# Router Teldat

## Facilidad NAT

Doc. *DM520* Rev. *8.40*
*Octubre, 2000*

# 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 usa 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 si 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.

Resumiendo NAT tiene diversas aplicaciones. Se puede utilizar para los siguientes casos:

- 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 si 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 a 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 cambiara la dirección local origen del paquete en 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, al 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)

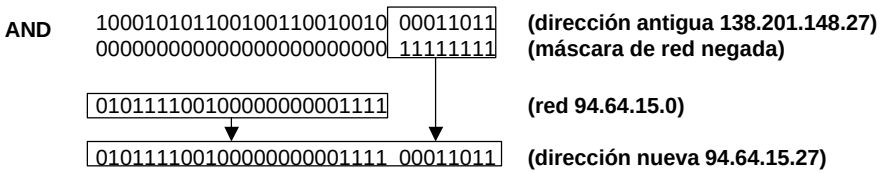
Con NAT estático se realiza traslación de redes locales en redes globales de mismo tamaño (con mismo número de direcciones IP). Un caso particular es cuando las dos redes contienen sólo una dirección IP (máscara de red 255.255.255.255). El proceso NAT puede describirse con la siguiente transformación:

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.




## 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 numero de direcciones

globales disponible. Cuando todas las direcciones globales están siendo usadas subsiguientes conexiones deben ser rechazadas devolviendo "host unreachable". El NAT dinámico es más complejo que el NAT estático ya que se debe mantener la cuenta de los equipos locales conectados y su correspondencia actual con direcciones globales.

**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 (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 en una misma dirección global. Como diferencia con el tipo de NAT anterior, ahora se permiten más conexiones que "n". 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 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: porque 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 en tiempo 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 router 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 a 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) FTP*

Los comandos del FTP **PORT** y **PASV** llevan información de dirección IP y puerto. Para que FTP funcione correctamente es necesario realizar la traslación de estas direcciones y puertos. La cosa se complica desde el momento en que este tipo de información viaja en formato ASCII con lo que al realizar el cambio el paquete resultante puede haber variado su longitud. Por esta razón aparece la necesidad de ajustar el número de secuencia de la cabecera TCP de dicho paquete y los siguientes de

la misma conexión. Aparece así la necesidad de almacenar información sobre saltos (deltas) de números de secuencia por conexión FTP.

Todo protocolo que intercambie la dirección o puerto local en sus paquetes de control tendrán el mismo problema que el FTP y no podrán funcionar a través de routers NAT de forma transparente siendo necesario almacenar información de estado para cada conexión.

### b) ICMP

Algunos mensajes ICMP, depende del tipo de mensaje, incluyen parte del paquete IP original que los provocó, incluyendo la cabecera IP. Si el paquete original sufrió una traslación, la cabecera contendrá información de la dirección trasladada y no de la dirección real. Dependiendo de como y donde se utilice dicha información esto puede provocar mal funcionamiento y en algunos caso se hace necesaria la traslación de dicha información.

### c) DNS

Obviamente, este servicio presentará problemas si el servidor de nombres de equipos de la red local debe proporcionarse en la red global. Una solución puede ser poseer dos DNSs, uno para la resolución de direcciones internas y otro para la resolución de direcciones externas.

### d) BOOTP

No debe presentar problemas en la mayoría de los casos ya que es poco común que dicho protocolo tenga que cruzar el router NAT.

### e) 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. Dependiendo del tipo de protocolo de routing esto será más o menos fácil de implementar. Se recomienda utilizar routing estático.

# 4. Implementación

Previamente ya existía una implementación de NAPT (o NAT extendido) que solo se puede utilizar para interfaces PPP. Además se ha implementado el NAT estático para cualquier interfaz.

El NAT estático implementado permite los siguientes aplicaciones:

- Todos aquellas aplicaciones que en sus datos no venga especificada la dirección local.
- Protocolo FTP: se ha tenido que analizar los datos de este protocolo para detectar y cambiar las direcciones locales que vienen especificadas en comandos de control como PORT y PASV. Para ello se ha tenido que guardar información de estado la cual puede ser visualizada en cualquier momento mediante comandos de monitorización de conexiones.
- Protocolo ICMP: se analizan los datos de los tipos de mensaje en los que viene un trozo del paquete IP que los provocó y se ha hecho también NAT sobre dichos datos.
- Fragmentación IP: al no haber cambio de puertos no hay problema en los fragmentos IP.
- Protocolo de rutado dinámico RIP: se ha realizado una modificación en este protocolo de tal manera que no se le permita enviar las rutas a direcciones locales a través de los interfaces globales.

# 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:

```
Config> PROTOCOL IP
IP config>
```

Desde ahí, se deberá introducir el siguiente comando:

```
IP config> NAT
NAT configuration
NAT 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:

```
NAT config> SET ENABLED
```

ó

```
NAT config> SET DISABLED
```

### 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 (identificador menor → primera regla en la lista). 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, por defecto aparece la última posición.

## 1.2. Interfaz local

Es el interfaz del router NAT interno, o 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. La manera de especificar 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: ETH/0 → 0.0.0.0).
- 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: ETH/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 del router NAT externo, o interfaz que está en contacto o a través del cual se llega a la red global (dominio global). La manera de especificar 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: (Ej. ETH/0 → 0.0.0.0).
- Un interfaz IP lógico: para ello hay que especificar el interfaz lógico IP introduciendo la dirección IP (numerada) del interfaz del router NAT. (Ej. ETH/0 con dos direcciones configuradas, para especificar el interfaz lógico hay que poner la dirección IP numerada deseada).

## 1.4. Red local

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

## 1.5. Red global

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

## 1.6. Tipo de transformación

Hay 2 tipos de transformación y significan lo siguiente:

- 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 de la transformación

Hay 5 sentidos de transformaciones que significan lo siguiente:

- 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 , Global a Local: las dos anteriores.
- 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.

- 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.

***NOTA: (origen o destino) depende del tipo de transformación.***

# 2. Comandos de configuración NAT

Esta sección resume y explica todos los 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.

Introducir los comandos de configuración NAT cuando se tenga el prompt NAT config>, para acceder a este prompt se debe teclear lo siguiente:

```
*P 4
User configuration
Config> PROTOCOL IP
Internet protocol user configuration
IP config> NAT
NAT configuration
NAT config>
```

| Comando | Función |
|---|---|
| **?** (AYUDA) | Lista comandos u opciones. |
| **A**DD | Añade información a la configuración NAT. |
| **D**ELETE | Borra la configuración NAT introducida con el comando **ADD**. |
| **L**IST | Lista la configuración de los elementos NAT. |
| **S**ET | Establece los modos de configuración de la facilidad NAT |
| **E**XIT | Sale de la configuración NAT. |

Las letras que están escritas en **negrita** son el número mínimo de caracteres que hay que teclear para que el comando sea efectivo.

## 2.1. ? (AYUDA)

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

**Sintaxis:**

```
NAT config> ?
```

**Ejemplo:**

```
NAT config> ?
ADD
DELETE
LIST
SET
EXIT
NAT config>
```

## 2.2. ADD

Utilizar el comando **ADD** para añadir más configuraciones NAT a la configuración actual. Este comando le permite añadir reglas NAT.

**Sintaxis:**

```
NAT config> ADD ?
RULE
```

### a) *ADD RULE*

Añade una entrada en la lista de reglas NAT. Este comando por defecto añade la entrada al final de la lista, si no inserta una entrada en la posición que se especifique. Cada entrada contiene: Posición o identificador, Interfaz local, Interfaz global, Red local, Red global, Sentido de transformación.

Hay 2 tipos de transformación: Origen interno, Destino interno.

Hay 5 sentidos de transformaciones: Local a Global, Global a Local, Las dos anteriores, No cambiar local, No cambiar global.

**Sintaxis:**

```
NAT config> ADD RULE <tipo_transformacion sentido_transformacion, interfaz_local,
interfaz_global, dir-ip-local, mascara_ip_local, dir_ip_global, mascara_ip_global,
posicion>
```

**Ejemplo:**

```
NAT config> ADD RULE 1 1 0.0.0.1  0.0.0.0  3.7.1.0  255.255.255.0 192.6.1.0
255.255.255.0 1
NAT config>
```

## 2.3. DELETE

Utilizar este comando para borrar un parámetro de la configuración NAT, previamente añadido con el comando **ADD**. En general se debe especificar que elemento se quiere borrar, de acuerdo con el comando **ADD**.

**Sintaxis:**

```
NAT config> DELETE ?
RULE
```

### a) DELETE RULE

Borra uno de los registros la lista de reglas NAT.

**Sintaxis:**

```
NAT config> DELETE RULE <posicion>
```

**Ejemplo:**

```
NAT config> DELETE RULE 1
NAT config>
```

## 2.4. LIST

Utilizar el comando **LIST** para visualizar distintos parámetros de la configuración NAT en función de la opción seleccionada.

**Sintaxis:**

```
NAT config> LIST ?
STATE
RULES
ALL
```

### a) LIST ALL

Muestra toda la configuración NAT.

**Sintaxis:**

```
NAT config> LIST ALL
```

**Ejemplo:**

```
NAT config> LIST ALL
NAT is: enabled
Pos Local_Ifc        Global_Ifc       Local_Net         Global_Net
--- ---------------  ---------------  ----------        ------------------
1   3.7.1.251        192.6.1.251      ...               !-S-< 192.6.1.255/32
2   3.7.1.251        192.6.1.251      ...               !-S-< 192.6.1.0/32
3   3.7.1.251        192.6.1.251      ...               !-S-< 192.6.1.251/32
4   3.7.1.251        192.6.1.251      3.7.1.0/24        <-S-> 192.6.1.0/24
NAT config>
```

### b) LIST RULES

Muestra una lista de las reglas NAT configuradas.

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

**Sintaxis:**

```
NAT config> LIST RULES
```

**Ejemplo:**

```
NAT config> LIST RULES
Pos Local_Ifc        Global_Ifc       Local_Net         Global_Net
--- ---------------  ---------------  ----------        --------------
1   3.7.1.251        192.6.1.251      ...               !-S-< 192.6.1.255/32
2   3.7.1.251        192.6.1.251      ...               !-S-< 192.6.1.0/32
3   3.7.1.251        192.6.1.251      ...               !-S-< 192.6.1.251/32
4   3.7.1.251        192.6.1.251      3.7.1.0/24        <-S-> 192.6.1.0/24
NAT config>
```

### c) LIST STATE

Muestra si está o no activa la facilidad NAT.

**Sintaxis:**

```
NAT config> LIST STATE
```

**Ejemplo:**

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

## 2.5. SET

Permite activar o desactivar la facilidad NAT.

**Sintaxis:**

```
NAT config> SET ?
DISABLED
ENABLED
```

### a) SET DISABLED

Permite desactivar la facilidad NAT.

**Ejemplo:**

```
NAT config> SET DISABLED
Conf NAT>
```

### b) SET ENABLED

Permite activar la facilidad NAT.

**Ejemplo:**

```
NAT config> SET ENABLED
NAT config>
```

## 2.6. EXIT

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

**Sintaxis:**

```
NAT config> EXIT
```

**Ejemplo:**

```
NAT config> EXIT
IP config>
```

# 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.

Introducir los comandos de monitorización NAT cuando se tenga el prompt NAT monit>, para acceder a este prompt se debe teclear lo siguiente:

```
*P 3
Console Operator
+PROTOCOL IP
IP>NAT
NAT monitoring
NAT monit>
```

| Comando | Función |
|---|---|
| **?**(AYUDA) | Lista comandos u opciones. |
| **L**IST | Lista parámetros del NAT. |
| **E**XIT | Sale de la monitorización NAT. |

Las letras que están escritas en **negrita** son el número mínimo de caracteres que hay que teclear para que el comando sea efectivo.

## 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:**

```
NAT monit> ?
```

**Ejemplo:**

```
NAT monit> ?
LIST
EXIT
NAT monit>
```

## 1.2. LIST

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

**Sintaxis:**

```
NAT 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:**

```
NAT monit> LIST CONNECTIONS
```

**Ejemplo:**

```
NAT 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
NAT monit>
```

## 1.3. EXIT

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

**Sintaxis:**

```
NAT monit> EXIT
```

**Ejemplo:**

```
NAT monit> EXIT
IP>
```

# Capítulo 4
# Ejemplos

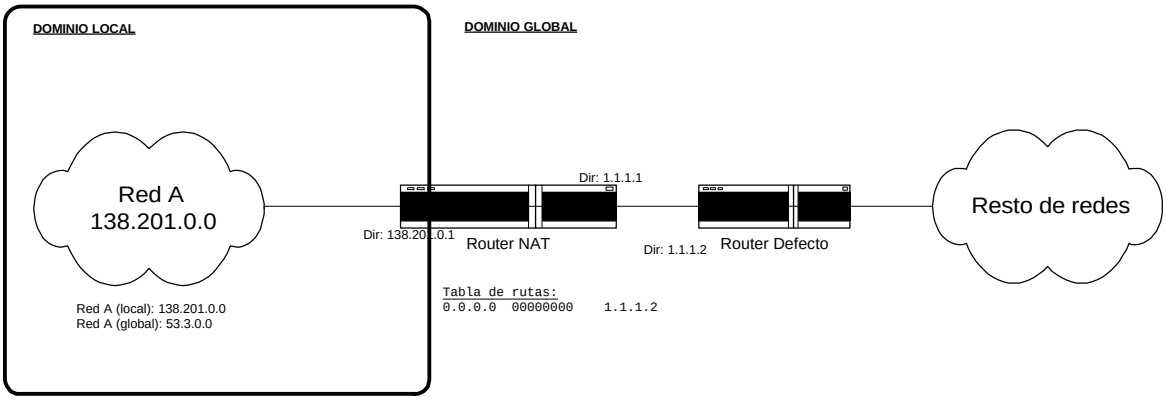
# 1. NAT estático

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 (53.0.0.0). 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. Veamos como se configuraría el router NAT:




- Monitorizamos las direcciones:

```
IP> INTERFACE
Interface  IP Address (es)    Mask (s)
---------  ---------------    -----------
Eth/0      138.201.0.1        255.255.0.0
FR/0       1.1.1.1            255.0.0.0
IP>
```

- Monitorizamos las rutas:

```
IP> DUMP
Type     Dest net         Mask       Cost  Age   Next hop (s)
-------  -------------    --------   ----  ---   ------------
Dir(1)   138.201.0.0      FFFF0000   1     0     Eth/0
Dir(1)   1.1.1.1          FF000000   1     0     FR/0
Stat(1)  0.0.0.0          00000000   1     0     1.1.1.2
IP>
```

- Configuramos las reglas NAT:

```
*P 4
Config> PROTOCOL IP
Internet protocol user configuration
IP config> NAT
NAT configuration
NAT config> ADD RULE
Translating type:
   1- Inside source
   2- Outside dest
Enter option:[1]? 1
Translating direction:
   1- Local to Global, global to local
   2- Local to Global
   3- Global to Local
   4- Skip Local
   5- Skip Global
Enter option:[1]? 1
Local net address [0.0.0.0]? 0.0.0.0 (ó 138.201.0.1)
Global net address [0.0.0.0]? 0.0.0.1 (ó 1.1.1.1)
Local Addresses [0.0.0.0]? 138.201.0.0
Local mask [0.0.0.0]? 255.255.0.0
Global Addresses [0.0.0.0]? 53.3.0.0
Global mask [0.0.0.0]? 255.255.0.0
Position [1]? 1
Rule added
NAT config>
```

- Habilitamos NAT:

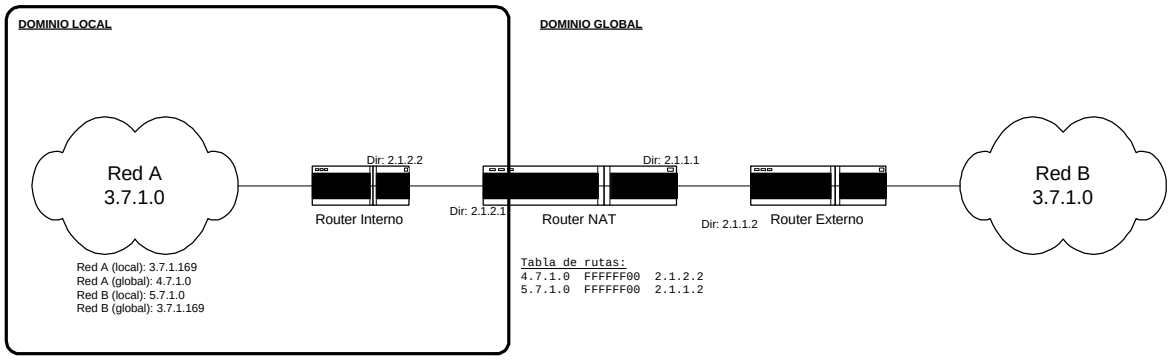
```
NAT config> SET ENABLED
```

- Listamos configuración de NAT:

```
NAT config> LIST RULES
Pos Local_Ifc    Global_Ifc  Local_Net          Global_Net
--- ---------    ----------  --------------     -----------
1   0.0.0.0      0.0.0.1     138.201.0.0/16     <-S->53.3.0.0/16
ó
1   138.201.0.1  1.1.1.1     138.201.0.0/16     <-S->53.3.0.0/16
NAT config>
```

## 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 publica (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.




- Monitorizamos las direcciones:

```
IP> INTERFACE
Interface   IP Address (es)         Mask (s)
---------   ------------------      ----------------
Eth/0       2.1.2.1                 255.255.255.0
Eth/0       2.1.1.1                 255.255.255.0
IP>
```

- Monitorizamos las rutas:

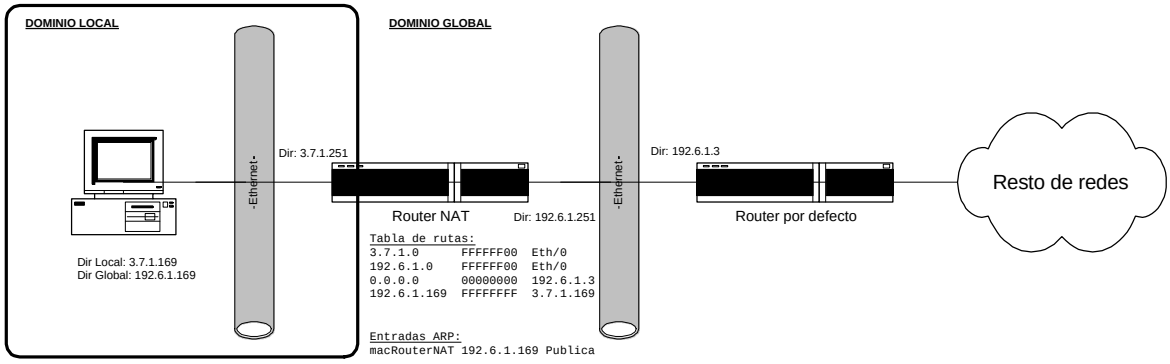
```
IP> DUMP
Type      Dest net       Mask      Cost  Age  Next hop (s)
------    --------       --------  ----  ---  ------------
Dir(1)    2.1.1.0        FFFFFF00  1     0    Eth/0
Dir(1)    2.1.2.0        FFFFFF00  1     0    Eth/0
Stat(1)   4.7.1.0        FFFFFF00  1     0    2.1.2.2
Stat(1)   5.7.1.0        FFFFFF00  1     0    2.1.1.2
IP>
```

- Listamos configuración de NAT:

```
NAT config> LIST RULES
Pos Local_Ifc  Global_Ifc  Local_Net     Global_Net
--- ---------  ----------  -----------   ---------------
1   2.1.2.1    2.1.1.1     3.7.1.0/24    <-S->4.7.1.0/24
2   2.1.2.1    2.1.1.1     5.7.1.0/24    <-D->3.7.1.0/24
NAT 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.




- Monitorizamos las direcciones:

```
IP> INTERFACE
Interface  IP Address (es)        Mask (s)
---------   -----------------     -------------
Eth/0      3.7.1.251              255.255.255.0
Eth/0      192.6.1.251            255.255.255.0
IP>
```

- Monitorizamos las rutas:

```
IP> DUMP
Type     Dest net       Mask       Cost  Age  Next hop (s)
------   ----------     --------   ----  ---  ------------
Dir(1)   3.7.1.0        FFFFFF00   1     0    Eth/0
Dir(1)   192.6.1.0      FFFFFF00   1     0    Eth/0
Stat(1)  0.0.0.0        00000000   1     0    192.6.1.3
Stat(1)  192.6.1.169    FFFFFFFF   1     0    3.7.1.169
IP>
```

- Listamos configuración de ARP:

```
ARP> DUMP
Enter interface: [0]? (Ethernet)

ARP entries for IP protocol
MAC address       IP address      Refresh
macRouterNAT      192.6.1.169     0  Public
ARP>
```

- Listamos configuración de NAT:

```
NAT config> LIST RULES
Pos Local_Ifc      Global_Ifc    Local_Net         Global_Net
--- -----------    -----------   -------------     ------------------
1     3.7.1.251    192.6.1.251   ...               !-S-<192.6.1.255/32
2     3.7.1.251    192.6.1.251   ...               !-S-<192.6.1.0/32
3     3.7.1.251    192.6.1.251   ...               !-S-<192.6.1.251/32
4     3.7.1.251    192.6.1.251   3.7.1.0/24        <-S->192.6.1.0/24
NAT config>
```