Router Teldat

Facilidad NAT

Doc. *DM720* Rev. *10.00*
Marzo, 2003

ÍNDICE

Capítulo 1
Introducción

1. Introducción al NAT

Dos de los principales problemas que posee Internet son la escasez de direcciones IP y el creciente tamaño de las tablas de rutas. La facilidad NAT (Network Address Translation) permite a la red IP de una empresa aparentar, de cara al resto de redes IP, que está usando un espacio de direccionamiento distinto al que internamente está usando. Por tanto NAT permite a una empresa que utiliza direcciones privadas (direcciones locales), y que por tanto no son accesibles por tabla de rutas de Internet, conectarse a Internet al convertir dichas direcciones en públicas (direcciones globales) que sí son accesibles desde Internet. NAT además permite a las empresas poner en marcha estrategias de redireccionamiento en las que los cambios en las redes IP locales son mínimos. NAT está descrito en la RFC 1631.

NAT tiene diversas aplicaciones, siendo algunos escenarios posibles los siguientes:

- Se quiere tener conectividad con Internet, pero no todos los equipos poseen direcciones IP globales (permitidas). En este caso se configura un router NAT como enlace entre el dominio privado (red local) y el dominio público (red pública: en este caso Internet). El router NAT traduce las direcciones locales en direcciones globales antes de enviar los paquetes al exterior.
- Una empresa requiere conectividad IP entre oficinas remotas. Dichas oficinas remotas posee redes IP internas que no cumplen con un plan de direccionamiento con lo que las tablas de rutas para lograr conectividad entre ellas es grande o imposible. En este caso sería suficiente con configurar NAT en los routers frontera de cada oficina, realizar así la transformación entre las redes internas de las oficinas a redes globales, que ahora sí cumplen con el plan de direccionamiento.
- Se necesitan cambiar la direcciones internas de muchos equipos. En lugar de realizar dicho cambio que sería muy costoso en tiempo se podría realizar NAT.

Una ventaja muy importante del NAT es que para cambiar la dirección de muchos equipos locales solo requiere realizar cambios en los routers NAT. Las desventajas del NAT aparecen cuando existen muchos equipos que requieren NAT simultáneamente o cuando las aplicaciones de red intercambian referencias a direcciones IP origen o destino: dichas aplicaciones no funcionan si su información viaja a través de un router NAT de forma transparente, en este caso la única solución es que el router NAT analice los paquetes de datos de dicha aplicación, averiguando y cambiando las referencias a direcciones IP locales.

Un router NAT tendrá al menos un interfaz local (interfaz en contacto con la red local) y un interfaz global (interfaz en contacto con la red global). En un entorno típico, la facilidad NAT se configura en el router frontera entre el dominio "stub" y el "backbone". Cuando un paquete abandona el dominio stub, el router NAT cambia la dirección local origen del paquete por una dirección global. Cuando un paquete entra en el dominio, la dirección destino global del paquete se cambia por la dirección destino local.

Un router configurado con NAT no debe anunciar las redes locales a través de los interfaces globales. Sin embargo las rutas globales si pueden ser anunciadas a través de los interfaces locales.

Como se ha dicho con anterioridad, el termino "local" representa a aquellas redes que pertenecen a una empresa y que deben ser traducidas. Dentro del dominio local un determinado equipo poseerá una dirección local, mientras que en el exterior aparentará que posee una dirección de otro espacio de direcciones. Por tanto, el primer espacio de direcciones es el "local" y el segundo espacio de direcciones es el "global".

2. Tipos de NAT

La traducción de direcciones puede ser:

- NAT estático: la correspondencia de direcciones locales y globales es unívoca.
- NAT dinámico: se establece una correspondencia de direcciones locales en un pool de direcciones globales. Por tanto la correspondencia entre direcciones globales y locales no es unívoca y depende de condiciones de ejecución.
- NAPT (Address Port Translation): se establece una correspondencia entre direcciones locales y una única dirección global. En este caso lo que se realiza es una traslación de los puertos de protocolos de transporte (UDP, TCP).

En los siguientes subapartados m y n significan:

m: número de direcciones IP locales.

n: número de direcciones IP globales.

2.1. NAT estático

m : n-Traslación, m, n ≥ 1 y m = n (m, n ∈ N)

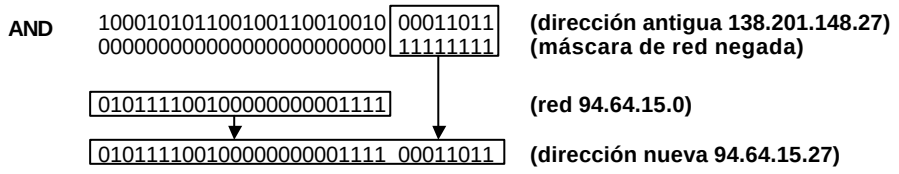
Con NAT estático se realiza traslación de redes locales en redes globales del mismo tamaño (con mismo número de direcciones IP). Un caso particular es cuando las dos redes contienen sólo una dirección IP (máscara de red 255.255.255.255). El proceso NAT puede describirse con la siguiente transformación:

dirección-global = red-global OR (dirección-local AND (NOT máscara-red))

dirección-local = red-local OR (dirección-global AND (NOT máscara-red))

Ejemplo:

- Regla NAT: trasladar todas las direcciones de la red local 138.201.148.0 en la red global 94.64.15.0, siendo la máscara de ambas redes 255.255.255.0.



Este manual se centra en la configuración de NAT estático, existiendo otros manuales Teldat para el resto de variedades de NAT.

2.2. NAT dinámico

m: n-Traslación, m ≥ 1 y m ≥ n (m, n ∈ N)

Este tipo de NAT es necesario cuando el número de direcciones globales disponibles es menor que el de locales, o iguales pero por alguna razón no interesa que el NAT sea estático. El número de equipos locales comunicándose con el exterior simultáneamente queda limitado al número de direcciones globales disponibles. Cuando todas las direcciones globales están siendo usadas, subsiguientes conexiones deben ser rechazadas devolviendo "host unreachable".

Ejemplo:

- Regla NAT: trasladar dinámicamente todas las direcciones de la red local 138.201.0.0 máscara 255.255.0.0 en direcciones de la red global 278.201.112.0 con máscara 255.255.255.0
- Cada nueva conexión desde la red local hacia el exterior obtiene una dirección global del pool de direcciones globales disponible.
- Si la dirección local ya posee una dirección global se vuelve a utilizar dicha correspondencia.

2.3. NAPT/PAT (Enmascaramiento)

m: n-Traslación, $m \geq 1$ y $n = 1$ ($m, n \in N$)

Es un caso particular de NAT dinámico. Es el tipo de NAT más usado actualmente. Aquí muchas direcciones locales son trasladadas a una misma dirección global. Como diferencia con el tipo de NAT anterior, ahora se permiten más de "n" conexiones. Ahora un número arbitrario de conexiones se multiplexan usando información de puertos (TCP, UDP). El número de conexiones simultáneas permitidas estará limitado al número de puertos NAT disponibles.

El problema principal de este tipo de NAT es que muchos servicios sólo aceptan conexiones provenientes de puertos privilegiados para así asegurar que no provienen de cualquier usuario. Para permitir NAPT se requiere mantener manejadores para cada conexión TCP, UDP.

Otra limitación es que, por defecto, las conexiones entrantes no están permitidas.

Ejemplo:

- Regla NAT: enmascarar las direcciones globales de la red 138.201.0.0 tras la dirección global del interfaz externo del router.
- Para cada paquete saliente la dirección origen del paquete se sustituye por la dirección del interfaz externo del router NAT y el puerto origen se cambia por un puerto NAT no utilizado todavía.
- Si el destino de los paquetes entrantes es la dirección del interfaz externo del router NAT y el puerto destino corresponde con un puerto NAT ya asignado se cambia dirección y puerto destino por la dirección local y puerto local correspondiente.

3. Problemas comunes a todas las técnicas NAT

Toda conexión que atraviese un router se identifica por una quintupla: protocolo, dirección y puerto origen, dirección y puerto destino. Si al router se le habilita NAT aparecerán 3 quintuplas para representar la misma conexión, una por cada sección:

- Primera sección o sección local: del origen al router NAT.
- Segunda sección o sección global: del router NAT al destino.
- Tercera sección o sección interna: el router NAT del interfaz interno o local al interfaz externo o global.

Sólo el router NAT posee información de lo que está ocurriendo en cada sección, pero esto también significa que el router NAT debe almacenar mucha información por conexión establecida, cosa que no necesitan hacer los router sin NAT.

Esto es algo que tienen en común con los Firewalls: ambos tipos de dispositivos no sólo realizan encaminamiento de los paquetes sino que deben analizar y controlar el tipo de información que se intercambia a través de ellos y mantener información del estado de cada conexión con lo que ello conlleva: una sobrecarga importante comparado con un router sin NAT.

Sobra decir que si se está habilitando NAT, todo paquete que viaje del dominio local al global debe ir a través del o de los routers NAT.

3.1. Información de estado

Excepto para el caso de NAT estático, los router NAT deben guardar información dinámica sobre las correspondencias actuales entre direcciones locales y globales. Además este tipo de información de estado debe tener un tiempo de vida limitado de tal manera que, si un determinado equipo ha parado de transmitir información, sea borrado de la lista.

3.2. Fragmentación

En las estrategias NAT en las que no sólo se traducen las direcciones sino también los puertos aparece otro problema en la fragmentación. Cuando un paquete IP es fragmentado el router NAT sólo puede utilizar la información de puerto del primer fragmento ya que el resto de fragmentos tienen el puerto a 0xFFFF. Por tanto en este tipo de NAT se hace necesaria guardar información de estado de los fragmentos.

3.3. Comportamiento según el tipo de protocolo

a) Aplicaciones "venenosas"

Denominamos aplicaciones "venenosas" a aquellas aplicaciones que incluyen información de direccionamiento IP y/o puertos TCP/UDP fuera de los campos de cabecera correspondientes. Cada aplicación de este tipo requiere un tratamiento específico. Ejemplos de estas aplicaciones son FTP, ICMP, etc.

b) Protocolos de Routing Dinámico (RIP, EGP, ...)

Un router configurado con NAT no debe anunciar las redes locales a través de los interfaces globales. Sin embargo las rutas globales si pueden ser anunciadas a través de los interfaces locales. Se recomienda utilizar routing estático.

Capítulo 2
Configuración

1. Configuración NAT

En este apartado se describen los pasos requeridos para configurar la facilidad NAT. Después de configurar las opciones deseadas, se debe guardar la configuración y reinicializar el router para que tenga efecto la nueva configuración. Las siguientes secciones describen el proceso de configuración con más detalle.

- Acceso al entorno de configuración NAT.
- Activar o desactivar NAT.
- Configuración de reglas NAT.
- Salir del proceso de configuración NAT.
- Reiniciar el router para que tenga efecto la nueva configuración.

Acceso al entorno de Configuración NAT

Para acceder al entorno de configuración NAT hay que previamente acceder al de IP:

```
*P 4
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config>
```

Desde ahí, se deberá introducir el siguiente comando:

```
IP config>NAT STATIC

-- Static NAT configuration --
SNAT config>
```

Activar o desactivar NAT

La facilidad NAT puede estar habilitado o deshabilitada. Para activar o desactivar la facilidad NAT hay que introducir los siguientes comandos:

```
SNAT config>ENABLE
```

```
SNAT config>DISABLE
```

o

```
SNAT config>NO ENABLE
```

Configurar reglas NAT

La facilidad NAT se basa en una lista ordenada global de reglas. Si la facilidad NAT está habilitada, cada paquete IP originado, traspasado o recibido será inspeccionado por la lista de reglas.

Cada regla está compuesta por los siguientes campos:

1.1. Posición o identificador

Cada regla posee un identificador único que especifica la posición en la lista:las reglas se analizan por orden según su identificador. Los identificadores deben ser número naturales (sin el cero) consecutivos. Al agregar una nueva regla hay que especificar la posición donde quiere insertarse dicha regla.

1.2. Interfaz local

Es el interfaz que está en contacto o a través del cual se llega a la red local (dominio local). Para cada regla hay que introducir un interfaz local asociado. El interfaz puede ser:

- Un interfaz físico: para ello hay que
  - especificar el número de interfaz físico usando la misma notación que al especificar las direcciones no numeradas: (Por ejemplo: ethernet0/0 → 0.0.0.0)
  - especificar el identificador del interfaz, por ejemplo: ethernet0/0, serial0/0, ...
- Un interfaz IP lógico: para ello hay que especificar el interfaz lógico IP introduciendo la dirección IP (numerada) del interfaz del router NAT. (Por ejemplo: ethernet0/0 con dos direcciones configuradas, para especificar el interfaz lógico hay que poner la dirección IP numerada deseada).

1.3. Interfaz global

Es el interfaz que está en contacto o a través del cual se llega a la red global (dominio global). Para cada regla hay que introducir un interfaz global asociado. El interfaz global se especifica del mismo modo utilizado para especificar el interfaz local.

1.4. Red local

Se especifica dando la dirección y máscara de la misma. Es el conjunto de direcciones locales sobre los que se quiere que actúe la regla. Dado que el NAT estático realiza una asociación uno-a-uno entre las direcciones del ámbito local y las del ámbito global, la máscara de ambas redes debe ser iguales: el equipo se encarga de garantizar que ambas máscaras sean iguales.

1.5. Red global

Se especifica dando la dirección y máscara de la misma. Es el conjunto de direcciones globales sobre los que se quiere que actúe la regla.

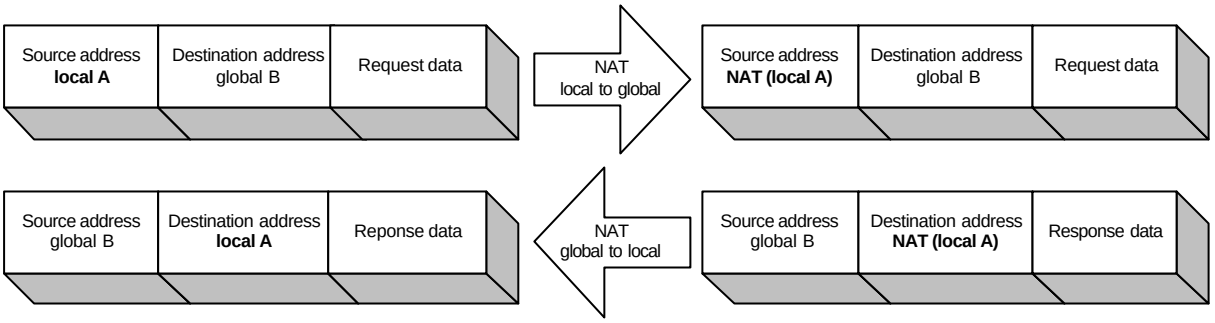
1.6. Tipo de transformación

Hay dos tipos de transformación:

- Origen interno:

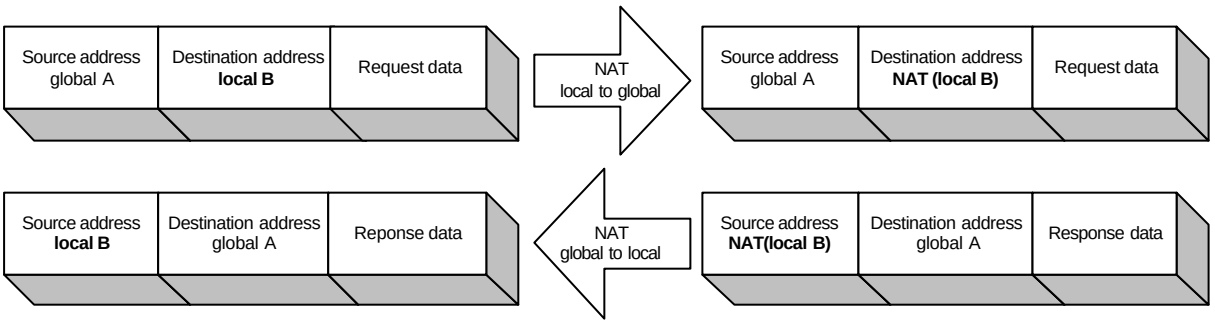
A todo paquete que pase del dominio local al global (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección origen local por la correspondiente global. Y a todo paquete que

pase del dominio global al local (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección destino global por su correspondiente local.



- Destino interno:

A todo paquete que pase del dominio local al global (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección destino local por la correspondiente global. Y a todo paquete que pase del dominio global al local (siempre que cumpla los demás requisitos de la regla) se le cambiará la dirección origen global por su correspondiente local.



1.7. Sentido o dirección de la transformación

Hay cinco sentidos de transformación:

- Local a Global:

Si el paquete entra por el interfaz local y sale por el interfaz global y su dirección (origen o destino) pertenece a la red local entonces cambiar dirección (origen o destino) local por su correspondiente dirección global.

- Global a Local:

Si el paquete entra por el interfaz global y su dirección (origen o destino) pertenece a la red global entonces cambiar dirección (origen o destino) global por su correspondiente dirección local.

- Local a Global y Global a Local: las dos anteriores simultáneamente.
- No cambiar local.

Si el paquete entra por el interfaz local y sale por el interfaz global y su dirección (origen o destino) pertenece a la red local entonces no realizar cambio alguno. Este tipo de regla sirve para definir excepciones y evitar que se apliquen otras reglas más genéricas.

- No cambiar global.

Si el paquete entra por el interfaz global y su dirección (origen o destino) pertenece a la red global entonces no realizar cambio alguno. Este tipo de regla sirve para definir excepciones y evitar que se apliquen otras reglas más genéricas.

NOTA: (origen o destino) lo determina el tipo de transformación.

2. Comandos de configuración NAT

Esta sección resume y explica todos bs comandos de configuración de la facilidad NAT del router. Estos comandos le permitirán configurar el comportamiento de la facilidad NAT del router, y poder de esta forma llegar a las especificaciones de funcionamiento deseadas.

Para acceder al prompt se debe teclear lo siguiente:

```
*P 4
User configuration
Config> PROTOCOL IP

-- Internet protocol user configuration --
IP config> NAT STATIC

-- Static NAT configuration --
SNAT config>
```

A continuación se describe cómo configurar las distintas posibilidades que ofrece el NAT.

Los comandos se definen según la siguiente nomenclatura:

`RULE`	Parte obligatoria
`<`*`rule id`*`>`	Parte obligatoria a determinar por el usuario
`<SOURCE | DESTINATION>`	Parte obligatoria con varias opciones

2.1. Configuración de una regla NAT

Como se ha indicado anteriormente, la configuración de una regla NAT permite realizar una traslación de direcciones entre el dominio STUB (local) y el dominio BACKBONE (global). Dispone de comandos para configurar cada uno de los parámetros que componen una regla NAT.

Para crear una regla NAT debe utilizar la opción `DEFAULT`, que crea una regla con los valores por defecto. Para modificar un parámetro de una regla NAT, basta con utilizar el comando relativo a dicho parámetro indicando el identificador de la regla a modificar.

Para facilitar la configuración/modificación, puede configurar varios parámetros en un mismo comando.

Los valores por defecto de los parámetros de una regla NAT son:

- Tipo de transformación: origen interno (`TRANSLATE SOURCE`)
- Sentido de la transformación: local a global y global a local (`DIRECTION BOTH`)
- Interfaz local: ethernet0/0
- Interfaz global: ethernet0/0
- Subred local: 0.0.0.0 máscara 0.0.0.0
- Subred global: 0.0.0.0 máscara 0.0.0.0

a) Configuración del tipo de transformación

```
RULE <rule id> TRANSLATE <SOURCE | DESTINATION>
```

SOURCE	→ origen interno
DESTINATION	→ destino interno

```
SNAT config>rule 1 translate destination
```

b) Configuración del sentido de transformación

```
RULE <rule id> DIRECTION <LOCAL-TO-GLOBAL | GLOBAL-TO-LOCAL |
                          BOTH | SKIP-LOCAL | SKIP-GLOBAL>
```

```
SNAT config>rule 1 direction skip-local
```

Si configura una regla como SKIP-LOCAL se ignorará el rango de direcciones global configurado para la regla. De igual modo, si configura la regla como SKIP-GLOBAL, se ignorará el rango de direcciones local configurado para la regla.

c) Configuración del rango de direcciones

Al configurar una regla NAT debe indicar las direcciones locales que deben transformarse en direcciones globales.

```
RULE <rule id> LOCAL-NETWORK <IP network address> <IP address  mask>
RULE <rule id> GLOBAL-NETWORK <IP network address> <IP address mask>
```

```
SNAT config>rule 1 local-network 192.6.2.0 255.255.255.0
SNAT config>rule 1 global-network 80.6.2.0 255.255.255.0
```

Si al configurar una de las subredes, la máscara de la otra subred no es igual, se modificará automáticamente la máscara para hacerlas concordar.

d) Configuración del Interfaz local y del Interfaz global

Al configurar una regla NAT debe indicar cuál es el interfaz que proporciona acceso al dominio local y cuál es el interfaz que proporciona acceso al dominio globla.

```
RULE <rule id> LOCAL-INTERFACE <IP address | Interface ID>
RULE <rule id> GLOBAL-INTERFACE <IP address | Interface ID>
```

Como se puede observar, el interfaz se puede especificar de dos modos:

- Dirección IP correspondiente al interfaz, ya sea una dirección estándar o una dirección no numerada (es decir, 0.0.0.x, donde x es el número del interfaz)
- Identificador del interfaz, es decir, ethernet0/0, serial0/0, ...

```
SNAT config>rule 1 local-interface 0.0.0.1

SNAT config>rule 1 local-interface serial0/0

SNAT config>rule 1 local-interface 192.168.1.1
```

2.2. Modificación de una regla NAT

Como se ha indicado anteriormente, para modificar un parámetro de una regla NAT, basta con utilizar el comando relativo a dicho parámetro indicando el identificador de la regla a modificar.

Imaginemos que tenemos configuradas las siguientes reglas NAT:

```
SNAT config>LIST ALL
NAT is: enabled
 Id Local_Ifc        Global_Ifc       Local_Net               Global_Net
--- ---------------  ---------------  ------------------      -----------------
1   ethernet0/0      serial0/0        192.6.2.0/24      >-S-! ...
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24

SNAT config>
```

Para modificar el sentido, el interfaz global y la red global de la regla número 1, ejecute el comando:

```
SNAT config>rule 1 direction both global-interface serial0/1
                                  global-network 80.23.3.0 255.255.255.0
```

El resultado es el siguiente:

```
SNAT config>LIST ALL
Static NAT is: enabled
 Id Local_Ifc        Global_Ifc       Local_Net               Global_Net
--- ---------------  ---------------  ------------------      -----------------
1   ethernet0/0      serial0/1        192.6.2.0/24      <-S-> 80.23.3.0/24
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24
SNAT config>
```

2.3. Borrado de una regla NAT

Para borrar una regla NAT, dispone del siguiente comando:

```
NO RULE <rule id>
```

```
SNAT config>no rule 1
   Rule deleted
```

2.4. Listado de las reglas NAT configuradas

Para listar las reglas NAT configuradas dispone del comando:

```
LIST RULES
```

Cada regla lleva asociado un número de registro. Este número es el número de orden o posición de la regla dentro de la lista.

El tipo y sentido de transformación viene especificado de la siguiente manera:

- <-S-> Tipo: Origen interno. Sentido: Local a Global y Global a Local.
- <-D-> Tipo: Destino interno. Sentido: Local a Global y Global a Local.
- >-S-> Tipo: Origen interno. Sentido: Local a Global.
- >-D-> Tipo: Destino interno. Sentido: Local a Global.
- <-S-< Tipo: Origen interno. Sentido :Global a Local.
- <-D-< Tipo: Destino interno. Sentido: Global a Local.
- >-S-! Tipo: Origen interno. Sentido: No cambiar local
- >-D-! Tipo: Destino interno. Sentido: No cambiar local
- !-S-< Tipo: Origen interno. Sentido: No cambiar global
- !-D-< Tipo: Destino interno. Sentido: No cambiar global

```
SNAT config> LIST RULES
Id  Local_Ifc        Global_Ifc       Local_Net               Global_Net
--- ---------------  ---------------  ------------------      ----------------
1   ethernet0/0      serial0/0        192.6.2.0/24      >-S-! ...
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24

SNAT config>
```

2.5. Habilitar / Deshabilitar la funcionalidad NAT

Puede activar o desactivar la funcionalidad NAT de modo global dispone de los siguiente comandos.

```
ENABLE
DISABLE ó NO ENABLE
```

```
SNAT config>ENABLE
```

```
SNAT config>DISABLE
```

2.6. Mostrar el estado de la funcionalidad NAT

Para consultar el estado global de la funcionalidad NAT, dispone del siguiente comando:

```
LIST STATE
```

```
SNAT config>LIST STATE
Static NAT is: enabled
```

2.7. EXIT

Permite volver al nivel superior (IP) de prompt.

```
SNAT config>EXIT
IP config>
```

3. Resumen de comandos

```
DISABLE
[NO] ENABLE

NO RULE <id>
   RULE <id> DEFAULT
             TRANSLATE <SOURCE | DESTINATION>
             DIRECTION <BOTH |LOCAL-TO-GLOBAL |GLOBAL-TO-LOCAL |SKIP-LOCAL |SKIP-GLOBAL>
             LOCAL-INTERFACE <IP address | Interface ID>
             GLOBAL-INTERFACE <IP address | Interface ID>
             LOCAL-NETWORK <IP address> <IP mask>
             GLOBAL-NETWORK <IP address> <IP mask>
```

La regla por defecto tiene la siguiente configuración:

TRANSLATE SOURCE

DIRECTION BOTH

LOCAL-INTERFACE ethernet0/0

GLOBAL-INTEFACE ethernet0/0

LOCAL-NETWORK 0.0.0.0 0.0.0.0

GLOBAL-NETWORK 0.0.0.0 0.0.0.0

Capítulo 3
Monitorización

1. Monitorización NAT

Esta sección resume y explica todos los comandos de monitorización de la facilidad NAT del router. Estos comandos le permitirán monitorizar el comportamiento de la facilidad NAT del router, y poder de esta forma llegar a las especificaciones de funcionamiento deseadas. Adicionalmente dispone de eventos de monitorización de NAT dentro de los eventos del subsitema IP (IP.026, IP.027, IP.028, IP.029 e IP.030).

Para acceder al prompt de monitorización se debe teclear lo siguiente:

```
*P 3
Console Operator
+PROTOCOL IP
IP>NAT STATIC
-- Static NAT monitoring --
SNAT monit>
```

Comando	Función
? (AYUDA)	Lista comandos u opciones.
LIST	Lista parámetros del NAT.
EXIT	Sale de la monitorización NAT.

1.1. ? (AYUDA)

Utilizar el comando **?** (AYUDA) para listar los comandos válidos en el nivel donde se está programando el router. También se puede utilizar este comando después de un comando específico para listar sus opciones.

Sintaxis:

```
SNAT monit>?
```

Ejemplo:

```
SNAT monit>?
LIST
EXIT
SNAT monit>
```

1.2. LIST

Utilizar este comando para visualizar distintos parámetros monitorizables de la facilidad NAT.

Sintaxis:

```
SNAT monit>LIST ?
CONNECTIONS
```

a) LIST CONNECTIONS

Muestra una lista de las conexiones no transparentes frente al NAT. En el caso del NAT estático sólo pertenecen a esta categoría las conexiones de control del FTP que tienen el cliente en el dominio local y el servidor en el dominio global y que han transmitido comandos PORT en los que ha habido cambio de longitud de paquetes.

Los campos de la lista de conexiones representan lo siguiente:

- Tipo: el tipo de conexión no transparente que está atravesando el router NAT, en el caso del NAT estático solo son conexiones no transparente la conexión de control del FTP.
- Dir:Puerto Origen y Dir:Puerto Destino: representan dirección origen, puerto origen, dirección detino y puerto destino de la conexión. Todos en formato global (como lo vería el dominio global).
- Edad: tiempo de vida que le queda a la entrada antes de ser borrada.
- Activo: indica si está activa o no la conexión (si el router NAT ha detectado que está activa o no la conexión).

Sintaxis:

```
SNAT monit>LIST CONNECTIONS
```

Ejemplo:

```
SNAT monit>LIST CONNECTIONS
Type       Addr:Port Source       Addr:Port Dest   Age    Active
---------  -----------------      --------------   ----   ------
FTP_CTRL   192.6.1.169:1146       192.6.1.3:21     1440   YES
FTP_CTRL   192.6.1.169:1147       192.6.1.5:21     1440   YES
SNAT monit>
```

1.3. EXIT

Utilizar el comando **EXIT** para volver al nivel de prompt en el que se estaba anteriormente.

Sintaxis:

```
SNAT monit>EXIT
```

Ejemplo:

```
SNAT monit>EXIT
IP>
```

Capítulo 4
Ejemplos

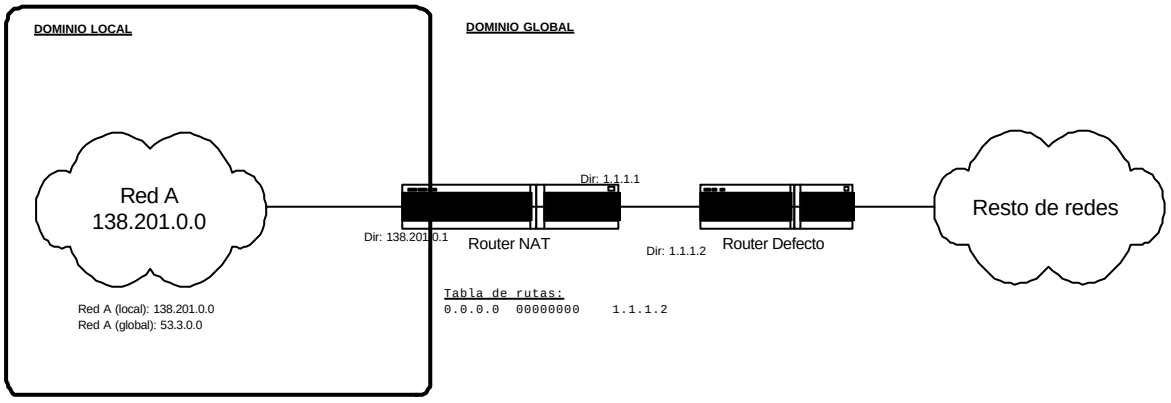
1. NAT estático

Durante los capítulos anteriores se han ido remarcando los posibles campos de aplicación del NAT estático, ahora se va a tratar de dar una serie de ejemplos para aprender a utilizar la implementación actual.

1.1. Cambiar las direcciones orígenes de una red entera

Este es el caso clásico del NAT estático. En este ejemplo se tiene una empresa grande que está usando una red IP de clase A (1.0.0.0). Surge un pequeño departamento en la empresa que por causas diversas necesita direcciones IP y pensando que nunca van a tener que conectarse con el resto de la empresa eligen arbitrariamente una red (138.201.0.0). Pasan los años y llega un momento en que surge la necesidad de conectividad total debido al creciente desarrollo de las nuevas tecnologías de comunicación. La primera solución que aparece es la de cambiar las direcciones de su dominio local por direcciones pertenecientes a la red asignada a la empresa, pero en seguida se dan cuenta que no pueden porque el departamento posee muchos clientes que han contratado servicio de conectividad continuada (las 24 horas al día y los 7 días a la semana) a las direcciones de dicho dominio local, y que por supuesto no aceptan ningún tipo de solución que provoque el incumplimiento de dicho contrato.

La solución para el departamento de esta empresa es configurar NAT estático en el router que realiza la conexión entre el departamento y el resto de la Intranet corporativa de modo que la red de dicho departamento sea accesible para el resto de la Intranet como 1.3.0.0. Veamos como se configuraría el router NAT:



- Configuración de IP

```
*P 4
Config>protocol ip

-- Internet protocol user configuration --
IP config>add ethernet0/0 138.201.0.1 255.255.0.0
IP config>add serial0/0 1.1.1.1 255.0.0.0

IP config>route 0.0.0.0 0.0.0.0 1.1.1.1 1
IP config>route 1.3.0.0 255.255.0.0 ethernet0/0 1
IP config>
```

- Configuración NAT

```
*p 4
Config>protocol ip

-- Internet protocol user configuration --
IP config>nat static

-- Static NAT configuration --
SNAT config>enable
SNAT config>rule 1 default
SNAT config>rule 1 local-interface ethernet0/0
SNAT config>rule 1 local-network 138.201.0.0 255.255.0.0
SNAT config>rule 1 global-interface serial0/0
SNAT config>rule 1 global-network 1.3.0.0 255.255.0.0
SNAT config>
```

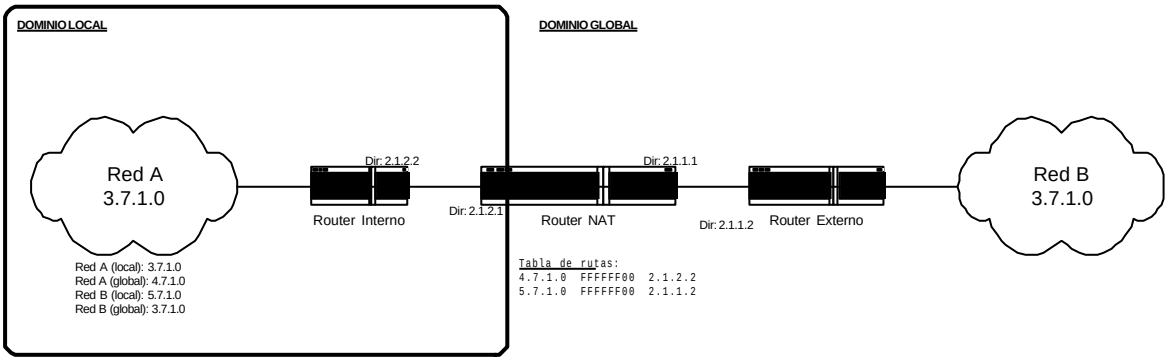
El comando "rule 1 default" es equivalente a los commandos:

"rule 1 translate source"

"rule 1 direction both"

1.2. Conectar dos redes que usan el mismo espacio de direccionamiento

El caso en el que una red privada que quiera conectarse a otra pública tenga direcciones IP que oficialmente pertenecen a esa red pública se denomina "solapamiento" (overlapping). Se puede utilizar NAT para conectar dichas redes. Hay que conseguir que en el dominio local la red pública (externa) que ya posee una dirección global sea vista como si poseyera otra dirección (NAT de tipo: cambio de destino interno). Al mismo tiempo hay que conseguir que en el dominio global la red privada (interna) sea vista con direcciones globales (NAT de tipo: cambio de origen interno). Con dos reglas bidireccionales se solucionaría el problema.



- Configuración de IP

```
*p 4
Config>protocol ip

-- Internet protocol user configuration --
IP config>add ethernet0/0 2.1.2.1 255.255.255.0
IP config>add ethernet0/0 2.1.1.1 255.255.255.0

IP config>route 4.7.1.0 255.255.255.0 2.1.2.1 1
IP config>route 5.7.1.0 255.255.255.0 2.1.1.2 1
IP config>
```

- Configuración NAT

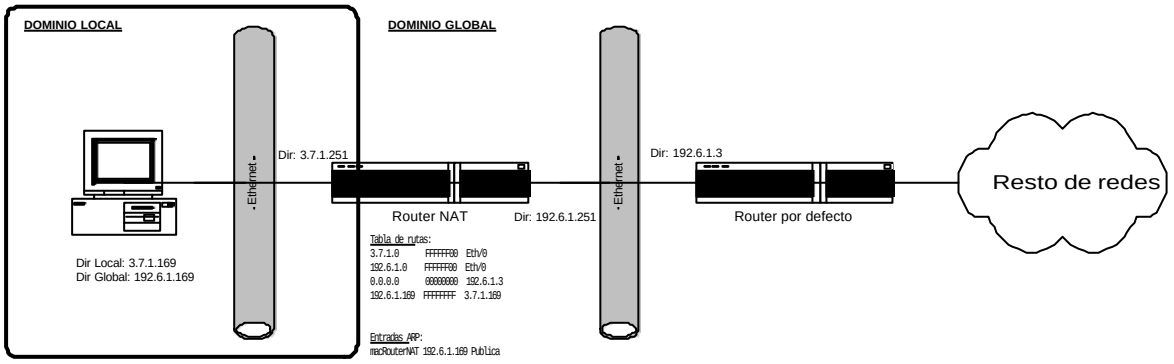
```
*p 4
Config>protocol ip

-- Internet protocol user configuration --
IP config>nat static

-- Static NAT configuration --
SNAT config>enable
SNAT config>rule 1 translate source
SNAT config>rule 1 direction both
SNAT config>rule 1 local-interface 2.1.2.1
SNAT config>rule 1 local-network 3.7.1.0 255.255.255.0
SNAT config>rule 1 global-interface 2.1.1.1
SNAT config>rule 1 global-network 4.7.1.0 255.255.255.0
SNAT config>rule 2 translate destination
SNAT config>rule 2 direction both
SNAT config>rule 2 local-interface 2.1.2.1
SNAT config>rule 2 local-network 5.7.1.0 255.255.255.0
SNAT config>rule 2 global-interface 2.1.1.1
SNAT config>rule 2 global-network 3.7.1.0 255.255.255.0
SNAT config>
```

1.3. Solapamiento de direcciones (autoaliasing)

A este caso se le denomina "autoaliasing". Muchos clientes quieren configurar NAT de tal manera que puedan traducir sus direcciones locales a direcciones globales no utilizadas de una subred directamente conectada al router NAT. Este caso requiere que el router responda a peticiones ARP de dichas direcciones globales de tal manera que todo paquete que vaya dirigido a una de esas direcciones globales sea aceptado y traducido por el router NAT. Para ello es necesario que se configure en el router entradas ARP permanentes y públicas. La creación de dichas entradas ARP no es automática y debe ser realizada como un paso más en el proceso de configuración seguido por el administrador del router NAT. Veamos un ejemplo sencillo de este caso.



- Configuramos las direcciones y las rutas:

```
*p 4
Config>protocol ip

-- Internet protocol user configuration --
IP config>add ethernet0/0 3.7.1.251 255.255.255.0
IP config>add ethernet0/0 192.6.1.251 255.255.255.0
```

```
IP config>route 0.0.0.0 0.0.0.0 192.6.1.3 1
IP config>route 192.6.1.169 255.255.255.255 3.7.1.169 1
IP config>
```

La ruta 192.6.1.169/32 via 3.7.1.169 es necesaria para que los paquetes dirigidos a la dirección IP 192.6.1.169 no se encaminen por el interfaz 192.6.1.251 sino por el interfaz 3.7.1.251.

- Configuramos ARP:

```
*p 4
Config>protocol arp

-- ARP user configuration --
ARP config>entry ethernet0/0 192.6.1.169 00-a0-26-5c-1-1c public
ARP config>
```

NOTA: la dirección MAC del router NAT la puede obtener mediante:

```
*p 3

+dev ethernet0/0

                                  Auto-test   Auto-test     Maintenance
Interface            CSR    Vect     valids    failures       failures
ethernet0/0     fa200a00      5E          0         434              0

Physical address:  00A0265C121C
PROM address:      00A0265C121C

 Input statistics:
  failed, frame too long             0  failed, FCS error                 0
  failed, alignment error            0  failed, FIFO overrun              0
  internal MAC rcv error             0  packets missed                    0
 Output statistics:
  deferred transmission              0  single collision                  0
  multiple collisions                0  total collisions                  0
  failed, excess collisions          0  failed, FIFO underrun             0
  failed, carrier sense err        869  SQE test error                   0
  late collision                     0  internal MAC trans errors         0
  Ethernet MAC code release 1
+
```

- Configuramos NAT:

```
SNAT Config>enable
SNAT config>rule 1 translate source
SNAT config>rule 1 direction skip-global
SNAT config>rule 1 local-interface 3.7.1.251
SNAT config>rule 1 global-interface 192.6.1.251
SNAT config>rule 1 global-network 192.6.1.255 255.255.255.255
SNAT config>rule 2 translate source
SNAT config>rule 2 direction skip-global
SNAT config>rule 2 local-interface 3.7.1.251
SNAT config>rule 2 global-interface 192.6.1.251
SNAT config>rule 2 global-network 192.6.1.0 255.255.255.255
SNAT config>rule 3 translate source
SNAT config>rule 3 direction skip-global
SNAT config>rule 3 local-interface 3.7.1.251
SNAT config>rule 3 global-interface 192.6.1.251
SNAT config>rule 3 global-network 192.6.1.251 255.255.255.255
SNAT config>rule 4 translate source
SNAT config>rule 4 direction both
SNAT config>rule 4 local-interface 3.7.1.251
SNAT config>rule 4 local-network 3.7.1.0 255.255.255.0
```

```
SNAT config>rule 4 global-interface 192.6.1.251
SNAT config>rule 4 global-network 192.6.1.0 255.255.255.0
```

Listamos la configuración completa:

```
Config>show config
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

protocol ip
; -- Internet protocol user configuration --
   address  ethernet0/0     3.7.1.251        255.255.255.0
   address  ethernet0/0     192.6.1.251      255.255.255.0
;  ROUTE IP-Destination, Address mask, Via gateway at, cost
   route 0.0.0.0         0.0.0.0         192.6.1.3       1
   route 192.6.1.169     255.255.255.255 3.7.1.169       1
   nat static
; -- Static NAT configuration –
      enable
      rule 1 default
       rule 1 direction skip-global
      rule 1 local-interface 3.7.1.251
      rule 1 global-interface 192.6.1.251
      rule 1 global-network 192.6.1.255 255.255.255.255
;
      rule 2 default
      rule 2 direction skip-global
      rule 2 local-interface 3.7.1.251
      rule 2 global-interface 192.6.1.251
      rule 2 global-network 192.6.1.0 255.255.255.255
;
      rule 3 default
      rule 3 direction skip-global
      rule 3 local-interface 3.7.1.251
      rule 3 global-interface 192.6.1.251
      rule 3 global-network 192.6.1.251 255.255.255.255
;
      rule 4 default
      rule 4 local-interface 3.7.1.251
      rule 4 global-interface 192.6.1.251
      rule 4 global-network 192.6.1.0 255.255.255.0
      rule 4 local-network 3.7.1.0 255.255.255.0
;
   exit
;
exit
;
protocol arp
; -- ARP user configuration --
   entry ethernet0/0 192.6.1.169 00-A0-26-5C-01-1C public
exit
;
```