172.17.3.15

Cuadro 3: Tabla de Direccionamiento LAN

Red	***Dirección de red***	***Mascara de subred***	***Dirección Inicial***	***Dirección Final***	***Broadcast***
Bog - Med	200.0.0.0	255.255.255.252	200.0.0.1	200.0.0.2	200.0.0.3
ISPCla - Bog	200.0.1.0	255.255.255.248	200.0.1.1	200.0.1.6	200.0.1.7
ISPMov - Med	200.0.1.8	255.255.255.248	200.0.1.9	200.0.1.14	200.0.1.15

Cuadro 4: Tabla de Direccionamiento WAN

De esta manera se realiza la configuración delos dispositivos en la red, teniendo así la configuración de los computadores en la red, de esta manera se tiene a su configuración de la forma:

Figura 7: Configuración de IP de dispositivo

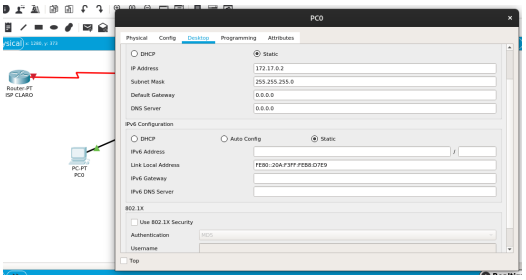

Figura 8: Configuración de IP de dispositivo

Por tanto luego de la asignación de las IP respectivas a cada uno de los equipos de la red se tiene:

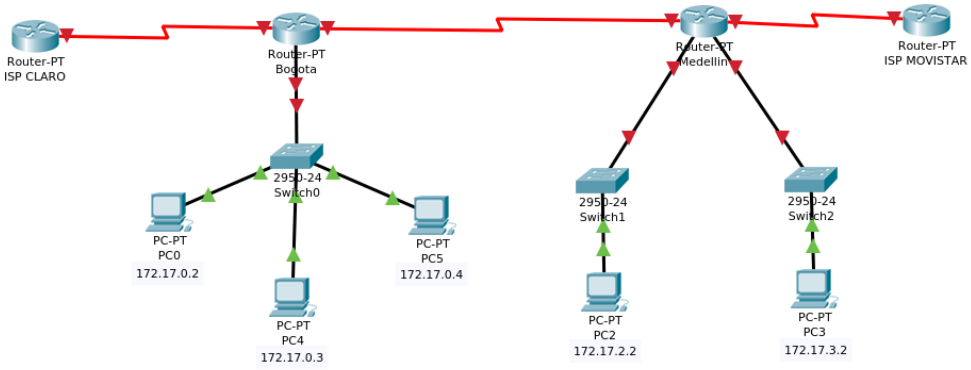

Figura 9: Configuración de IP de todos los dispositivos

Así se tiene de forma inicial la configuración local (LAN) de **Medellín**:

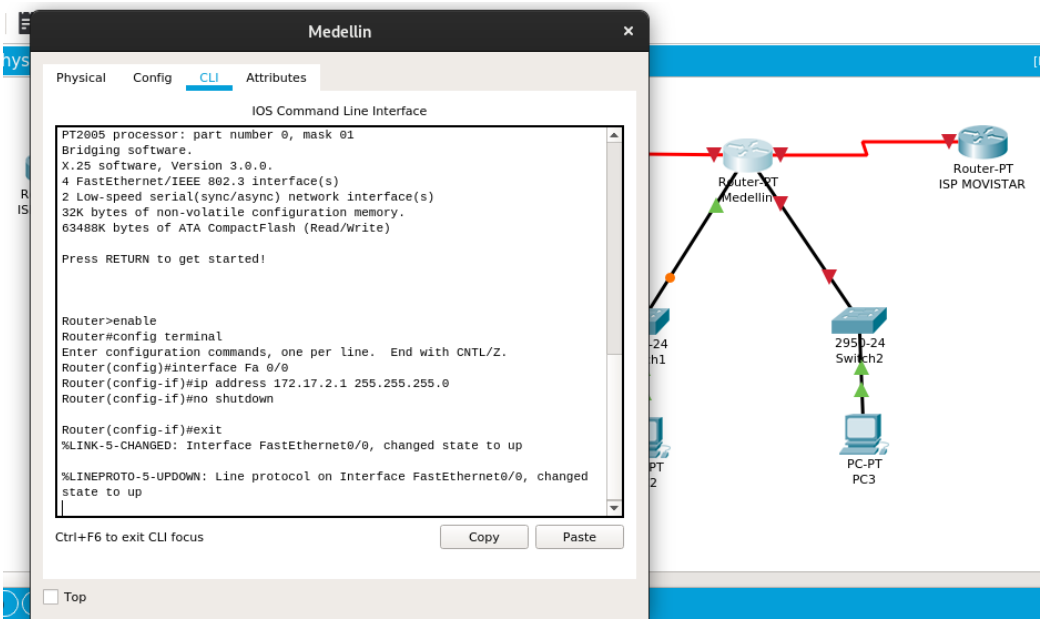

Figura 10: Direccionamiento de Subred 1

La cual se obtiene con el uso de los comandos en el router:

```
enable
config terminal
interface Fa 0/0
ip address 172.17.2.1 255.255.255.0
no shutdown
exit
```

De igual forma para la segunda subred, se tiene:

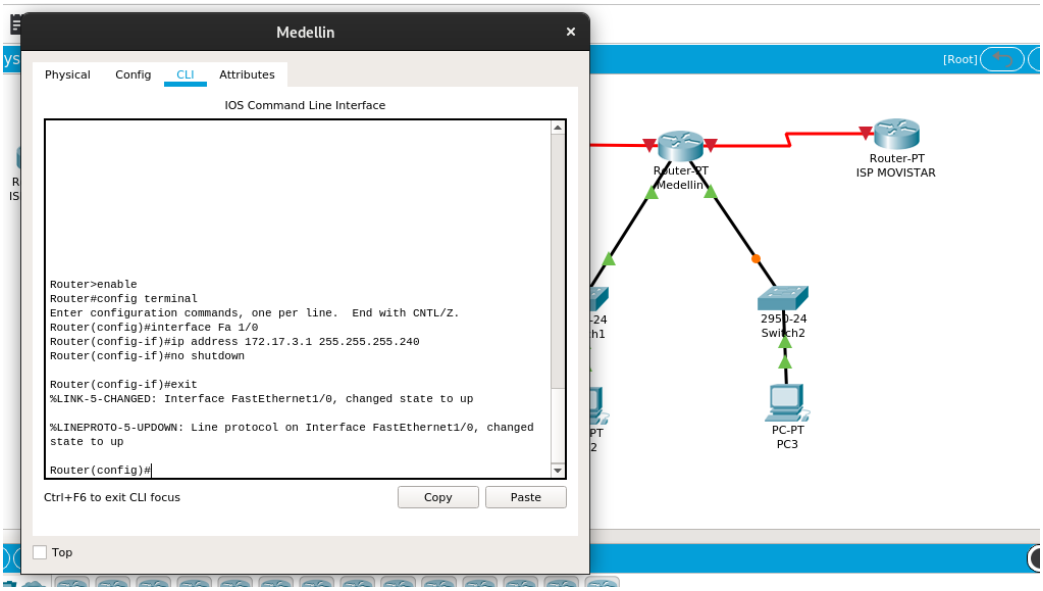

Figura 11: Direccionamiento de Subred 2

Con los comandos:

```
enable
config terminal
interface Fa 1/0
ip address 172.17.3.1 255.255.255.240
no shutdown
exit
```

Así se tiene de forma inicial la configuración local (LAN) de **Bogotá**:

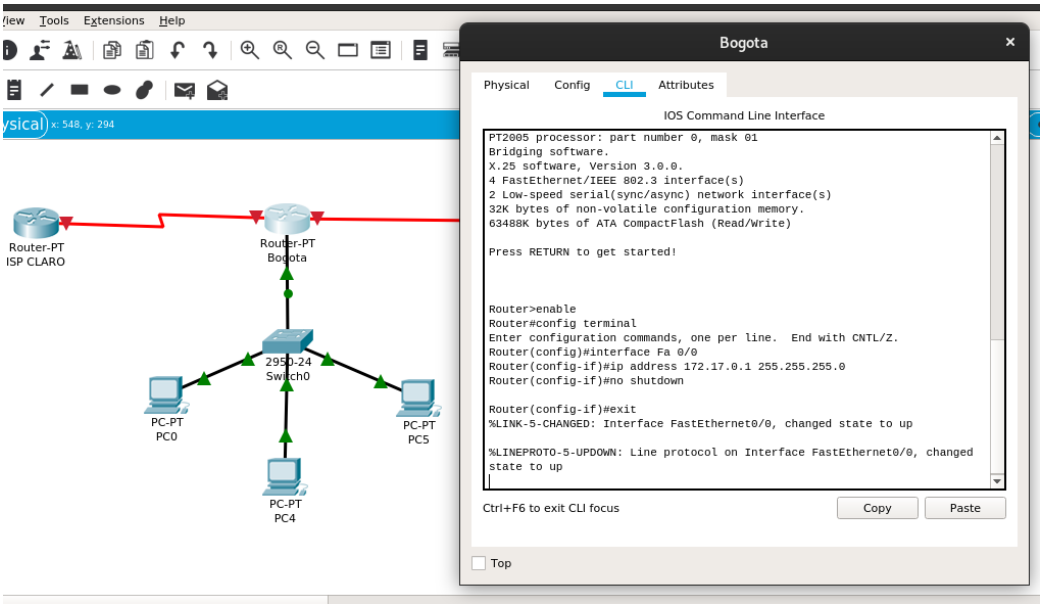

Figura 12: Direccionamiento de Subred

La cual se obtiene con el uso de los comandos en el router:

```
enable
config terminal
interface Fa 0/0
ip address 172.17.0.1 255.255.255.0
no shutdown
exit
```

Para el proceso de enrutamiento se tiene como protocolo a usar *RIP Versión 2*, se tiene para Medellín: De forma inicial se implementa el siguiente comando con el fin de no hacer uso de resumen de ruta:

```
no auto-summary
```

Así aplicando la asignación de de puertos en la red RIP, como:

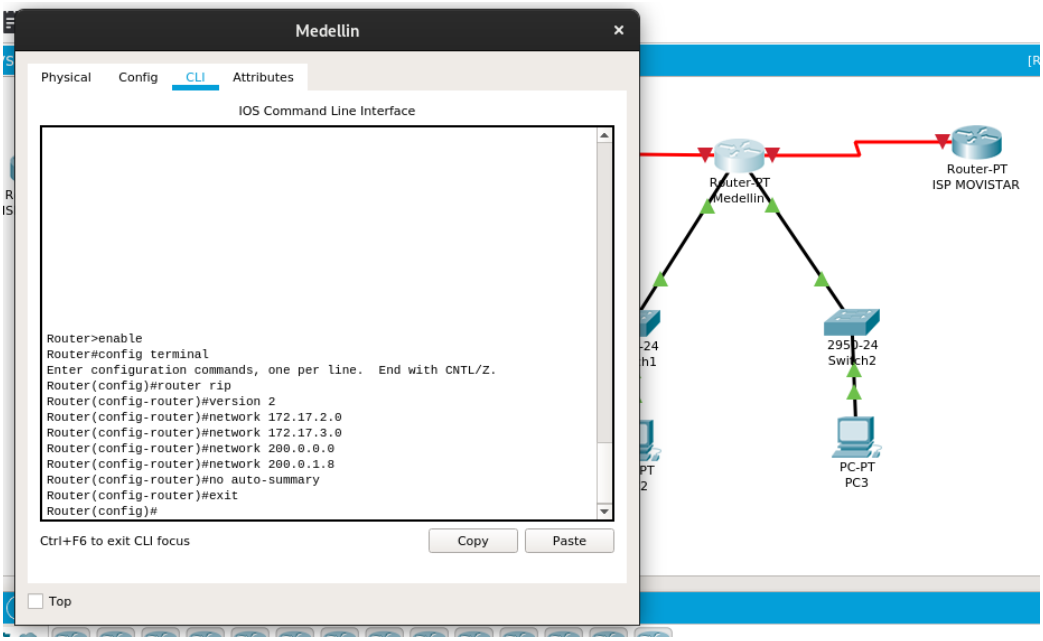

Figura 13: Configuración de RIP v2

Con los comandos:

```
enable
configure terminal
router rip
version 2
network 172.17.2.0
network 172.17.3.0
network 200.0.0.0
network 200.0.1.8
no auto-summary
exit
```

De igual forma para Bogotá:

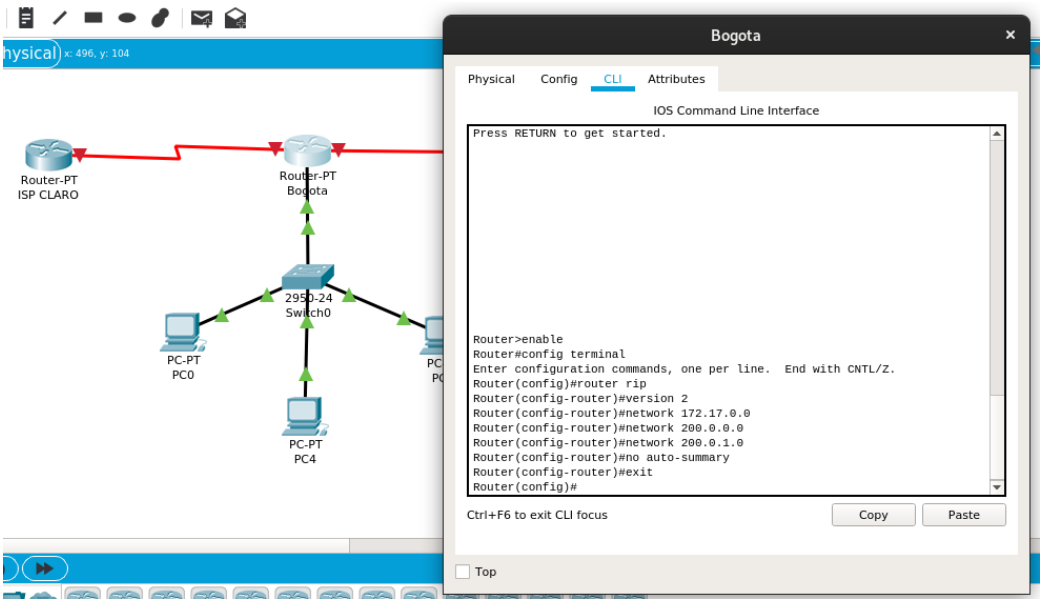

Figura 14: Configuración de RIP v2

Con los comandos:

```
enable
config terminal
router rip
version 2
network 172.17.0.0
network 200.0.0.0
network 200.0.1.0
no auto-summary
exit
```

De esta manera se procede a habilitar las conexiones seriales en ambos routers:

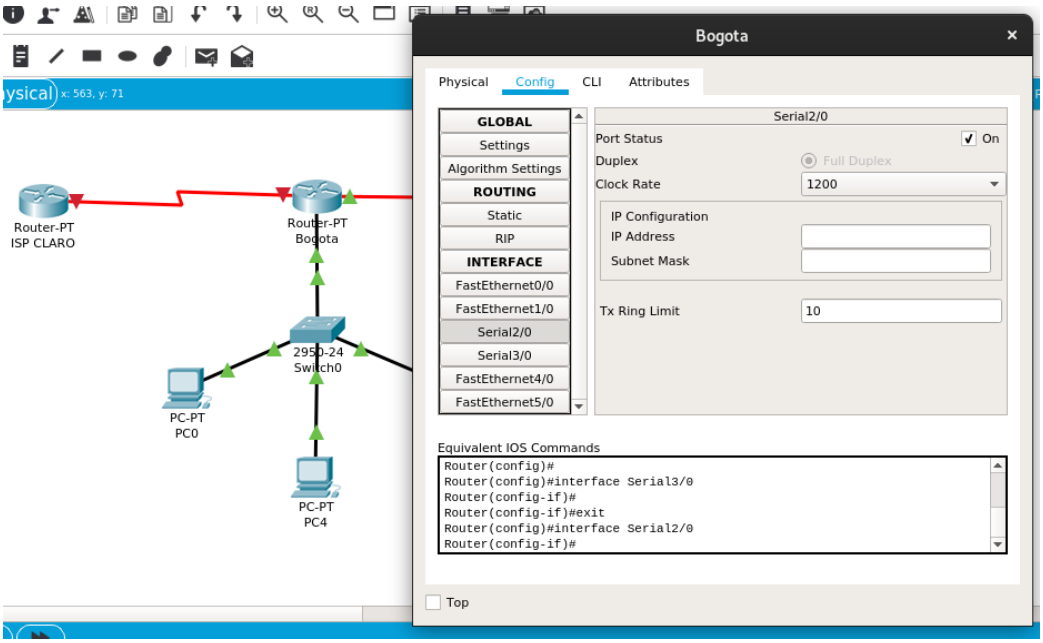

Figura 15: Activación de puertos seriales en router Bogotá

Teniendo en cuenta los NAT a configurar se tiene que, teniendo que para Medellín, se implementa ***NAT Estático***, se tiene que:

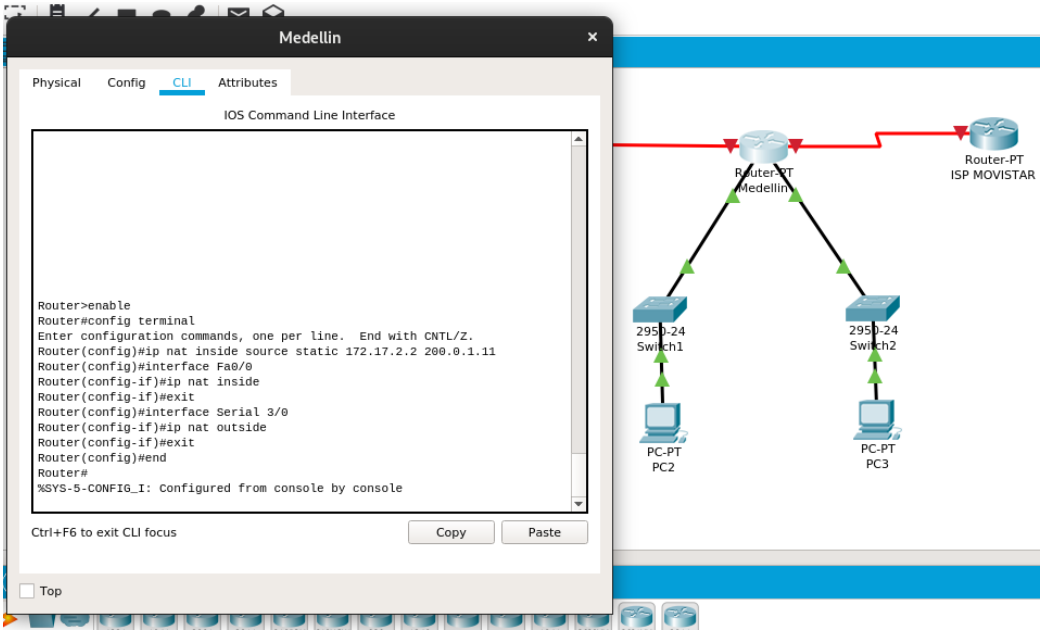

Figura 16: Configuración de NAT Estatico

Con los comandos:

```
enable
config terminal
ip nat inside source static 172.17.2.2 200.0.1.11
interface Fa0/0
ip nat inside
exit
interface Serial 3/0
ip nat outside
exit
end
```

Haciéndose posible observar su tabla NAT con el comando:

```
show ip nat translation
```

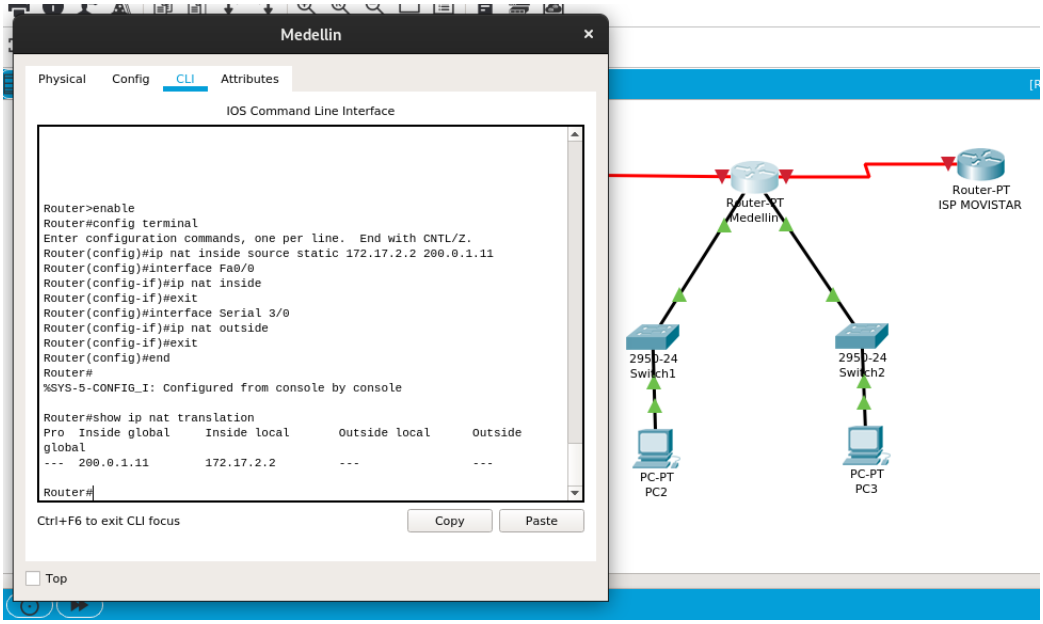

Figura 17: Tabla NAT

De igual forma se tiene que para Bogotá la configuración a realizar es la de ***NAT Dinámico***, teniendo:

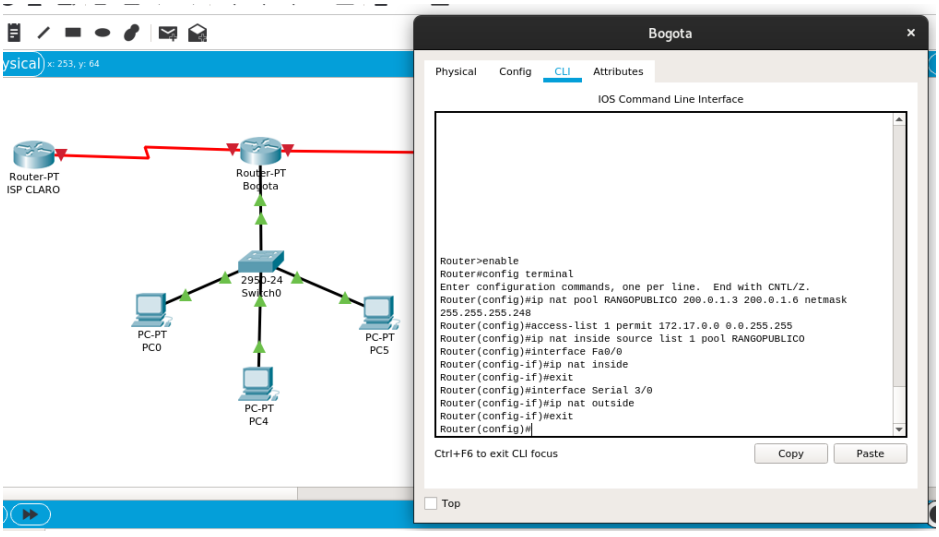

Figura 18: Configuración de NAT Dinámico

Realizada con los comandos:

```
enable
configure terminal
ip nat pool RANGOPUBLICO 200.0.1.3 200.0.1.6
  netmask 255.255.255.248
access-list 1 permit 172.17.0.0 0.0.255.255
ip nat inside source list 1 pool RANGOPUBLICO
interface Fa 0/0
ip nat inside
exit
interface Serial 3/0
ip nat outside
exit
```

De esta forma se hace posible observar la conexión establecida entre dicho routers así:

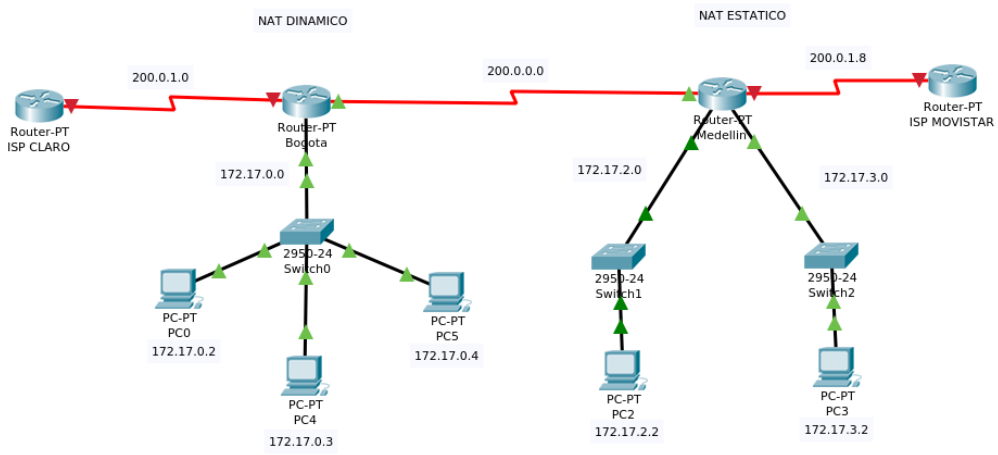

Figura 19: Conexión entre routers Bogotá y Medellín

Posteriormente se activan las interfaz de os routers ISP:

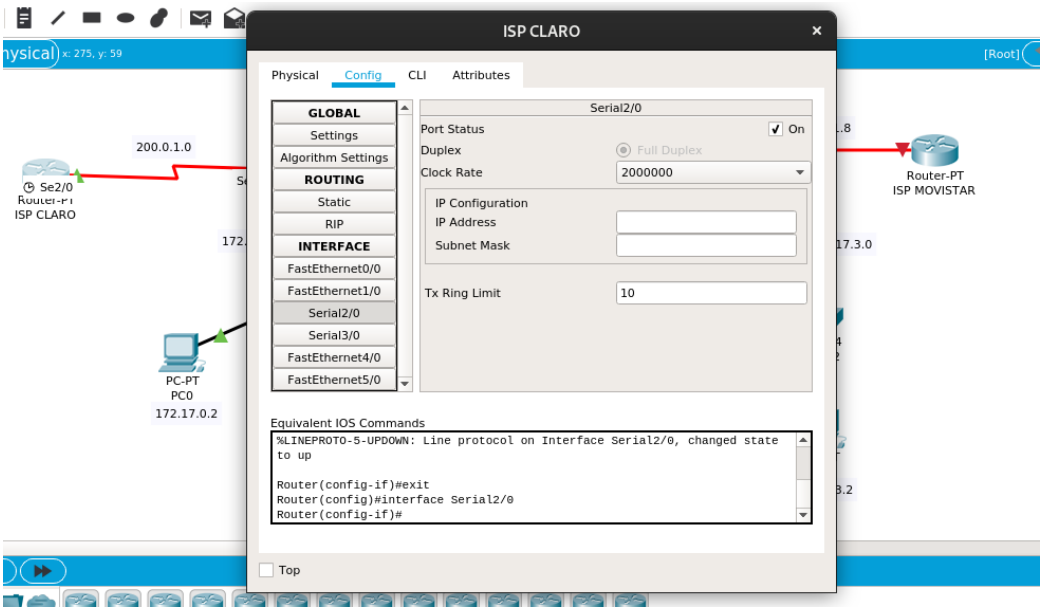

Figura 20: Activación de puertos seriales de ISP

Finalmente se tiene a la topología como:

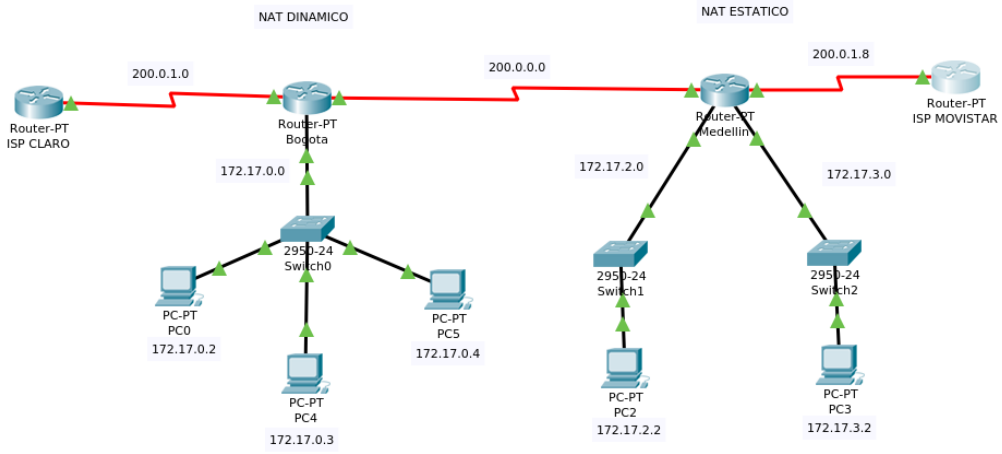

Figura 21: Topología configurada

Preguntas

- Cuáles son las diferencias, ventajas y desventajas entre NAT dinámico y estático? **Rta/:** La diferencia entre las NAT estáticas y dinámicas respectivamente consiste esencialmente en la cantidad de direcciones publicas que cada una de estas usaría para la comunicación de lo dispositivos internos a la red con la red publica a la cual esta se encuentre conectada, teniendo que en la definición de un *NAT Dinámica* como aquella que se sirve de asignar dinámicamente a un conjunto de direcciones publicas, una o un conjunto de redes determinadas, cuando estas se encuentre involucradas en un proceso de transmisión de datos dentro de la red; que relaciona una red privada a una publica, que es única para su inmersión dentro de una interconexión dentro de la red, haciendo así mas rígida la conexión ya que para el acceso de un numero determinado de equipos se hace necesario contar con el mismo numero de ip publicas, que en contraste los *NAT Estático* , causa un gasto adicional y notable, ya que este ultimo permite el no desperdicio de redes publicas teniendo en cuenta que este e si puede conectar un numero mas reducidos de conexiones con la red publica, no obstante es de recalar como limitante de la misma que cada elemento de la red que al emplear una conexión donde un conjunto de equipos se conectan con una red publica determinada se puede dar el agotamiento u ocupación de la red bloqueando así el acceso de toda una red privada a la red publica.

- Es posible enviar solicitudes desde el PC0 al router ISP Movistar? ¿Por qué?
  Rta/: Efectivamente se puede realizar el envió de peticiones desde el el PC0 al router ISP Movistar, teniendo en cuenta que la red sobre la cual se soporta dicho PC es dinámica, teniendo que el mismo tiene una red publica asignada, este usando RIP como protocolo dinámico de transmisión delega la responsabilidad de transmisión al router de Medellín produciendo lo que se denomina salto.

- Es posible enviar solicitudes desde el PC3 al router ISP Claro? ¿Por qué?
  Rta/: De igual forma al anterior se tiene al PC3 configurado en NAT Estático lo cual le asignaría una red para conectarse a la red publica, hecho que con un salto a través del router Bogota, permitiría la

transmisión de datos hasta el router del ISP Claro, siempre que la red publica del NAT Estatico no se encuentre ocupada.

- Es posible enviar solicitudes desde el PC2 al router ISP Movistar? ¿Por qué?
  Rta/: Efectivamente, teniendo en cuenta que no se producen saltos adicionales del router al que se encuentra conectado, teniendo que este se encuentra directamente relacionado al router del ISP Movistar, siendo adyacente al mismo, que con el protocolo RIP permiten el envió rápido de la información.

- Describa la tabla NAT y sus componentes.
  Rta/: Hay cierta terminología que se aplica dentro de NAT. Y es acerca sobre la terminología dada por la tabla NAT con cada uno de sus componentes descritos de esa manera, ante ello, se eligen los datos necesarios que se comportan en este.

  - **Inside Local:** Se conoce como Inside Local a la dirección IP interna privada de algún PC de la red LAN.
  - **Inside Global:** Es la dirección IP pública que está siendo utilizada para traducir las IP privadas. La IP WAN del Router en la interfaz f0/1 es considerada Inside Global, así mismo como todas las IP de los rangos públicos.
  - **Outside Local:** Corresponde a la dirección IP de un host ubicado en la red externa (Internet) tal como se muestra en la red LAN interna. No necesariamente tiene que ser una IP pública legítima.
  - **Outside Global:** Es la dirección IP pública de un host de destino en la red externa.

- Describa la funcionalidad de cada comando en el proceso de configuración de los tipos de NAT(estático -dinámico).
  Rta/:

  - **NAT Estático**

    ```
    enable
    ```

    Ingresa al modo EXEC Privilegiado

    ```
    configure terminal
    ```

Configura la terminal manualmente desde la terminal de consola

```
ip nat inside source static 172.17.2.2 200.0.1.11
```

Mapeo en la línea.

```
interface Fa0/0
```

Configura un tipo de interfaz y entra al modo de configuración de interfaz

```
ip nat inside
```

Define al router como parte interna.

```
interface Serial 3/0
```

Configura un tipo de interfaz y entra al modo de configuración de interfaz.

```
ip nat outside
```

Lo hace propio en la interfaz que apunta hacia Internet.

- **NAT Dinámico**

```
ip nat pool RANGOPUBLICO 200.0.1.3 200.0.1.6
  netmask 255.255.255.248
```

Permite crear el rango de direcciones IP públicas que vamos a asignar al NAT dinámico y asociarlo a un nombre.

```
access-list 1 permit 172.17.0.0 0.0.255.255
```

Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que llegan desde un Origen. Este último parámetro puede ser una di- rección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any.

```
ip nat inside source list 1 pool RANGOPUBLICO
```

Define al router como parte interna.

```
interface Fa0/0
```

Configura un tipo de interfaz y entra al modo de configuración de interfaz

```
ip nat inside
```

Define al router como parte interna.

```
interface Serial 3/0
```

Configura un tipo de interfaz y entra al modo de configuración de interfaz.

```
ip nat outside
```

Lo hace propio en la interfaz que apunta hacia Internet.

- Liste que otros comandos son útiles en el manejo de NAT.
  Rta/:

```
show ip nat translation
```

Comando para verificar las traducciones de NAT en el router.

```
debug ip nat
```

Comando para verificar el funcionamiento de la función NAT mostrando información sobre cada paquete traducido por el enrutador.

```
clear ip nat translations
```

Limpia la tabla de traducciones

```
no ip nat inside
no ip nat outside
```

Aplicados posteriormente a la elección de una interface sirve para desactivar las interfaces inside y outside

- ¿En qué se diferencia NAT de PAT?
  Rta/: Dentro de las diferencias que tienen NAT y PAT esta que, NAT se usa para utilizar direcciones privadas y proveer aun así conectividad con el resto de Internet. NAT cambia la dirección de origen en cada paquete salida; En cambio PAT, hace la traducción de las direcciones de puertos, el objetivo de PAT es la conservación de direcciones IP, también, PAT permite que una sola dirección IP sea utilizada por varias maquinas en internet.

Conclusiones

- El uso de NAT, es fundamental en la definición de profesos como la seguridad, así como la optimización de direcciones de red, dentro de una red publica.
- El NAT Publico consiste en la asignación de IP publicas a un conjunto determinado de IP Privados, teniendo así la conexión dinámica de los equipos internos a la red publia.
- El NAT Estático define la conexión de un conjunto de equipos de una red privada a una red publica a través de la asignación especifica de IP publicas a los elementos de la red donde se encuentren, teniendo que de otro modo los equipos de la red se conectan a través de una única red publica a la red principal.
- PAT hace la traducción de las direcciones de puertos, el objetivo de PAT es la conservación de direcciones IP, también, PAT permite que una sola dirección IP sea utilizada por varia maquinas en internet.

Bibliografía

[1] Anónimo (2011) *NAT (Network Address Translation): Qué es y cómo funciona* https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

[2] Anónimo (2018) *What is Network Address Translation (NAT)?* https://www.iplocation.net/nat

[3] Anónimo *Traducción de direcciones de red (NAT)* https://www.speedcheck.org/es/wiki/nat/

[4] CISCO *Configurar NAT para habilitar la comunicación entre redes superpuestas* https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

[5] Colomés,P (2018) *Implementando NAT en routers Cisco* http://www.redescisco.net/sitio/2010/08/18/implementando-nat-en-routers-cisco/