NAT

Antes de Imprimir este documento
considere si es necesario
Ayudemos al Ambiente !!!!

Universidad San Carlos de Guatemala

DANILO ESCOBAR

NAT

Network Address Translation (NAT)

A principios de los años 90 el crecimiento explosivo del internet empezó a causar preocupación entre los expertos debido al rápido crecimiento de las tablas de enrutamiento y el agotamiento de direcciones disponibles. A la espera de soluciones que pudieran funcionar a largo plazo se crearon una serie de pequeños arreglos destinados originalmente a ser soluciones temporales de estos problemas sin contar con su enorme y rápida adopción lo que ha ocasionado que estos sigan vigentes, por lo menos hasta el momento en que se presenta este trabajo.

Uno de estos ajustes fue la reserva de ciertas direcciones para que pudieran ser reutilizables dentro de cada organización, ralentizando de esta manera el agotamiento de direcciones disponibles y que hoy en día reciben el nombre de direcciones privadas.

Al dejar de ser únicas, las direcciones reservadas para su uso privado dejaron de ser enrutables a través de *internet* por lo que se hizo necesario la creación de un mecanismo que permitiera cambiar o traducir estas direcciones a otras que pudieran comunicarse utilizando la red pública.

Para realizar dicha función se creó la traducción de direcciones de red comúnmente referida como *network address translation* (NAT).

Al estar en contraposición con la visión original del internet en donde se favorecía la conexión de extremo a extremo y al ser considerado solamente como un paliativo temporal, NAT jamás fue estandarizado, lo que ocasionó que cada fabricante realizará su propia implementación y que muchos protocolos presenten problemas al ser utilizados en combinación con esta tecnología.

No obstante los inconvenientes, NAT presenta también grandes ventajas al permitir que muchos dispositivos se conecten a la red utilizando unas pocas direcciones públicas, reduciendo costos y facilitando la migración de un proveedor de servicios hacia otro.

NAT

Tipos de NAT

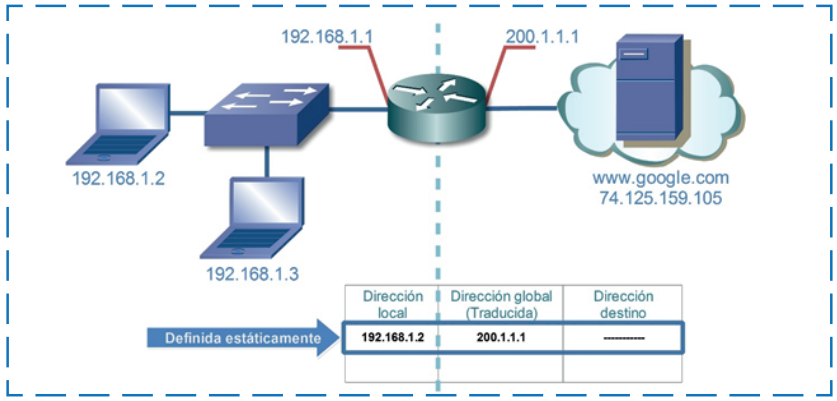
Cisco define tres tipos de traducción: Estática, dinámica y sobrecargada. En dichas traducciones se distingue entre las direcciones locales y globales, siendo las primeras aquellas utilizadas dentro de las organizaciones y las últimas empleadas fuera de las mismas.

NAT Estático

Es una traducción configurada manualmente y la única que permite el inicio de una conexión desde una red externa.

Puede realizarse de una manera sencilla traduciendo una dirección a otra o de una forma más granular, utilizando también distintos protocolos y números de puerto.

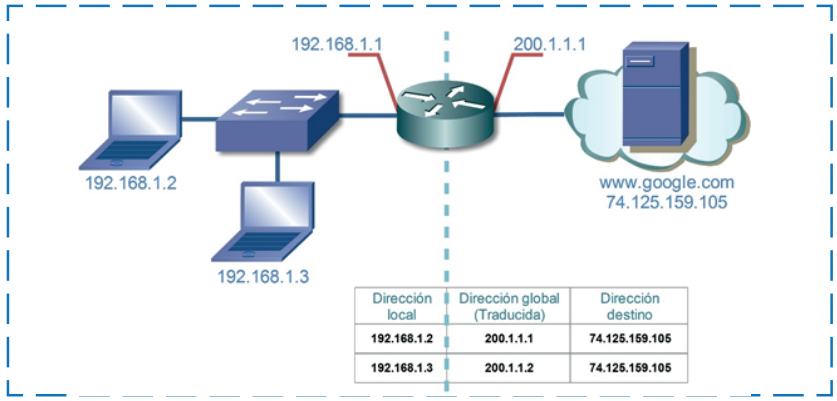
Es utilizada regularmente cuando se necesita que un servicio presente en la red interna sea accesible desde la red pública.



NAT estático

NAT Dinámico

Es una traducción realizada de manera automática. Con carácter temporal, esta puede realizarse de una dirección a otra; perteneciente a una interfaz o a una piscina de direcciones públicas, siendo este tipo de traducción el que más consume de estas últimas ya que se necesita de una dirección enrutable en *internet* por cada dispositivo que requiera comunicarse a través de la misma.

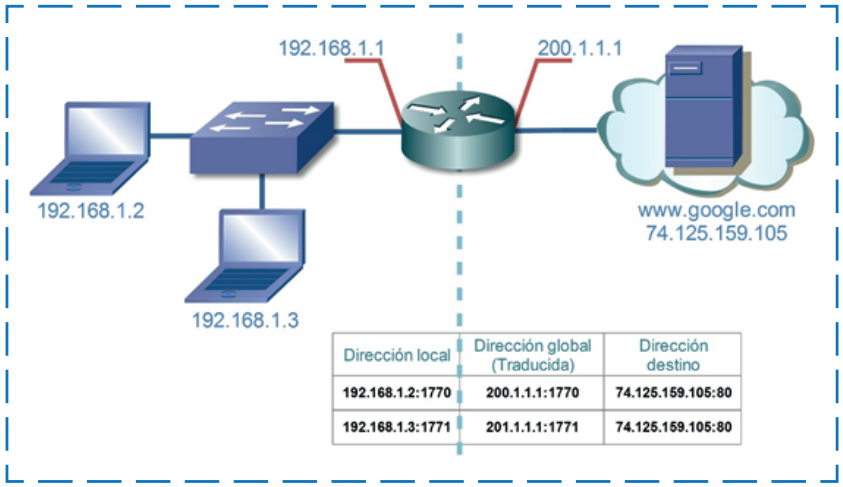


NAT dinámico.

NAT

NAT Sobrecargado

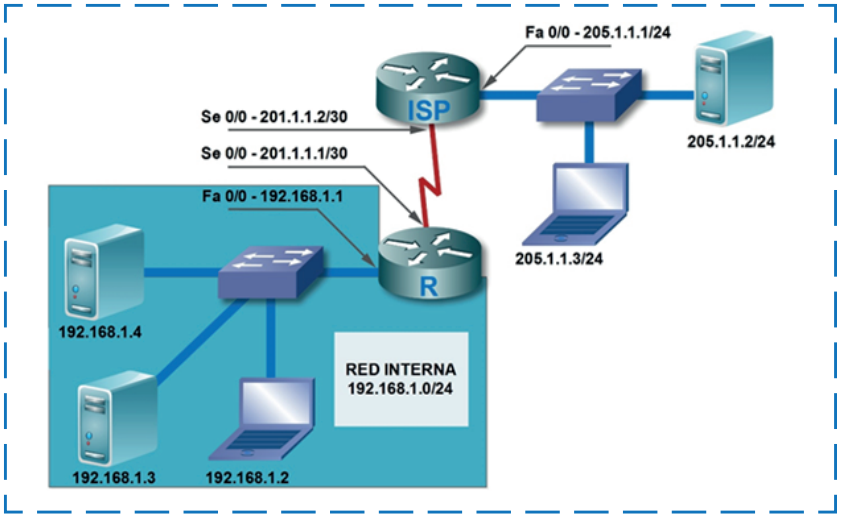
También conocido como *port address translation* (PAT), es una traducción que se realiza de manera automática utilizando la dirección presente en una interfaz o en una piscina de direcciones, pero que se distingue de NAT dinámico debido a que es capaz de utilizar números de puerto durante la traducción por lo que varios dispositivos privados pueden compartir una sola dirección pública característica por la cual es el tipo de traducción más común.



NAT sobrecargado o PAT

Configuración tradicional

Para mostrar la implementación de NAT se presenta la siguiente topología, en donde todas las interfaces han sido previamente configuradas como se muestran y existe una lista de control de acceso en el *router* del proveedor de servicios de *internet* (ISP) encargada de descartar las transmisiones provenientes de redes que utilizan direccionamiento privado.



Topología para mostrar la implementación de NAT.

NAT

En este ejercicio se trabajará exclusivamente con el *router* R, perteneciente a la empresa en cuestión y donde deben cumplirse los siguientes objetivos:

1. Posibilitar la conectividad entre la red interna y el *internet.*
2. Hacer accesibles desde el *internet* aquellos servidores presentes en la red interna, esto se logra utilizando:
    a. Direcciones públicas distintas para cada servidor.
    b. La misma dirección pública para ambos servidores.

Para cumplir el primer objetivo debe configurarse NAT sobrecargado dentro del *router* R, para que los dispositivos de la red interna con direcciones privadas puedan compartir una sola dirección pública, siendo en este caso la dirección perteneciente a la interfaz Serial 0/0 (201.1.1.1)

De manera general los pasos a seguir para posibilitar la traducción de direcciones consisten en identificar el tráfico que será traducido mediante una ACL, identificar el rol de las interfaces ubicadas adentro (*inside*) o afuera (*outside*) de la red y habilitar NAT desde el modo de configuración global.

Para identificar el tráfico de la red interna a ser traducido se crea la lista de control estándar llamada “traducir” como se muestra a continuación.

```
R(config)# ip access-list standard traducir
R(config-std-nacl)# remark [> Esta lista identifica el tráfico a
traducir <]
R(config-std-nacl)# permit 192.168.0.0 0.0.255.255
R(config-std-nacl)# deny any
```

Acto seguido debe identificarse las interfaces correspondientes a la parte interna y externa de la red. En esta oportunidad la interfaz *FastEthernet* 0/0 pertenece adentro mientras que la interfaz Serial 0/0 pertenece afuera de la misma.

```
R(config)# interface fastEthernet 0/0
R(config-if)#ip nat inside

R(config)#interface serial 0/0
R(config-if)#ip nat outside
```

Finalmente, es posible habilitar NAT con la siguiente instrucción.

```
R(config)# ip nat inside source list traducir interface serial 0/0 overload
```

Dicha instrucción indica al *router* que habilite la traducción de las direcciones pertenecientes al interior de la red, utilizando aquellas definidas en la lista con el nombre “traducir”, y que estas sean alteradas para utilizar en su lugar la dirección asignada a la interfaz Serial 0/0 (201.1.1.1).

NAT

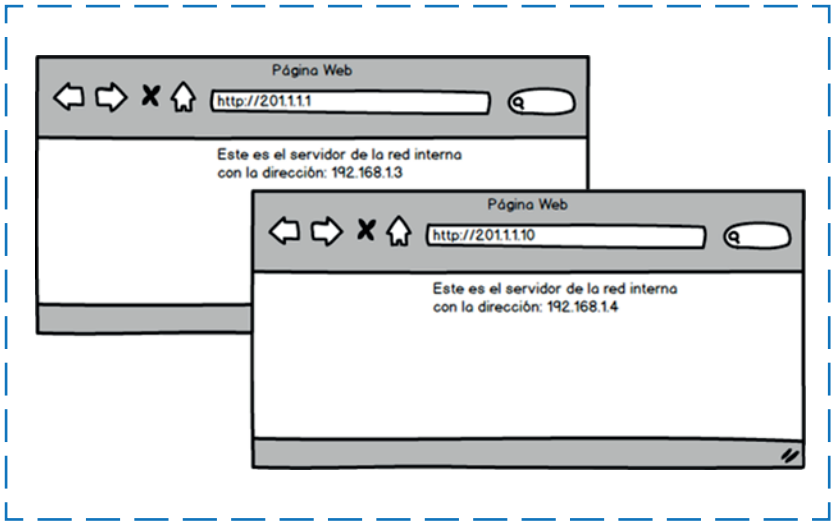
La palabra clave *overload* (sobrecarga) habilita NAT sobrecargado, resultando la omisión de la misma en la activación de NAT dinámico.

Una vez lograda la conectividad con el *internet* se procede a hacer los servidores internos accesibles desde la red pública, donde se parte del hecho que los roles (*inside/outside*) necesarios en NAT han sido configurados en el paso anterior por lo que se procede a realizar una traducción estática.

Para cumplir con el primer inciso del segundo objetivo, se emplea una dirección IP pública distinta para cada uno de ellos.

```
R(config)# ip nat inside source static ?
  A.B.C.D   Inside local IP address
  esp
    IPSec-ESP (Tunnel mode) support
  network  Subnet translation
  tcp
    Transmission Control Protocol
  udp       User Datagram Protocol

R(config)# ip nat inside source static 192.168.1.3 ?
  A.B.C.D   Inside global IP address
  interface  Specify interface for global address

R(config)# ip nat inside source static 192.168.1.3 201.1.1.1
R(config)# ip nat inside source static 192.168.1.4 201.1.1.10
```

En esta ocasión se le indica a NAT que implemente una entrada estática (la cual siempre estará activa) para traducir entre una dirección local y una global, lo que significa que los servidores con las direcciones privadas 192.168.1.3 y 192.168.1.4 serán accesibles desde el mundo exterior a través de las direcciones publicas 201.1.1.1 y 201.1.1.10 respectivamente.



Servidores internos vistos desde la red pública.

NAT

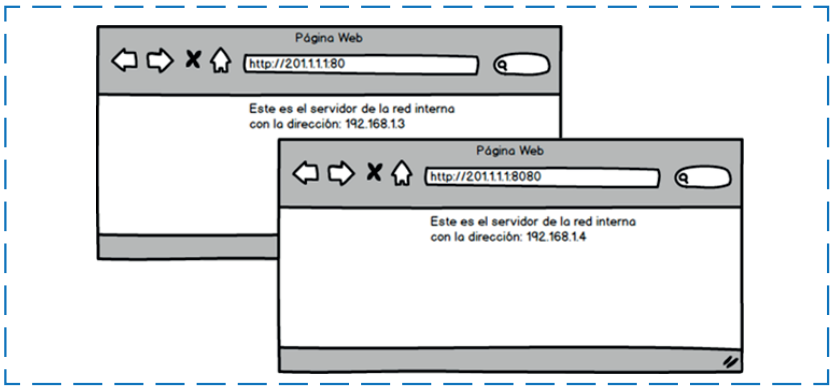
Si bien es necesario que el proveedor de servicios envié todo el tráfico destinado a la dirección 201.1.1.10 al *router* de la empresa, adviértase que esta dirección no ha sido asignada en ningún momento a interfaz alguna de dicho dispositivo. Esto es debido a que la traducción de direcciones es realizada antes que el router consulte su tabla de enrutamiento, en otras palabras, NAT tiene precedencia.

No obstante la solución anterior es aceptable en algunos casos, se vuelve problemática en el momento en que se desea volver accesibles desde la red pública más de unos cuantos servicios, por ese motivo y para finalizar este ejercicio, se eliminarán las entradas estáticas creadas anteriormente y se procederá a realizar una traducción más granular para que ambos servidores utilicen la misma dirección pública, pero un número de puerto diferente.

```
R(config)# no ip nat inside source static 192.168.1.3 201.1.1.1
R(config)# no ip nat inside source static 192.168.1.4 201.1.1.10

R(config)# ip nat inside source static ?
  A.B.C.D  Inside local IP address
  esp
    IPSec-ESP (Tunnel mode) support
  network  Subnet translation
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol

R(config)#ip nat inside source static tcp 192.168.1.3 ?
  <1-65535>  Local UDP/TCP port
```

```
R(config)#ip nat inside source static tcp 192.168.1.3 ?
  <1-65535>  Local UDP/TCP port

R(config)#ip nat inside source static tcp 192.168.1.3 80 201.1.1.1 ?
  <1-65535>  Global UDP/TCP port

R(config)# ip nat inside source static tcp 192.168.1.3 80 201.1.1.1 80
R(config)# ip nat inside source static tcp 192.168.1.4 80 201.1.1.1
8080
```

En este caso se está realizando una traducción de los *sockets* compuestos por las direcciones privadas y el puerto 80 (Puerto por defecto de HTTP) y la dirección pública. Nótese que junto a esta última debe utilizarse dos números de puerto diferentes (el 80 y el 8080) para poder realizar las dos traducciones requeridas.



Servidores internos vistos desde la red pública.

NAT

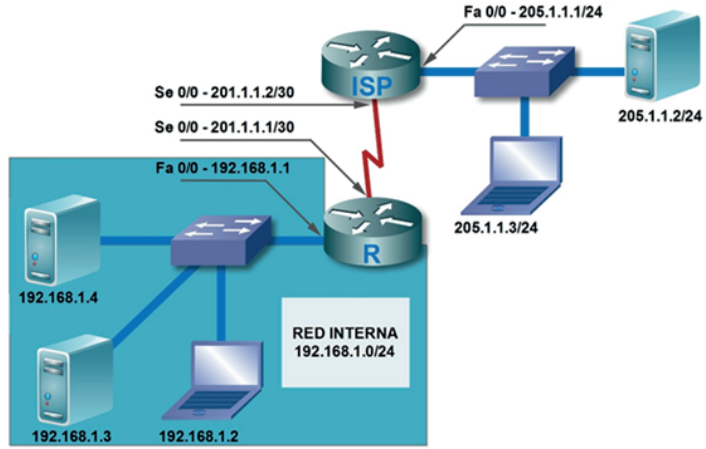
Para mostrar las traducciones (estáticas y dinámicas) puede utilizarse la instrucción *show ip nat translations*, como se muestra a continuación.

R# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	201.1.1.1:80	192.168.1.3:80	-----	-----
tcp	201.1.1.1:8080	192.168.1.4:80	-----	-----
icmp	201.1.1.1:2644	192.168.1.4:2644	205.1.1.2:2644	205.1.1.2:2644
icmp	201.1.1.1:2900	192.168.1.4:2900	205.1.1.2:2900	205.1.1.2:2900
icmp	201.1.1.1:3156	192.168.1.4:3156	205.1.1.2:3156	205.1.1.2:3156
icmp	201.1.1.1:3412	192.168.1.4:3412	205.1.1.2:3412	205.1.1.2:3412

NAT

Resumen de la configuración



Router ISP

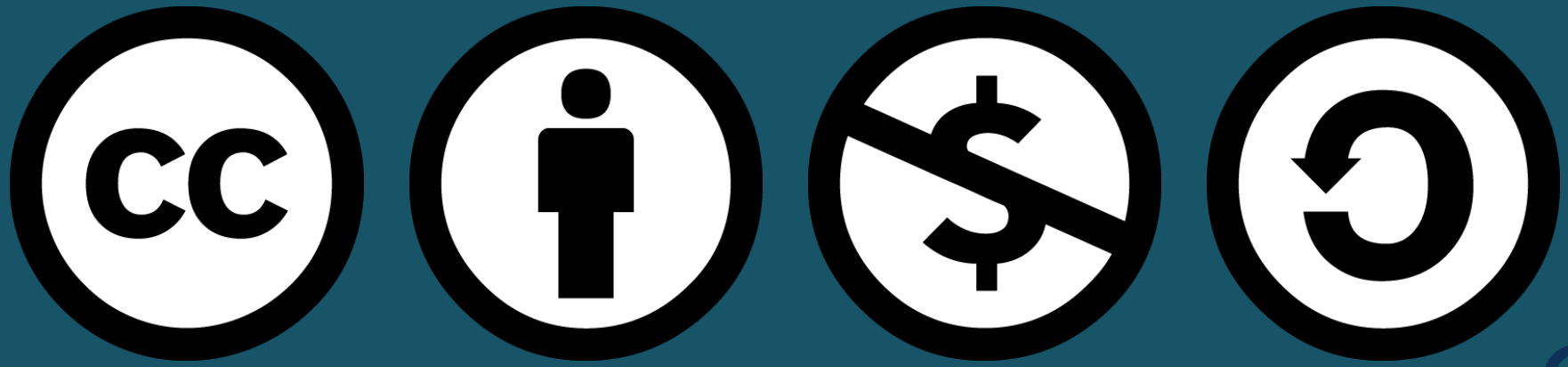
```
ISP(config)# interface fastEthernet 0/0
ISP(config-if)# ip address 205.1.1.1 255.255.255.0
ISP(config-if)# no shutdown

ISP(config)# interface serial 0/0
ISP(config-if)# ip address 201.1.1.2 255.255.255.252
ISP(config-if)# ip access-group DenegarPrivadas in
ISP(config-if)# no shutdown

ISP(config)# ip access-list standard DenegarPrivadas
ISP(config)# deny 192.168.0.0 0.0.255.255
ISP(config)# deny 172.16.0.0 0.15.255.255
ISP(config)# deny 10.0.0.0 0.255.255.255
ISP(config)# permit any

ISP(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0
```

Router R

```
R(config)# ip access-list standard traducir
R(config-std-nacl)# remark [> Esta lista identifica el tráfico a traducir <]
R(config-std-nacl)# permit 192.168.0.0 0.0.255.255
R(config-std-nacl)# deny any

R(config)# interface fastEthernet 0/0
R(config-if)# ip address 205.1.1.1 255.255.255.0
R(config-if)#  no shutdown
R(config-if)# ip nat inside

R(config)# interface serial 0/0
R(config-if)# ip address 201.1.1.1 255.255.255.252
R(config-if)#  no shutdown
R(config-if)# ip nat outside

R(config)# ip nat inside source list traducir interface serial 0/0 overload
R(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
R(config)#  !!!!!  Para usar direcciones distintas
R(config)# ip nat inside source static 192.168.1.3 201.1.1.1
R(config)# ip nat inside source static 192.168.1.4 201.1.1.10
```

```
R(config)#  !!!!!  Para usar la misma dirección pero un número de puerto diferente
R(config)# ip nat inside source static tcp 192.168.1.3 80 201.1.1.1 80
R(config)# ip nat inside source static tcp 192.168.1.4 80 201.1.1.1 8080
```



Diseño y edición:

María Esther Pineda
Carolina Villatoro

Descargo de Responsabilidad

El autor y los colaboradores de este trabajo han hecho su mejor esfuerzo en la preparación del mismo para asegurar que su contenido sea lo más exacto posible, sin embargo, no se hacen responsables por el uso de la información en este documento así como de errores u omisiones que pudieran resultar en pérdida de cualquier tipo.

La información está proporcionada "como está" para ser utilizada bajo "su propia cuenta y riesgo".