

TALLER INVESTIGATIVO DE NAT Y PAT

Miguel Angel Ocampo Chavarro
 Edgar Andres Gomez Leon
*Universidad de Investigacion y Desarrollo
 Barrancabermeja, Colombia*

Resumen – Este es un artículo investigativo de NAT y PAT un concepto de redes de computadoras que desarrollan los routers para intercambiar paquetes entre dos redes para el nat y una característica del estándar NAT que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerta de la red interna para el PAT.

I. INTRODUCCION

Las redes NAT y PAT son conceptos de redes de computadores que se usan cuando se quieren comunicar dos redes que son incompatibles y que necesitan compartir o buscar información entre sí. Un ejemplo es cuando existen dos empresas, una desea obtener información de la otra porque es el proveedor. De este modo para comunicarse las dos redes se utiliza NAT. NAT permite comunicar una red con el mundo exterior y permita que la red remota pueda entenderla.

II. ¿QUÉ ES NAT?

La NAT (*Network Address Translation*) es un mecanismo que permite que se conecten a internet las redes IP privadas que emplean ip no registradas. Convierte las direcciones IP en direcciones legales antes de que la información sea enviada a otra red. La red NAT permite que una dirección sea empleada por el mundo exterior para toda la red esto puede proveer seguridad para la red porque se esta ocultando una red privada.

III. ¿CUÁLES SON LOS TIPOS DE FUNCIONAMIENTO DE NAT?

A. NAT ESTATICA

La NAT estática traduce la IP privada a una red a una IP pública. Este modo de funcionamiento permite a un host dentro de la red ser visible en internet.

B. NAT DINAMICA

La NAT dinámica asigna un grupo de IPs públicas en un router para que sea asignada una ip publica diferente para todos los elementos de una red privada. Esto puede aumentar la seguridad de la red debido se tiene mas dificultad de acceder a un host porque las direcciones van cambiando.

C. NAT CON SOBRECARGA(PAT)

NAT con sobrecarga o Port Address Translation asigna las direcciones de los host de una red privada a una ip publica, el router guarda la ip privada origen y el puerto destino y lo convierte a una ip publica origen y un puerto destino aleatoria, cuando la información es enviada al router comprueba la tabla y lo envía a la ip privada y al puerto que le corresponda.

D. NAT SOLAPAMIENTO

El nat solapamiento es una forma de remplazar una IP publica que está siendo utilizada en una red por una dirección publica única. Asi se evitan conflictos entre diferentes redes.

IV.PROCESO DE CONFIGURACION ESTATICA Y DINAMICA DE NAT

A. NAT ESTATICA

La NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. Permite que los dispositivos externos inicien conexiones a los dispositivos internos mediante la dirección pública asignada de forma estática. Por ejemplo, se puede asignar una dirección global interna específica a un servidor web interno de modo que se pueda acceder a este desde redes externas.

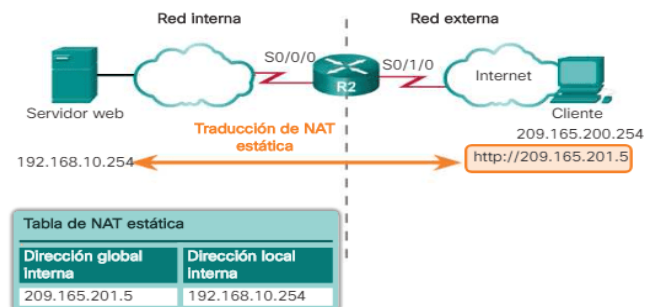


Figura 1. Topología NAT estática

Existen dos pasos básicos para configurar las traducciones NAT estáticas.

PASO 1

Consiste en crear una asignación entre la dirección local interna y las direcciones globales internas. Por ejemplo, la dirección local interna 192.168.10.254 y la dirección global interna 209.165.201.5 se configuraron como traducción NAT estática.

PASO 2

Una vez configurada la asignación, las interfaces que participan en la traducción se configuran como interna o externa con respecto a NAT. En el ejemplo, la interfaz Serial 0/0/0 del R2 es una interfaz interna, y la interfaz Serial 0/1/0 es una interfaz externa.

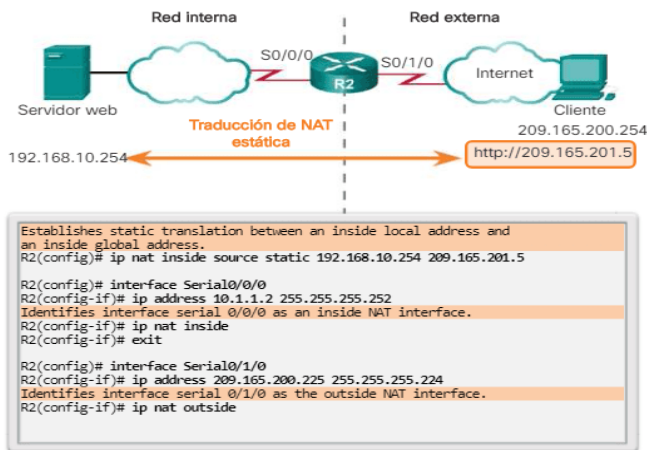


Figura2. Configuración de NAT estática de ejemplo

B. NAT DINAMICA

La topología de ejemplo que se muestra en la ilustración tiene una red interna que usa direcciones del espacio de direcciones privadas definido en RFC 1918. Hay dos LAN conectadas al router R1: 192.168.10.0/24 y 192.168.11.0/24. El router R2, es decir, el router de frontera, se configuró para NAT dinámica con un conjunto de direcciones IPv4 públicas de 209.165.200.226 a 209.165.200.240.

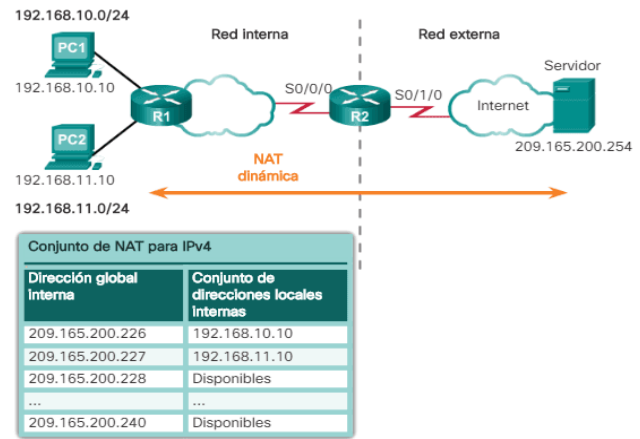


Figura3. Topología NAT dinámica

```

R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
  
```

Figura 4. Configuración de una NAT estática de ejemplo

V.PROCESO DE VERIFICACION DE NAT

A. NAT ESTATICA

El comando **show ip nat translations** es útil para verificar el funcionamiento de NAT. Este comando muestra las traducciones NAT activas. A diferencia de las traducciones dinámicas, las traducciones estáticas siempre figuran en la tabla de NAT.

La traducción estática siempre está presente en la tabla de NAT.

```

R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.201.5 192.168.10.254 --- ---
R2#
  
```

La traducción estática durante una sesión activa.

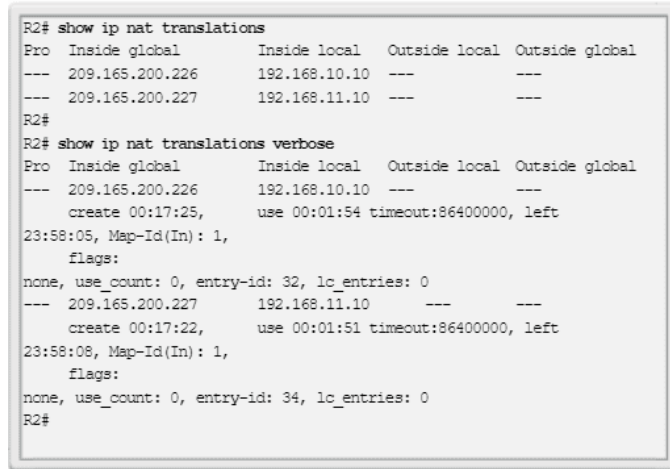
```

R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254 209.165.200.254
R2#
  
```

Figura 5. Verificación de NAT estática

B. NAT DINAMICA

El resultado del comando `show ip nat translations` muestra los detalles de las dos asignaciones de NAT anteriores. El comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que se crearon a causa del tráfico.



```

R2# show ip nat translations
Pro Inside global      Inside local  Outside local  Outside global
--- 209.165.200.226     192.168.10.10 ---          ---
--- 209.165.200.227     192.168.11.10 ---          ---
R2#
R2# show ip nat translations verbose
Pro Inside global      Inside local  Outside local  Outside global
--- 209.165.200.226     192.168.10.10 ---          ---
    create 00:17:25,    use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227     192.168.11.10 ---          ---
    create 00:17:22,    use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
  
```

Figura 6. Verificación de nat dinámica

VI. ¿QUE ES FRAME RELAY?

Frame Relay o (Frame-mode Bearer Service) Protocolo de red orientado a la tecnología de conmutación de paquetes ofrecido por las compañías telefónicas. Define el proceso para enviar datos sobre la red pública, constituye una tecnología de enlace de datos orientado a la conexión de alto rendimiento y eficacia. Es un servicio diseñado especialmente para cubrir las necesidades de uso e interconexión de Redes de Área Local (LAN)

VII. TERMINOLOGIA FRAME RELAY

A. PVC

(*Permanent Virtual Circuit*) es un sistema de comunicación por el cual los datos de un usuario origen pueden ser transmitidos a otro usuario destino a través de más de un circuito de comunicaciones real durante un cierto periodo de tiempo, pero en el que la conmutación es transparente para el usuario. Un ejemplo de protocolo de circuito virtual es el ampliamente utilizado TCP (Protocolo de Control de Transmisión).

B. SVC

Los **circuitos virtuales conmutados (SVC)** por lo general se crean *ex profeso* y de forma dinámica para cada llamada o conexión, y se desconectan cuando la sesión o llamada es terminada. Como ejemplo de circuito virtual conmutado se tienen los enlaces ISDN. Se utilizan principalmente en situaciones donde las transmisiones son esporádicas. En terminología ATM esto se conoce como conexión virtual

conmutada. Se crea un circuito virtual cuando se necesita y existe sólo durante la duración del intercambio específico

C. DLCI

Data Link Connection Identifier (DLCI) es el identificador de canal del circuito establecido en Frame Relay. Este identificador se aloja en la trama e indica el camino a seguir por los datos, es decir, el circuito virtual establecido.

El DLCI puede valer normalmente entre 0 y 1023 (10 bits), los valores del 0 al 15 y del 1008 al 1023 están reservados para funciones especiales.

El DLCI tiene significado local, es decir, en el circuito virtual, cada extremo puede tener un identificador de circuito diferente para identificar el mismo circuito.

D. CIR

Al contratar un servicio Frame Relay, contratamos un ancho de banda determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (*Committed Information Rate*). Esta velocidad, surge de la división de Bc (*Committed Burst*), entre Tc (el intervalo de tiempo). No obstante, una de las características de Frame Relay es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, adaptándose muy bien al tráfico en ráfagas

E. ARP INVERSO

En red de computadoras, el **protocolo de resolución de direcciones (ARP)**, del inglés *Address Resolution Protocol* es un protocolo de comunicaciones de la capa de enlace de datos,¹ responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

F. LMI

la LMI (Local Management Interface) es un mecanismo activo que proporciona información de estado sobre las conexiones Frame Relay entre el router (DTE) y el switch Frame Relay (DCE). Cada 10 segundos aproximadamente, el dispositivo final sondea la red en busca de una respuesta de secuencia no inteligente o información de estado de canal. Si la red no responde con la información solicitada, el dispositivo del usuario puede considerar que la conexión está inactiva. Cuando la red responde con una respuesta FULL STATUS, incluye información de estado sobre los DLCI que están asignados a esa línea. El dispositivo final puede usar esta información para determinar si las conexiones lógicas pueden transmitir datos.

G. FECN

FECN es usado con protocolos de sistema final que controlan el flujo de datos entre emisor y receptor, como el mecanismo "windowing" de TCP/IP; en teoría, el receptor puede ajustar su tamaño de "ventana" en respuesta a las tramas que llegan con el bit FECN activado.

H. BECN

La BECN se controlan mediante un único bit incluido en el encabezado de la trama. Le informan al router que hay congestión y que debe detener la transmisión hasta que la condición se revierta. Cuando el DCE establece el bit BECN en 1, notifica a los dispositivos en el sentido del origen (ascendente) que hay congestión en la red.